NetIQ® eDirectory™

Guide d’administration

Octobre 2019

Mentions légales

À propos de ce guide et de la bibliothèque **17**
À propos de NetIQ Corporation **19**

1 Présentation de NetIQ eDirectory **21**

Gestion simplifiée grâce à NetIQ iManager . . . 22
Arborescence élaborée . . . 22
Utilitaire de gestion basé sur le Web . . . 24
Connexion et authentification uniques . . . 25
Classes et propriétés des objets . . . 25
Liste des objets . . . 25
Classes des objets Conteneur . . . 27
Classes des objets Feuille . . . 31
Contexte et dénomination . . . 48
Nom distinctif . . . 49
Nom avec type . . . 49
Résolution de nom . . . 49
Contexte de poste de travail actuel . . . 50
Point initial . . . 50
Assignation d'un nom relatif . . . 50
Point final . . . 50
Contexte et assignation de nom sous Linux . . . 51
Schéma . . . 51
Gestion du schéma . . . 52
Classes, attributs et syntaxes de schéma . . . 52
Attributs obligatoires et facultatifs - Présentation . . . 57
Exemple de schéma . . . 57
Conception du schéma . . . 58
Partitions . . . 58
Partitions . . . 59
Distribution de répliques en vue de l'amélioration des performances . . . 60
Partitions et liaisons WAN . . . 60
Répliques . . . 61
Types de réplique . . . 62
Répliques filtrées . . . 65
Synchronisation des serveurs dans un anneau de répliques . . . 67
Accès aux ressources . . . 67
Droits eDirectory . . . 68
Assignations d'ayant droit et objets cible . . . 68
Concepts relatifs aux droits eDirectory . . . 69
Droits par défaut pour un nouveau serveur . . . 74
Administration déléguée . . . 74
Gestion des droits . . . 75

2 Conception de votre réseau NetIQ eDirectory **81**

Notions de base relatives à la conception d'un réseau eDirectory . . . 81
Topologie réseau . . . 81
Structure organisationnelle . . . 82
Préparation de la conception du réseau eDirectory . . . 82
Conception de l'arborescence eDirectory . . . 82
Création d'un document relatif aux standards de dénomination . . . 82
Conception des couches supérieures de l'arborescence . . . 85
Conception des couches inférieures de l'arborescence . . . 88
Instructions concernant la partition de votre arborescence . . . 89
Détermination des partitions pour les couches supérieures de l'arborescence . . . 89
Détermination des partitions pour les couches inférieures de l'arborescence . . . 90
Détermination de la taille des partitions . . . 90

Prise en compte des variables réseau . . . 90
Instructions concernant la réplication de votre arborescence . . . 91
Besoins des groupes de travail . . . 91
Tolérance aux pannes . . . 91
Détermination du nombre de répliques . . . 92
Réplication de la partition Arborescence . . . 93
Réplication pour l'administration . . . 93
Gestion du trafic WAN . . . 93
Planification de l'environnement utilisateur . . . 93
Analyse des besoins des utilisateurs . . . 94
Création des instructions d'accessibilité . . . 94
Conception d'eDirectory pour l'e-Business . . . 94
Présentation de NetIQ Certificate Server . . . 95
Droits requis pour exécuter des tâches sur NetIQ Certificate Server . . . 96
Opérations eDirectory sécurisées sur des ordinateurs Linux . . . 97
Synchronisation des heures réseau . . . 100
Synchronisation horaire sur les ordinateurs Linux . . . 100
Vérification de la synchronisation horaire . . . 100

3 Gestion des objets 101

Tâches d'objet générales . . . 101
Recherche dans l'arborescence eDirectory . . . 102
Création d'un objet . . . 104
Modification des propriétés d'un objet . . . 105
Copie d'objets . . . 105
Déplacement d'objets . . . 105
Suppression d'objets . . . 106
Attribution de nouveaux noms à des objets . . . 106
Gestion des comptes utilisateur . . . 106
Création et modification des comptes utilisateur . . . 107
Paramétrage de fonctions de compte facultatives . . . 108
Désactivation de l'intervalle de mise à jour de l'heure de connexion . . . 111
Configuration de scripts de connexion . . . 111
Restrictions des heures de connexion pour les utilisateurs distants . . . 112
Suppression de comptes utilisateur . . . 113
Configuration des services basés sur le rôle . . . 114
Définition des rôles RBS . . . 116
Définition de tâches RBS personnalisées . . . 118

4 Gestion des processus en arrière-plan 121

Synchronisation . . . 121
Caractéristiques de la synchronisation . . . 122
Synchronisation normale ou des répliques . . . 124
Synchronisation de priorité . . . 126
Réplication basée sur des stratégies . . . 134
Configuration manuelle des threads de synchronisation . . . 135
Configuration de la synchronisation sortante asynchrone . . . 136
Configuration des processus en arrière-plan . . . 137
Stratégie de limite stricte . . . 137
Stratégie dynamique basée sur l'UC . . . 137
Intervalle des processus en arrière-plan . . . 137

5 Gestion du schéma 139

Extension du schéma . . . 140
Création d'une classe . . . 140

Suppression d'une classe . . . 140
Création d'un attribut . . . 141
Ajout d'un attribut facultatif à une classe . . . 141
Suppression d'un attribut . . . 142
Création d'une classe auxiliaire . . . 142
Extension d'un objet avec les propriétés d'une classe auxiliaire . . . 143
Modification des propriétés auxiliaires d'un objet . . . 143
Suppression des propriétés auxiliaires d'un objet . . . 143
Affichage du schéma . . . 144
Affichage des informations sur la classe . . . 144
Affichage des informations sur l'attribut . . . 144
Extension manuelle du schéma . . . 144
Extension du schéma sous Windows . . . 145
Extension du schéma sous Linux . . . 145
Drapeaux de schéma ajoutés à eDirectory 8.7 et versions ultérieures . . . 147
Utilisation du client pour effectuer des opérations sur le schéma . . . 148
Utilisation de l'outil eMTool DSSchema . . . 148
Options de l'outil EMTool DSSchema . . . 149

6 Gestion des partitions et des répliques 151

Création d'une partition . . . 152
Fusion d'une partition . . . 153
Déplacement de partitions . . . 154
Annulation des opérations de création ou de fusion de partitions . . . 155
Gestion des répliques . . . 155
Ajout d'une réplique . . . 156
Suppression d'une réplique . . . 156
Changement du type d'une réplique . . . 157
Configuration et gestion des répliques filtrées . . . 158
Utilisation de l'Assistant de de réplique filtrée . . . 159
Définition d'un statut de partition . . . 159
Configuration d'un filtre de serveur . . . 160
Affichage des partitions et des répliques . . . 161
Affichage des partitions d'un serveur . . . 162
Affichage des répliques d'une partition . . . 162
Affichage des informations concernant une partition . . . 162
Affichage de la hiérarchie des partitions . . . 162
Affichage des informations concernant une réplique . . . 163

7 Utilitaires de gestion de NetIQ eDirectory 165

Utilitaire Importation/Conversion/Exportation NetIQ . . . 165
Utilisation de l'assistant Importation/Conversion/Exportation de NetIQ iManager . . . 166
Utilisation de l'interface de ligne de commande . . . 174
Règles de conversion . . . 193
Protocole LBURP (LDAP Bulk Update/Replication Protocol) . . . 202
Amélioration de la vitesse des importations LDIF . . . 203
Gestionnaire d'index . . . 205
Création d'un index . . . 205
Suppression d'un index . . . 206
Mise hors ligne d'un index . . . 206
Gestion des index sur d'autres serveurs . . . 207
Gestionnaire de services eDirectory . . . 207
Utilisation de l'outil Service Manager eMTool du client . . . 208
Utilisation du plug-in du Gestionnaire de services pour NetIQ iManager . . . 209
Utilitaire de chargement en bloc hors connexion . . . 209
Amélioration des performances de chargement par lots . . . 210

Utilisation de ldif2dib pour le chargement en bloc . . . 214
Instances multiples . . . 215
Optimisation de ldif2dib . . . 215
Limites . . . 216
Avertissements . . . 217
Fichiers LDIF . . . 218
Comprendre LDIF . . . 219
Débogage des fichiers LDIF . . . 227
Utilisation de LDIF pour étendre le schéma . . . 232
Limitations ldif2dib . . . 236

8 Surveillance d'eDirectory 239

Utilisation de NetIQ iMonitor . . . 239
Configuration système requise . . . 240
Accès à iMonitor . . . 241
Architecture iMonitor . . . 242
Caractéristiques d'iMonitor . . . 247
Opérations iMonitor sécurisées . . . 268
Configuration d'un objet Serveur HTTP . . . 269
Configuration des paramètres de la pile HTTP à l'aide de ndsconfig . . . 270
Utilisation de cn=monitor pour la surveillance . . . 271
Affichage des statistiques de surveillance . . . 271
Utilisation de DSTrace . . . 281
Fonctions de base . . . 281
Messages de débogage . . . 282
Processus à l'arrière plan . . . 285
Messages DSTrace . . . 289
Linux . . . 290
Windows . . . 291
Filtrage des messages d'iMonitor . . . 293
Filtrage des messages de SAL . . . 293
Configuration des niveaux de gravité . . . 293
Définition du chemin de fichier journal . . . 294

9 Configuration de SecretStore pour un serveur eDirectory 295

Linux . . . 295
Windows . . . 295

10 Fusion d'arborescences NetIQ eDirectory 297

fusion des arborescences eDirectory . . . 298
Conditions préalables . . . 298
Exigences relatives à l'arborescence cible . . . 298
Exigences relatives au schéma . . . 299
Fusion de l'arborescence source avec l'arborescence cible . . . 299
Modification des partitions . . . 299
Préparation des arborescences source et cible . . . 300
Synchronisation des heures avant la fusion . . . 301
Fusion de deux arborescences . . . 302
Tâches postérieures à la fusion . . . 303
Greffe d'une arborescence à serveur unique . . . 304
Changement des noms de contexte - Présentation . . . 306
Préparation des arborescences source et cible . . . 307
Exigences liées à l'endiguement pour le greffage . . . 308
Greffe des arborescences source et cible . . . 309
Changement du nom d'une arborescence . . . 310

Utilisation du client pour fusionner des arborescences . . . 311
Utilisation de l'outil eMTool DSMerge . . . 311
Options de l'outil eMTool DSMerge . . . 312

11 Chiffrement des données dans eDirectory 315

Attributs codés . . . 315
Utilisation de modèles de chiffrement . . . 317
Gestion des règles des attributs codés . . . 317
Accès aux attributs codés . . . 322
Affichage des attributs codés . . . 323
Chiffrement et déchiffrement des données de sauvegarde . . . 324
Clonage de l'ensemble de fichiers DIB contenant des attributs codés . . . 324
Ajout de serveurs eDirectory à des anneaux de répliques . . . 324
Compatibilité avec les versions précédentes . . . 324
Migration vers des attributs codés . . . 325
Réplication des attributs codés . . . 325
Réplication codée . . . 325
Avantage de la réplication codée . . . 326
Activation de la réplication codée . . . 326
Ajout d'une nouvelle réplique à un anneau de répliques . . . 330
Synchronisation et réplication codée . . . 331
Affichage de l'état de la réplication codée . . . 331
Règles de sécurité lors du chiffrement de données . . . 332
Chiffrement de données dans une toute nouvelle configuration . . . 333
Chiffrement de données dans une configuration existante . . . 333
Conclusion . . . 335

12 Réparation de la base de données NetIQ eDirectory 337

Opérations de réparation de base . . . 338
Réalisation d'une réparation complète sans surveillance . . . 339
Réparation de la base de données locale . . . 340
Vérification des références externes . . . 341
Réparation d'un seul objet . . . 341
Suppression des objets Feuille inconnus . . . 342
Affichage et configuration du fichier journal des réparations . . . 342
Ouverture du fichier journal . . . 343
Définition des options du fichier journal . . . 343
Exécution d'une réparation dans NetIQ iMonitor . . . 343
Réparation des répliques . . . 344
Réparation de toutes les répliques . . . 344
Réparation de répliques sélectionnées . . . 345
Réparation des tampons horaires . . . 345
Désignation d'un serveur comme la nouvelle réplique maîtresse . . . 346
Destruction de la réplique sélectionnée . . . 347
Réparation des anneaux de répliques . . . 347
Réparation de tous les anneaux de répliques . . . 347
Réparation de l'anneau de répliques sélectionné . . . 348
Envoi de tous les objets à chaque serveur de l'anneau . . . 348
Réception de tous les objets de la réplique maîtresse sur la réplique sélectionnée . . . 349
Suppression d'un serveur de l'anneau de répliques . . . 349
Maintenance du schéma . . . 350
Demande du schéma de l'arborescence . . . 350
Reconfiguration du schéma local . . . 350
Améliorations de schéma facultatives . . . 351
Importation du schéma distant . . . 351
Déclaration d'une nouvelle période de schéma . . . 351

Réparation des adresses réseau du serveur . . . 352
Réparation de toutes les adresses réseau . . . 352
Réparation des adresses réseau du serveur . . . 353
Opérations de synchronisation . . . 354
Synchronisation de la réplique sélectionnée sur ce serveur . . . 354
Indication de l'état de synchronisation sur un serveur . . . 354
Indication de l'état de la synchronisation sur tous les serveurs . . . 355
Synchronisation horaire . . . 355
Planification d'une synchronisation immédiate . . . 356
Options DSRepair . . . 356
Exécution de DSRepair sur le serveur eDirectory . . . 356
Options de ligne de commande DSRepair . . . 358
Utilisation des paramètres DSRepair avancés . . . 360
Utilisation du client pour réparer une base de données . . . 361
Utilisation de l'outil eMTool DSRepair . . . 361
Options de l'outil eMTool DSRepair . . . 362
Utilitaire graphique DS Repair . . . 363

13 Présentation des services LDAP pour NetIQ eDirectory 365

Termes clés des services LDAP . . . 366
Clients et serveurs . . . 366
Objets . . . 366
Références . . . 367
Comprendre le fonctionnement de LDAP avec eDirectory . . . 368
Connexion à eDirectory à partir de LDAP . . . 369
Assignations de classes et d'attributs . . . 372
Autorisation d'une sortie de schéma non standard . . . 375
Différences de syntaxe . . . 375
Contrôles et extensions LDAP NetIQ pris en charge . . . 376
Utilisation des outils LDAP sous Linux . . . 377
Outils LDAP . . . 378
Filtre de recherche de concordance extensible . . . 388
Transactions LDAP . . . 390
Limites . . . 392

14 Configuration des services LDAP pour NetIQ eDirectory 393

Chargement et déchargement des services LDAP pour eDirectory . . . 393
Vérification du chargement du serveur LDAP . . . 394
Vérification du fonctionnement du serveur LDAP . . . 395
Scénarios . . . 395
Vérification du fonctionnement du serveur LDAP . . . 396
Vérification de l'écoute d'un périphérique . . . 396
Prévention des attaques POODLE en désactivant SSLv3 . . . 397
Configuration des objets LDAP . . . 397
Configuration des objets Serveur LDAP et Groupe LDAP sous Linux . . . 399
Configuration des protocoles et des chiffrements à l'aide de l'attribut ldapSSLConfig . . . 408
Rafraîchissement du serveur LDAP . . . 410
Authentification et sécurité . . . 411
Utilisation de TLS en cas de liaison simple avec mot de passe . . . 411
Démarrage et arrêt de TLS . . . 412
Configuration du serveur pour TLS . . . 412
Configuration du client pour TLS . . . 414
Exportation de la racine approuvée . . . 414
Authentification auprès d'un certificat client . . . 415
Utilisation d'autorités de certification de fournisseurs tiers . . . 415

Création et emploi d'utilisateurs proxy LDAP . . . 415
Utilisation de SASL. . . . 416
Utilisation de connexions NMAS pour l'authentification LDAP . . . 419
Utilisation du serveur LDAP pour effectuer des recherches dans l'annuaire . . . 419
Définition de limites de recherche . . . 419
Utilisation des renvois . . . 420
Recherche de répliques filtrées . . . 428
Configuration des renvois supérieurs . . . 428
Scénario : renvois supérieurs dans une arborescence fédérée . . . 429
Création d'une zone non experte . . . 430
Spécification des données de référence . . . 431
Mise à jour des informations de références par l'intermédiaire de LDAP. . . . 432
Opérations touchées . . . 432
Prise en charge des références supérieures . . . 432
Recherche persistante : configuration d'événements eDirectory . . . 433
Gestion des recherches persistantes . . . 434
Contrôle de l'emploi de l'opération étendue de surveillance des événements. . . . 435
Obtention d'informations sur le serveur LDAP . . . 435
Configuration de la prise en charge de l'heure au format généralisé . . . 437
Configuration du contrôle permissif des modifications . . . 437
Contrôle de l'autorisation par proxy . . . 438
Contrôle du DN étendu LDAP . . . 438
Audit d’événements LDAP . . . 441

15 Sauvegarde et restauration de NetIQ eDirectory 443

Liste de contrôle pour la sauvegarde . . . 445
Comprendre les services de sauvegarde et de restauration. . . . 447
À propos de l'outil de sauvegarde d'eDirectory . . . 448
Différence entre sauvegarde et restauration dans l'utilitaire DSBK et TSA pour NDS . . . 448
Présentation du processus de restauration avec l'outil de restauration . . . 450
Format de l'en-tête des fichiers de sauvegarde . . . 451
Format du fichier journal de sauvegarde . . . 455
Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre . . . 456
Vecteurs de transition et processus de vérification de la restauration . . . 458
Utilisation des fichiers journaux de transactions individuelles. . . . 458
Considérations utiles concernant la consignation de transactions individuelles par fichier . . . 460
Emplacement des fichiers journaux de transactions individuelles . . . 461
Sauvegarde et suppression des journaux de transactions individuelles . . . 462
Avertissement : la suppression d'eDirectory entraîne également celle des fichiers journaux de transaction individuelle. . . . 463
Préparation d'une restauration . . . 463
Conditions préalables à la restauration . . . 463
Localisation des fichiers de sauvegarde requis pour une restauration . . . 464
Utilisation de DSBK . . . 466
Conditions préalables. . . . 467
Utilisation de DSBK sur plusieurs plates-formes . . . 467
Sauvegarde manuelle avec DSBK. . . . 470
Automatisation de la sauvegarde d'eDirectory. . . . 471
Configuration des fichiers journaux de transaction individuelle avec DSBK . . . 471
Restauration à partir de fichiers de sauvegarde avec DSBK . . . 472
Options de ligne de commande pour la sauvegarde et la restauration . . . 474
Exécution de DSBK en tant que tâche cron . . . 483
Sauvegarde et restauration de NICI . . . 483
Sauvegarde de NICI. . . . 484
Restauration de NICI . . . 484
Récupération de la base de données en cas d'échec de la vérification de la restauration. . . . 485
Nettoyage de l'anneau de répliques. . . . 486

Réparation du serveur défaillant et réinstallation des répliques . . . 488
Scénarios de sauvegarde et de restauration . . . 489
Scénario : perte d'un disque dur contenant eDirectory dans un réseau monoserveur . . . 489
Scénario : perte d'un disque dur contenant eDirectory dans un environnement multiserveur . . . 491
Scénario : perte d'un serveur complet dans un environnement multiserveur . . . 493
Scénario : perte de plusieurs serveurs dans un environnement multiserveur . . . 494
Scénario : perte de tous les serveurs dans un environnement multiserveur . . . 494
Utilisation de DSBK dans un plan de reprise après sinistre . . . 496
Plan de reprise après sinistre sous Linux . . . 496
Plan de reprise après sinistre sous Windows . . . 497
Sauvegarde LDAP . . . 498
Avantage de la sauvegarde LDAP . . . 499
Pour plus d'informations . . . 499
Sauvegarde d'eDirectory avec SMS . . . 499

16 Configuration d'eDirectory en mode SuiteB 501

Activation de SuiteB dans une nouvelle installation . . . 502
Activation de SuiteB dans Certificate Server . . . 503
Configuration des services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB . . . 504
Création d'une clé SDI AES 256 bits . . . 507
Activation de l'authentification en arrière-plan . . . 507
Configuration de SuiteB sur des serveurs existants . . . 507

17 Activation de l'authentification EBA (Enhanced Background Authentication) 509

Activation de l'authentification EBA . . . 511
Activation de l'authentification EBA sur une arborescence eDirectory . . . 511
Activation de l'authentification EBA sur un serveur eDirectory . . . 512
Désactivation de l'authentification EBA sur un serveur eDirectory . . . 513
Affichage des informations relatives à l'authentification EBA . . . 513
Gestion de l'autorité de certification EBA à l'aide . . . 515
Exécution de l'utilitaire ebaclientinit . . . 516
Restrictions des opérations eDirectory en cas d'activation de l'authentification EBA . . . 517
Restrictions concernant la modification des types de réplique . . . 517
Restrictions concernant la modification de la réplique maîtresse d'une partition . . . 517
Restrictions concernant la fusion de partitions . . . 517
Restrictions concernant la reconfiguration d'un serveur pour lequel l'authentification EBA est activée . . . 518
Sauvegarde d'un serveur pour lequel l'authentification EBA est activée . . . 518
Déplacement du rôle d'autorité de certification EBA vers un nouveau serveur . . . 518

18 Prise en charge du protocole SNMP pour NetIQ eDirectory 521

SNMP : définitions et terminologie . . . 521
Présentation des services SNMP . . . 522
eDirectory et SNMP . . . 524
Avantages de l'instrumentation de SNMP sur eDirectory . . . 524
Présentation du fonctionnement de SNMP avec eDirectory . . . 524
Installation et configuration des services SNMP pour eDirectory . . . 526
Chargement et déchargement du module serveur SNMP . . . 527
Configuration du sous-agent . . . 527
Configuration des services SNMP pour eDirectory . . . 530
Surveillance d'eDirectory à l'aide de SNMP . . . 533
Trappes . . . 533
Configuration des trappes . . . 547

Statistiques . . . 555
Dépannage . . . 560

19 Maintenance de NetIQ eDirectory 561

Évaluation avancée des coûts de renvoi . . . 561
Amélioration de la connexion entre les serveurs . . . 562
Avantages de la fonction d'évaluation des coûts de renvoi . . . 564
Déploiement de l'évaluation avancée des coûts de renvoi . . . 565
Activation de l'évaluation avancée des coûts de renvoi . . . 566
Optimisation de l'évaluation avancée des coûts de renvoi . . . 567
Surveillance de l'évaluation avancée des coûts de renvoi . . . 568
Préservation de l'état de santé d'eDirectory . . . 570
Fréquence des vérifications de l'état de santé . . . 571
Présentation de la vérification de l'état de santé . . . 571
Contrôle de l'état de santé d'eDirectory à l'aide d'iMonitor . . . 572
Pour plus d'informations . . . 573
Ressources de surveillance . . . 573
Mise à niveau du matériel ou remplacement d'un serveur . . . 574
Mise à niveau planifiée du matériel ou d'un périphérique de stockage sans remplacement du serveur . . . 574
Remplacement planifié d'un serveur . . . 577
Modification de l'adresse IP du serveur . . . 580
Restauration d'eDirectory après une panne matérielle . . . 580
Amélioration des performances de recherche dans les sous-arborescences . . . 581
Préparation des conteneurs . . . 582

20 Gestionnaire DHost iConsole 583

Définition de DHost . . . 584
Exécution de DHost iConsole . . . 584
Exécution de DHost iConsole sous Windows . . . 585
Exécution de DHost iConsole sous Linux . . . 585
Gestion des modules eDirectory . . . 585
Chargement et déchargement de modules sous Windows . . . 586
Chargement et déchargement de modules sous Linux . . . 586
Demande d'informations DHost . . . 587
Affichage des paramètres de configuration . . . 587
Affichage des informations sur le protocole . . . 588
Affichage des propriétés de connexion . . . 588
Affichage des statistiques de réserves de threads . . . 588
Pile de processus . . . 589

21 Définition du mot de passe de l'utilisateur sadmin 591

22 eDirectory Management Toolbox 593

Utilisation du client à ligne de commande . . . 594
Affichage de l'aide sur la ligne de commande . . . 595
Exécution du client à ligne de commande en mode interactif . . . 595
Exécution du client à ligne de commande en mode de traitement par lots . . . 599
Options du client à ligne de commande eMBox . . . 601
Établissement d'une connexion sécurisée avec le client . . . 602
Recherche des numéros de port eDirectory . . . 602
Utilisation de l'enregistreur . . . 603
Utilisation du client à ligne de commande « outil de consignation . . . 603
Utilisation de la fonction Enregistreur dans NetIQ iManager . . . 604

Utilisation du client eMBox pour la sauvegarde et la restauration 604
Conditions préalables. 605
Sauvegarde manuelle à l'aide du client eMBox 606
Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox 607
Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox 609
Restauration à partir de fichiers de sauvegarde avec le client eMBox. 611
Sauvegarde et restauration à l'aide de NetIQ iManager 613
Sauvegarde manuelle avec iManager 613
Configuration des fichiers journaux de transactions individuelles avec iManager 615
Restauration à partir de fichiers de sauvegarde avec iManager 616

23 Audit des événements eDirectory 619

Audit avec Novell Audit 619
Plates-formes prises en charge 619
Conditions préalables. 620
Installation des paquetages Novell Audit 620
Installation du plug-in Novell Audit iManager 621
Configuration de Novell Audit Platform Agent 621
Configuration de Novell Audit pour eDirectory 622
Chargement du module d'audit 623
Comprendre la création de rapports d'événements eDirectory 624
Comprendre les types d'événements eDirectory 624
Comprendre le filtrage des événements d'audit eDirectory 626
Surveillance des événements eDirectory avec Sentinel 627
Désinstallation des paquetages Novell Audit 629
Audit avec XDAS. 629
Configuration de XDAS 630
Audit à l'aide de CEF 651
Configuration de CEF. 651
Caching des événements de journal. 670
Audit LDAP 671
Nécessité d'un audit LDAP. 671
Utilisation de l'audit LDAP 672
Pour plus d'informations. 672

24 Présentation de l'infrastructure d'authentification d'eDirectory 673

Fonctionnalités de NMAS 673
Phase d'identification de l'utilisateur. 673
Phase d'authentification (connexion) 674
Phase de détection de retrait de périphérique 676
Méthodes et séquences de connexion et de post-connexion 676
Caching des objets Sécurité. 677
Logiciel NMAS. 677
Installation des logiciels serveur et client 678
Logiciel de méthodes de connexion et partenaires 678
Mot de passe universel 679
Gestion à l'aide 679
Gestion des méthodes et des séquences de connexion et de post-connexion 679
Procédures d'installation d'une méthode de connexion 680
Mise à jour de méthodes de connexion et de post-connexion 681
Gestion des séquences de connexion 682
Autorisation de séquences de connexion pour les utilisateurs. 684
Configuration de séquences de connexion par défaut. 684
Suppression d'une méthode de connexion 685
Suppression d'une séquence de connexion. 686
Connexion au réseau à l'aide de NMAS 686

Champ de mot de passe . . . 686
Connexion avancée . . . 687
Déverrouillage du poste de travail . . . 687
Capture d'une trace du client NMAS . . . 688
Affichage de l'état d'autorisation NMAS . . . 688
Historique des mots de passe NetIQ . . . 688
Connexion basée sur HOTP NMAS . . . 689
Présentation . . . 689
Installation . . . 690
Resynchronisation du compteur . . . 692
Configuration . . . 693
Problèmes connus . . . 694
L'utilitaire nmashotpconf ne peut pas modifier la fenêtre de resynchronisation des utilisateurs . . . 694
Autres tâches d'administration . . . 694
Utilisation de la commande de fréquence de rafraîchissement de stratégie . . . 695
Utilisation de la commande LoginInfo . . . 695
Désactivation des connexions NMAS pour LDAP . . . 698
Appel des commandes NMAS . . . 699
Définition du délai entre les tentatives de connexion infructueuses . . . 699
Utilisation de DSTrace . . . 699
Désactivation et désinstallation du client NMAS . . . 700
Audit des événements NMAS . . . 700
Considérations relatives à la sécurité . . . 701
Méthodes de connexion développées par des partenaires . . . 701
Stratégies de connexion . . . 701
NMASInst . . . 702
Mot de passe universel . . . 702
Clé SDI . . . 704

25 Présentation du serveur de certificats 705

Fonctionnalités de NetIQ Certificate Server . . . 705
Composants de NetIQ Certificate Server . . . 706
NetIQ Certificate Server . . . 706
Infrastructure cryptographique de Novell International . . . 713
Configuration de NetIQ Certificate Server . . . 713
Choix du type d'autorité de certification à utiliser . . . 713
Création d'un objet Autorité de certification organisationnelle . . . 714
Autorité de certification subordonnée . . . 716
Restrictions associées à la création d'un objet Autorité de certification . . . 719
Configuration de l'autorité de certification en mode SuiteB . . . 719
Création d'un objet Certificat de serveur . . . 720
Configuration des applications codées . . . 721
Composants supplémentaires à configurer . . . 721
Gestion de NetIQ Certificate Server . . . 723
Tâches concernant l'autorité de certification . . . 725
Tâches concernant l'objet Certificat de serveur . . . 734
Tâches relatives au certificat utilisateur . . . 744
Auto-provisioning du certificat X.509 . . . 750
Utilisation des certificats eDirectory avec des applications externes . . . 753
Tâches relatives à l'objet Racine approuvée . . . 756
Tâches relatives aux listes de révocation de certificats . . . 758
Tâches relatives à eDirectory . . . 766
Tâches relatives aux applications . . . 767
Vérification de l'état de santé PKI . . . 768
Cryptographie à clé publique - Notions . . . 771
Présentation . . . 772
Transmissions sécurisées . . . 772
Paires de clés . . . 772

Mise en place d'une relation de confiance . . . 775
Droits sur les entrées nécessaires à la réalisation des tâches . . . 778

26 Gestion des mots de passe 783

Présentation du mot de passe universel . . . 783
Quel est le niveau de sécurité du mot de passe universel ? . . . 783
Mot de passe universel . . . 785
Stratégies de mot de passe . . . 785
Synchronisation de mot de passe . . . 786
Présentation du stockage de mots de passe non réversibles . . . 786
Activation du stockage de mots de passe non réversibles . . . 787
Stratégies de mot de passe . . . 787
Déploiement du mot de passe universel . . . 787
Étape 1 : identifiez votre besoin d'un mot de passe universel . . . 788
Étape 2 : vérifiez la disponibilité de votre conteneur de sécurité . . . 788
Étape 3 : vérifiez que vos serveurs de clés de domaine SDI sont prêts pour le mot de passe universel . . . 788
Étape 4 : vérifiez la cohérence des clés SDI pour l'arborescence . . . 790
Étape 5 : activez le mot de passe universel . . . 790
Compatibilité avec les versions précédentes . . . 791
Administration des mots de passe . . . 791
Problèmes à surveiller . . . 791
Gestion des mots de passe à l'aide de stratégies de mot de passe . . . 792
Présentation des fonctionnalités de la stratégie de mot de passe . . . 793
Planification de stratégies de mot de passe . . . 793
Tâches préalables à l'utilisation des stratégies de mot de passe . . . 797
Création de règles de mot de passe . . . 798
Assignation de stratégies de mot de passe aux utilisateurs . . . 814
Recherche de la stratégie d'un utilisateur . . . 816
Définition d'un mot de passe utilisateur . . . 816
Utilitaire de diagnostic de mot de passe universel . . . 817
Dépannage des stratégies de mot de passe . . . 818
Self-service de mot de passe . . . 819
Présentation du self-service de mot de passe . . . 819
Conditions préalables à l'utilisation du self-service de mot de passe . . . 820
Gestion des mots de passe oubliés . . . 820
Self-service de réinitialisation de mot de passe proposé aux utilisateurs . . . 833
Ajout d'un message de changement de mot de passe . . . 833
Configuration de la notification par message électronique pour le self-service de mot de passe . . . 833
Test du self-service de mot de passe . . . 835
Ajout du self-service de mot de passe à votre portail d'entreprise . . . 835
Dépannage du self-service de mot de passe . . . 836
Application de mots de passe universels respectant la casse . . . 836
Avantage des mots de passe respectant la casse . . . 837
Déploiement des mots de passe respectant la casse . . . 837
Mise à niveau des anciens clients et utilitaires Novell . . . 838
Pour plus d'informations . . . 839
Considérations relatives à la sécurité . . . 839
Importation des mots de passe basés sur le hachage dans eDirectory . . . 841

27 Services REST 843

Planification de l'installation des services REST pour eDirectory . . . 844
Configuration des services REST pour eDirectory . . . 846
Gestion de la persistance des données . . . 848
Audit avec les services REST . . . 848
Présentation des événements REST . . . 848

Modification d'un mot de passe LDAP à l'aide d'un conteneur REST . . . 849
Modification d'un certificat de serveur à l'aide d'un conteneur REST . . . 850

A Considérations relatives à NMAS 851

Configuration d'un conteneur Sécurité en tant que partition distincte . . . 851
Fusion des arborescences avec conteneurs de sécurité multiples . . . 851
Opérations à effectuer par produit avant une fusion d'arborescences . . . 852
Fusion des arborescences . . . 855
Opérations à effectuer par produit après la fusion . . . 855

B Commandes et syntaxe NetIQ eDirectory Linux 857

Utilitaires généraux . . . 857
Commandes spécifiques de LDAP . . . 862

C Configuration de OpenSLP pour eDirectory 865

Protocole SLP . . . 865
Concepts fondamentaux de SLP . . . 865
Protocole SLP NetIQ . . . 866
Agents Utilisateur . . . 867
Agents Service . . . 867
Paramètres de configuration . . . 868

D Fonctionnement de NetIQ eDirectory avec DNS 871

E Configuration de GSSAPI avec eDirectory 873

Concepts . . . 873
Définition de Kerberos . . . 873
Définition de SASL . . . 874
Définition de GSSAPI . . . 874
Fonctionnement de GSSAPI avec eDirectory . . . 874
Conditions préalables à la configuration de GSSAPI . . . 875
Hypothèses concernant les caractéristiques réseau . . . 876
Installation du plug-in Kerberos pour iManager . . . 876
Ajout d'extensions LDAP Kerberos . . . 877
Exportation du certificat de racine approuvée . . . 878
Configuration de la méthode SASL-GSSAPI . . . 879
Fusion d'arborescences eDirectory configurées avec la méthode SASL-GSSAPI . . . 879
Gestion de la méthode SASL-GSSAPI . . . 879
Extension du schéma Kerberos . . . 880
Gestion de l'objet Domaine Kerberos . . . 880
Gestion d'un principal de service . . . 882
Édition de principaux étrangers . . . 886
Configuration de l'authentification SASL GSSAPI si le KDC Kerberos MIT utilise eDirectory comme interface dorsale . . . 886
Création d'une séquence de connexion . . . 887
Utilisation de SASL-GSSAPI par LDAP . . . 887
Messages d'erreur . . . 887
Terminologie courante . . . 887

F Considérations relatives à la sécurité 889

Liaisons LDAP . . . 889

Résultats de l'analyse Nessus 889

G Configuration de l'agent de mot de passe Kerberos 891

Conditions préalables à la configuration de mot de passe Kerberos 891
Activation de la fonctionnalité KPA pour un domaine Kerberos 891
Agent de mot de passe Kerberos 892
Génération de clés 892
Remarques relatives au mot de passe universel 893

H Assignation d'événements eDirectory à des événements XDAS 895

Assignation d'événements eDirectory à des événements XDAS 895
Événements XDAS 904
Événements de gestion de compte 905
Événements de gestion des approbations 910
Événements de gestion des éléments de données 913
Événements de sécurité 916
Événements de gestion de service ou d'application 926
Événements opérationnels 929

I Assignation d'événements eDirectory à des événements CEF 933

Assignation d'événements eDirectory à des événements CEF 933
Événements CEF 938
Événements de sécurité 938
Événements d'objets 944
Événements d'attributs 946
Événements EBA 947

J Dépannage 949

Dépannage des problèmes liés à XDAS 949
Dépannage du protocole SNMP 951
Dépannage d'iMonitor 954
Dépanner iManager 956
Dépannage des notices nécrologiques 956
Migration vers NetIQ eDirectory 960
Résolution des problèmes du schéma 966
Dépannage DSRepair 966
Dépannage de la réplication 967
Dépannage du clonage de DIB 967
Dépannage des services d'infrastructure de clés publiques de NetIQ 968
Utilitaires de dépannage sous Linux 973
Dépannage de NMAS 974
Accès à HTTPSTK lorsque les services Annuaire ne sont pas chargés 977
Dépannage du codage des données 978
eDirectory Management Toolbox 981
Dépannage de SASL-GSSAPI 983
Gestion de la consignation des erreurs dans eDirectory 984
Divers 988
Dépannage d'IPV6 995
Dépannage EBA 996

À propos de ce guide et de la bibliothèque

Le *Guide d'administration* décrit comment gérer et configurer le produit NetIQ eDirectory (eDirectory).

Public

Le présent guide est destiné aux administrateurs réseau.

Autres documents dans la bibliothèque

La bibliothèque propose les manuels suivants :

Guide d’installation

Décrit comment installer eDirectory. Il est destiné aux administrateurs réseau.

Guide d'optimisation pour les plates-formes Linux)

Décrit comment analyser et configurer eDirectory sur les plates-formes Linux afin d’obtenir de meilleures performances dans tous les déploiements.

Ces guides sont disponibles sur le site Web de documentation de NetIQ eDirectory 9.2.

Pour plus d'informations sur l'utilitaire de gestion d'eDirectory, reportez-vous au *guide d'administration de NetIQ iManager 3.2*.

À propos de NetIQ Corporation

Fournisseur international de logiciels d'entreprise, nos efforts sont constamment axés sur trois défis inhérents à votre environnement (le changement, la complexité et les risques) et la façon dont vous pouvez les contrôler.

Notre point de vue

Adaptation au changement et gestion de la complexité et des risques : rien de neuf

Parmi les défis auxquels vous êtes confronté, il s'agit peut-être des principaux aléas qui vous empêchent de disposer du contrôle nécessaire pour mesurer, surveiller et gérer en toute sécurité vos environnements informatiques physiques, virtuels et en nuage (cloud computing).

Services métiers critiques plus efficaces et plus rapidement opérationnels

Nous sommes convaincus qu'en proposant aux organisations informatiques un contrôle optimal, nous leur permettons de fournir des services dans les délais et de manière plus rentable. Les pressions liées au changement et à la complexité ne feront que s'accroître à mesure que les organisations évoluent et que les technologies nécessaires à leur gestion deviennent elles aussi plus complexes.

Notre philosophie

Vendre des solutions intelligentes et pas simplement des logiciels

Pour vous fournir un contrôle efficace, nous veillons avant tout à comprendre les scénarios réels qui caractérisent les organisations informatiques telles que la vôtre, et ce jour après jour. De cette manière, nous pouvons développer des solutions informatiques à la fois pratiques et intelligentes qui génèrent assurément des résultats éprouvés et mesurables. En même temps, c'est tellement plus gratifiant que la simple vente de logiciels.

Vous aider à réussir, telle est notre passion

Votre réussite constitue le fondement même de notre manière d'agir. Depuis la conception des produits jusqu'à leur déploiement, nous savons que vous avez besoin de solutions informatiques opérationnelles qui s'intègrent en toute transparence à vos investissements existants. En même temps, après le déploiement, vous avez besoin d'une formation et d'un support continus. En effet, il vous faut un partenaire avec qui la collaboration est aisée... pour changer. En fin de compte, votre réussite est aussi la nôtre.

Nos solutions

- Gouvernance des accès et des identités
- Gestion des accès
- Gestion de la sécurité
- Gestion des systèmes et des applications

- Gestion des charges de travail
- Gestion des services

Contacter le support

Pour toute question concernant les produits, tarifs et fonctionnalités, contactez votre partenaire local. Si vous ne pouvez pas contacter votre partenaire, contactez notre équipe de support ventes.

Monde :	www.netiq.com/about_netiq/officelocations.asp
États-Unis et Canada :	1-888-323-6768
Courrier électronique :	info@netiq.com
Site Web :	www.netiq.com

Contacter le support technique

Pour tout problème spécifique au produit, contactez notre équipe du support technique.

Monde :	www.netiq.com/support/contactinfo.asp
Amérique du Nord et du Sud :	1-713-418-5555
Europe, Moyen-Orient et Afrique :	+353 (0) 91-782 677
Courrier électronique :	support@netiq.com
Site Web :	www.netiq.com/support

Contacter le support en charge de la documentation

Notre objectif est de vous proposer une documentation qui réponde à vos besoins. Si vous avez des suggestions d'améliorations, cliquez sur le bouton **Add Comment** (Ajouter un commentaire) au bas de chaque page dans les versions HTML de la documentation publiée à l'adresse www.netiq.com/documentation. Vous pouvez également envoyer un message électronique à l'adresse Documentation-Feedback@netiq.com. Nous accordons une grande importance à vos commentaires et sommes impatients de connaître vos impressions.

Contacter la communauté d'utilisateurs en ligne

La communauté en ligne de NetIQ, Qmunity, est un réseau collaboratif vous mettant en relation avec vos homologues et des spécialistes de NetIQ. En proposant des informations immédiates, des liens utiles vers des ressources et un accès aux experts NetIQ, Qmunity vous aide à maîtriser les connaissances nécessaires pour tirer pleinement parti du potentiel de vos investissements informatiques. Pour plus d'informations, consultez le site http://community.netiq.com.

1 Présentation de NetIQ eDirectory

Pour simplifier, NetIQ eDirectory est une liste d'objets qui représentent des ressources réseau, telles que des utilisateurs, des serveurs, des imprimantes, des files d'attente d'impression et des applications réseau. NetIQ eDirectory est un service d'annuaire sécurisé, extrêmement évolutif et performant. Il peut stocker et gérer des millions d'objets, comme des utilisateurs, des applications, des périphériques réseau et des données. NetIQ eDirectory est une solution de gestion sécurisée et évolutive des identités multi plates-formes, qui autorise un déploiement sur Internet.

En plus d'une gestion centralisée des identités, NetIQ eDirectory fournit l'infrastructure, la sécurité à l'échelle du réseau et l'évolutivité nécessaires à tous les types d'applications qui s'exécutent derrière un pare-feu et au-delà de celui-ci. NetIQ eDirectory comprend des fonctions de gestion à partir du Web et de périphériques sans fil. Vous pouvez ainsi accéder à l'annuaire, aux utilisateurs, aux droits d'accès et aux ressources réseau, et les gérer à partir d'un navigateur Web et de divers appareils de poche.

NetIQ eDirectory gère en mode natif la norme d'annuaire LDAP (Lightweight Directory Access Protocol) 3 et prend en charge les services TLS/SSL basés sur le code source OpenSSL.

Pour plus d'informations sur le moteur eDirectory, reportez-vous à la page Web eDirectory Process Requests (http://support.novell.com/techcenter/articles/anp20020801.html) (Requêtes de traitement eDirectory).

La Figure 1-1 affiche une partie des objets tels qu'ils apparaissent dans l'utilitaire de gestion de NetIQ iManager.

Figure 1-1 *Objets eDirectory dans iManager*

Il se peut que certaines classes d'objet ne soient pas disponibles, en fonction du schéma effectif configuré sur le serveur eDirectory et du système d'exploitation exécutant eDirectory.

Pour plus d'informations sur les objets, reportez-vous à la « Classes et propriétés des objets » page 25.

Si le réseau compte plusieurs serveurs eDirectory, l'annuaire peut être répliqué sur plusieurs serveurs.

Ce chapitre comprend les informations suivantes :

- « Gestion simplifiée grâce à NetIQ iManager » page 22
- « Classes et propriétés des objets » page 25

- « Contexte et dénomination » page 48
- « Schéma » page 51
- « Partitions » page 58
- « Répliques » page 61
- « Synchronisation des serveurs dans un anneau de répliques » page 67
- « Accès aux ressources » page 67
- « Droits eDirectory » page 68

Gestion simplifiée grâce à NetIQ iManager

NetIQ eDirectory garantit une gestion facile, souple et efficace des ressources réseau. Il joue également le rôle de référentiel d'informations utilisateur pour les applications de groupware et les autres applications. Ces applications peuvent accéder à votre Annuaire via le protocole LDAP (Lightweight Directory Access Protocol) standard.

eDirectory est doté de fonctionnalités visant à en faciliter la gestion, et comprenant entre autres une puissante arborescence, un utilitaire de gestion intégré et un système unique de connexion et d'authentification.

NetIQ iManager permet de gérer l'annuaire et les utilisateurs, ainsi que les droits d'accès et les ressources réseau qui figurent dans l'annuaire, depuis un navigateur Web et tout un éventail de appareils de poche. Grâce aux plug-ins eDirectory pour iManager, vous accédez aux tâches élémentaires de gestion d'annuaire, ainsi qu'aux utilitaires de gestion eDirectory que vous deviez auparavant exécuter sur le serveur eDirectory, tels que DSRepair, DSMerge et l'utilitaire de sauvegarde et de restauration.

Pour plus d'informations, reportez-vous au *Guide d'administration de NetIQ iManager*.

Arborescence élaborée

NetIQ eDirectory organise les objets dans une arborescence au sommet de laquelle se trouve l'objet Arborescence, qui porte le nom de l'arborescence.

Que les serveurs eDirectory soient exécutés sous Linux ou Windows, toutes les ressources peuvent être hébergées dans la même arborescence. Vous n'avez pas besoin d'accéder à un serveur ou à un domaine spécifique pour créer des objets, octroyer des droits, modifier les mots de passe ou gérer les applications.

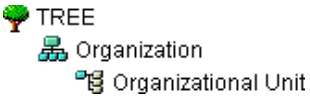
La structure hiérarchique de l'arborescence vous permet de bénéficier d'une grande souplesse et d'une grande liberté en matière de gestion. Ces avantages résultent principalement des deux fonctionnalités suivantes :

- « Objets Conteneur » page 22
- « Héritage » page 23

Objets Conteneur

Les objets Conteneur vous permettent de gérer les autres objets par groupes, et non plus séparément. Trois classes courantes sont disponibles pour les objets Conteneur, comme le montre la Figure 1-2 :

Figure 1-2 Classes courantes d'objets Conteneur



L'objet Arborescence est l'objet Conteneur situé au sommet de l'arborescence. Il contient en général l'objet Organisation de votre entreprise.

Organisation est en principe la première classe de conteneurs sous l'objet Arborescence. L'objet Organisation porte généralement le nom de votre entreprise. La gestion des petites entreprises est simplifiée car tous les autres objets dépendent directement de l'objet Organisation.

Des objets Unité organisationnelle peuvent être créés sous l'objet Organisation pour représenter différentes zones géographiques, différents sites du réseau ou des services spécifiques. Vous pouvez également créer des objets Unité organisationnelle dans des objets de ce même type pour subdiviser encore l'arborescence.

Pays et Lieu sont des classes d'objets Conteneur utilisées en principe uniquement sur les réseaux multinationaux.

L'objet Domaine peut être créé sous l'objet Arborescence ou sous les objets Organisation, Unité organisationnelle, Pays et Lieu.

Vous pouvez effectuer une tâche sur l'objet Conteneur et l'appliquer à tous les objets de ce conteneur. Supposons que vous souhaitiez accorder à une utilisatrice nommée Amy le contrôle de gestion complet sur tous les objets du conteneur de facturation qui contient l'application de base de données, le groupe de comptables, l'imprimante laser et les utilisateurs Amy, Bill et Bob.

Pour ce faire, accédez à l'onglet Afficher les objets dans iManager, puis sélectionnez l'arborescence parent de l'objet **Facturation** dans le volet de gauche. Dans le volet de droite, sélectionnez **Facturation**, puis cliquez sur **Opérations** > **Modifier les ayants droit**. Cliquez sur **Ajouter un ayant droit** et ajoutez Amy comme ayant droit. Cliquez ensuite sur **Droits assignés** et sélectionnez les droits que vous souhaitez accorder à Amy. Amy dispose désormais de droits de gestion sur l'application de base de données, le groupe de comptables, l'imprimante laser et les utilisateurs Bill et Bob, en plus d'elle-même.

Héritage

L'autre particularité d'eDirectory est l'héritage. Le terme « héritage » signifie que des droits sont transmis de manière descendante à tous les conteneurs de l'arborescence. Ainsi, vous pouvez accorder des droits en procédant à très peu d'assignations. Supposez, par exemple, que vous souhaitiez concéder des droits de gestion aux objets illustrés dans la Figure 1-3 page 23.

Figure 1-3 Exemples d'objets eDirectory

Vous pouvez alors effectuer l'une des assignations suivantes :

- Si vous accordez à un utilisateur des droits sur Allentown, l'utilisateur peut uniquement gérer les objets du conteneur Allentown.
- Si vous accordez à un utilisateur des droits sur Est, cet utilisateur peut alors gérer les objets situés dans les conteneurs East, Allentown et Yorktown.
- Si vous accordez à un utilisateur des droits sur YourCo, cet utilisateur peut gérer les objets qui figurent dans tous les conteneurs illustrés.

Pour plus d'informations sur l'assignation de droits, reportez-vous à la « Droits eDirectory » page 68.

Utilitaire de gestion basé sur le Web

iManager est un outil Web qui permet d'administrer, de gérer et de configurer les objets eDirectory. iManager vous donne la possibilité d'assigner des tâches ou des responsabilités particulières aux utilisateurs, et de leur présenter uniquement les outils (et les droits associés) nécessaires pour celles-ci.

Pour exécuter iManager, vous devez utiliser un poste de travail sur lequel est installé l'un des navigateurs suivants : Microsoft Internet Explorer 6.0 SP1 (navigateur recommandé), Mozilla 1.7, Mozilla Firefox 0.9.2 ou toute version ultérieure de ces produits.

IMPORTANT : même s'il est possible d'accéder au logiciel par le biais d'un autre navigateur Web que ceux mentionnés ci-dessus, nous ne garantissons pas une compatibilité intégrale avec iManager.

---

iManager permet d'effectuer les tâches de supervision suivantes :

- configurer les accès LDAP et XML à eDirectory ;
- Création d'objets représentant les utilisateurs, les périphériques et les ressources réseau
- Définition de modèles pour créer de nouveaux comptes utilisateur
- Recherche, modification, déplacement et suppression d'objets sur le réseau
- Définition de droits et de rôles afin de déléguer une autorité administrative
- étendre le schéma eDirectory afin d'autoriser les propriétés et les types personnalisés pour les objets ;
- partitionner et répliquer la base de données eDirectory sur plusieurs serveurs ;
- exécuter des utilitaires de gestion eDirectory tels que DSRepair et DSMerge, ou encore l'utilitaire de sauvegarde et de restauration.

iManager permet en outre d'exécuter d'autres fonctions de gestion, selon les plug-ins qui ont été chargés. Les plug-ins eDirectory suivants sont fournis avec iManager 2.7 :

- eDirectory Backup and Restore
- eDirectory Log Files
- eDirectory Merge
- eDirectory Repair
- eDirectory Service Manager
- eGuide Content
- iManager Base Content
- Import Convert Export Wizard

- Index Management
- iPrint
- LDAP
- Universal Password Enforcement
- Priority Sync
- Encrypted Attributes
- Encrypted Replication
- NetIQ Licensing Services (NLS)
- NetIQ Modular Authentication Service (NMAS)
- PKI/Certificate
- Filtered Replica Configuration Wizard
- SNMP
- WAN Traffic Manager

Pour plus d'informations sur l'installation, la configuration et l'exécution d'iManager, reportez-vous au *Guide d'administration de NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html).

Connexion et authentification uniques

Avec eDirectory, les utilisateurs se connectent à un annuaire global. Par conséquent, il n'est pas nécessaire de gérer plusieurs comptes de serveur ou de domaine pour chacun d'eux, de même qu'il est inutile de gérer les relations approuvées ou l'authentification directe entre les domaines.

L'authentification des utilisateurs constitue une fonction de sécurité de l'Annuaire. Pour qu'un utilisateur puisse se connecter, son objet Utilisateur doit être créé dans l'Annuaire. L'objet Utilisateur a certaines propriétés, par exemple un nom et un mot de passe.

Lorsque l'utilisateur se connecte, eDirectory compare son mot de passe à celui enregistré dans l'Annuaire pour cet utilisateur et, s'ils sont identiques, autorise l'accès.

Classes et propriétés des objets

Chaque type d'objet eDirectory est défini par une classe d'objet. Par exemple, Utilisateur et Organisation sont des classes d'objets. Chacune des classes d'objets possède des propriétés particulières. Un objet Utilisateur, par exemple, possède un prénom, un nom et beaucoup d'autres propriétés.

Le schéma définit les classes et les propriétés des objets, ainsi que les règles d'endiguement (autrement dit, quels sont les objets que tel conteneur peut contenir). eDirectory est livré avec un schéma de base que vous, ou les applications que vous utilisez, pouvez étendre. Pour plus d'informations sur les schémas, reportez-vous à la « Schéma » page 51.

Les objets Conteneur contiennent d'autres objets et permettent de diviser l'arborescence en branches ; les objets Feuille représentent quant à eux les ressources réseau.

Liste des objets

Les tableaux suivants présentent les classes d'objet eDirectory. Des services supplémentaires peuvent créer dans eDirectory de nouvelles classes d'objet qui ne sont pas listées ci-dessous.

Classes d'objet Conteneur eDirectory

Icône dans iManager	Objet Conteneur (abréviation)	Description
	Arborescence	Représente le premier élément de votre arborescence. Pour plus d'informations, reportez-vous à la section « Arborescence » page 28.
	Pays (C)	Désigne les pays (« Countries » en anglais) couverts par votre réseau et organise les autres objets d'annuaire au sein de ces pays. Pour plus d'informations, reportez-vous à la section « Country » page 30.
	Conteneur de licences (LC)	Créé automatiquement lorsque vous installez un certificat de licence ou que vous créez un certificat avec compteur à l'aide de la technologie NLS (NetIQ Licensing Services). Lorsqu'une application utilisant les NLS est installée, elle ajoute un objet Conteneur de licences à l'arborescence et un objet Feuille Certificat de licence à ce conteneur.
	Organisation (O)	Vous permet d'organiser d'autres objets dans l'Annuaire. L'objet Organisation se trouve un niveau plus bas que l'objet Pays (si vous utilisez l'objet Pays). Pour plus d'informations, reportez-vous à la section « Organisation » page 28.
	Unité organisationnelle (OU)	Vous aide à organiser de manière plus précise les autres objets dans l'Annuaire. L'objet Unité organisationnelle se trouve un niveau plus bas que l'objet Organisation. Pour plus d'informations, reportez-vous à la section « Unité organisationnelle » page 29.
	Domaine (DC)	Vous aide à organiser de manière plus précise les autres objets dans l'Annuaire. L'objet Domaine peut être créé sous l'objet Arborescence ou sous les objets Organisation, Unité organisationnelle, Pays et Lieu. Pour plus d'informations, reportez-vous à la section « Domaine » page 31.

Classes d'objet Feuille eDirectory

Icône dans iManager	Objet Feuille	Description
	Serveur AFP	Représente un serveur AppleTalk* Filing Protocol qui fonctionne comme un noeud sur votre réseau eDirectory. En général, il joue également le rôle de routeur vers plusieurs ordinateurs Macintosh* et de serveur AppleTalk pour ces mêmes ordinateurs.
	Alias	Pointe vers l'emplacement réel d'un objet dans l'Annuaire. Tout objet situé à un emplacement donné de l'Annuaire peut également apparaître ailleurs dans l'Annuaire par le biais d'un alias. Pour plus d'informations, reportez-vous à la section « Alias » page 45.
	Application	Représente une application réseau. Les objets Application simplifient les tâches administratives telles que l'assignation de droits, la personnalisation des scripts de connexion et le lancement des applications.
	Ordinateur	Représente un ordinateur du réseau.

Icône dans iManager	Objet Feuille	Description
	Assignation de répertoire	Fait référence à un répertoire du système de fichiers. Pour plus d'informations, reportez-vous à la section « Assignation de répertoire » page 47.
	Groupe	Permet d'attribuer un nom à une liste d'objets Utilisateur de l'Annuaire. Vous pouvez assigner des droits au groupe plutôt qu'à chaque utilisateur. Les droits sont alors transférés à chaque utilisateur du groupe. Pour plus d'informations, reportez-vous à la section « Groupe » page 35.
	Certificat de licence	Utilisation avec la technologie NLS pour installer les certificats de licence du produit en tant qu'objets dans la base de données. Les objets Certificat de licence sont ajoutés au conteneur Produit sous licence lorsqu'une application reconnaissant la technologie NLS est installée.
	Rôle organisationnel	Définit une position ou un rôle au sein d'une organisation.
	File d'attente d'impression	Représente une file d'attente d'impression du réseau.
	Serveur d'impression	Représente un serveur d'impression du réseau.
	Imprimante	Représente un périphérique d'impression du réseau.
	Profil	Représente un script de connexion utilisé par un groupe d'utilisateurs qui ont besoin d'utiliser des commandes de script de connexion communes. Les utilisateurs ne doivent pas nécessairement se trouver dans le même conteneur. Pour plus d'informations, reportez-vous à la section « Profil » page 48.
	Serveur	Représente un serveur exécutant un système d'exploitation quelconque. Pour plus d'informations, reportez-vous à la section « Serveur » page 32.
	Modèle	Représente les propriétés standard de l'objet Utilisateur qui peuvent être appliquées aux nouveaux objets Utilisateur.
	Inconnu	Représente un objet pour lequel iManager ne possède pas d'icône spécifique.
	Utilisateur	Représente les utilisateurs de votre réseau. Pour plus d'informations, reportez-vous à la section « Utilisateur » page 33.
	Volume	Représente un volume physique du réseau. Pour plus d'informations, reportez-vous à la section « Volume » page 32.

Classes des objets Conteneur

- « Arborescence » page 28
- « Organisation » page 28
- « Unité organisationnelle » page 29
- « Country » page 30
- « Domaine » page 31

Arborescence

Le conteneur Arborescence, anciennement appelé [Root], est créé lorsque vous installez eDirectory pour la première fois sur un serveur de votre réseau. En tant que conteneur le plus élevé de l'arborescence, il contient en général des objets Organisation, Pays ou Alias.

Objet Arborescence - Définition

L'objet Arborescence représente le sommet de l'arborescence.

Utilisation

L'objet Arborescence est utilisé pour les assignations universelles de droits. Du fait de l'héritage, les assignations de droits que vous effectuez sur l'objet Arborescence (cible) sont appliquées à tous les objets de l'arborescence. Reportez-vous à la « Droits eDirectory » page 68. Par défaut, l'ayant droit [Public] dispose du droit Parcourir et l'administrateur du droit Superviseur sur l'objet Arborescence.

Propriétés importantes

- L'objet Arborescence possède une propriété Nom, qui correspond au nom d'arborescence que vous avez indiqué lors de l'installation du premier serveur. Le nom d'arborescence est indiqué dans la hiérarchie d'iManager.
- Le nom de l'arborescence ne peut pas dépasser 32 caractères.

Organisation

Un objet Conteneur Organisation est créé lorsque vous installez pour la première fois eDirectory sur un serveur de votre réseau. En tant que conteneur le plus élevé après l'objet Arborescence, il contient généralement des objets Unité organisationnelle et Feuille.

L'objet Utilisateur dénommé Admin est créé par défaut dans votre premier conteneur Organisation.

Objet Organisation - Définition

En principe, l'objet Organisation représente votre entreprise, mais vous pouvez créer d'autres objets Organisation sous l'objet Arborescence. Cela se fait couramment pour des réseaux qui représentent des régions géographiques distinctes, ou pour des entreprises qui ont fusionné et qui possèdent des arborescences eDirectory distinctes.

Utilisation

La manière dont vous utilisez les objets Organisation de votre arborescence dépend de la taille et de la structure de votre réseau. Si le réseau est petit, il est conseillé de stocker tous les objets Feuille sous un seul objet Organisation.

Pour des réseaux plus importants, vous pouvez créer des objets Unité organisationnelle dans l'objet Organisation pour faciliter la localisation et la gestion des ressources. Par exemple, vous pouvez créer des objets Unité organisationnelle pour chacun des services ou chacune des divisions de votre entreprise.

Pour les réseaux couvrant plusieurs sites, vous devez créer, dans l'objet Organisation, un objet Unité organisationnelle pour chacun des sites. Ainsi, si vous disposez (ou prévoyez de disposer) de suffisamment de serveurs pour effectuer la partition de l'Annuaire, vous pouvez le faire de manière logique, en respectant les limites des sites.

Pour simplifier le partage des ressources de l'entreprise (telles que les imprimantes, les volumes ou les applications), créez les objets correspondants sous l'Organisation.

Propriétés importantes

Les propriétés les plus utiles pour l'objet Organisation sont précisées ci-après. Seule la propriété Nom est requise. Pour obtenir la liste complète des propriétés d'un objet Organisation, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur **Aide**.

- Nom

  En règle générale, la propriété Nom est identique au nom de votre entreprise. Vous pouvez bien sûr le raccourcir dans un souci de simplicité. Par exemple, si le nom de votre entreprise est Société TUVWXYZ, vous pouvez utiliser l'abréviation YourCo.

  Le nom de l'objet Organisation est intégré au contexte pour tous les objets qui lui sont subordonnés.
- Script de connexion

  La propriété Script de connexion contient les commandes qui sont exécutées par les objets Utilisateur situés immédiatement sous l'objet Organisation. Ces commandes sont exécutées lorsqu'un utilisateur se connecte.
- Le nom de l'organisation peut contenir 64 caractères.

Unité organisationnelle

Vous pouvez créer des objets Conteneur Unité organisationnelle (OU) pour subdiviser l'arborescence. Les unités organisationnelles sont créées à l'aide d'iManager sous une organisation, un pays ou une autre unité organisationnelle.

Les objets Unité organisationnelle peuvent contenir d'autres objets de ce type et des objets Feuille, tels que Utilisateur et Application.

Objet Unité organisationnelle - Définition

En principe, l'objet Unité organisationnelle représente un service, qui contient un groupe d'objets ayant besoin d'accéder les uns aux autres. L'exemple typique est un groupe d'objets Utilisateur, ainsi que les objets Imprimante, Volume et Application dont ils ont besoin.

Au niveau le plus élevé des objets Unité organisationnelle, chacun de ces objets peut représenter un site particulier du réseau (connecté aux autres sites par une liaison WAN).

Utilisation

La manière dont vous utilisez les objets Unité organisationnelle de votre arborescence dépend de la taille et de la structure de votre réseau. Si le réseau est petit, vous n'aurez sans doute pas besoin de créer des objets Unité organisationnelle.

Pour des réseaux plus importants, vous pouvez créer des objets Unité organisationnelle dans l'objet Organisation pour faciliter la localisation et la gestion des ressources. Par exemple, vous pouvez créer des objets Unité organisationnelle pour chacun des services ou chacune des divisions de votre entreprise. N'oubliez pas que les objets Utilisateur sont plus simples à administrer lorsque vous stockez également dans l'objet Unité organisationnelle les ressources qu'ils utilisent le plus souvent.

Pour les réseaux couvrant plusieurs sites, vous devez créer, dans l'objet Organisation, un objet Unité organisationnelle pour chacun des sites. Ainsi, si vous disposez (ou prévoyez de disposer) de suffisamment de serveurs pour effectuer la partition de l'Annuaire, vous pouvez le faire de manière logique, en respectant les limites des sites.

Propriétés importantes

Les propriétés les plus utiles pour l'objet Unité organisationnelle sont précisées ci-après. Seule la propriété Nom est requise. Pour obtenir la liste complète des propriétés d'un objet Unité organisationnelle, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur **Aide**.

- Nom

  En règle générale, la propriété Nom est identique au nom du service. Vous pouvez bien sûr le raccourcir dans un souci de simplicité. Par exemple, si le nom du service dont vous dépendez est Comptabilité fournisseurs, vous pouvez utiliser l'abréviation CF.

  Le nom de l'objet Unité organisationnelle est intégré au contexte pour tous les objets qui lui sont subordonnés.
- Script de connexion

  La propriété Script de connexion contient les commandes exécutées par les objets Utilisateur situés immédiatement sous l'objet Unité organisationnelle. Ces commandes sont exécutées lorsqu'un utilisateur se connecte.
- Le nom de l'unité organisationnelle peut comporter 64 caractères.

Country

Vous pouvez créer des objets Pays directement sous l'objet Arborescence à l'aide d'iManager. Les objets Pays sont facultatifs. Ils sont requis uniquement en cas de connexion à certains annuaires globaux X.500.

Objet Pays - Définition

L'objet Pays représente l'identité politique de sa branche dans l'arborescence.

Utilisation

Le plus souvent, les administrateurs ne créent pas d'objet Pays, même si le réseau couvre plusieurs pays, puisque ce type d'objet ne fait qu'ajouter un niveau inutile à l'arborescence. Vous pouvez créer un ou plusieurs objets Pays sous l'objet Arborescence, en fonction de la nature multinationale de votre réseau. Les objets Pays ne peuvent contenir que des objets Organisation.

Si vous ne créez pas d'objet Pays et que vous en ayez besoin par la suite, il vous suffit de modifier l'arborescence et d'y ajouter un objet de ce type.

Propriétés importantes

- La propriété Nom de l'objet Pays se compose de deux lettres. Le nom des objets Pays est représenté par un code standard de deux lettres, comme US, FR ou DE.
- Le nom du pays ne peut pas dépasser 2 caractères.

Domaine

Vous pouvez créer des objets Domaine directement sous l'objet Arborescence à l'aide d'iManager. Vous pouvez également en créer sous des objets Organisation, Unité organisationnelle, Pays et Lieu.

Définition

L'objet Domaine représente des composants DNS. Les objets Domaine vous permettent d'utiliser l'emplacement DNS des ressources de type service (DNS SRV) afin de localiser des services dans votre arborescence.

À l'aide d'objets Domaine, une arborescence peut être structurée comme suit :

```
DS=Novell.DC=Provo.DC=USA
```

Dans cet exemple, tous les sous-conteneurs sont des domaines. Vous pouvez également utiliser des objets Domaine dans une arborescence mixte. Exemple :

```
DC=Novell.O=Provo.C=USA
```

Ou

```
OU=Novell.DC=Provo.C=USA
```

En règle générale, l'objet Domaine le plus élevé correspond à l'objet Arborescence global et contient tous les sous-domaines. Par exemple, ordinateur1.novell.com pourrait être représenté comme suit dans une arborescence : `DC=ordinateur1.DC=novell.DC=com`. Les domaines vous offrent un moyen plus générique d'élaborer une arborescence eDirectory. Si tous les conteneurs et sous-conteneurs sont des objets DC, les utilisateurs n'ont pas besoin de mémoriser les objets C, O ou OU lorsqu'ils recherchent des objets.

Utilisation

Le nom du domaine peut comporter 64 caractères.

Classes des objets Feuille

- « Serveur » page 32
- « Volume » page 32
- « Utilisateur » page 33
- « Groupe » page 35
- « Groupes imbriqués » page 39
- « Alias » page 45
- « Assignation de répertoire » page 47
- « Profil » page 48

Serveur

Un objet Serveur est automatiquement créé dans l'arborescence chaque fois que vous installez eDirectory sur un serveur. La classe d'objet peut correspondre à n'importe quel serveur qui exécute eDirectory.

Objet Serveur - Définition

L'objet Serveur représente un serveur exécutant eDirectory ou un serveur de Bindery.

Utilisation

L'objet Serveur joue le rôle de point de référence pour les opérations de réplication. Un objet Serveur qui représente un serveur de Bindery vous permet de gérer les volumes du serveur à l'aide d'iManager.

Propriétés importantes

L'objet Serveur possède entre autres une propriété Adresse réseau. Celle-ci indique le protocole et le numéro d'adresse du serveur. Elle est utile pour le dépannage au niveau des paquets

Pour obtenir la liste complète des propriétés d'un objet Serveur, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur **Aide**.

Volume

Lorsque vous créez un volume physique sur un serveur, un objet Volume est automatiquement créé dans l'arborescence. Par défaut, le nom de l'objet Volume est le nom du serveur suivi d'un caractère de soulignement et du nom du volume physique (par exemple, `VOTRESERVEUR_SYS`).

Les partitions d'un système de fichiers Linux ne peuvent pas être gérées à l'aide d'objets Volume. Les objets Volume sont pris en charge uniquement sous OES Linux.

Objet Volume - Définition

Un objet Volume représente un volume physique d'un serveur, qu'il s'agisse d'un disque accessible en écriture, d'un CD-ROM ou d'un autre support d'archivage. L'objet Volume d'eDirectory ne contient pas d'informations sur les fichiers et répertoires du volume. Pour accéder à ces informations, utilisez iManager. Les informations concernant les fichiers et les répertoires sont stockées dans le système de fichiers.

Utilisation

Dans iManager, cliquez sur l'icône **Volume** pour gérer les fichiers et les répertoires de ce volume. iManager fournit des informations concernant le volume, notamment l'espace disque disponible, l'espace correspondant aux entrées de répertoire et les statistiques de compression.

Propriétés importantes

Outre les propriétés Nom et Serveur hôte, qui sont obligatoires, les objets Volume ont d'autres propriétés importantes.

- Nom

  Il s'agit du nom de l'objet Volume de l'arborescence. Par défaut, le nom de cet objet est tiré du nom du volume physique, mais vous pouvez le modifier.
- Serveur hôte

  Serveur sur lequel réside le volume.
- Version

  Version eDirectory du serveur qui héberge le volume.

Utilisateur

Un objet Utilisateur est requis pour se connecter. Lorsque vous installez le premier serveur dans une arborescence, un objet Utilisateur dénommé Admin est créé. Connectez-vous la première fois en tant qu'utilisateur Admin.

Vous pouvez utiliser les méthodes suivantes pour créer ou importer des objets Utilisateur :

- iManager

  Pour plus d'informations sur iManager, reportez-vous au *Guide d'administration de NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html).

- Lots issus de fichiers de base de données

  Pour plus d'informations sur l'utilisation des fichiers de traitement par lots, reportez-vous à la « Conception de l'arborescence eDirectory » page 82.

Objet Utilisateur - Définition

Un objet Utilisateur représente une personne sur le réseau.

Utilisation

Vous devez créer des objets Utilisateur pour toutes les personnes qui sont amenées à utiliser le réseau. Bien que vous puissiez gérer les objets Utilisateur individuellement, il est plus rapide de procéder comme suit :

- Utilisez les objets Modèle pour définir les propriétés par défaut de la plupart des objets Utilisateur. L'objet Modèle est automatiquement appliqué aux objets Utilisateur que vous créez (mais non aux objets Utilisateur existants).
- Créez des objets Groupe pour gérer les groupes d'utilisateurs.
- Assignez des droits en utilisant les objets Conteneur comme ayants droit si vous souhaitez que ces droits soient appliqués à tous les objets Utilisateur du conteneur.
- Sélectionnez plusieurs objets Utilisateur en maintenant la touche Maj ou Ctrl enfoncée tout en cliquant. Une fois les objets Utilisateur sélectionnés, vous pouvez changer les valeurs de leurs propriétés.

Propriétés importantes

Les objets Utilisateur peuvent posséder plus de 80 propriétés. Pour obtenir la liste complète des propriétés d'un objet Utilisateur, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur **Aide**.

Les propriétés Nom de connexion et Nom sont obligatoires. Ces propriétés, ainsi que les propriétés les plus utiles, sont répertoriées ci-dessous.

- Date d'expiration du compte vous permet de limiter la durée de vie d'un compte utilisateur. Après la date d'expiration, le compte est verrouillé et l'utilisateur ne peut plus se connecter.
- Compte désactivé est une valeur générée par le système, qui indique que le compte est verrouillé. L'utilisateur ne peut donc plus se connecter. Le compte peut être verrouillé s'il a expiré ou si l'utilisateur a entré successivement trop de mots de passe incorrects.
- Changement périodique du mot de passe obligatoire vous permet de renforcer la sécurité en demandant à l'utilisateur de changer son mot de passe après un certain laps de temps.

- Adhésion aux groupes permet de lister tous les objets Groupe dont l'utilisateur est membre.
- Dernière connexion est une propriété générée par le système, qui indique la date et l'heure auxquelles l'utilisateur s'est connecté pour la dernière fois.
- Bien qu'elle soit obligatoire, la propriété Nom n'est pas utilisée directement par eDirectory. Les applications qui se servent de la base de noms eDirectory peuvent utiliser cette propriété, ainsi que d'autres propriétés d'identification, telles que Prénom, Titre, Emplacement et Numéro de télécopie.
- Limiter connexions simultanées permet de définir le nombre maximal de sessions qu'un utilisateur peut ouvrir de façon simultanée sur le réseau.
- Nom de connexion est le nom affiché par l'icône Utilisateur dans iManager. C'est également le nom fourni par l'utilisateur lorsqu'il se connecte.

  Avec eDirectory, il n'est pas nécessaire que chaque nom de connexion soit unique sur tout le réseau ; il doit toutefois l'être dans chacun des conteneurs. Vous pouvez malgré tout décider d'étendre leur unicité à l'ensemble de l'entreprise pour en simplifier l'administration.

  En général, le nom de connexion est une combinaison du nom et du prénom de l'utilisateur. Par exemple, JEANT ou JTHOMAS pour Jean Thomas.
- Script de connexion vous permet de créer des commandes de connexion spécifiques pour un objet Utilisateur. Lorsqu'un utilisateur se connecte, le script de connexion de conteneur est exécuté en premier. Si l'objet Utilisateur a été ajouté à la liste des membres d'un objet Profil, le script de connexion de profil est ensuite exécuté. Enfin, le script de connexion utilisateur est exécuté (le cas échéant).

  Il est recommandé de placer la plupart des commandes de connexion dans des scripts de connexion de conteneur pour gagner du temps. Vous pouvez éditer le script de connexion utilisateur pour gérer les exceptions aux besoins communs.
- Restrictions des heures de connexion vous permet de définir les jours et les heures auxquels l'utilisateur peut se connecter.
- La propriété Adresses réseau contient des valeurs générées par le système qui répertorient toutes les adresses IPX™ et/ou IP à partir desquelles l'utilisateur se connecte. Ces valeurs sont utiles pour résoudre les problèmes de réseau au niveau des paquets.
- Exiger un mot de passe vous permet de déterminer si l'utilisateur doit fournir un mot de passe. D'autres propriétés apparentées vous permettent de définir des contraintes communes en ce qui concerne les mots de passe, par exemple leur longueur.
- Droits sur des fichiers et des répertoires indique toutes les assignations de droits effectuées pour cet utilisateur sur le système de fichiers Vous pouvez également contrôler, à l'aide d'iManager, les droits effectifs que possède un utilisateur sur des fichiers et des répertoires, y compris les droits hérités d'autres objets.

Groupe

Vous pouvez créer des objets Groupe pour faciliter la gestion d'ensembles d'objets Utilisateur.

Objet Groupe - Définition

Un objet Groupe représente un groupe d'objets Utilisateur.

Utilisation

Les objets Conteneur permettent de gérer tous les objets Utilisateur du conteneur considéré, alors que les objets Groupe servent à gérer des sous-ensembles dans un ou plusieurs conteneurs.

Les objets Groupe servent principalement dans deux cas :

- Ils vous permettent de concéder des droits simultanément à plusieurs objets Utilisateur.
- Ils vous permettent d'entrer des commandes de script de connexion à l'aide de la syntaxe `IF MEMBER OF`.

Groupes statiques

Les groupes statiques permettent d'identifier les objets membres de manière explicite. Chaque membre est assigné explicitement à un groupe.

Ces groupes fournissent une liste statique des membres et assurent l'intégrité référentielle entre la liste des membres du groupe et les membres des attributs d'un objet. L'appartenance au groupe est gérée explicitement au moyen de l'attribut Membre.

Groupes dynamiques

Les groupes dynamiques utilisent une URL LDAP pour définir un ensemble de règles qui, si elles sont satisfaites par des objets Utilisateur eDirectory, déterminent les membres du groupe. Les membres d'un groupe dynamique partagent un ensemble d'attributs communs, définis par le filtre de recherche spécifié dans l'URL. Pour plus d'informations sur le format d'URL LDAP, reportez-vous au fichier RFC 2255 (http://www.ietf.org/rfc/rfc2255.txt).

Les groupes dynamiques vous permettent de définir les critères à utiliser lors de l'évaluation des adhésions à un groupe. Les membres du groupe sont évalués de manière dynamique par eDirectory, ce qui vous permet de les définir en termes de regroupement logique. eDirectory peut ainsi ajouter et supprimer automatiquement des membres d'un groupe. Cette solution, plus facilement adaptable, permet de réduire les coûts d'administration et peut compléter les groupes classiques dans LDAP pour offrir une flexibilité accrue.

eDirectory vous permet de créer un groupe dynamique lorsque vous souhaitez regrouper automatiquement des utilisateurs en fonction d'un attribut, ou lorsque vous souhaitez appliquer des listes de contrôle d'accès (ACL) à des groupes spécifiques qui contiennent des noms distinctifs (DN) correspondants. Vous pouvez, par exemple, créer un groupe qui inclut automatiquement tout DN possédant l'attribut Department=Marketing. Si vous appliquez un filtre de recherche pour Department=Marketing, la recherche renvoie un groupe comprenant l'ensemble des DN possédant l'attribut Department=Marketing. Vous pouvez ensuite définir un groupe dynamique à partir du résultat de la recherche obtenu au moyen de ce filtre. Tout objet Utilisateur ajouté à l'annuaire, qui satisfait au critère Department=Marketing est alors automatiquement ajouté au groupe. De la même façon, tout objet Utilisateur pour lequel la valeur de « Department » a été modifiée (ou tout objet Utilisateur supprimé de l'annuaire) est automatiquement supprimé du groupe.

Dans eDirectory, les groupes dynamiques sont créés par l'intermédiaire d'objets du type objectclass=dynamicGroup. Il est possible de convertir un groupe statique en groupe dynamique en associant une classe auxiliaire (dynamicGroupAux) à l'objet Groupe. L'attribut memberQueryURL est associé au groupe dynamique.

L'attribut dgIdentity pour l'objet Groupe dynamique peut prendre comme valeur le nom distinctif d'une entrée dont les références et les droits doivent être utilisés pour augmenter le nombre de membres dynamiques du groupe.

La gestion des groupes s'effectue au moyen de l'attribut memberQueryURL. Un attribut memberQueryURL type comporte un DN de base, une étendue, un filtre et une extension facultative. Le DN de base précise la base de recherche. L'étendue définit les niveaux sur lesquels doit porter la recherche sous la base. Le filtre permet de sélectionner des entrées spécifiques de l'étendue lors des recherches.

REMARQUE : afin de prendre en charge les exceptions à la liste créée par l'attribut memberQueryURL, les groupes dynamiques permettent aussi l'inclusion et l'exclusion explicite d'utilisateurs.

Il est possible de créer et de gérer des groupes dynamiques par le biais de NetIQ iManager. Pour accéder aux tâches de gestion de groupes, cliquez sur le rôle **Groupes** de la page Rôles et tâches.

Vous pouvez également utiliser des commandes LDAP pour gérer ces groupes. Les propriétés les plus utiles associées aux groupes dynamiques sont dgIdentity et memberQueryURL.

Propriétés importantes

Les propriétés les plus utiles de l'objet Groupe sont Membres et Droits sur des fichiers et des répertoires. Pour obtenir la liste complète des propriétés d'un objet Groupe, sélectionnez un objet de ce type dans iManager. Pour afficher une description de chaque page de propriétés, cliquez sur **Aide**.

- dgAllowDuplicates

  Indique si les doublons sont autorisés ou non lors de l'impression de membres de groupes dynamiques. La valeur par défaut est TRUE.

- dgIdentity

  Cette propriété indique le DN dont l'identité est utilisée par le groupe dynamique pour les authentifications au cours des recherches. L'identité doit figurer sur la même partition que le groupe dynamique. L'objet spécifié par dgIdentity doit avoir les droits requis pour effectuer la recherche définie dans l'attribut memberQueryURL.

  Par exemple, si la valeur de memberQueryURL est

  ```
  l"dap:///o=nov??sub?(title=*)
  ```

  dgIdentity doit avoir les droits de lecture/comparaison sur l'intitulé d'attribut figurant sous le conteneur `o=nov`.

- dgTimeout

  Cette propriété indique le délai maximal alloué à un serveur pour lire ou comparer un attribut member avant expiration. Lorsque ce délai est dépassé, l'erreur -6016 s'affiche.

- memberQueryURL

  Cette propriété définit l'ensemble des règles qui correspondent aux attributs des membres du groupe.

  memberQueryURL est un attribut à valeurs multiples, conformément à sa définition dans le schéma. Cependant, les serveurs eDirectory 8.6.1 n'utilisaient que la première valeur.

  Par exemple :

  Un administrateur crée un groupe dynamique possédant deux valeurs memberQueryURL :

  ```
  l"dap:///o=nov??sub?cn=*
  ```

  ```
  l"dap:///o=org??sub?cn=*
  ```

  Les serveurs eDirectory 8.6.*x* utilisent `l"dap:///o=nov??sub?cn=*"` pour déterminer les membres du groupe. Ils acceptent plusieurs requêtes, mais ne lisent que la première.

Cette limitation n'existe plus depuis eDirectory 8.7 et versions ultérieures. Les serveurs eDirectory déterminent les membres en fonction de l'ensemble des valeurs memberQueryURL. Ainsi, l'ensemble de membres correspond à la synthèse des membres obtenus à partir de chacune des valeurs de memberQueryURL.

Dans l'exemple ci-dessus, les membres résultants du groupe dynamique correspondent à l'ensemble des entrées pour lesquelles o=org et o=nov, et qui possèdent des valeurs cn.

- member

  Cette propriété liste tous les objets du groupe. Les assignations de droits effectuées sur un objet Groupe sont appliquées à tous les membres de ce groupe. L'ajout de valeurs à la propriété member d'un groupe dynamique entraîne l'ajout des membres statiques à ce groupe. Cela peut servir à inclure certains membres.

- excludedMember

  Cette propriété indique les DN spécifiquement exclus de la liste d'adhésion à un groupe dynamique. Elle peut servir à constituer des listes d'exclusion pour les groupes dynamiques.

  excludedMember s'emploie pour interdire à des DN de devenir des membres dynamiques d'un groupe dynamique.

  Ainsi, un DN est un membre dynamique d'un groupe dynamique uniquement s'il a été sélectionné en fonction des critères définis dans memberQueryURL et s'il n'est pas spécifié dans excludedMember ou ajouté de manière explicite à uniqueMember ou member.

- staticMember

  Cette propriété lit les membres statiques d'un groupe dynamique et détermine si un DN est un membre statique d'un groupe dynamique. staticMember permet de rechercher les groupes dynamiques dans lesquels un DN est un membre statique unique, ainsi que ceux ne comprenant que des membres dynamiques (sans aucun membre statique).

  Pour l'ajouter aux groupes dynamiques existants, étendez le schéma à l'aide du fichier `dgstatic.sch`.

Mise à niveau de groupes dynamiques dans des bases de données antérieures à eDirectory 8.6.1

La fonctionnalité des groupes dynamiques exige certaines valeurs internes stockées dans les objets Groupe dynamique, qui sont créées lorsqu'un groupe dynamique est créé localement ou reçu dans le cadre d'une synchronisation.

S'ils sont capables de contenir des groupes dynamiques, les serveurs plus anciens ne peuvent pas générer ces valeurs, puisque les groupes dynamiques ont été introduits avec eDirectory 8.6.1.

eDirectory 8.6.2 prévoit la mise à niveau automatique des objets Groupe dynamique d'une base de données antérieure à la version 8.6.1, afin que celle-ci corresponde à une base de données eDirectory 8.6.1.

Prise en charge d'autres syntaxes de memberQueryURL

L'attribut memberQueryURL peut contenir un filtre de recherche utilisé par le serveur eDirectory pour déterminer les membres d'un groupe dynamique.

Dans eDirectory 8.6.1, les syntaxes des attributs employés dans le filtre étaient limitées aux types de chaîne élémentaire suivants :

- SYN_CE_STRING
- SYN_CI_STRING
- SYN_PR_STRING

- SYN_NU_STRING
- SYN_CLASS_NAME
- SYN_TEL_NUMBER
- SYN_INTEGER
- SYN_COUNTER
- SYN_TIME
- SYN_INTERVAL
- SYN_BOOLEAN
- SYN_DIST_NAME
- SYN_PO_ADDRESS
- SYN_CI_LIST
- SYN_FAX_NUMBER
- SYN_EMAIL_ADDRESS

Depuis eDirectory 8.7.3, les syntaxes d'attributs ci-dessous sont également reconnues pour une valeur memberQueryURL :

- SYN_PATH
- SYN_TIMESTAMP
- SYN_TYPED_NAME

Dans eDirectory 8.6.1 comme dans eDirectory 8.7.x, les syntaxes binaires telles que SYN_OCTET_STRING et SYN_NET_ADDRESS ne sont pas admises dans les filtres de recherche memberQueryURL.

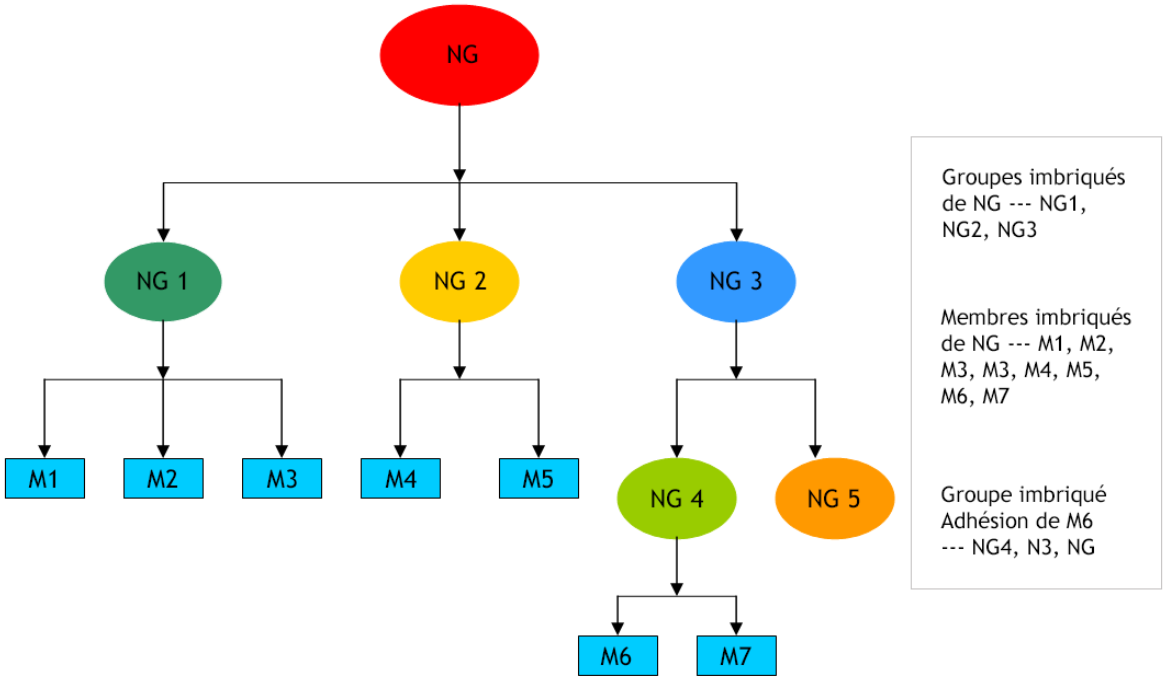
Pour plus d'informations, reportez-vous au document « How to Manage and Use Dynamic Groups in NetIQ eDirectory » (http://support.novell.com/techcenter/articles/ana20020405.html) (Gestion et utilisation des groupes dynamiques dans NetIQ eDirectory).

Groupes imbriqués

Les groupes imbriqués permettent de regrouper des groupes de manière plus structurée. L'attribut groupMember spécifie les groupes imbriqués dont les membres deviennent des membres imbriqués de l'objet Conteneur Groupe imbriqué. Les objets Groupe sont spécifiés statiquement dans l'attribut groupMember. Le groupe contenant d'autres groupes est appelé groupe conteneur et les groupes faisant partie de ce groupe sont appelés groupes contenus. eDirectory prend en charge l'imbrication de groupes tant statiques que dynamiques. L'imbrication peut comporter jusqu'à 200 niveaux.

IMPORTANT : Elle est prise en charge au sein du serveur local uniquement. Si un groupe contenu n'est pas présent sur le serveur local, ses membres ne sont pas répertoriés comme membres imbriqués du groupe conteneur.

Figure 1-4 *Groupes imbriqués*



Vous pouvez utiliser iManager ou les outils LDAP pour créer les groupes imbriqués.

- « Création de groupes imbriqués à l'aide des outils LDAP » page 40
- « Création de groupes imbriqués avec iManager » page 40

Création de groupes imbriqués à l'aide des outils LDAP

Vous pouvez utiliser les outils LDAP pour créer les groupes imbriqués. Une nouvelle classe auxiliaire, nestedGroupAux, ainsi que la classe structurelle Groupe représentent un groupe imbriqué. Cette classe auxiliaire peut être ajoutée à l'objet Groupe statique existant pour le convertir en groupe imbriqué.

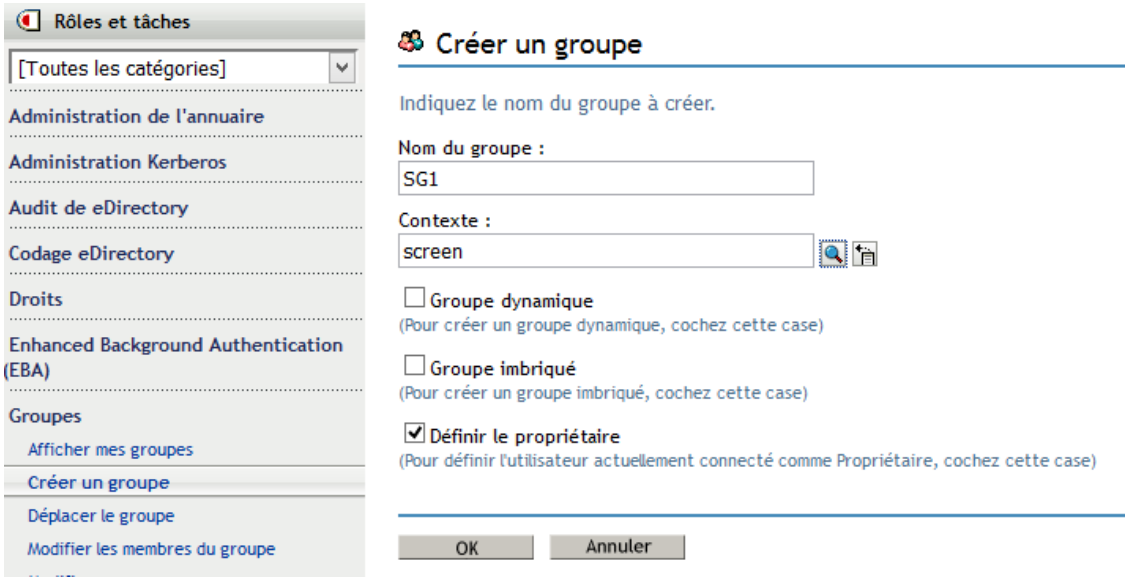
Le groupe conteneur et le groupe contenu doivent être des objets Groupe imbriqué. Si le groupe contenu est un groupe imbriqué (et uniquement dans ce cas), il peut renseigner l'attribut groupMembership (cet attribut ne fait pas partie d'un groupe statique) défini pour lui-même afin de spécifier le groupe conteneur. Si les groupes contenus ne sont pas du même type que le groupe conteneur, seuls les membres statiques du groupe contenu sont répertoriés comme membres imbriqués.

Vous pouvez utiliser des fichiers LDIF et les outils LDAP pour gérer ces groupes. Les propriétés les plus utiles associées aux groupes imbriqués sont groupMember et nestedConfig.

Création de groupes imbriqués avec iManager

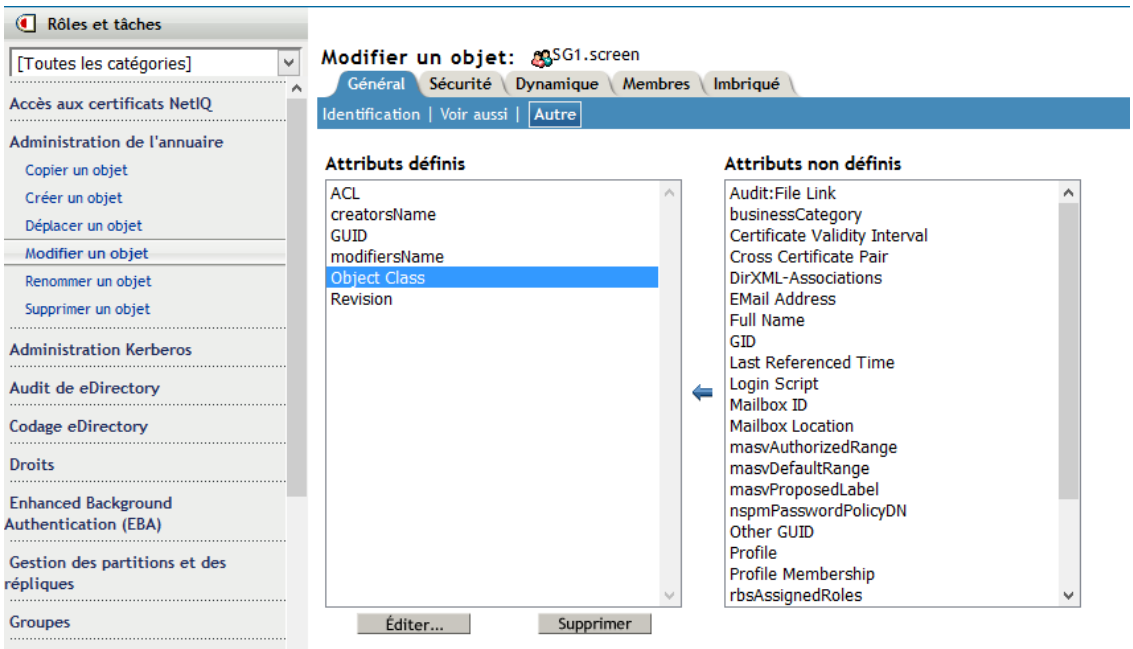
Vous pouvez utiliser les plug-ins iManager pour créer un groupe imbriqué ou pour convertir un groupe statique en groupe imbriqué afin de l'associer à un autre groupe.

1 Connectez-vous à iManager en tant qu'administrateur et sélectionnez **Groupes** > **Créer un groupe** dans le panneau de gauche pour créer un groupe statique. Par exemple, SG1.



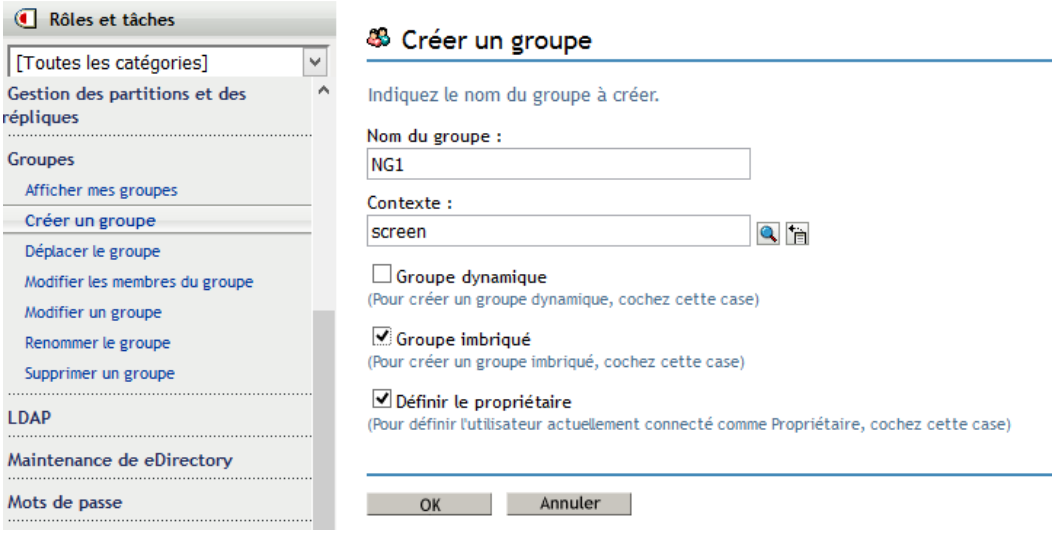
2 Sélectionnez **Administration de l'annuaire > Modifier un objet** dans le panneau de gauche, puis recherchez et sélectionnez l'objet *SG1.novell*.

3 Cliquez sur l'onglet **Autre**, puis sélectionnez **Classe d'objet** dans la liste **Attributs non définis**.

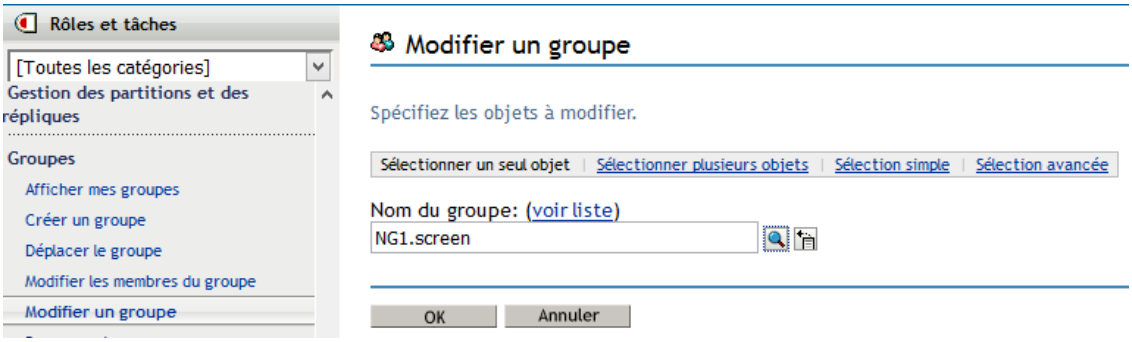


4 Ajoutez la valeur **nestedGroupAux** à la **Classe d'objet**, puis cliquez sur **OK** et sur **Appliquer**.

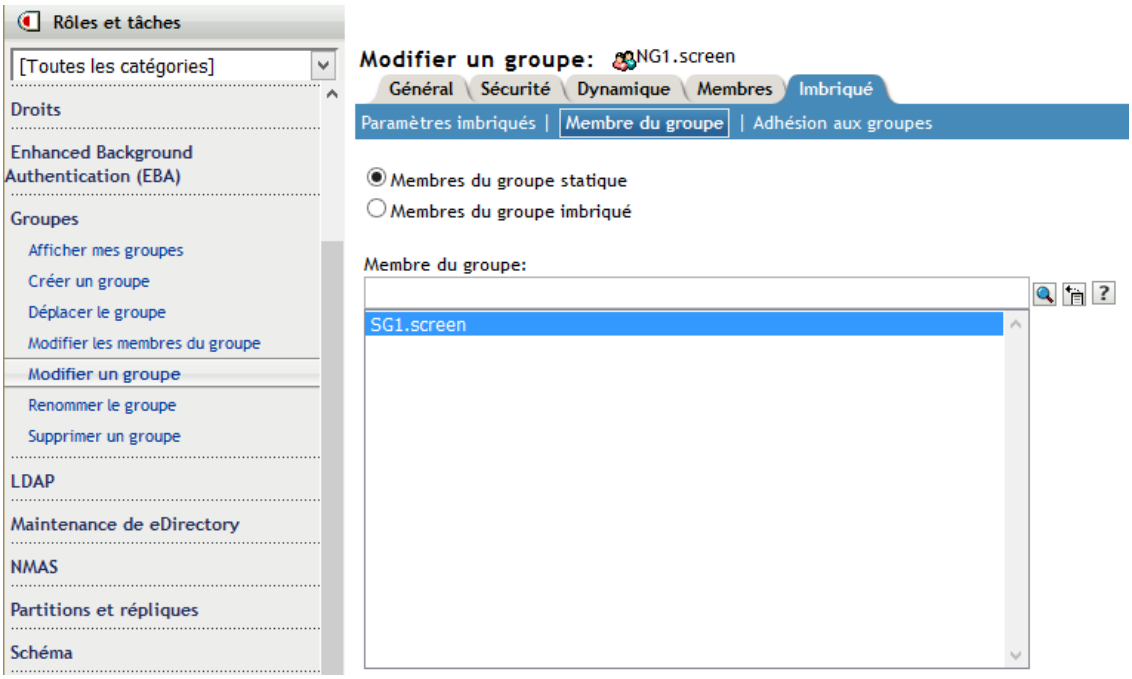
5 Sélectionnez **Groupes** > **Créer un groupe** dans le panneau de gauche, cochez la case **Groupe imbriqué** pour créer un groupe imbriqué portant le nom NG1, puis cliquez sur **OK**.



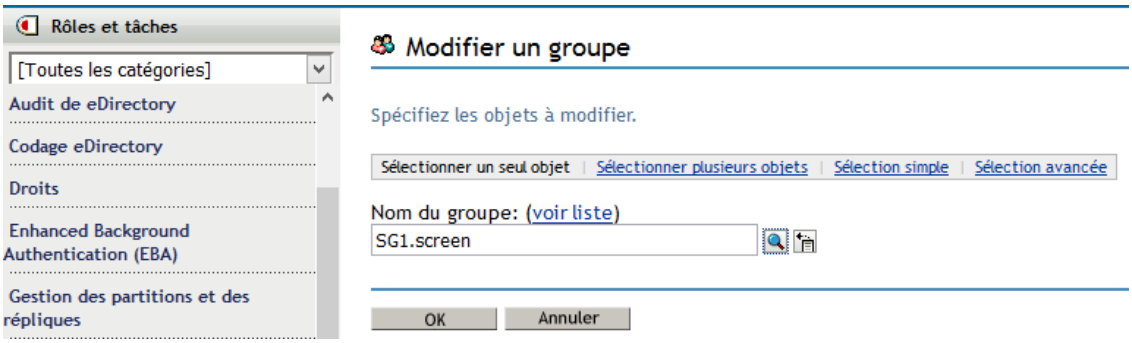
6 Sélectionnez **Groupes** > **Modifier un groupe** dans le panneau de gauche, cochez la case **Groupe imbriqué** pour modifier le groupe imbriqué portant le nom NG1, puis cliquez sur **OK**.



7 Pour modifier le groupe imbriqué, sélectionnez **Groupes > Modifier un groupe**, puis recherchez et sélectionnez **NG1.novell**.



8 Pour associer un groupe statique à **NG1**, sélectionnez l'onglet **Imbriqué > Membre du groupe**, puis recherchez et sélectionnez le groupe statique SG1.



9 Cliquez sur **Appliquer**, puis sur **OK** pour convertir le groupe statique SG1 en groupe imbriqué NG1.

Le groupe statique que vous avez converti en groupe imbriqué est désormais membre du groupe statique.

Pour vérifier les détails d'adhésion de SG1, sélectionnez **Groupes > Modifier un groupe** dans le panneau de gauche, puis **SG1.novell**. Sélectionnez l'onglet **Imbriqué > Adhésion au groupe** pour vérifier les informations d'adhésion au groupe statique en tant que **NG1.novell**.

Propriétés des groupes imbriqués

- groupMember

  Par défaut, les membres d'un groupe imbriqué incluent tous les membres imbriqués. Par conséquent, la liste d'attributs de membres renvoie toujours tous les membres imbriqués, et l'assertion sur l'attribut de membre renvoie tous les objets Groupe imbriqué. Si la configuration est définie sur 1 (aucune imbrication), elle fait uniquement référence aux membres directs.

- Group Membership

  L'attribut groupMembership spécifie le groupe auquel appartient cet objet (en général, un objet Utilisateur). Il est associé à la classe nestedGroupAux et contient le DN du groupe imbriqué dont ce groupe est membre. Lorsqu'il est associé à un objet Groupe, il indique le groupe imbriqué dont ce groupe est membre (plus particulièrement, un groupMember). Comme member et groupMember, l'attribut groupMembership répertorie tous les groupes imbriqués dont ce groupe affiche une valeur groupMembership via une relation imbriquée. La valeur nestedConfig s'applique également à l'attribut groupMembership. Pour les objets non membres du groupe, la valeur nestedConfig de groupes spécifiques est utilisée.

- nestedConfig

  L'attribut nestedConfig définit la configuration de l'objet Groupe imbriqué. Les valeurs de configuration actuellement prises en charge sont 0 (imbrication du serveur local) et 1 (aucune imbrication). Par défaut, il imbrique toujours le serveur local. Si seules des valeurs directes telles que member, groupMember ou groupMembership doivent être répertoriées pour l'attribut, la configuration peut être définie sur 1.

- excludedMember

  La valeur excludedMember fait partie de la classe nestedGroupAux, mais l'attribut n'est pas utilisé actuellement. Si un groupe inclut des classes de groupe imbriqué et de groupe dynamique, excludedMember s'applique uniquement aux membres dynamiques au niveau du groupe.

Opérations sur les groupes imbriqués

1. Un groupe peut être membre d'un autre groupe via l'attribut groupMember. Pour ces deux groupes, tant contenus que conteneurs, la classe auxiliaire de groupe imbriqué doit être associée avec l'objet Groupe.

   ```
   dn: cn=finance,o=nov

   objectclass: group

   objectclass: nestedGroupAux

   groupMember: cn=accounts,o=nov

   member: cn=jim,o=nov


   dn: cn=accounts,o=nov

   objectclass: group

   objectclass: nestedGroupAux

   member: cn=allen,o=nov

   member: cn=ESui,o=nov

   member: cn=YLi,o=nov
   ```

2. La lecture de l'attribut de membre d'un groupe imbriqué entraîne également le renvoi des membres du groupe contenu si le groupe contenu et le groupe conteneur sont tous les deux présents localement sur le serveur :

   ```
   dn: cn=finance,o=nov
   member: cn=jim,o=nov
   member: cn=allen,o=nov
   member: cn=ESui,o=nov
   member: cn=YLi,o=nov
   ```

   Il en va de même pour l'attribut groupMember.

3. L'attribut réciproque de l'attribut de membres est groupMembership. Cela implique que pour l'objet Utilisateur `cn=allen,o=nov`, l'attribut groupMembership doit être renseigné avec le DN de groupe `cn=accounts,o=nov`. L'attribut groupMembership du groupe `cn=accounts,o=nov` doit être renseigné avec `cn=finance,o=nov`. À la lecture de l'attribut groupMembership de l'objet Utilisateur `cn=allen,o=nov`, les deux groupes sont renvoyés.

   ```
   dn: cn=allen,o=nov
   groupMembership: cn=accounts,o=nov
   groupMembership: cn=finance,o=nov
   ```

4. Les ACL peuvent être assignées à un groupe imbriqué et tous les objets qui sont membres du groupe imbriqué vont acquérir les droits. Dans le champ des droits assignés, un bit ACL imbriquée supplémentaire (0x80000000) doit être défini en plus des droits assignés.

```
dn: cn=finance,o=nov
groupMember: cn=accounts,o=nov
```

```
dn: cn=accounts,o=nov
member: cn=allen,o=nov
```

```
dn: ou=MyCo,o=nov
objectclass: Organizational Unit
ACL: 2147483650#entry#cn=finance,o=nov#[All Attributes Rights]
```

La valeur des droits – 2147483650 (0x80000002) a un bit ACL imbriquée (0x80000000) et un bit droits de lecture (0x00000002) définis. Par conséquent, l'objet Utilisateur `cn=allen,o=nov` s'est vu accorder des droits de lecture sur tous les attributs de l'objet MyCo via le groupe imbriqué `cn=finance,o=nov`.

5. Les applications peuvent utiliser des assertions de filtre sur les attributs member, groupMember et groupMembership. Dans l'exemple ci-dessus, une assertion de `member=cn=allen,o=nov` renverrait les éléments suivants :

   ```
   dn: cn=accounts,o=nov
   dn: cn=finance,o=nov
   ```

   Une assertion de `groupMembership=cn=finance,o=nov` renverrait les objets suivants :

   ```
   dn: cn=allen,o=nov
   dn: cn=jim,o=nov
   dn: cn=ESui,o=nov
   dn: cn=YLi,o=nov
   dn: cn=accounts,o=nov
   ```

   REMARQUE : aucune limite n'existe pour les niveaux d'imbrication dans les cas ci-dessus. La détection de boucle dans les groupes imbriqués s'effectue lors de la lecture des attributs mentionnés ci-dessus.

Limites

- Les relations imbriquées ne s'étendent pas au-delà du serveur local. Les objets, utilisateurs et groupes concernés doivent être localement présents sur le serveur.
- Les doublons ne sont pas éliminés dans la liste des membres.
- Les ACL imbriquées et la sémantique d'imbrication ne sont pas prises en charge sur les serveurs eDirectory plus anciens (8.8 SP1 et versions antérieures).

Alias

Vous pouvez créer un objet Alias qui pointe sur un autre objet de l'arborescence. Un objet Alias offre à un utilisateur un nom local pour un objet qui se trouve à l'extérieur de son conteneur.

Lorsque vous renommez un conteneur, vous pouvez créer un objet Alias à l'ancien emplacement du conteneur qui pointe vers le conteneur que vous venez de renommer. Ainsi, les postes de travail et les commandes de script de connexion qui font référence à des objets du conteneur peuvent toujours accéder à ceux-ci, même si le nom du conteneur n'a pas été mis à jour.

Objet Alias - Définition

Un objet Alias représente un autre objet, par exemple un conteneur, un objet Utilisateur ou tout autre objet de l'arborescence. Un objet Alias n'est pas doté de droits d'ayants droit. L'autorité d'ayant droit que vous accordez à l'objet Alias est appliquée à l'objet qu'il représente. Cependant, l'objet Alias peut être la cible d'une assignation d'ayant droit.

Utilisation

Créez un objet Alias pour faciliter la résolution de nom. Étant donné qu'il est plus simple d'attribuer un nom aux objets du contexte actuel, il est conseillé de créer dans ce contexte des objets Alias se rapportant à des ressources situées en dehors de ce contexte.

Supposons, par exemple, que des utilisateurs se connectent et qu'ils établissent le contexte actuel dans le conteneur South (comme illustré sur la Figure 1-5), mais qu'ils aient besoin d'accéder à l'objet File d'attente d'impression QualCoul dans le conteneur North.

Figure 1-5 *Exemples de conteneurs*

Vous pouvez créer un objet Alias dans le conteneur South, comme l'illustre la Figure 1-6.

Figure 1-6 *Objet Alias dans un conteneur eDirectory*

L'objet Alias pointe vers l'objet QualCoul d'origine ; la configuration de l'impression pour les utilisateurs implique donc un objet local.

Propriétés importantes

Les objets Alias possèdent une propriété dénommée Objet en alias, qui associe l'objet Alias à l'objet d'origine.

Assignation de répertoire

L'objet Assignation de répertoire pointe vers un chemin du système de fichiers du serveur. Il vous permet de faire référence plus simplement aux répertoires.

Si aucun volume ne se trouve sur votre réseau, vous ne pouvez pas créer d'objets Assignation de répertoire.

Objet Assignation de répertoire - Définition

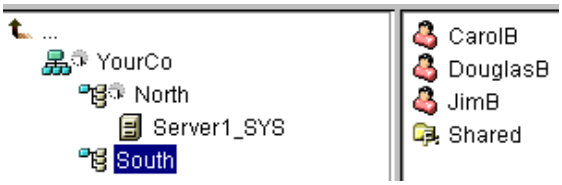
Un objet Assignation de répertoire représente un répertoire sur un volume En revanche, un objet Alias représente un objet.

Utilisation

Vous pouvez créer un objet Assignation de répertoire pour simplifier l'assignation d'unités, en particulier dans les scripts de connexion. Si vous utilisez un objet Assignation de répertoire, vous pouvez réduire les chemins complexes de système de fichiers à un seul nom.

En outre, quand vous déplacez un fichier, il est inutile de modifier les scripts de connexion et les fichiers de traitement par lots pour qu'ils indiquent son nouvel emplacement. Vous devez seulement modifier l'objet Assignation de répertoire. Supposons, par exemple, que vous éditiez le script de connexion du conteneur South, illustré sur la Figure 1-7.

Figure 1-7 *Exemple de conteneur eDirectory*



Une commande assignant des unités au répertoire Shared du volume `sys:` aurait la syntaxe suivante :

```
MAP N:=sys.North.:Shared
```

Si vous avez créé l'objet Assignation de répertoire Partagé, la commande d'assignation est beaucoup plus simple :

```
MAP N:=Shared
```

Propriétés importantes

L'objet Assignation de répertoire possède les propriétés suivantes :

- Nom

  Identifie l'objet dans l'annuaire (par exemple, Partagé). Le nom est également utilisé dans les commandes MAP.

- Volume

  La propriété Volume indique le nom de l'objet Volume désigné par l'objet Assignation de répertoire. Par exemple, Sys.North.YourCo.

- Chemin

  Désigne le répertoire par un chemin d'accès à partir de la racine du volume, par exemple `public\winnt\nls\english`.

Profil

Les objets Profil vous aident à gérer les scripts de connexion.

Objet Profil - Définition

Un objet Profil représente un script de connexion qui s'exécute entre le script de connexion de conteneur et le script de connexion utilisateur.

Utilisation

Créez un objet Profil si vous souhaitez que les commandes de script de connexion ne soient exécutées que pour les utilisateurs sélectionnés. Les objets Utilisateur peuvent se trouver dans le même conteneur ou dans des conteneurs différents. Une fois l'objet Profil créé, vous devez ajouter les commandes à sa propriété Script de connexion. Transformez ensuite les objets Utilisateur en ayants droit de l'objet Profil, puis ajoutez ce dernier à leur propriété Profil de membre du groupe.

Propriétés importantes

L'objet Profil possède deux propriétés importantes :

- Script de connexion

  Contient les commandes que vous souhaitez exécuter pour les utilisateurs du profil.
- Droits sur des fichiers et des répertoires

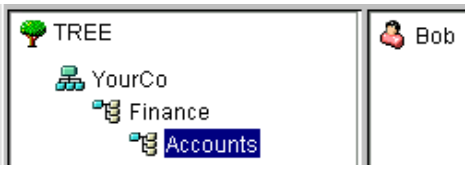
  Si le script de connexion contient des instructions de type INCLUDE, utilisez la propriété Droits sur les fichiers et les répertoires pour accorder à l'objet Profil des droits sur les fichiers inclus.

Contexte et dénomination

Le contexte d'un objet est sa position dans l'arborescence. Il est pratiquement équivalent à un domaine DNS.

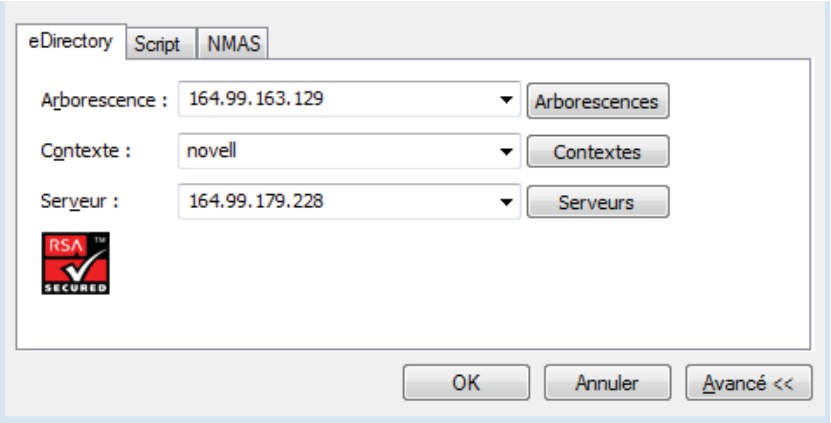
Sur la Figure 1-8, vous pouvez observer que l'utilisateur nommé Bob se trouve dans l'unité organisationnelle Accounts, elle-même dans l'unité organisationnelle Finance, laquelle se trouve dans l'organisation YourCo.

Figure 1-8 *Exemple de conteneur eDirectory*



Il est parfois nécessaire d'indiquer explicitement le contexte d'un objet dans un utilitaire eDirectory. Par exemple, si vous configurez le poste de travail de Bob, vous serez probablement amené à fournir un contexte de nom, comme l'illustre la Figure 1-9.

Figure 1-9 *Page NDS du client Novell*



Le contexte se présente sous la forme d'une liste de conteneurs séparés par des points entre l'objet concerné et le sommet de l'arborescence.

Nom distinctif

Le nom distinctif d'un objet est le nom de cet objet, suivi du contexte. Par exemple, le nom complet de l'objet Utilisateur Bob est : Bob.Accounts.Finance.YourCo.

Nom avec type

Des noms avec type apparaissent parfois dans les utilitaires eDirectory. Ces noms comprennent les abréviations de type d'objet indiquées dans le tableau ci-dessous :

Classe d'objet	Type	Abréviation
Toutes les classes d'objets Feuille	Nom courant	CN
Organisation	Organisation	O
Unité organisationnelle	Unité organisationnelle	OU
Country	Country	C
Lieu	Lieu ou état/province	L ou S

Pour créer un nom avec type, eDirectory utilise l'abréviation du type, suivie du signe égal et du nom de l'objet. Par exemple, le nom avec type partiel de Bob est : CN=Bob. Le nom avec type complet de Bob est : CN=Bob.OU=Accounts.OU=Finance.O=YourCo. Vous pouvez utiliser des noms avec ou sans type dans les utilitaires eDirectory.

Résolution de nom

Le processus mis en oeuvre par eDirectory pour trouver l'emplacement d'un objet dans l'arborescence Annuaire est appelé *résolution de nom*. Lorsque vous utilisez des noms d'objet dans les utilitaires eDirectory, eDirectory résout les noms par rapport au contexte actuel ou au sommet de l'arborescence.

Contexte de poste de travail actuel

Un contexte est défini sur les postes de travail lorsque le logiciel réseau est exécuté sur ces postes. Ce contexte identifie de manière relative l'emplacement du poste de travail sur le réseau. Par exemple, le poste de travail de Bob a le contexte actuel suivant :

```
Accounts.Finance.YourCo
```

Le contexte actuel permet de comprendre l'utilisation des points initiaux, des noms relatifs et des points finaux (voir sections suivantes).

Point initial

Utilisez un point initial pour résoudre le nom depuis le sommet de l'arborescence, indépendamment de l'endroit où le contexte actuel est défini. Dans l'exemple suivant, le point initial permet d'indiquer à l'utilitaire CX (Changer de contexte) de résoudre le nom par rapport au sommet de l'arborescence.

```
CX .Finance.YourCo
```

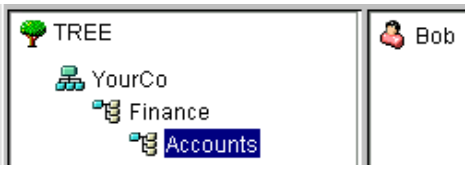
eDirectory interprète la commande de la manière suivante : « changer le contexte en utilisant le conteneur Finance, qui se trouve dans le conteneur YourCo, à partir du sommet de l'arborescence ».

Assignation d'un nom relatif

L'assignation d'un nom relatif implique que les noms sont résolus en fonction du contexte actuel du poste de travail, et non à partir du sommet de l'arborescence. Un nom relatif n'inclut jamais de point initial, puisqu'un tel point indique une résolution à partir du sommet de l'arborescence.

Supposez que le contexte actuel d'un poste de travail soit paramétré sur Finance. Reportez-vous à la Figure 1-10.

Figure 1-10 *Exemple de conteneur eDirectory*



Le nom d'objet relatif de Bob est alors :

```
Bob.Accounts
```

eDirectory interprète le nom de la manière suivante : « Bob, qui se trouve dans Accounts, résolu à partir du contexte actuel qui est Finance ».

Point final

Les points finaux s'emploient uniquement pour les noms relatifs. Par conséquent, vous ne pouvez pas utiliser simultanément un point initial et un point final. Un point final change le conteneur à partir duquel eDirectory résout le nom.

Chaque point final déplace le point de résolution d'un conteneur vers le sommet de l'arborescence. Par exemple, supposons que vous vouliez déplacer le contexte actuel de votre poste de travail de Timmins à Allentown (voir la Figure 1-11).

Figure 1-11 *Exemple de conteneur eDirectory*

La commande CX appropriée utilise l'assignation de nom relatif avec des points finals :

```
CX Allentown.East..
```

eDirectory interprète cette commande de la manière suivante : « changer le contexte en utilisant Allentown, qui se trouve dans East et qui est résolu à partir des deux conteneurs au-dessus du contexte actuel dans l'arborescence ».

De même, si Bob se trouve dans le conteneur Allentown et que le contexte actuel de votre poste de travail est Timmins, le nom relatif de Bob est :

```
Bob.Allentown.East..
```

Contexte et assignation de nom sous Linux

Lorsque des comptes utilisateur Linux sont migrés vers eDirectory, le contexte eDirectory n'est pas utilisé pour nommer les utilisateurs.

Schéma

Le schéma définit les types d'objets (Utilisateur, Imprimante ou Groupe, par exemple) qui peuvent être créés dans l'arborescence, et indique quelles informations sont obligatoires ou facultatives lors de la création d'un objet. Chaque objet dispose d'une classe de schéma définie selon le type d'objet.

Le schéma livré à l'origine avec le produit est appelé schéma de base. Une fois que le schéma de base a été modifié de quelque manière que ce soit (par exemple en lui ajoutant une nouvelle classe ou un nouvel attribut), il est considéré comme un schéma étendu.

Il n'est pas nécessaire, mais néanmoins possible, d'étendre le schéma. Le rôle Schéma d'iManager vous permet d'étendre le schéma pour répondre aux besoins de votre organisation. Par exemple, si votre organisation exige des chaussures spéciales pour les employés et que vous devez assurer le suivi des pointures des employés, vous souhaiterez peut-être créer un nouvel attribut nommé `Shoe Size` et ajouter cet attribut à une classe auxiliaire. Vous pourrez ensuite utiliser cette classe auxiliaire pour étendre les objets Utilisateur en fonction de vos besoins. Pour plus d'informations sur la création de classes auxiliaires, reportez-vous à la « Création d'une classe auxiliaire » page 142.

Pour plus d'informations sur l'utilisation du schéma eDirectory, reportez-vous au Chapitre 5, « Gestion du schéma », page 139.

Gestion du schéma

Le rôle Schéma de NetIQ iManager permet aux utilisateurs disposant de droits Superviseur sur une arborescence de personnaliser le schéma de cette arborescence. Le rôle Schéma et les tâches qui lui sont associées sont accessibles à partir de la page Rôles et tâches d'iManager.

Le rôle Schéma permet :

- Afficher la liste de toutes les classes et de tous les attributs du schéma
- Afficher les informations concernant un attribut, par exemple sa syntaxe et ses indicateurs
- Étendre le schéma par l'ajout d'une classe ou d'un attribut
- Créer une classe en lui attribuant un nom et en définissant des attributs, des drapeaux, des conteneurs auxquels elle peut être ajoutée, ainsi que des classes parentes dont elle peut hériter les attributs
- Créer un attribut en lui attribuant un nom et en spécifiant sa syntaxe et ses indicateurs
- Ajouter un attribut facultatif à une classe existante
- Supprimer une classe ou un attribut non utilisé ou obsolète

Classes, attributs et syntaxes de schéma

- « Classes » page 52
- « Attributs » page 53
- « Syntaxes » page 53

Classes

Une classe correspond au modèle d'un objet Annuaire. Un objet Annuaire est une classe qui est complétée par des données. En d'autres termes :

CLASSE + DONNEES = OBJET ANNUAIRE

Chaque classe possède un nom, une classe d'héritage (sauf si elle se trouve au sommet de la hiérarchie des classes), des indicateurs et un groupe d'attributs. Les classes sont nommées de la même façon que les objets d'annuaire (Utilisateur, Imprimante, File d'attente, Serveur, etc.), bien qu'elles ne soient que des structures vides.

Une classe d'héritage est une classe prise comme point de départ pour définir d'autres classes d'objets. Les classes situées sous la classe d'héritage dans la hiérarchie héritent de tous les attributs de cette classe.

Une hiérarchie de classes indique la manière dont une classe est associée à sa classe parent. Il s'agit d'une méthode qui permet d'associer des classes identiques et d'autoriser l'héritage des attributs. Elle définit également les types de conteneur dans lesquels la classe est valide.

Lorsque vous créez une classe, vous pouvez utiliser la hiérarchie de classes et les attributs supplémentaires disponibles pour la personnaliser. Vous pouvez indiquer une classe d'héritage (ce qui permet à la nouvelle classe d'hériter de tous les attributs et indicateurs de la classe supérieure dans la hiérarchie), puis personnaliser la nouvelle classe en sélectionnant un ou plusieurs attributs à ajouter aux attributs hérités. Vous pouvez définir les attributs supplémentaires comme obligatoires, facultatifs ou servant à la dénomination.

Vous pouvez également modifier des classes en leur ajoutant des attributs facultatifs.

Attributs

Les attributs sont les champs de données de la base de données eDirectory. Par exemple, si vous assimilez une classe à un formulaire, alors un attribut correspond à un champ de ce formulaire. Lorsqu'un attribut est créé, un nom (par exemple *nom de famille* ou *numéro d'employé*) et un type de syntaxe (*chaîne* ou *nombre*) lui sont attribués. L'attribut est alors disponible dans les listes d'attributs du Gestionnaire de schéma.

REMARQUE : en raison d'un problème de réplication, les attributs dans eDirectory autres que le type d'attribut de flux ne peuvent pas contenir des valeurs supérieures à 60 Ko ou 30 000 caractères. Si un utilisateur ou une application définit la valeur d'un attribut binaire ou de chaîne et dépasse cette limite, eDirectory renvoie une erreur -649 indiquant que la valeur est trop longue.

Syntaxes

Vous pouvez choisir entre plusieurs options de syntaxe. Ces options permettent d'indiquer le type des données entrées pour chaque attribut. La syntaxe ne peut être spécifiée que lors de la création d'un attribut. Vous ne pouvez plus la modifier par la suite. Les syntaxes disponibles sont les suivantes :

- Lien en amont

  Permet d'assurer le suivi des autres serveurs qui font référence à un objet. Ce lien est utilisé à des fins de gestion interne dans eDirectory.

- Opérateur booléen

  Syntaxe utilisée par les attributs dont les valeurs sont Vrai (chiffre 1) ou Faux (chiffre 0). Le drapeau à valeur unique est employé pour ce type de syntaxe.

- Chaîne avec distinction de la casse

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes Unicode différenciées selon la casse lors des opérations de comparaison. Deux chaînes avec distinction de la casse concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, y compris pour la casse.

- Liste sans distinction de la casse

  Syntaxe utilisée par les attributs dont les valeurs sont des séquences ordonnées de chaînes Unicode non différenciées selon la casse lors des opérations de comparaison. Deux listes sans distinction de la casse concordent lorsqu'elles comptent toutes deux le même nombre de chaînes et que toutes les chaînes correspondantes concordent (c'est-à-dire qu'elles sont de la même longueur et que leurs caractères respectifs sont identiques).

- Chaîne sans distinction de la casse

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes Unicode non différenciées selon la casse lors des opérations de comparaison. Deux chaînes sans distinction de la casse concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite de la casse.

- Nom de classe

  Syntaxe utilisée par les attributs dont les valeurs sont des noms de classe d'objets. Deux noms de classe concordent lorsqu'ils sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite de la casse.

- Compteur

Syntaxe utilisée par les attributs dont les valeurs sont des nombres entiers numériques avec signe et modifiés par incrémentation. Les attributs de type Compteur sont des attributs à valeur unique. Cette syntaxe se distingue de la syntaxe Nombre entier en ce que les valeurs ajoutées à un attribut fondé sur cette syntaxe sont ajoutées au total de façon arithmétique et que les valeurs supprimées sont soustraites de ce total de façon arithmétique.

- Nom distinctif

  Syntaxe utilisée par les attributs dont les valeurs sont des noms d'objets de l'arborescence eDirectory. Les noms distinctifs (DN) ne sont pas différenciés selon la casse, même si l'un des attributs d'assignation de nom fait la distinction de la casse.

- EMail Address

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes d'informations binaires. eDirectory accepte toute structure pour le contenu des chaînes.

- Facsimile Telephone Number

  Spécifie une chaîne compatible avec la norme E.123 pour le stockage des numéros de téléphone internationaux ainsi qu'une chaîne de bit facultative formatée selon la recommandation T.20. Les valeurs Facsimile Telephone Number correspondent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, si ce n'est que tous les espaces et traits d'union sont ignorés pendant la comparaison.

- En attente

  Syntaxe utilisée par les attributs qui sont des quantités comptables, dont les valeurs sont des nombres entiers avec signe. Cette syntaxe est une quantité comptable (montant retenu provisoirement à même la limite de crédit d'une personne, dans l'attente de l'achèvement d'une transaction). Le montant en attente est traité comme dans le cas de la syntaxe Compteur : les nouvelles valeurs sont ajoutées ou soustraites du total de base. Lorsque le montant en attente évalué atteint la valeur zéro (0), l'enregistrement En attente est supprimé.

- Nombre entier

  Syntaxe utilisée par les attributs représentés en tant que valeurs numériques avec signe. Deux valeurs Nombre entier concordent si elles sont identiques. La comparaison de classement suit les règles relatives aux nombres entiers avec signe.

- Integer 64

  Utilisé par les attributs représentés comme des valeurs de nombre entier de 64 bits. Les attributs Integer 64 prennent en charge la syntaxe d'entier long Microsoft et peuvent être utilisés pour stocker des valeurs d'entier long ou des dates antérieures à 1970 ou postérieures à 2038.

  REMARQUE : eDirectory utilise sa syntaxe existante et des valeurs 32 bits pour les tampons horaires internes.

- Interval

  Syntaxe utilisée par les attributs dont les valeurs sont des nombres entiers numériques avec signe qui représentent des intervalles de temps. La syntaxe Intervalle utilise la même représentation que la syntaxe Nombre entier. La valeur Intervalle représente le nombre de secondes dans l'intervalle de temps.

- Adresse réseau

  Représente une adresse de couche réseau dans l'environnement serveur. L'adresse est au format binaire. Deux valeurs d'adresse réseau concordent lorsque leur type, leur longueur et leur valeur sont identiques.

- Chaîne numérique

Syntaxe utilisée par les attributs dont les valeurs sont des chaînes numériques conformes à la définition CCITT X.208 d'une chaîne numérique. Deux chaînes numériques concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques. Les chiffres (compris entre 0 et 9) et les espaces sont les seuls caractères valides dans le jeu de caractères de chaîne numérique.

- ACL des objets

  Syntaxe utilisée par les attributs dont les valeurs représentent des entrées ACL (Access Control List - liste de contrôle d'accès). Une valeur d'ACL des objets peut protéger un objet ou un attribut.

- Liste d'octets

  Décrit une séquence ordonnée de chaînes d'informations binaires ou de chaînes d'octets. Une liste d'octets concorde avec une liste stockée si elle est un sous-ensemble de cette dernière. Deux listes d'octets sont équivalentes si elles sont de même longueur et si leurs séquences de bits (octet) sont identiques.

- Chaîne d'octets

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes d'informations binaires qui ne sont pas interprétées par eDirectory. Ces chaînes d'octets sont des chaînes non-Unicode. Deux chaînes d'octets concordent lorsqu'elles sont de la même longueur et que leurs séquences de bits (octets) sont identiques.

- Chemin

  Les attributs qui représentent un chemin d'accès à un système de fichiers contiennent toutes les informations nécessaires pour localiser un fichier sur un serveur. Deux chemins d'accès concordent lorsqu'ils sont de la même longueur et que leurs caractères respectifs, y compris la casse, sont identiques.

- Adresse postale

  Syntaxe utilisée par les attributs dont les valeurs sont des chaînes Unicode représentant des adresses postales. L'adresse postale est habituellement constituée d'attributs sélectionnés à partir de la spécification MHS Version 1, « Unformatted Postal O/R Address », conformément à la recommandation F.401. Elle doit compter au maximum 6 lignes de 30 caractères chacune, y compris un nom de pays. Deux adresses postales concordent lorsqu'elles comptent toutes deux le même nombre de chaînes et que toutes les chaînes correspondantes concordent (c'est-à-dire qu'elles sont de la même longueur et que leurs caractères respectifs sont identiques).

- Chaîne imprimable

  Utilisée par les attributs dont les valeurs sont des chaînes imprimables, selon la définition x.208 du CCITT. Le jeu de caractères imprimables comporte les éléments suivants :

  - Les caractères alphabétiques majuscules et minuscules
  - Les chiffres (0 à 9)
  - Les espaces
  - Guillemet simple ouvrant (’)
  - Les parenthèses gauche et droite ()
  - Le signe plus (+)
  - La virgule (,)
  - Le trait d'union (-)
  - Le point (.)
  - Barre oblique (/)
  - Deux-points (:)

- Le signe égal (=)
- Point d'interrogation (?)

Deux chaînes imprimables concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques. Les majuscules et les minuscules sont différenciées.

- Pointeur sur réplique

  Syntaxe utilisée par les attributs dont les valeurs représentent des répliques de partition. Une partition d'une arborescence eDirectory peut être répliquée sur différents serveurs. Cette syntaxe est constituée de six éléments :

  - Nom du serveur
  - Type de réplique (principale, secondaire, lecture seule, référence subordonnée)
  - Numéro de réplique
  - ID de la racine de réplique
  - Numéro de l'adresse
  - Enregistrement d'adresse

- Flux

  Représente des informations binaires arbitraires. La syntaxe Flux permet de créer un attribut eDirectory à partir d'un fichier situé sur un serveur de fichiers. Elle est utilisée par les scripts de connexion et d'autres attributs de flux. Les données stockées dans un fichier de flux ne sont soumises à aucune règle de syntaxe particulière. Il s'agit de données totalement arbitraires, définies par l'application qui les a créées et qui les utilise.

- Numéro de téléphone

  Syntaxe utilisée par les attributs dont les valeurs sont des numéros de téléphone. Deux valeurs de numéro de téléphone concordent lorsqu'elles sont de la même longueur et que leurs caractères respectifs sont identiques, exception faite des espaces et des traits d'union qui sont ignorés au cours des opérations de comparaison.

- Heure

  Syntaxe utilisée par les attributs dont les valeurs sont des nombres entiers sans signe qui représentent une heure exprimée en secondes.

- Tampon horaire

  Syntaxe utilisée par les attributs dont les valeurs indiquent l'heure à laquelle un événement particulier s'est produit. Lorsqu'un événement important survient, un serveur eDirectory crée une valeur Tampon horaire et l'associe à l'événement. Chaque valeur Tampon horaire est unique au sein d'une partition eDirectory. Cela permet d'obtenir la liste ordonnée de tous les événements qui se sont produits sur tous les serveurs contenant les répliques d'une partition.

- Nom avec type

  Syntaxe utilisée par les attributs dont les valeurs représentent un niveau et un intervalle associés à un objet. Cette syntaxe attribue un nom à un objet eDirectory et associe à ce dernier les deux valeurs numériques suivantes :

  - Niveau de l'attribut (à savoir son niveau de priorité)
  - Intervalle indiquant le nombre de secondes écoulées entre certains événements ou la fréquence de référence

- Inconnu

  Syntaxe utilisée par les attributs dont la définition a été supprimée du schéma. Cette syntaxe représente des chaînes d'informations binaires.

Attributs obligatoires et facultatifs - Présentation

La classe de schéma de chaque objet a été définie pour ce type d'objet ; une classe est un groupe d'attributs organisés de manière cohérente. Certains de ces attributs sont obligatoires, d'autres sont simplement facultatifs.

Attributs obligatoires

Un attribut obligatoire doit être fourni au moment de la création d'un objet. Par exemple, si vous décidez de créer un utilisateur à l'aide de la classe Utilisateur, dont le numéro d'employé est un attribut obligatoire, le nouvel objet Utilisateur ne peut être créé que si vous donnez le numéro d'employé.

Attributs facultatifs

Un attribut facultatif peut être complété ou non. Par exemple, si vous décidez de créer un objet Utilisateur à l'aide de la classe Utilisateur, dont l'un des attributs facultatifs est Autres noms, le nouvel objet peut être créé avec ou sans les données fournies pour cet attribut, suivant que le nouvel utilisateur porte ou non d'autres noms.

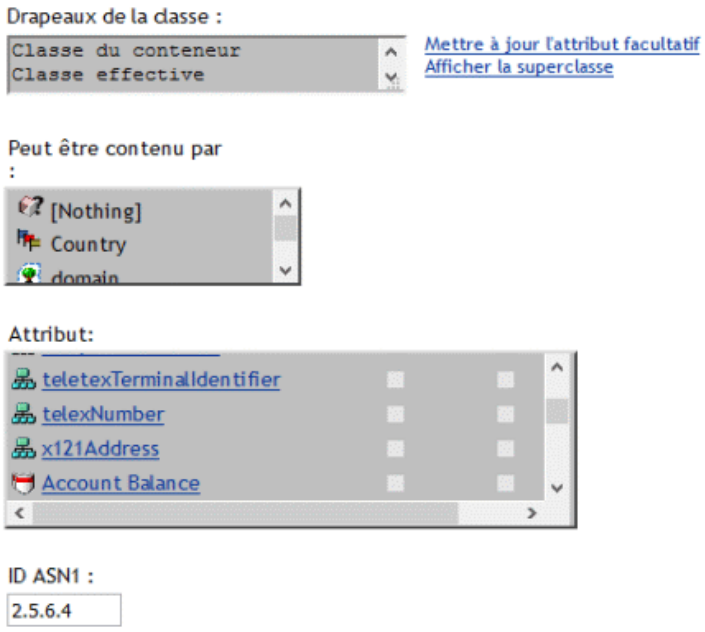
Une exception est faite à cette règle lorsqu'un attribut facultatif est utilisé pour la dénomination ; dans ce cas, l'attribut devient obligatoire.

Exemple de schéma

La Figure 1-12 fournit un exemple de partie de schéma qui peut être similaire à votre schéma de base. Elle affiche des informations sur la classe Organisation. La plupart des renseignements affichés à cet écran ont été spécifiés lorsque la classe a été créée. Certains attributs facultatifs ont toutefois été ajoutés ultérieurement.

Cette icône est assignée à tous les attributs et classes qui sont des extensions du schéma de base.

Figure 1-12 *Page Informations sur la classe d'iManager*



Conception du schéma

Si vous concevez votre schéma dès le départ, vous économisez du temps et des efforts à long terme. Vous pouvez afficher le schéma de base et déterminer s'il répond à vos besoins ou si des modifications sont requises. Si des modifications sont nécessaires, étendez le schéma à l'aide du Gestionnaire de schéma. Reportez-vous à la « Extension du schéma » page 140 et à la « Affichage du schéma » page 144 pour plus d'informations.

Partitions

Une partition est une division logique de la base de données eDirectory. Une partition d'Annuaire forme une unité de données distincte dans l'arborescence qui contient les informations de l'Annuaire.

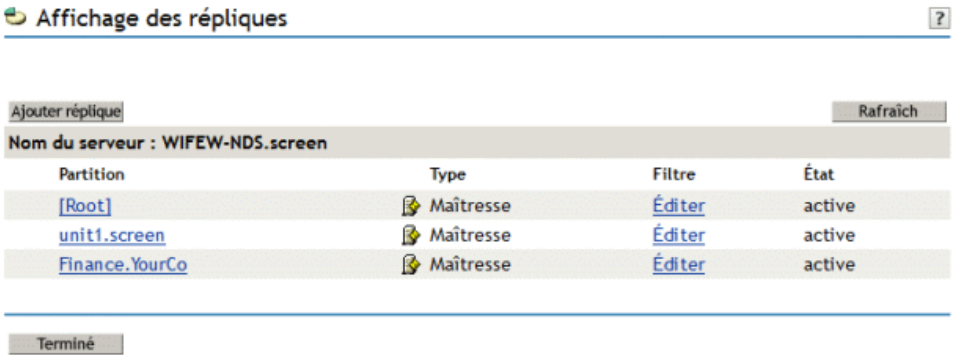
La partition vous permet de déplacer une partie de l'Annuaire d'un serveur sur un autre.

Si les liaisons WAN sont à débit lent ou peu fiables, ou si l'Annuaire comprend un nombre d'objets élevé entraînant une surcharge du serveur et que l'accès soit lent, partitionnez l'Annuaire. Pour obtenir des informations complètes sur les partitions, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

Chaque partition de l'Annuaire se compose d'un ensemble d'objets Conteneur, de tous les objets qu'ils incluent et des données concernant ces objets. Les partitions eDirectory ne comprennent pas d'informations sur le système de fichiers, ni sur les répertoires et fichiers de ce système.

Le partitionnement est effectué à l'aide de NetIQ iManager. Les partitions sont identifiées dans iManager par l'icône de partition suivante ( ).

Figure 1-13 *Affichage des répliques d'un serveur*



Dans l'exemple ci-dessus, l'icône de partition se trouve en regard de l'objet Arborescence. Cela signifie que cet objet est le conteneur le plus élevé dans la partition. Aucune icône de partition n'apparaît en regard des autres conteneurs, la seule partition est donc celle de l'arborescence.

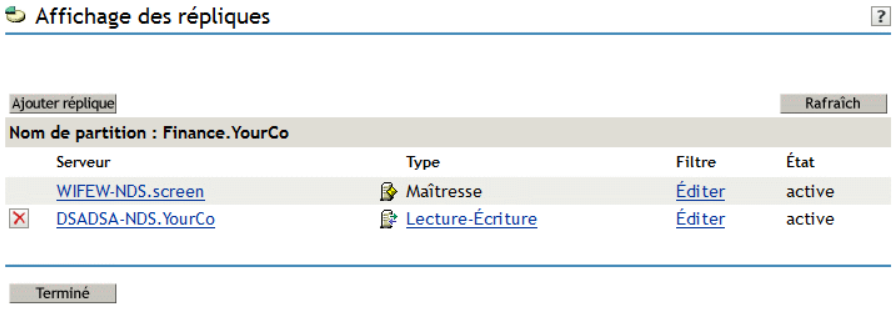
La partition par défaut pour eDirectory consiste en effet à conserver l'annuaire complet dans une seule partition.

Notez que, dans cet exemple, l'affichage des répliques apparaît. Lorsque l'affichage des répliques apparaît pour un serveur dans iManager, toutes les répliques de ce serveur sont affichées dans la partie droite de l'écran. Dans ce cas, Server1 contient une réplique de la partition unique. Pour plus d'informations, reportez-vous à la « Répliques » page 61 et à la rubrique « Affichage des répliques sur un serveur eDirectory » page 160.

Partitions

Les partitions se voient attribuer un nom d'après leur conteneur le plus élevé. Dans la Figure 1-14 deux partitions sont présentes : Arborescence et Finances. La partition Finances est appelée partition enfant de la partition Arborescence, car elle est extraite de cette dernière. La partition Arborescence est appelée partition parent de Finances.

Figure 1-14 *Affichage des répliques d'une partition*



Vous pouvez envisager de créer cette partition si l'Annuaire compte tant d'objets que le serveur est surchargé et si l'accès à eDirectory est lent. En créant cette partition, vous pouvez diviser la base de données et transmettre les objets de cette branche à un autre serveur.

L'exemple ci-dessus représente l'affichage des répliques de la partition Finances. Lorsque l'affichage des répliques apparaît pour une partition dans iManager, tous les serveurs comportant une réplique de cette partition sont affichés dans la partie droite de l'écran. Dans le cas présent, Server1 contient une réplique Lecture/écriture de la partition Finance. Pour plus d'informations, reportez-vous à la section « Affichage des répliques d'une partition » page 162.

Distribution de répliques en vue de l'amélioration des performances

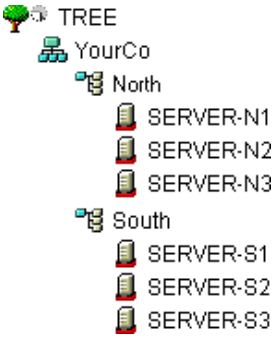
Dans l'exemple précédent, supposez que Server1 contienne des répliques des partitions Tree et Finance. À ce stade, les performances d'eDirectory ne sont pas supérieures puisque Server1 contient toujours l'Annuaire complet (les répliques des deux partitions).

Pour améliorer les performances, vous devez déplacer l'une des répliques sur un autre serveur. Par exemple, si vous déplacez la partition Tree vers Server2, ce dernier contient tous les objets issus des conteneurs Tree et YourCo. Server1 ne contient alors plus que les objets des conteneurs Finances et Comptes. La charge de Server1 et de Server2 est inférieure à ce qu'elle serait sans partition.

Partitions et liaisons WAN

Supposez que votre réseau couvre deux sites, North et South, connectés entre eux par une liaison WAN. Chacun des sites comporte trois serveurs.

Figure 1-15 *Exemple de conteneurs eDirectory*



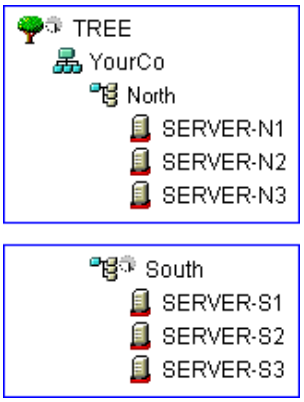
Dans ce cas, le fonctionnement d'eDirectory est plus rapide et plus fiable si l'annuaire est divisé en deux partitions.

Avec une seule partition, les répliques sont soit conservées sur un site, soit partagées entre les deux sites. Cette méthode s'avère lourde pour deux raisons :

- Si toutes les répliques sont stockées sur les serveurs du site Nord, par exemple, les utilisateurs du site South subiront des contretemps lorsqu'ils tenteront de se connecter ou d'accéder aux ressources. En cas d'interruption de la liaison, ces utilisateurs ne pourront plus du tout se connecter ni accéder aux ressources.
- Si les répliques sont réparties entre les sites, les utilisateurs pourront accéder à l'Annuaire localement.. Toutefois, la synchronisation des répliques entre les serveurs s'effectue via la liaison WAN ; il peut donc se produire des erreurs eDirectory si cette liaison n'est pas fiable. Les modifications apportées à l'Annuaire sont répercutées lentement via la liaison WAN.

La solution à deux partitions présentée à la Figure 1-16 permet de résoudre ces problèmes de performances et de fiabilité sur la liaison WAN.

Figure 1-16 *Exemple de partitions*



Les répliques de la partition Tree sont conservées sur les serveurs du site North. Les répliques de la partition South sont conservées sur le serveur du site Sout, comme l'illustre la Figure 1-17.

Figure 1-17 *Exemple de partitions, serveurs et répliques*

Partition	Server	Replica Type
TREE	SERVER-N1	Master
	SERVER-N2	Read/write
	SERVER-N3	Read/write
South	SERVER-S1	Master
	SERVER-S2	Read/write
	SERVER-S3	Read/write

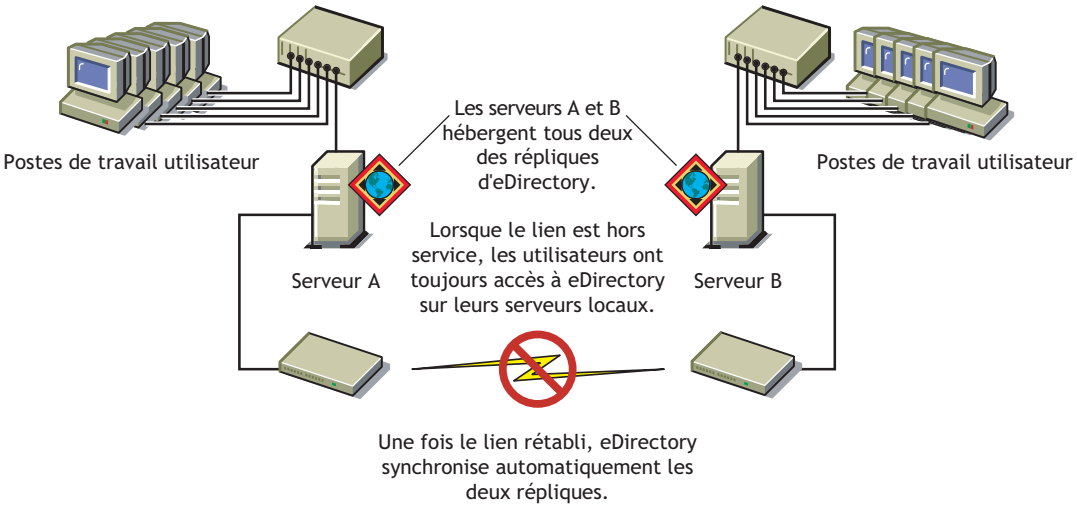
Pour chacun des sites, les objets qui représentent les ressources locales sont stockés localement. Le trafic de synchronisation entre les serveurs se produit également au niveau local via le réseau LAN, plutôt que via la liaison WAN, à débit lent et peu fiable.

Cependant, lorsqu'un utilisateur ou un administrateur accède aux objets d'un autre site, le trafic eDirectory est généré sur la liaison WAN.

Répliques

Une réplique est une copie (ou instance) d'une partition définie par l'utilisateur, qui est placée sur un serveur eDirectory. Si votre réseau comporte plusieurs serveurs eDirectory, vous pouvez avoir plusieurs répliques (copies) de l'annuaire. Ainsi, en cas de panne d'un serveur ou de défaillance d'une connexion réseau à celui-ci, les utilisateurs pourront toujours se connecter et accéder aux autres ressources du réseau. (voir Figure 1-18).

Figure 1-18 *Répliques eDirectory*



Chaque serveur peut héberger plus de 65 000 répliques eDirectory. Toutefois, un serveur ne peut contenir qu'une seule réplique d'une même partition définie par l'utilisateur. Pour obtenir des informations complètes sur les répliques, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

Il est recommandé de posséder trois répliques pour garantir la tolérance aux pannes dans eDirectory (en supposant que vous disposiez de trois serveurs eDirectory sur lesquels les stocker). Un même serveur peut contenir les répliques de plusieurs partitions.

Un serveur de répliques est un serveur employé uniquement pour stocker des répliques eDirectory. Ce type de serveur est parfois appelé serveur DSMASTER. Cette configuration est appréciée de certaines entreprises qui possèdent de nombreux bureaux distants dotés d'un seul serveur. Le serveur de réplique permet de stocker des répliques supplémentaires pour la partition d'un site distant.

Il peut aussi faire partie d'un plan de reprise après sinistre, comme expliqué à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre » page 456.

La fonction de réplication eDirectory ne garantit pas la tolérance aux pannes au niveau du système de fichiers du serveur, car seules les informations relatives aux objets eDirectory sont répliquées. Vous pouvez toutefois assurer cette tolérance grâce au système de suivi des transactions TTS™ (Transaction Tracking System™), à la mise en miroir ou à la duplication de disques, à des systèmes RAID ou aux services NRS (NetIQ Replication Services).

Une réplique maîtresse ou une réplique en lecture/écriture est requise sur les serveurs qui fournissent des services de Bindery.

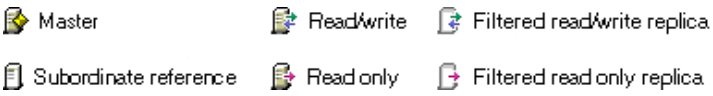
Si les utilisateurs accèdent régulièrement aux informations eDirectory au moyen d'une liaison WAN, vous pouvez réduire le temps d'accès et le trafic WAN en plaçant une réplique contenant les informations nécessaires sur un serveur auquel ils peuvent accéder localement.

Il en est de même à un degré moindre pour un lien LAN. Lorsque vous distribuez des répliques aux serveurs du réseau, les informations sont généralement récupérées sur le serveur disponible le plus proche.

Types de réplique

eDirectory prend en charge les types de répliques représentés sur la figure suivante :

Figure 1-19 *Types de réplique*



- « Réplique maîtresse » page 63
- « Réplique en lecture/écriture » page 64
- « Réplique en lecture seule » page 64
- « Réplique en lecture/écriture filtrée » page 64
- « Réplique en lecture seule filtrée » page 65
- « Réplique de référence subordonnée » page 65

Réplique maîtresse


Une réplique maîtresse est une réplique inscriptible utilisée pour apporter initialement des modifications à un objet ou une partition. Ce type de réplique permet d'effectuer les opérations suivantes sur les partitions eDirectory :

- ajouter des répliques sur des serveurs ;
- supprimer des répliques sur des serveurs ;
- créer des partitions dans l'arborescence eDirectory ;
- supprimer des partitions dans l'arborescence eDirectory ;
- déplacer une partition dans l'arborescence eDirectory.

La réplique maîtresse permet également d'effectuer les opérations suivantes sur les objets eDirectory :

- ajouter de nouveaux objets à l'arborescence eDirectory ;
- supprimer, renommer ou déplacer des objets dans l'arborescence eDirectory ;
- authentifier des objets pour l'arborescence eDirectory ;
- ajouter de nouveaux attributs d'objet à l'arborescence eDirectory ;
- modifier ou supprimer des attributs.

Par défaut, le premier serveur eDirectory du réseau est celui qui héberge la réplique maîtresse. Chacune des partitions ne possède qu'une seule réplique maîtresse. Si vous créez d'autres répliques, il s'agit par défaut de répliques en lecture/écriture.

Si vous pensez arrêter plusieurs jours le serveur qui contient la réplique maîtresse, vous pouvez convertir en réplique maîtresse l'une des répliques en lecture/écriture. La réplique maîtresse initiale est automatiquement convertie en lecture/écriture.

Une réplique maîtresse doit être disponible sur le réseau pour qu'eDirectory puisse effectuer des opérations, comme créer une réplique ou une partition.

Réplique en lecture/écriture

eDirectory peut consulter les informations sur les objets et les modifier tant dans une réplique Lecture-écriture que dans la réplique maîtresse. Toutes les modifications sont alors automatiquement répercutées dans toutes les répliques.

Si eDirectory répond lentement aux utilisateurs en raison de retards dans l'infrastructure du réseau (liaisons WAN à débit faible ou routeurs occupés, par exemple), vous pouvez créer une réplique Lecture-écriture plus proche des utilisateurs qui en ont besoin. Vous pouvez disposer d'autant de répliques Lecture/écriture que vous avez de serveurs pour les stocker. Notez cependant qu'une augmentation du nombre de répliques entraîne un accroissement du trafic pour assurer leur synchronisation.

Réplique en lecture seule

Une réplique en lecture seule est une réplique lisible utilisée pour obtenir des informations sur tous les objets qui se trouvent dans les limites d'une partition. Les répliques en lecture seule reçoivent des mises à jour de synchronisation des répliques maîtresse et en lecture/écriture ; aucune modification n'est reçue directement des clients. Si la mise à jour de la connexion est activée, la connexion à la réplique en lecture seule échoue, car elle implique des mises à jour d'attributs.

Ce type de réplique ne permet pas d'émuler la Bindery, mais garantit la tolérance aux pannes dans eDirectory. Si la réplique maîtresse et toutes les répliques en lecture/écriture viennent à être détruites ou endommagées, la réplique en lecture seule peut devenir la nouvelle réplique maîtresse.

Ce type de réplique autorise en outre la lecture des objets NDS, la tolérance aux pannes (la réplique contient tous les objets compris dans les limites de la partition) et les connexions à l'arborescence NDS (la réplique contient l'objet Racine de partition).

Une réplique Lecture seule ne doit cependant jamais servir à l'établissement d'une règle de sécurité au sein d'une arborescence pour limiter les opérations de modification des objets, étant donné que le client peut toujours accéder à une réplique Lecture/écriture pour apporter des modifications. L'annuaire comporte d'autres outils pour la sécurité, notamment le filtre de droits hérités. Pour plus d'informations, reportez-vous à la section « Filtre des droits hérités (IRF - Inherited Rights Filter) » page 74.

Réplique en lecture/écriture filtrée

Les répliques Lecture-écriture filtrées contiennent un ensemble filtré d'objets ou de classes d'objets accompagné d'un ensemble filtré des attributs et des valeurs correspondant à ces objets. Le contenu est limité aux types d'objets eDirectory et aux propriétés spécifiques du filtre de réplication du serveur hôte. Les utilisateurs peuvent lire et modifier le contenu de la réplique ; eDirectory peut accéder aux informations d'objet sélectionnées et les modifier. Les modifications sélectionnées sont alors automatiquement répercutées sur toutes les répliques.

Avec les répliques filtrées, vous ne pouvez disposer que d'un seul filtre par serveur. Cela signifie que tout filtre défini pour un serveur s'applique à toutes les répliques filtrées présentes sur ce serveur. Vous pouvez toutefois disposer d'autant de répliques filtrées que vous possédez de serveurs, mais un nombre élevé de répliques entraîne une augmentation du trafic afin d'assurer leur synchronisation.

Pour plus d'informations, reportez-vous à la section « Répliques filtrées » page 65.

Réplique en lecture seule filtrée

Les répliques en lecture seule filtrées contiennent un ensemble filtré d'objets ou de classes d'objets, accompagné d'un ensemble filtré des attributs et des valeurs correspondant à ces objets. Ces répliques reçoivent des mises à jour de synchronisation des répliques maîtresse et en lecture/écriture ; aucune modification n'est reçue directement des clients. Les utilisateurs peuvent afficher le contenu de ces répliques, mais ils ne peuvent pas le modifier. Le contenu est limité aux types d'objets eDirectory et aux propriétés spécifiques du filtre de réplication du serveur hôte.

Pour plus d'informations, reportez-vous à la section « Répliques filtrées » page 65.

Réplique de référence subordonnée

Les répliques de référence subordonnée sont créées par le système. Elles ne contiennent pas toutes les données d'objet d'une réplique maîtresse ou d'une réplique en lecture/écriture. Elles ne contribuent donc pas à la tolérance aux pannes. Il s'agit de pointeurs internes générés pour contenir assez d'informations afin que eDirectory puisse résoudre les noms d'objet entre les partitions.

Vous ne pouvez pas supprimer une réplique de référence subordonnée. eDirectory la supprime automatiquement lorsqu'elle est inutile. Les répliques de référence subordonnée sont créées uniquement sur les serveurs qui possèdent une réplique d'une partition parente, mais aucune réplique des partitions enfants de cette dernière.

Si une réplique de la partition enfant est copiée sur un serveur contenant la réplique de la partition parent, la réplique de référence subordonnée est automatiquement supprimée.

Répliques filtrées

Les répliques filtrées contiennent un ensemble filtré d'objets ou de classes d'objets, accompagné d'un ensemble filtré des attributs et des valeurs correspondant à ces objets. Par exemple, vous pouvez avoir besoin de créer sur un même serveur un ensemble de répliques filtrées qui contienne uniquement des objets Utilisateur provenant de diverses partitions de l'arborescence eDirectory. En outre, vous pouvez choisir de n'inclure qu'un sous-ensemble des données des objets Utilisateur (par exemple Prénom, Nom et Numéro de téléphone).

Une réplique filtrée peut générer une vue des données eDirectory sur un seul serveur. À cette fin, les répliques filtrées vous permettent de créer une étendue et un filtre. Le serveur eDirectory peut alors héberger un ensemble de données bien défini provenant de nombreuses partitions de l'arborescence.

Les descriptions de l'étendue du serveur et des filtres de données sont enregistrées dans eDirectory et peuvent être gérées dans iManager, via l'objet Serveur.

Un serveur qui héberge une ou plusieurs répliques filtrées est doté d'un seul filtre de réplication. Par conséquent, toutes les répliques filtrées sur ce serveur contiennent le même sous-ensemble d'informations provenant de leurs partitions respectives. La réplique de partition maîtresse d'une réplique filtrée doit être hébergée sur un serveur eDirectory exécutant eDirectory 8.5 ou une version ultérieure.

Les répliques filtrées présentent les avantages suivants :

- Réduction du trafic de synchronisation vers le serveur en réduisant le volume de données à répliquer à partir d'autres serveurs.
- Réduction du nombre d'événements que NetIQ Identity Manager doit filtrer.

Pour plus d'informations sur NetIQ Identity Manager, reportez-vous au *Guide d'Administration de NetIQ Identity Manager*.

- Réduction de la taille de la base de données de l'Annuaire.

  Chaque réplique augmente la taille de la base de données. La création d'une réplique filtrée (au lieu d'une réplique complète), contenant uniquement des classes précises, permet de réduire la taille de la base de données locale.

  Par exemple, si l'arborescence contient 10 000 objets, mais que seul un pourcentage réduit de ceux-ci correspond à des objets Utilisateur, vous pouvez créer une réplique filtrée contenant uniquement des objets Utilisateur, au lieu d'une réplique complète contenant 10 000 objets.

Tout en permettant de filtrer les données stockées dans une base de données locale, la réplique filtrée est semblable à une réplique eDirectory normale. Vous pouvez à tout instant la convertir en une réplique complète.

REMARQUE : par défaut, les répliques filtrées ont pour filtres obligatoires Organisation et Unité organisationnelle.

Pour plus d'informations sur la configuration et la gestion des répliques filtrées, reportez-vous à la « Configuration et gestion des répliques filtrées » page 158.

Autorisation des connexions locales à des répliques filtrées

En plus de sélectionner l'option **Activer la connexion locale** dans iManager, pour autoriser les connexions locales à une réplique filtrée, vous devez aussi ajouter la classe ndsLoginProperties au filtre.

Avant de vous connecter à la réplique filtrée, vous devez définir les attributs suivants :

- Détection d'intrus
- Intervalle de réinitialisation après des tentatives d'intrusion
- Heure de la dernière connexion
- Verrouillé par l'intrus
- Verrouillage après détection
- Durée de connexion autorisée Assigner
- Connexion désactivée
- Heure d'expiration de la connexion
- Nombre de connexions gracieuses
- Connexions gracieuses restantes
- Adresse de l'auteur des tentatives d'intrusion
- Tentatives d'intrusion
- Nombre maximum de tentatives d'intrusion
- Heure de réinitialisation des tentatives d'intrusion
- Nombre maximum de connexions simultanées
- Heure de connexion
- Adresse réseau
- Adresse réseau Limitation
- Intervalle d'expiration du mot de passe

- Heure d'expiration du mot de passe
- Clé privée
- Clé publique
- nspmDoNotExpirePassword
- nspmPasswordKey
- nspmPasswordPolicyDN
- pwdAccountLockedTime
- pwdFailureTime
- sasLoginFailureDelay
- sasOTPCounter
- sasOTPDigits
- sasOTPEnabled
- sasOTPReSync
- sasUpdateLoginInfo
- sasUpdateLoginTimeInterval

REMARQUE : les attributs ci-dessus peuvent être définis sur l'objet Utilisateur, le conteneur parent ou la stratégie de connexion.

Synchronisation des serveurs dans un anneau de répliques

Lorsque plusieurs serveurs contiennent des répliques de la même partition, ces serveurs sont considérés comme un anneau de répliques. La synchronisation est le transfert d'informations sur l'annuaire d'une réplique vers une autre, pour garantir la cohérence des deux partitions. eDirectory garde automatiquement ces serveurs synchronisés. Pour plus d'informations, reportez-vous à la « Synchronisation » page 121.

Les types de synchronisation eDirectory sont les suivants :

- Synchronisation normale ou synchronisation des répliques
- Synchronisation de priorité

Accès aux ressources

eDirectory offre un niveau de sécurité élémentaire pour l'accès au réseau, au moyen de droits définis par défaut. Vous pouvez renforcer le contrôle de l'accès en exécutant les tâches ci-dessous.

- Assignation de droits

  Chaque fois qu'un utilisateur tente d'accéder à une ressource réseau, le système évalue ses droits effectifs sur cette ressource. Pour vous assurer que les utilisateurs disposent des droits effectifs appropriés sur des ressources, vous pouvez effectuer des assignations d'ayant droit explicites, accorder des équivalences de sécurité et filtrer les droits hérités.

  Pour simplifier l'assignation de droits, vous pouvez créer des objets Groupe et Rôle organisationnel, puis assigner des utilisateurs à ces objets.

- Ajout de la sécurité au niveau de la connexion

  Aucune sécurité n'est fournie par défaut au niveau de la connexion. Il existe plusieurs mesures de sécurité facultatives avec lesquelles vous pouvez configurer vos paramètres de connexion. Vous pouvez par exemple définir des mots de passe de connexion, restreindre les emplacements et les périodes à partir desquels les utilisateurs peuvent se connecter, limiter le nombre de sessions de connexion concurrentes, activer la détection d'intrusion, et désactiver la connexion.

- Configuration de l'administration fondée sur les rôles

  Vous pouvez configurer des administrateurs pour des propriétés d'objet spécifiques et leur octroyer des droits uniquement sur ces propriétés. Vous pouvez ainsi créer des administrateurs ayant des responsabilités spécifiques dont les subordonnés d'un objet Conteneur donné peuvent hériter. Un administrateur défini sur la base d'un rôle peut avoir des responsabilités sur tout type de propriétés spécifiques, comme celles qui ont trait aux informations concernant les employés ou aux mots de passe.

  Pour obtenir des instructions sur la configuration des services basés sur le rôle, reportez-vous à la section Installation de la fonctionnalité RBS dans le *Guide d'administration de NetIQ iManager* (https://www.netiq.com/documentation/imanager-3/imanager_admin/).

  Vous pouvez également définir des rôles sous forme de tâches spécifiques que les administrateurs peuvent effectuer dans des applications d'administration basée sur les rôles. Pour plus d'informations, reportez-vous à la section Configuration des services basés sur le rôle.

Droits eDirectory

Lorsque vous créez une arborescence, les assignations de droits par défaut généralisent l'accès et la sécurité sur votre réseau. Vous trouverez ci-dessous certaines des assignations par défaut :

- L'utilisateur Admin dispose du droit Superviseur sur le sommet de l'arborescence, ce qui lui procure un contrôle total sur l'intégralité de l'Annuaire. L'administrateur bénéficie également du droit Superviseur sur l'objet Serveur, ce qui lui permet de contrôler tous les volumes de ce serveur.
- L'utilisateur [Public] dispose du droit Parcourir sur le sommet de l'arborescence. Tous les utilisateurs sont donc autorisés à afficher les objets situés dans cette arborescence.
- Les objets créés via un processus de mise à niveau, tel qu'une mise à niveau d'impression ou une migration d'utilisateur Windows, reçoivent des assignations d'ayant droit appropriées pour la plupart des situations.

Assignations d'ayant droit et objets cible

L'assignation de droits implique un ayant droit et un objet cible. L'ayant droit représente l'utilisateur ou le groupe d'utilisateurs qui reçoit l'autorité. La cible représente les ressources réseau dont les utilisateurs ont le contrôle.

- Si vous choisissez un alias comme ayant droit, les droits sont appliqués uniquement à l'objet que l'alias représente. L'objet Alias peut toutefois être une cible explicite.
- Un fichier ou un répertoire du système de fichiers peut également constituer une cible, même si les droits sur ce système de fichiers sont enregistrés dans le système lui-même et non dans eDirectory.

REMARQUE : L'ayant droit [Public] n'est pas un objet. Il s'agit d'un ayant droit spécial qui, pour des raisons d'assignation de droits, représente un utilisateur réseau quelconque qui est ou non connecté.

[Ceci] est un type spécial d'ayant droit, défini pour être un objet authentifié, lorsque son nom correspond à l'entrée consultée. Cela permet à l'administrateur de spécifier facilement des droits (comme celui permettant à chaque utilisateur de gérer son propre numéro de téléphone), avec une ACL unique en haut de l'arborescence et [Ceci] comme ayant droit.

Concepts relatifs aux droits eDirectory

Les concepts ci-dessous servent à expliquer les droits eDirectory.

- « Droits d'objet (droits d'entrée) » page 69
- « Droits de propriété » page 70
- « Droits effectifs » page 70
- « Détermination des droits effectifs » page 70
- « Équivalence de sécurité » page 73
- « Liste de contrôle d'accès (ACL - Access Control List) » page 74
- « Filtre des droits hérités (IRF - Inherited Rights Filter) » page 74

Droits d'objet (droits d'entrée)

Lorsque vous procédez à une assignation d'ayant droit, vous pouvez accorder des droits d'objet et de propriété. Les droits d'objet concernent la manipulation de l'ensemble de l'objet, alors que les droits de propriété s'appliquent uniquement à certaines propriétés de l'objet. Un droit d'objet équivaut à un droit d'entrée car il fournit une entrée dans la base de données eDirectory.

Chaque droit d'objet est décrit ci-dessous:

- **Superviseur** inclut tous les droits sur l'objet et toutes ses propriétés.
- **Parcourir** permet à l'ayant droit d'afficher l'objet dans l'arborescence. Il ne donne pas le droit d'afficher les propriétés de l'objet.
- **Créer** ne s'applique que lorsque l'objet cible est un conteneur. Le droit Créer permet à l'ayant droit de créer des objets subordonnés au conteneur ; il comprend également le droit Parcourir.
- **Supprimer** permet à l'ayant droit de supprimer la cible de l'annuaire.
- **Renommer** permet à l'ayant droit de changer le nom de la cible.

Droits de propriété

Lorsque vous procédez à une assignation d'ayant droit, vous pouvez accorder des droits d'objet et de propriété. Les droits d'objet concernent la manipulation de l'ensemble de l'objet, alors que les droits de propriété s'appliquent uniquement à certaines propriétés de l'objet.

iManager propose deux options de gestion des droits de propriété :

- Vous pouvez gérer simultanément toutes les propriétés lorsque l'élément **[Tous les droits d'attribut]** est sélectionné.
- Vous pouvez gérer individuellement une ou plusieurs propriétés lorsque la propriété correspondante est sélectionnée.

IMPORTANT : si vous accordez à un ayant droit un accès en lecture à la propriété [Tous les droits d'attribut] d'un utilisateur, l'ayant droit bénéficie d'un accès en lecture à l'attribut `Gestion des mots de passe` de cet utilisateur. L'ayant droit peut alors lire les mots de passe de l'utilisateur.

Pour plus d'informations sur la création et la gestion des stratégies de mot de passe, reportez-vous à la « Création de règles de mot de passe » page 798.

Chaque droit de propriété est décrit ci-dessous :

- **Superviseur** permet à l'ayant droit de contrôler entièrement la propriété.
- **Comparer** permet à l'ayant droit de comparer la valeur d'une propriété à une valeur donnée. Ce droit permet d'effectuer une recherche et ne renvoie qu'un résultat vrai ou faux. Il ne permet pas à l'ayant droit d'afficher réellement la valeur de la propriété.
- **Lire** permet à l'ayant droit d'afficher les valeurs d'une propriété. Il comprend le droit Comparer.
- **Écrire** permet à l'ayant droit de créer, de modifier et de supprimer les valeurs d'une propriété.
- **S'ajouter** permet à l'ayant droit d'ajouter ou de retirer son nom en tant que valeur de propriété. Il ne s'applique qu'aux propriétés dont les valeurs sont des noms d'objet, telles que les listes d'adhésions ou les listes ACL (Access Control Lists - Listes de contrôle d'accès).

Droits effectifs

Les utilisateurs reçoivent des droits de plusieurs manières : par le biais d'assignations d'ayant droit explicites, d'un héritage ou d'une équivalence de sécurité. Vous pouvez également limiter les droits par l'intermédiaire de filtres des droits hérités, et les modifier ou les révoquer à l'aide d'assignations d'ayant droit inférieures. Le résultat de toutes ces actions, c'est-à-dire les droits que peut employer un utilisateur, est appelé *droits effectifs*.

Les droits effectifs d'un utilisateur sur un objet sont évalués chaque fois que l'utilisateur tente d'effectuer une action.

Détermination des droits effectifs

Chaque fois qu'un utilisateur tente d'accéder à une ressource réseau, eDirectory détermine les droits effectifs dont il dispose sur la ressource cible en procédant de la manière suivante :

1. eDirectory liste les ayants droit dont les droits doivent être pris en compte dans le processus, à savoir : Ces ayants droit incluent :
   - l'utilisateur qui tente d'accéder à la ressource cible ;.
   - les objets sur lesquels l'utilisateur dispose d'une équivalence de sécurité.
2. eDirectory détermine les droits effectifs de chaque ayant droit de la liste de la manière suivante :

   2a eDirectory commence par les droits héritables que l'ayant droit possède au sommet de l'arborescence.

   eDirectory recherche, dans la propriété Ayants droit de l'objet (ACL) de l'objet Arborescence, les entrées où figure l'ayant droit. Si des droits héritables existent dans ces entrées, eDirectory les utilise comme groupe de droits effectifs initial pour l'ayant droit.

   2b eDirectory descend d'un niveau dans la branche de l'arborescence qui contient la ressource cible.

   2c eDirectory supprime tous les droits filtrés à ce niveau.

   eDirectory recherche, dans la liste ACL de ce niveau, les IRF (Inherited Rights Filters – filtres des droits hérités) qui correspondent aux types (objet, toutes propriétés ou propriété spécifique) des droits effectifs de l'ayant droit. Si de tels filtres existent, eDirectory retire des droits effectifs de l'ayant droit les droits bloqués par ces IRF.

Par exemple, si les droits effectifs de l'ayant droit incluent jusqu'à présent une assignation de droit Écrire sur toutes les propriétés, mais qu'un IRF à ce niveau annule ce droit, le système retire celui-ci des droits effectifs de l'ayant droit.

2d eDirectory ajoute les droits héritables assignés à ce niveau, en remplaçant, le cas échéant, les assignations existantes.

eDirectory recherche, dans la liste ACL de ce niveau, les entrées où figure l'ayant droit. S'il en existe et que leurs droits sont héritables, eDirectory copie ceux-ci dans les droits effectifs de l'ayant droit, en remplaçant les assignations existantes, le cas échéant.

Supposez, par exemple, que les droits effectifs de l'ayant droit incluent jusqu'ici les droits d'objet Créer et Supprimer, mais aucun droit de propriété, et que l'ACL à ce niveau contienne à la fois une assignation n'englobant aucun droit d'objet et une assignation de droit Écrire sur toutes les propriétés pour cet ayant droit. Dans ce cas, le système annule les droits d'objet existants de l'ayant droit (Créer et Supprimer) et ajoute les nouveaux droits de propriété.

2e eDirectory répète les opérations de filtrage et d'ajout (étapes Étape 2c et Étape 2d ci-dessus) à chaque niveau de l'arborescence, y compris au niveau de la ressource cible.

2f eDirectory ajoute les droits non héritables assignés au niveau de la ressource cible, en remplaçant les assignations existantes, le cas échéant.

eDirectory utilise le même processus qu'à l'Étape 2d ci-dessus. Le groupe de droits qui en résulte constitue les droits effectifs de l'ayant droit.

3 eDirectory associe les droits effectifs de tous les ayants droit de la liste comme suit :

3a eDirectory inclut tous les droits détenus par les ayants droit de la liste et exclut uniquement les droits qui ne sont assignés à aucun d'eux. Il ne mélange pas les différents types de droit. Par exemple, ils n'ajoutent pas les droits d'une propriété spécifique à ceux de toutes les propriétés, ou vice-versa.

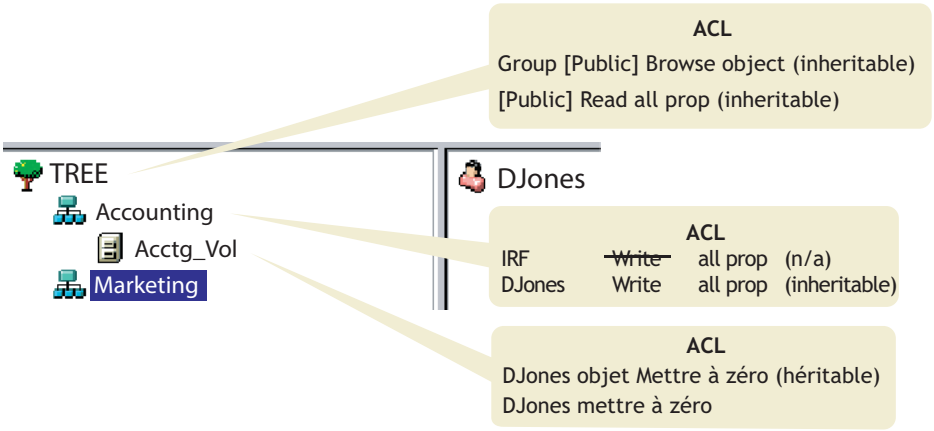
3b eDirectory ajoute les droits qui dépendent des droits effectifs actuels.

L'ensemble de droits qui en résulte constitue les droits effectifs de l'utilisateur sur la ressource cible.

Exemple

L'utilisateur DJones tente d'accéder au volume Vol_Compta. Reportez-vous à la Figure 1-20.

Figure 1-20 *Exemple de droits d'ayant droit*



Le processus suivant montre la façon dont eDirectory détermine les droits effectifs de l'utilisateur DJones sur le volume Vol_Compta :

1. Les ayants droit dont les droits doivent être pris en compte dans le calcul sont DJones, Marketing, Tree et [Public].

   Cela suppose que DJones ne fait partie d'aucun groupe ni rôle, et que des équivalences de sécurité ne lui ont pas été explicitement assignées.
2. Vous trouverez ci-dessous les droits effectifs de chacun des ayants droit :
   - DJones : objet Mettre à zéro, toutes les propriétés Mettre à zéro

     L'assignation des droits « zéro ttes propriétés » sur le volume Vol_Compta est prioritaire par rapport à l'assignation du droit Écrire sur toutes les propriétés au niveau de Comptabilité.
   - Marketing : toutes les propriétés Mettre à zéro

     L'assignation du droit Écrire sur toutes les propriétés à la racine de l'arborescence est rejetée par les IRF au niveau de Facturation.
   - Tree : aucun droit

     Aucun droit n'est assigné à l'objet Arborescence dans la branche appropriée de l'arborescence.
   - [Public] : objet Parcourir, toutes les propriétés Lire

     Ces droits sont assignés à la racine et ne sont pas filtrés ou annulés dans la branche appropriée de l'arborescence.
3. En combinant les droits de tous ces ayants droit, nous obtenons :

   DJones : objet Parcourir, toutes les propriétés Lire
4. Après ajout du droit de comparaison de toutes les propriétés, qui découle du droit Lire toutes les propriétés, nous obtenons pour DJones l'ensemble de droits effectifs suivant sur Vol_Compta :

   DJones : objet Parcourir, toutes les propriétés Lire et Comparer

Annulation de droits effectifs

Étant donné le mode de calcul des droits effectifs, vous pouvez éprouver des difficultés à éviter que les droits particuliers d'un utilisateur deviennent effectifs sans avoir recours à un IRF (en effet, un IRF bloque les droits de tous les utilisateurs).

Pour éviter que les droits particuliers d'un utilisateur deviennent effectifs sans avoir recours à un IRF, procédez de l'une des manières suivantes :

- Assurez-vous que ni l'utilisateur ni aucun des objets pour lesquels l'utilisateur dispose d'une équivalence de sécurité n'obtiennent ces droits, que ce soit au niveau de la ressource cible ou à un niveau supérieur dans l'arborescence.
- Si l'utilisateur ou tout objet pour lequel il bénéficie d'une équivalence de sécurité se voit malgré tout attribuer ces droits, veillez à ce que l'objet dispose également d'une assignation omettant ces droits à un niveau inférieur dans l'arborescence. Répétez l'opération pour chaque ayant droit (associé à l'utilisateur) disposant des droits non souhaités.

Équivalence de sécurité

L'équivalence de sécurité signifie qu'un objet dispose des mêmes droits qu'un autre objet. Lorsque vous attribuez à un objet une sécurité équivalente à celle d'un autre objet, les droits de ce deuxième objet sont ajoutés à ceux du premier lorsque le système calcule les droits effectifs de ce dernier.

Supposons, par exemple, que vous attribuiez à l'objet Utilisateur Joseph une équivalence de sécurité par rapport à l'objet Admin. Une fois l'équivalence de sécurité créée, Joseph dispose des mêmes droits qu'Admin sur l'arborescence et sur le système de fichiers.

Trois types d'équivalence de sécurité sont disponibles :

- Explicite : par assignation
- Automatique : par appartenance à un groupe ou un rôle
- Implicite : équivalent à tous les conteneurs parents et à l'ayant droit [Public]

L'équivalence de sécurité est valable une fois seulement. Par exemple, si vous accordez à un troisième utilisateur une sécurité équivalente à celle de Joseph de l'exemple précédent, cet utilisateur ne reçoit pas les droits d'Admin.

L’équivalence de sécurité est enregistrée dans eDirectory sous la forme de valeurs de la propriété Sécurité égale à pour l’objet Utilisateur.

Lorsque vous ajoutez un objet Utilisateur en tant que titulaire à un objet Rôle organisationnel, cet objet bénéficie automatiquement d'une équivalence de sécurité par rapport à l'objet Rôle organisationnel. Il en est de même lorsqu'un utilisateur devient membre d'un objet Rôle de groupe.

Liste de contrôle d'accès (ACL - Access Control List)

La liste de contrôle d'accès (ACL) est également connue sous le nom de propriété Ayants droit de l'objet. Chaque fois que vous assignez un ayant droit, celui-ci est ajouté sous la forme d'une valeur à la propriété Ayants droit de l'objet (ACL) de la cible.

Cette propriété a d'importantes conséquences en matière de sécurité du réseau pour les raisons suivantes :

- Toute personne disposant du droit Superviseur ou Écrire sur la propriété Ayants droit de l'objet (ACL) d'un objet peut déterminer l'ayant droit de cet objet.
- Un utilisateur qui dispose du droit S'ajouter pour la propriété Ayants droit de l'objet (ACL) d'un objet peut changer ses propres droits se rapportant à cet objet. Par exemple, il peut s'accorder à lui-même le droit Superviseur.

C'est pourquoi vous devez être vigilant lorsque vous attribuez des droits S'ajouter à toutes les propriétés d'un objet Conteneur. Du fait de cette assignation, l'ayant droit peut devenir le superviseur de ce conteneur, de tous les objets qu'il contient et de tous les objets des conteneurs qui lui sont subordonnés.

Filtre des droits hérités (IRF - Inherited Rights Filter)

Le filtre des droits hérités (Inherited Rights Filter – IRF) permet de bloquer la transmission des droits vers le bas de l'arborescence eDirectory. Pour plus d'informations sur la configuration de ce filtre, reportez-vous à la section « Blocage des droits hérités sur un objet ou une propriété eDirectory » page 79.

Droits par défaut pour un nouveau serveur

Lorsque vous installez un nouvel objet Serveur dans une arborescence, les assignations d'ayant droit suivantes sont effectuées :

Ayants droit par défaut	Droits par défaut
Admin (pour le premier serveur eDirectory dans l'arborescence)	Droit d'objet Superviseur sur l'objet Arborescence L'administrateur dispose du droit d'objet Superviseur sur l'objet Serveur, ce qui signifie qu'il possède également ce droit sur le répertoire racine du système de fichiers des volumes installés sur le serveur.
[Public] (pour le premier serveur eDirectory dans l'arborescence)	Droit d'objet Parcourir sur l'objet Arborescence
Arborescence	Droit de propriété Lecture de l'arborescence sur les propriétés Nom du serveur hôte et Ressource hôte de tous les objets Volume. Ainsi, tous les objets ont accès aux noms du volume et du serveur physiques.
Objets Conteneur	Droits Lire et Analyse de fichiers sur le dossier `sys:\public`. Les objets Utilisateur subordonnés à l'objet Conteneur peuvent ainsi accéder aux utilitaires du répertoire `\public`. **REMARQUE :** ces droits ne s'appliquent qu'aux serveurs qui exécutent OES Linux.
Objets Utilisateur	Si des répertoires privés sont automatiquement créés pour les utilisateurs, ces derniers disposent du droit Superviseur sur ces répertoires.

Administration déléguée

eDirectory vous permet de déléguer l'administration d'une branche de l'arborescence, en révoquant vos propres droits de gestion sur cette branche. Des exigences de sécurité particulières nécessitant un administrateur différent disposant d'un contrôle total sur cette branche peuvent constituer l'un des motifs de cette délégation.

Pour déléguer l'administration :

1. Accordez le droit d'objet Superviseur à un conteneur.
   - **1a** Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
   - **1b** Cliquez sur **Droits** > **Modifier les ayants droit**.
   - **1c** Entrez le nom et le contexte de l'objet Conteneur dont vous souhaitez contrôler l'accès, puis cliquez sur **OK**.
   - **1d** Cliquez sur **Droits assignés**.
   - **1e** Cochez la case **Superviseur** pour les propriétés souhaitées.
   - **1f** Cliquez sur **Terminé**, puis sur **OK**.

2 Créez un IRF dans le conteneur qui filtre le droit Superviseur et les autres droits que vous voulez bloquer.

   2a Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .

   2b Cliquez sur **Droits** > **Modifier le filtre des droits hérités**.

   2c Spécifiez le nom et le contexte de l'objet dont vous souhaitez modifier le filtre des droits hérités, puis cliquez sur **OK**.

   2d Modifiez la liste des filtres de droits hérités, le cas échéant.

   Pour éditer la liste de filtres, vous devez disposer du droit Superviseur ou Contrôle d'accès sur la propriété ACL de l'objet. Vous pouvez définir des filtres qui annulent les droits hérités sur l'objet dans son entier, sur toutes les propriétés de l'objet et sur des propriétés en particulier.

   REMARQUE : Ces filtres n'annulent pas les droits qui sont explicitement accordés à un ayant droit sur cet objet, car de tels droits ne sont pas hérités.

   2e Cliquez sur **OK**.

IMPORTANT : si vous déléguez l'administration à un objet Utilisateur et que vous supprimez cet objet par la suite, aucun objet disposant de droits ne gère cette branche.

Pour déléguer l'administration de propriétés eDirectory spécifiques, telles que la gestion des mots de passe, reportez-vous à la section « Accord d'équivalence » page 77.

Pour déléguer l'utilisation de fonctions spécifiques dans les applications d'administration basée sur les rôles, reportez-vous à la « Configuration des services basés sur le rôle » page 114.

Gestion des droits

- « Assignation explicite de droits » page 76
- « Accord d'équivalence » page 77
- « Blocage des droits hérités sur un objet ou une propriété eDirectory » page 79
- « Affichage des droits effectifs sur un objet ou une propriété eDirectory » page 80

Assignation explicite de droits

Lorsque les assignations de droits par défaut de votre arborescence eDirectory offrent aux utilisateurs un accès trop important ou insuffisant aux ressources, vous pouvez créer ou modifier des assignations de droits explicites. Lorsque vous créez ou modifiez une assignation de droits, vous commencez par sélectionner la ressource dont vous voulez contrôler l'accès ou l'ayant droit (c'est-à-dire l'objet eDirectory qui possède, ou qui possédera, les droits).

SUGGESTION : Pour gérer les droits des utilisateurs de façon collective plutôt qu'individuelle, transformez en ayant droit un objet Groupe, Rôle ou Conteneur. Pour restreindre l'accès global à une ressource (pour tous les utilisateurs), reportez-vous à la section « Blocage des droits hérités sur un objet ou une propriété eDirectory » page 79.

- « Contrôle de l'accès à NetIQ eDirectory par une ressource » page 76
- « Contrôle de l'accès à NetIQ eDirectory par un ayant droit » page 77

Contrôle de l'accès à NetIQ eDirectory par une ressource

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Droits** > **Modifier les ayants droit**.
3. Spécifiez le nom et le contexte de la ressource eDirectory (objet) dont vous souhaitez contrôler l'accès, puis cliquez sur **OK**.

   Sélectionnez un conteneur si vous souhaitez contrôler l'accès à tous les objets en aval de cette ressource.
4. Éditez la liste des ayants droit ainsi que leurs assignations de droits à votre convenance.

   4a Pour modifier l'assignation des droits d'un ayant droit, sélectionnez l'ayant droit, cliquez sur **Droits assignés**, modifiez l'assignation des droits à votre convenance, puis cliquez sur **Terminé**.

   4b Pour ajouter un objet de type Ayant droit, cliquez sur **Ajouter un ayant droit**, sélectionnez l'objet, cliquez sur **OK**, sur **Droits assignés** pour assigner les droits d'ayant droit, puis sur **Terminé**.

   Lorsque vous créez ou modifiez une assignation de droits, vous pouvez accorder ou refuser l'accès à la totalité de l'objet, à toutes les propriétés de l'objet ou à des propriétés individuelles.

   4c Pour supprimer un objet en tant qu'ayant droit, sélectionnez l'ayant droit, puis cliquez sur **Supprimer l'ayant droit**.

   L'ayant droit supprimé n'a plus de droits explicites sur l'objet ou les propriétés de celui-ci, mais peut toujours disposer de droits effectifs via l'héritage ou l'équivalence de sécurité.
5. Cliquez sur **OK**.

Contrôle de l'accès à NetIQ eDirectory par un ayant droit

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Droits** > **Droits sur d'autres objets**.
3. Entrez le nom et le contexte de l'ayant droit (c'est-à-dire l'objet qui possède, ou possèdera, les droits) dont vous voulez modifier les droits.
4. Dans la zone **Contexte à partir duquel effectuer la recherche**, indiquez la partie de l'arborescence eDirectory où doivent être recherchés les objets eDirectory sur lesquels l'ayant droit a actuellement des assignations de droits.
5. Cliquez sur **OK**.

   Un écran apparaît, affichant la progression de la recherche. Une fois la recherche terminée, la page Droits sur d'autres objets apparaît et affiche les résultats de la recherche.
6. Éditez les assignations de droits eDirectory de l'ayant droit à votre convenance.

   6a Pour ajouter une assignation de droits, cliquez sur **Ajouter un objet**, sélectionnez l'objet dont l'accès doit être contrôlé, cliquez sur **OK**, puis sur **Droits assignés**, assignez les droits d'ayant droit et cliquez enfin sur **Terminé**.

   6b Pour modifier une assignation de droits, sélectionnez l'objet dont vous voulez contrôler l'accès, cliquez sur **Droits assignés**, modifiez l'assignation de droits de l'ayant droit, puis cliquez sur **Terminé**.

   Lorsque vous créez ou modifiez une assignation de droits, vous pouvez accorder ou refuser l'accès à la totalité de l'objet, à toutes les propriétés de l'objet ou à des propriétés individuelles.

6c Pour supprimer une assignation de droits, sélectionnez l'objet dont vous voulez contrôler l'accès, puis cliquez sur **Supprimer un objet**.

L'ayant droit n'a plus de droits explicites sur l'objet ou les propriétés de celui-ci, mais peut toujours disposer de droits effectifs via l'héritage ou l'équivalence de sécurité.

7 Cliquez sur **OK**.

Accord d'équivalence

Un utilisateur qui bénéficie d'une sécurité équivalente à celle d'un autre objet eDirectory possède de fait tous les droits de cet objet. Un utilisateur dispose automatiquement du même niveau de sécurité que les groupes et rôles auxquels il appartient. Tous les utilisateurs bénéficient implicitement d'une équivalence de sécurité avec l'ayant droit [Public] ainsi qu'avec chaque conteneur au-dessus de leurs objets Utilisateur dans l'arborescence eDirectory, y compris l'objet Arborescence. Vous pouvez également accorder à un utilisateur une sécurité équivalente à celle d'un quelconque objet eDirectory.

REMARQUE : les tâches de cette section vous permettent de déléguer la responsabilité d'administration à l'aide de droits eDirectory. Si vous avez des applications d'administration qui utilisent les rôles RBS (Role-Based Services – Services basés sur le rôle), vous pouvez également déléguer la responsabilité d'administration en assignant à des utilisateurs une adhésion à ces rôles.

- « Accord d'équivalence sécurité par adhésion » page 78
- « Accord explicite de l'équivalence de sécurité » page 78
- « Configuration d'un administrateur pour les propriétés eDirectory spécifiques d'un objet » page 79

Accord d'équivalence sécurité par adhésion

1 Si vous ne l'avez pas déjà fait, créez l'objet Groupe ou Rôle avec lequel vous souhaitez que les utilisateurs disposent d'une équivalence de sécurité.

Reportez-vous à la « Création d'un objet » page 104 pour plus d'informations.

2 Attribuez au groupe ou au rôle les droits eDirectory que vous voulez accorder aux utilisateurs.

Reportez-vous à la « Assignation explicite de droits » page 76 pour plus d'informations.

3 Éditez l'adhésion du groupe ou du rôle afin d'inclure ces utilisateurs qui ont besoin des droits du groupe ou du rôle.

- Pour un objet Groupe, utilisez la fenêtre **Modifier les membres du groupe**.

  Dans NetIQ iManager, cliquez sur **Rôles et tâches** > **Groupes** > **Modifier les membres du groupe**, spécifiez le nom et le contexte d'un objet Groupe, puis cliquez sur **OK**. Sous l'onglet Général, spécifiez les membres à ajouter au groupe, puis cliquez sur **OK**.

- Pour un objet Rôle, utilisez la fenêtre **Modifier un objet**.

  Dans NetIQ iManager, cliquez sur **Rôles et tâches** > **Administration de l'annuaire** > **Modifier un objet**, spécifiez le nom et le contexte d'un objet Rôle organisationnel, puis cliquez sur **OK**. Cliquez sur **Autre**, sélectionnez **rbsMember**, puis cliquez sur **Éditer**. Dans la fenêtre Éditer un attribut, spécifiez les membres à ajouter au rôle et cliquez sur **OK**.

4 Cliquez sur **OK**.

Accord explicite de l'équivalence de sécurité

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

3 Accédez ou entrez le nom et le contexte de l'utilisateur ou de l'objet à partir duquel vous souhaitez accorder l'équivalence de sécurité à l'utilisateur, puis cliquez sur **OK**.

4 Cliquez sur l'onglet **Sécurité**, puis accordez l'équivalence de sécurité comme suit :

- Si vous avez choisi un utilisateur, cliquez sur **Sécurité égale à**, sélectionnez ou accédez au nom et au contexte de l'objet à partir duquel vous souhaitez accorder l'équivalence de sécurité, puis cliquez sur **OK**.
- Si vous avez choisi un objet à partir duquel vous souhaitez accorder l'équivalence de sécurité à l'utilisateur, cliquez sur **Sécurité égale à moi**, sélectionnez ou accédez au nom et au contexte de l'utilisateur à partir duquel vous souhaitez accorder l'équivalence de sécurité à l'objet, puis cliquez sur **OK**.

Le système synchronise le contenu de ces deux pages de propriétés.

5 Cliquez sur **OK**.

Configuration d'un administrateur pour les propriétés eDirectory spécifiques d'un objet

1 Si vous ne l'avez pas encore fait, créez l'objet Utilisateur, Groupe, Rôle ou Conteneur que vous voulez définir comme ayant droit des propriétés spécifiques d'un objet donné.

Si vous créez un conteneur en tant qu'ayant droit, tous les objets à l'intérieur et en aval de ce conteneur disposeront des droits que vous accordez. Toutefois, la propriété doit être héritable pour que le conteneur et ses membres puissent bénéficier des droits en aval de celui-ci.

Pour plus d'informations, reportez-vous à la section « Création d'un objet » page 104.

2 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .

3 Cliquez sur **Droits** > **Modifier les ayants droit**.

4 Spécifiez le nom et le contexte du conteneur de niveau supérieur qui doit être géré par l'administrateur, puis cliquez sur **OK**.

5 Sur la page Modifier les ayants droit, cliquez sur **Ajouter un ayant droit**, sélectionnez l'objet qui représente l'administrateur, puis cliquez sur **OK**.

6 Cliquez sur **Droits assignés** pour l'ayant droit que vous venez d'ajouter, puis cliquez sur **Ajouter une propriété**.

7 Sélectionnez les propriétés à ajouter à la liste des propriétés, puis cliquez sur **OK**.

8 Pour chaque propriété que l'administrateur va gérer, assignez les droits requis.

Veillez à cocher la case **Héritable** sur chaque assignation de droits.

9 Cliquez sur **Terminé**, puis sur **OK**.

Blocage des droits hérités sur un objet ou une propriété eDirectory

Dans eDirectory, les assignations de droits relatives aux conteneurs peuvent être héritables ou non. Dans le système de fichiers, toutes les assignations de droits sur les dossiers sont héritables. Dans eDirectory, vous pouvez bloquer le processus d'héritage au niveau de certains éléments subordonnés, afin que les droits ne soient pas effectifs pour ces éléments, et ce quel que soit l'ayant droit.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Droits** > **Modifier le filtre des droits hérités**.
3. Spécifiez le nom et le contexte de l'objet dont vous souhaitez modifier le filtre des droits hérités, puis cliquez sur **OK**.

   Cette opération affiche une liste de filtres de droits hérités qui ont déjà été définis sur l'objet.
4. Dans la page Propriétés, apportez les modifications voulues à la liste des filtres de droits hérités.

   Pour éditer la liste de filtres, vous devez disposer du droit Superviseur ou Contrôle d'accès sur la propriété ACL de l'objet. Vous pouvez définir des filtres qui annulent les droits hérités sur l'objet dans son entier, sur toutes les propriétés de l'objet et sur des propriétés en particulier.

   REMARQUE : ces filtres ne bloquent pas les droits qui sont explicitement accordés à un ayant droit sur cet objet, car ces droits ne sont pas hérités.

   ---
5. Cliquez sur **OK**.

Affichage des droits effectifs sur un objet ou une propriété eDirectory

Les droits effectifs sont les droits réels que les utilisateurs peuvent exercer sur des ressources réseau spécifiques. Ils sont déterminés par eDirectory en fonction des assignations de droits explicites, de l'héritage et des équivalences de sécurité. Vous pouvez interroger le système pour déterminer les droits effectifs d'un utilisateur sur une ressource.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Droits** > **Afficher les droits effectifs**.
3. Entrez le nom et le contexte de l'ayant droit dont vous souhaitez afficher les droits effectifs et cliquez sur **OK**.
4. Choisissez l'une des options suivantes :

Option	Description
Nom de propriété	Liste les propriétés sur lesquelles l'ayant droit dispose de droits effectifs. Les propriétés sont lues à partir d'eDirectory et sont dès lors toujours affichées en anglais. Les éléments de la liste sont de l'un des types suivants : [Tous les droits d'attribut] – Représente toutes les propriétés de l'objet. [Droits d'entrée] – Représente l'objet comme un tout. Les droits sur cet élément ne présupposent aucun droit de propriété, sauf dans le cas du Superviseur. Propriétés spécifiques – Il s'agit de propriétés spécifiques sur lesquelles l'ayant droit possède individuellement des droits. Par défaut, seules les propriétés de cette classe d'objet sont indiquées (voir ci-après).
Droits effectifs	Affiche les droits effectifs de l'ayant droit sur la propriété sélectionnée, tels qu'ils ont été déterminés par eDirectory.
Afficher toutes les propriétés dans le schéma	Laissez cette case désélectionnée pour n'afficher que les propriétés de cette classe d'objet. Cochez cette case pour afficher les propriétés de toutes les classes définies dans le schéma eDirectory. Les propriétés supplémentaires ne s'appliquent que si cet objet est un conteneur, ou s'il a été étendu afin d'inclure les propriétés d'une classe auxiliaire. Les propriétés supplémentaires sont affichées sans puce.

5 Cliquez sur **Terminer**.

2 Conception de votre réseau NetIQ eDirectory

La conception de NetIQ eDirectory a une incidence sur presque tous les utilisateurs et toutes les ressources réseau. Un réseau eDirectory bien conçu permet d'améliorer les performances et la valeur de l'ensemble du réseau en optimisant l'efficacité, la tolérance aux pannes, la sécurité, l'évolutivité et le fonctionnement. Ce chapitre propose des idées de conception de réseau eDirectory.

- « Notions de base relatives à la conception d'un réseau eDirectory » page 81
- « Conception de l'arborescence eDirectory » page 82
- « Instructions concernant la partition de votre arborescence » page 89
- « Instructions concernant la réplication de votre arborescence » page 91
- « Planification de l'environnement utilisateur » page 93
- « Conception d'eDirectory pour l'e-Business » page 94
- « Présentation de NetIQ Certificate Server » page 95
- « Synchronisation des heures réseau » page 100

Notions de base relatives à la conception d'un réseau eDirectory

Un réseau eDirectory efficace repose sur la topologie réseau et sur la structure organisationnelle de la société ; elle implique également une préparation appropriée.

Si vous concevez un réseau eDirectory pour e-Business, reportez-vous à la « Conception d'eDirectory pour l'e-Business » page 94.

Topologie réseau

La topologie réseau correspond à la configuration physique du réseau. Pour développer une conception de réseau eDirectory efficace, vous devez tenir compte des éléments suivants :

- Les liaisons WAN
- Les utilisateurs qui requièrent un accès distant
- Ressources réseau (par exemple, nombre de serveurs)
- Conditions du réseau (par exemple pannes de courant fréquentes)
- L'anticipation des modifications à apporter à la topologie réseau

Structure organisationnelle

La structure organisationnelle de la société influe sur la conception du réseau eDirectory. Pour développer une conception eDirectory efficace, vous avez besoin :

- de l'organigramme de l'entreprise et d'une bonne compréhension du fonctionnement de la société ;
- d'un personnel suffisamment qualifié pour effectuer la conception et la mise en oeuvre de l'arborescence eDirectory.

  Vous avez besoin d'identifier le personnel capable d'effectuer les opérations suivantes :

  - cibler et planifier la conception du réseau eDirectory ;
  - comprendre la conception du réseau eDirectory, les normes de conception et la sécurité ;
  - Comprendre la structure physique du réseau et en assurer la maintenance
  - Gérer l'épine dorsale inter-réseau, les télécommunications, la conception WAN et le placement du routeur

Préparation de la conception du réseau eDirectory

Avant d'implémenter la conception du réseau eDirectory, vous devez effectuer les opérations suivantes :

- Définir des attentes réalistes en matière d'étendue et de planification.
- avertir tous les utilisateurs concernés par la conception de la mise en oeuvre du réseau eDirectory ;
- passer en revue les informations des sections « Topologie réseau » page 81 et « Structure organisationnelle » page 82.

Conception de l'arborescence eDirectory

La conception de l'arborescence eDirectory est la procédure la plus importante lorsqu'il s'agit de créer et de mettre en place un réseau. Cette conception est composée des tâches suivantes :

- « Création d'un document relatif aux standards de dénomination » page 82
- « Conception des couches supérieures de l'arborescence » page 85
- « Conception des couches inférieures de l'arborescence » page 88

Création d'un document relatif aux standards de dénomination

L'utilisation de noms standard tels que des noms d'objet rend l'utilisation du réseau plus intuitive, aussi bien pour les utilisateurs que pour les administrateurs. Des normes écrites peuvent également indiquer comment les administrateurs doivent définir d'autres valeurs de propriété, comme les adresses et les numéros de téléphone.

Les recherches et la navigation dans le répertoire reposent principalement sur la cohérence des valeurs de dénomination et de propriété.

L'utilisation de noms standard permet également à NetIQ Identity Manager de transférer plus facilement les données entre eDirectory et d'autres applications. Pour plus d'informations sur Identity Manager, reportez-vous au *NetIQ Identity Manager Setup Guide* (Guide de configuration de NetIQ Identity Manager).

Conventions de dénomination

- « Objets » page 83
- « Objets Serveur » page 83
- « Objets Pays » page 83

Objets

- Le nom doit être unique dans le conteneur. Ainsi, les utilisateurs Debora Jones et Daniel Jones ne peuvent pas porter tous les deux le nom DJONES s'ils se trouvent dans le même conteneur.
- Caractères spéciaux autorisés. Cependant, les signes plus (+) et égal (=), et le point (.) doivent toujours être précédés d'une barre oblique inverse (\). D'autres conventions de dénomination sont appliquées aux objets Serveur et o, ainsi qu'aux services de Bindery et aux environnements multilingues.
- Les majuscules et les minuscules, ainsi que les caractères de soulignement et les espaces, sont affichés comme vous les avez saisis, mais ils ne sont pas différenciés. Par exemple, `Manager_Profile` et `MANAGER PROFILE` sont considérés identiques.
- Si vous utilisez des espaces, vous devrez mettre le nom entre guillemets lorsque vous le saisirez sur la ligne de commande ou dans des scripts de connexion.

Objets Serveur

- Les objets Serveur sont automatiquement créés lorsque vous installez de nouveaux serveurs.
- Vous pouvez créer d'autres objets Serveur pour les serveurs Windows existants, ainsi que pour les serveurs eDirectory se trouvant dans d'autres arborescences. Toutefois, ils sont tous traités comme des objets de Bindery.
- Lorsque vous créez un objet Serveur, son nom doit correspondre au nom physique du serveur, qui :
  - est unique sur l'ensemble du réseau ;
  - comporte de 2 à 47 caractères ;
  - ne contient que des lettres (A-Z), des chiffres (0-9), des traits d'union, des points et des traits de soulignement ;
  - ne peut avoir un point pour premier caractère.
- Une fois nommé, l'objet Serveur ne peut pas être renommé dans NetIQ iManager. Si vous le renommez à partir du serveur, son nouveau nom apparaît automatiquement dans iManager.

Objets Pays

Les objets Pays doivent respecter le code ISO normalisé pour les pays (deux lettres).

Pour plus d'informations, reportez-vous à la liste des codes ISO 3166 (https://www.iso.org/iso-3166-country-codes.html).

Questions touchant les langues

Si vos postes de travail fonctionnent dans différentes langues, vous pouvez limiter les noms d'objet aux caractères qui peuvent être affichés sur tous les postes de travail. Il peut arriver, par exemple, qu'un nom entré en japonais contienne des caractères qui ne peuvent pas être affichés dans les langues occidentales.

IMPORTANT : Le nom de l'arborescence doit toujours être indiqué en anglais.

Exemple de document relatif aux standards

Le document suivant contient un exemple de standards pour certaines des propriétés les plus fréquemment utilisées. Vous avez uniquement besoin des normes correspondant aux propriétés que vous utilisez. Distribuez ce document à tous les administrateurs chargés de la création et de la modification des objets.

Classe d'objet | Propriété	Standard	Exemples	Explication
Nom d'utilisateur | de connexion	Initiale du prénom, du deuxième prénom (le cas échéant) et nom (en minuscules). Huit caractères au maximum. Tous les noms communs doivent être uniques dans l'entreprise.	mdupont, bjohnson	eDirectory n'exige pas l'utilisation de noms uniques au niveau de l'entreprise, mais cette méthode permet d'éviter des conflits au sein d'un même contexte (ou d'un contexte de Bindery).
Nom de famille de l'utilisateur	Nom (première lettre en majuscule).	Smith	Utilisé pour générer des étiquettes d'expédition.
Numéros de téléphone et de télécopie	Numéros séparés par des tirets.	États-Unis : 123-456-7890 Autres : 44-344-123456	Utilisé par les logiciels de numérotation automatique.
Classes | Emplacement multiples	Code d'emplacement à deux lettres (majuscules), tiret, boîte aux lettres interne.	BA-C23	Utilisé par les coursiers inter-bureaux.
Organisation | Nom	Nom de votre entreprise pour toutes les arborescences.	YourCo	En cas d'arborescences distinctes, choisissez un nom standard pour l'objet Organisation pour pouvoir fusionner ultérieurement les arborescences.
Unité organisationnelle | Nom (sur la base de l'emplacement)	Code de localité à deux ou trois lettres, toutes en majuscules.	STG, MEZ, LIL, PAR, LYN, BDX, QPR	Utilisez des noms courts et standard pour effectuer une recherche efficace.
Unité organisationnelle | Nom (sur la base du service)	Nom ou abréviation du service.	Ventes, Ing	Utilisez des noms courts et standard pour faciliter l'identification du service pris en charge par le conteneur.

Classe d'objet | Propriété	Standard	Exemples	Explication
Groupe | Nom	Nom descriptif.	Chefs de projet	Évitez les noms trop longs. Certains utilitaires ne peuvent pas les afficher.
Assignation de répertoire | Nom	Contenu du répertoire indiqué par l'objet Assignation de répertoire.	DOSAPPS	Utilisez des noms courts et standard pour faciliter l'identification du service pris en charge par le conteneur.
Profil | Nom	Rôle du profil.	Utilisateur mobile	Utilisez des noms courts et standard pour faciliter l'identification du service pris en charge par le conteneur.
Serveur | Nom	SERV, tiret, service, tiret, numéro unique.	SERV-Ing-1	eDirectory nécessite que les noms de serveur soient uniques dans l'arborescence.

Conception des couches supérieures de l'arborescence

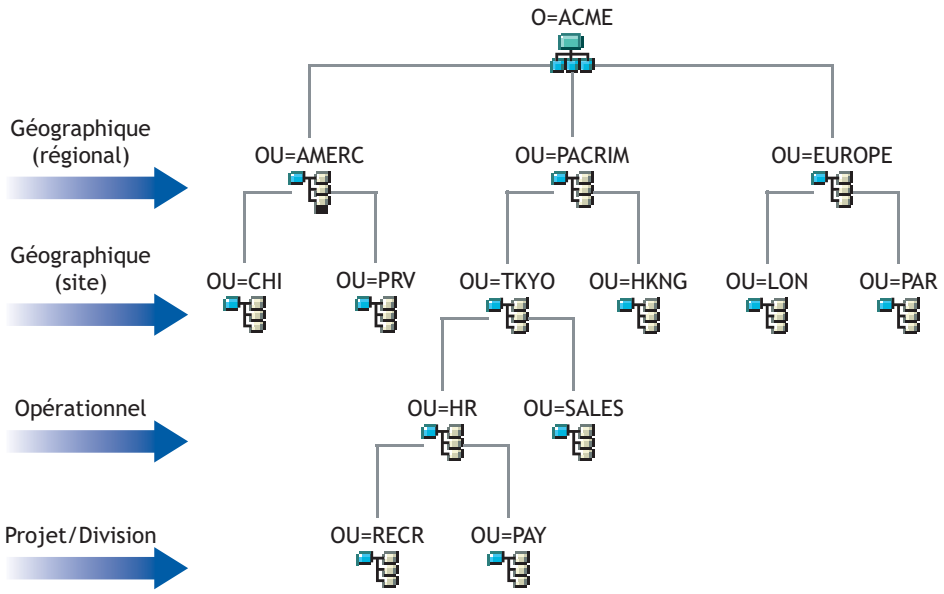
Vous devez très soigneusement concevoir les couches supérieures de l'arborescence : en effet, si jamais vous devez par la suite effectuer des modifications sur ces couches, la totalité de l'arborescence en est affectée, notamment si votre entreprise est dotée de liaisons WAN. Vous devez concevoir le sommet de l'arborescence de manière à ce que peu de modifications soient nécessaires ultérieurement.

Utilisez les règles de conception suivantes pour créer l'arborescence eDirectory :

- Utilisez une conception pyramidale.
- Utilisez une seule arborescence eDirectory portant un nom unique.
- Créez un seul objet Organisation.
- Créez des unités organisationnelles de premier niveau qui représentent l'infrastructure réseau physique.

La Figure 2-1 illustre les règles de conception d'eDirectory.

Figure 2-1 Règles de conception



Pour créer les couches supérieures de l'arborescence, reportez-vous aux sections « Création d'un objet » page 104 et « Modification des propriétés d'un objet » page 105.

Utilisation d'une conception pyramidale

Les réseaux eDirectory conçus en pyramide facilitent la gestion, la modification de grands groupes et la création de partitions logiques.

L'alternative à une conception pyramidale est une arborescence simple dans laquelle tous les objets sont placés dans les couches supérieures de l'arborescence. eDirectory prend en charge une conception d'arborescence simple. Toutefois, ce type de conception peut compliquer la gestion et le partitionnement.

Utilisation d'une seule arborescence eDirectory portant un nom unique

Une seule arborescence est la conception optimale pour la plupart des organisations. Par défaut, une seule arborescence est créée. Une arborescence unique implique une seule identité d'utilisateur sur le réseau, une administration de la sécurité plus simple et un seul point de gestion.

Ces recommandations concernant une arborescence unique pour une utilisation commerciale n'excluent pas la mise en place d'arborescences supplémentaires pour les tests et le développement.

Certaines organisations, cependant, peuvent avoir besoin de plusieurs arborescences en raison de problèmes législatifs, politiques ou professionnels. Par exemple, une organisation constituée de plusieurs entités autonomes peut avoir besoin de créer plusieurs arborescences. Si votre organisation requiert la création de plusieurs arborescences, envisagez l'utilisation de NetIQ Identity Manager pour en simplifier la gestion. Pour plus d'informations sur Identity Manager, reportez-vous au *NetIQ Identity Manager Setup Guide* (Guide de configuration de NetIQ Identity Manager).

Lorsque vous attribuez un nom à l'arborescence, utilisez un nom unique qui n'entrera pas en conflit avec celui d'autres arborescences. Utilisez un nom court et descriptif, comme EDL-ARBO.

Si deux arborescences portent le même nom et qu'elles sont situées sur le même réseau, vous risquez de rencontrer les problèmes suivants :

- Mises à jour appliquées à la mauvaise arborescence
- Disparition de ressources
- Disparition de droits
- Altération

Vous pouvez modifier le nom de l'arborescence à l'aide de l'utilitaire DSMerge, mais procédez avec précaution. La modification du nom d'une arborescence a une incidence sur le réseau car vous devez reconfigurer les clients pour qu'ils prennent en compte le nouveau nom de l'arborescence.

Création d'un seul objet Organisation

En règle générale, une arborescence eDirectory doit comporter un objet Organisation. Par défaut, un objet Organisation unique est créé et nommé en fonction de la société. Vous pouvez ainsi configurer les modifications qui s'appliquent à la totalité de la société à partir d'un emplacement unique de l'arborescence.

Par exemple, vous pouvez utiliser ZENworks® pour créer un objet Règle d'importation de postes de travail dans l'objet Organisation. Dans cette règle, qui influe sur la totalité de l'organisation, vous définissez la manière dont les objets Poste de travail sont nommés lorsqu'ils sont créés dans eDirectory.

Dans le conteneur Organisation, les objets suivants sont créés :

- Admin
- Serveur
- Volume

  Les réseaux qui ne comportent qu'un seul serveur Windows ou Linux exécutant eDirectory ne contiennent aucun objet Volume.

Vous créerez plusieurs objets Organisation si votre société a les besoins suivants :

- Elle comporte plusieurs sociétés qui ne partagent pas le même réseau.
- Elle a besoin de représenter séparément les différentes unités ou organisations.
- Elle dispose d'une règle ou de lignes directrices internes qui énoncent que les organisations restent séparées.

Création d'unités organisationnelles représentant le réseau physique

La conception d'unités organisationnelles de premier niveau est importante car elle a une incidence sur le partitionnement et l'efficacité d'eDirectory.

Dans le cas de réseaux couvrant plusieurs bâtiments ou emplacements à l'aide d'un LAN ou d'un WAN, la conception de l'objet Unité organisationnelle de premier niveau doit être basée sur l'emplacement. Vous pouvez ainsi créer des partitions eDirectory de manière à conserver tous les objets d'une partition à un même emplacement. Vous obtenez en outre un emplacement naturel où effectuer les assignations de sécurité et d'administrateur pour chaque emplacement.

Conception des couches inférieures de l'arborescence

Vous devez concevoir les couches inférieures d'une arborescence en fonction de l'organisation des ressources réseau. La conception des couches inférieures d'une arborescence eDirectory n'ayant d'impact que sur les objets situés au même emplacement, elle vous laisse plus de liberté que celle des couches supérieures.

Pour créer les couches inférieures de l'arborescence, reportez-vous aux sections « Création d'un objet » page 104 et « Modification des propriétés d'un objet » page 105.

Détermination de la taille du conteneur, de l'arborescence et de la base de données

Le nombre d'objets Conteneur de niveau inférieur que vous créez dépend du nombre total d'objets de l'arborescence, de l'espace disque disponible et des limitations de vitesse d'E/S au niveau du disque. eDirectory a été testé avec plus d'un milliard d'objets regroupés au sein d'une arborescence eDirectory unique. Ses performances sont donc uniquement limitées par l'espace disque, la vitesse d'E/S du disque et la mémoire vive. N'oubliez pas qu'une réplication peut avoir un impact important sur une arborescence de grande taille.

La taille habituelle d'un objet dans eDirectory est comprise entre 3 et 5 Ko. À l'aide de cette taille d'objet, vous pouvez rapidement calculer l'espace requis sur le disque dur pour le nombre d'objets que vous possédez ou dont vous avez besoin. N'oubliez pas que la taille des objets augmente en fonction du nombre d'attributs pour lesquels des données ont été définies et en fonction de la nature de ces données. Lorsque des objets contiennent des données BLOB (large objet binaire), telles que des images, du son ou des informations biométriques, leur taille est forcément accrue.

Plus les partitions sont volumineuses, plus le temps de réplication est long. Si vous utilisez des produits qui requièrent l'utilisation d'eDirectory, tels que ZENworks et les services DNS/DHCP, les objets eDirectory créés par de tels produits ont une incidence sur la taille des conteneurs dans lesquels ils sont situés. Il est recommandé de placer dans leur propre partition les objets créés à des fins uniquement administratives, tels que les objets DNS/DHCP, afin que l'accès utilisateur ne soit pas affecté par une réplication plus lente. En outre, la gestion des partitions et des répliques est ainsi facilitée.

Si cela vous intéresse, vous pouvez facilement déterminer la taille de votre base de données eDirectory ou de l'ensemble DIB (Directory Information Base - base de données des informations de l'Annuaire).

- Sous Windows, recherchez l'ensemble DIB dans le répertoire `\novell\nds\dibfiles`.
- Sous Linux, recherchez l'ensemble DIB dans le répertoire spécifié pendant l'installation.

Choix des conteneurs à créer

Généralement, vous devez créer des conteneurs pour des objets qui partagent les besoins d'accès avec d'autres objets eDirectory. Cela permet de gérer plusieurs utilisateurs avec une assignation d'ayant droit ou un script de connexion. Vous pouvez créer des conteneurs dans le but précis de rendre les scripts de connexion de conteneur plus efficaces, ou encore, vous pouvez placer deux services de votre entreprise dans un même conteneur pour faciliter la maintenance des scripts de connexion.

Conservez les utilisateurs dans des emplacements proches des ressources dont ils ont besoin afin de limiter le trafic réseau. Par exemple, les personnes au sein d'un même service travaillent généralement en étroite collaboration les unes avec les autres. Elles ont généralement besoin d'accéder au même système de fichiers et elles utilisent les mêmes imprimantes.

Il est simple de gérer les exceptions aux limites générales des groupes de travail. Par exemple, si deux groupes de travail utilisent une imprimante commune, vous pouvez créer un objet Alias pour l'imprimante dans l'un des groupes. Vous pouvez créer des objets Groupe pour gérer certains objets Utilisateur au sein d'un groupe de travail ou pour gérer des objets Utilisateur répartis sur plusieurs groupes de travail. Vous pouvez créer des objets Profil pour des sous-groupes d'utilisateurs partageant les mêmes exigences en termes de script de connexion.

Instructions concernant la partition de votre arborescence

Lorsque vous partitionnez eDirectory, vous permettez à des parties de la base de données d'exister sur plusieurs serveurs. Grâce à cette fonctionnalité, vous pouvez optimiser l'utilisation du réseau en répartissant sur plusieurs serveurs la charge que représentent le stockage et le traitement des données eDirectory. Par défaut, une seule partition est créée. Pour plus d'informations sur les partitions, reportez-vous à la « Partitions » page 58. Pour plus d'informations sur la création de partitions, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

Vous trouvez ci-après des instructions concernant la plupart des réseaux. Cependant, en fonction de la configuration, du matériel et du débit du trafic propres au réseau, vous devrez peut-être adapter certaines de ces instructions à vos besoins.

Détermination des partitions pour les couches supérieures de l'arborescence

Tout comme vous concevez votre arborescence de façon pyramidale, vous créez également des partitions avec une structure pyramidale. La structure des partitions est la suivante : les partitions sont peu nombreuses au sommet de l'arborescence, mais leur nombre augmente au fur et à mesure que vous vous déplacez vers le bas de cette arborescence. Une telle conception génère moins de références subordonnées qu'une structure d'arborescence eDirectory qui contient plus de partitions en haut qu'en bas.

Vous pouvez obtenir cette conception pyramidale si vous créez toujours les partitions relativement près des objets Feuille, notamment des utilisateurs.

REMARQUE : La partition créée à la racine de l'arborescence au cours de l'installation est une exception.

Lorsque vous concevez les partitions pour les couches supérieures, gardez à l'esprit les éléments suivants :

- Partitionnez le sommet de l'arborescence sur la base d'une infrastructure WAN. Placez un nombre moins élevé de partitions en haut de l'arborescence et un nombre plus élevé en bas.

  Vous pouvez créer des conteneurs pour chaque site séparé par des liaisons WAN (en plaçant chaque objet Serveur dans son conteneur local), puis créer une partition pour chaque site.
- Dans un réseau comportant des liaisons WAN, les partitions ne doivent pas couvrir plusieurs emplacements.

  Cette conception garantit que le trafic de réplication entre différents sites ne consomme pas inutilement la largeur de bande WAN.
- Effectuez un partitionnement local autour des serveurs. Gardez les serveurs physiquement distants dans des partitions différentes.

Détermination des partitions pour les couches inférieures de l'arborescence

Lorsque vous concevez les partitions pour les couches inférieures de l'arborescence eDirectory, tenez compte des points suivants :

- Définissez les partitions de couche inférieure par divisions organisationnelles, par services et par groupes de travail ; définissez également les ressources qui leur sont associées.
- Créez des partitions de manière à ce que tous les objets de chacune d'entre elles se trouvent dans un emplacement unique. Cela garantit que les mises à jour vers eDirectory se produisent sur un serveur local.

Détermination de la taille des partitions

Avec les eDirectory, nous vous recommandons les limites de conception suivantes pour les tailles des partitions :

Élément	Limite
Taille de la partition	Objets illimités
	Base de données des informations de l'Annuaire (DIB) de réplique limitée à ITB
Nombre total de partitions dans l'arborescence	Illimité
Nombre de partitions enfant par partition parent	150
Nombre de répliques par partition	50
	Limité par la DIB de réplique
Nombre de répliques par serveur de répliques	250

Cette modification des instructions de conception par rapport aux versions 6 et 7 des services NDS® vient des modifications apportées à l'architecture de la version 8 des NDS. Ces recommandations s'appliquent aux environnements distribués, tels que les sociétés. Ces recommandations risquent de ne pas être valables pour le commerce électronique ou les applications.

Bien que les utilisateurs de l'e-Business requièrent généralement que toutes les données soient stockées sur un serveur unique, eDirectory fournit des répliques filtrées qui contiennent un sous-ensemble d'objets et d'attributs issus de différentes zones de l'arborescence. Cela permet de répondre aux mêmes besoins en commerce électronique sans avoir à stocker toutes les données sur le serveur. Pour plus d'informations, reportez-vous à la section « Répliques filtrées » page 65.

Prise en compte des variables réseau

Lorsque vous planifiez des partitions, tenez compte des variables réseau suivantes et de leurs limitations:

- Nombre et vitesse des serveurs
- Vitesse de l'infrastructure réseau (adaptateurs réseau, hubs et routeurs)
- Importance du trafic réseau

Instructions concernant la réplication de votre arborescence

La création de plusieurs partitions eDirectory n'augmente pas à proprement parler la tolérance aux pannes et n'améliore pas les performances de l'annuaire, contrairement à une utilisation stratégique de plusieurs répliques. L'emplacement des répliques est extrêmement important pour des questions d'accessibilité et de tolérance aux pannes. Les données eDirectory doivent en effet être disponibles aussi rapidement que possible et être copiées à plusieurs endroits pour garantir cette tolérance. Pour plus d'informations sur la création de répliques, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

Les instructions suivantes permettent de déterminer la stratégie de placement des répliques.

- « Besoins des groupes de travail » page 91
- « Tolérance aux pannes » page 91
- « Détermination du nombre de répliques » page 92
- « Réplication de la partition Arborescence » page 93
- « Réplication pour l'administration » page 93
- « Gestion du trafic WAN » page 93

Besoins des groupes de travail

Placez des répliques de chaque partition sur les serveurs physiquement proches du groupe de travail qui utilise les informations situées dans ces partitions. Si les utilisateurs à une extrémité d'une liaison WAN accèdent souvent à une réplique stockée sur un serveur situé à l'autre extrémité de ce lien, placez une réplique sur les serveurs aux deux extrémités de la liaison WAN.

Placez les répliques dans les emplacements auxquels les utilisateurs, les groupes et les services accèdent le plus. Si des groupes d'utilisateurs dans deux conteneurs séparés ont besoin d'accéder au même objet au sein des limites d'une autre partition, placez la réplique sur un serveur qui existe dans le conteneur situé au-dessus des deux conteneurs contenant le groupe.

Tolérance aux pannes

Si un disque est endommagé ou si un serveur tombe en panne, les répliques des serveurs qui se trouvent dans d'autres emplacements peuvent toujours être utilisées pour authentifier les utilisateurs auprès du réseau et pour fournir des informations sur les objets qui se trouvent dans les partitions stockées sur le serveur désactivé.

Étant donné que les mêmes informations sont réparties sur plusieurs serveurs, vous n'êtes pas tributaire d'un seul serveur pour vous authentifier sur le réseau ou vous fournir des services (la connexion par exemple).

Pour générer une tolérance aux pannes, prévoyez trois répliques pour chaque partition si l'arborescence Annuaire contient assez de serveurs pour prendre en charge ce nombre. Deux répliques locales au moins doivent exister pour la partition locale. Trois répliques sont suffisantes, à moins que vous n'ayez besoin de fournir une accessibilité aux données situées sur d'autres emplacements, ou à moins que vous ne preniez part au commerce électronique ou que vous n'utilisiez d'autres applications qui requièrent plusieurs instances des données pour assurer l'équilibrage des charges et garantir une tolérance aux pannes.

Vous ne pouvez avoir qu'une seule réplique maîtresse. Les autres répliques doivent être en lecture/écriture, en lecture seule ou filtrées. La plupart des répliques doivent être en lecture/écriture. Tout comme la réplique maîtresse, elles prennent en charge l'affichage et la gestion des objets, ainsi que les connexions utilisateur. Elles envoient les informations à synchroniser lorsqu'une modification est effectuée.

Vous ne pouvez pas écrire dans des répliques en lecture seule. Elles permettent de rechercher et d'afficher les objets et sont automatiquement mises à jour lors de la synchronisation des répliques de la partition.

Afin d'offrir une tolérance aux pannes, vous ne devez pas dépendre d'une référence subordonnée ni de répliques filtrées. Une référence subordonnée est un pointeur et ne contient pas d'autres objets que l'objet racine de la partition. Les répliques filtrées ne contiennent pas la totalité des objets situés dans la partition.

eDirectory autorise un nombre illimité de répliques par partition, mais le trafic réseau augmente proportionnellement au nombre de répliques. Trouvez un équilibre entre les besoins de garantie d'une tolérance aux pannes et les besoins de performances réseau.

Vous ne pouvez stocker qu'une seule réplique par partition sur un serveur. Un même serveur peut contenir les répliques de plusieurs partitions.

En fonction du plan antisinistre de votre organisation, la majeure partie du travail de reconstruction du réseau après la perte d'un serveur ou d'un emplacement peut être assurée grâce aux répliques de partition. Si l'emplacement ne comporte qu'un seul serveur, sauvegardez régulièrement eDirectory. Envisagez d'acquérir un autre serveur pour la réplication dans le cadre de la tolérance aux pannes.

REMARQUE

- Certains logiciels de sauvegarde ne sauvegardent pas eDirectory automatiquement.
- Il est recommandé d'exclure le répertoire DIB présent sur votre serveur eDirectory de la portée de tout antivirus ou processus de logiciel de sauvegarde. Utilisez l'outil de sauvegarde d'eDirectory pour sauvegarder votre répertoire DIB. Pour plus d'informations sur la sauvegarde d'eDirectory, reportez-vous à la section « Sauvegarde et restauration de NetIQ eDirectory » page 443.

Détermination du nombre de répliques

Le temps de traitement et la quantité de trafic requis pour synchroniser plusieurs répliques sont des facteurs qui restreignent la création de plusieurs répliques. Lorsqu'un objet est modifié, ce changement est transmis à toutes les répliques de l'anneau de répliques. Plus un anneau de répliques comporte de répliques, plus la communication requise pour synchroniser les changements est importante. Si vous devez synchroniser des répliques via une liaison WAN, cette opération demande un temps considérable.

Si vous planifiez des partitions pour de nombreux sites géographiques, certains serveurs recevront de nombreuses répliques de références subordonnées. eDirectory peut distribuer ces références subordonnées sur un plus grand nombre de serveurs si vous créez des partitions régionales.

Réplication de la partition Arborescence

La partition Arborescence est la partition la plus importante de l'arborescence eDirectory. Si l'unique réplique de cette partition est altérée, le fonctionnement du réseau l'est aussi jusqu'à ce que la partition soit réparée ou que l'arborescence eDirectory soit complètement reconstruite. Par ailleurs, vous ne pouvez pas modifier la conception d'une arborescence en ce qui concerne l'objet Arborescence.

Lorsque vous créez des répliques de la partition Arborescence, trouvez un équilibre entre le coût de la synchronisation des références subordonnées et le nombre de répliques de la partition Arborescence.

Réplication pour l'administration

Étant donné que les partitions ne peuvent être initialement modifiées qu'au niveau des répliques maîtresses, placez ces dernières sur des serveurs proches de l'administrateur réseau, dans un emplacement central. Il pourrait sembler logique de conserver les répliques maîtresses sur des sites distants. Toutefois, les répliques maîtresses doivent se trouver là où les opérations de partition sont effectuées.

Il est préférable que les principales opérations eDirectory, comme le partitionnement, soient gérées par une seule personne ou un seul groupe dans un emplacement central. Cette façon de procéder permet de limiter les erreurs qui pourraient avoir des effets néfastes sur les opérations des eDirectory ; elle permet également une sauvegarde centralisée des répliques maîtresses.

L'administrateur réseau doit effectuer des activités exigeant énormément de ressources, telles que la création d'une réplique, à des moments où le trafic réseau est peu important.

Gestion du trafic WAN

Si les utilisateurs accèdent actuellement à des informations sur un répertoire particulier à l'aide d'une liaison WAN, vous pouvez diminuer le temps d'accès et le trafic WAN en plaçant une réplique contenant les informations nécessaires sur un serveur auxquels ils ont accès localement.

Si vous répliquez les répliques maîtresses vers un site distant, ou si vous êtes obligé de placer des répliques sur le WAN pour des raisons d'accessibilité et de tolérance aux pannes, n'oubliez pas que la largeur de bande est utilisée pour la réplication.

Vous devez placer les répliques sur des sites non locaux afin de garantir la tolérance aux pannes si vous ne parvenez pas à obtenir les trois répliques recommandées, afin d'augmenter l'accessibilité, et afin de fournir une gestion et un stockage centralisés des répliques maîtresses.

Planification de l'environnement utilisateur

Une fois que vous avez conçu la structure de base de l'arborescence eDirectory et que vous avez configuré les opérations de partitionnement et de réplication, vous devez planifier l'environnement utilisateur pour simplifier la gestion et optimiser l'accès aux ressources réseau. Pour créer un plan d'environnement utilisateur, analysez les besoins des utilisateurs et créez des instructions d'accessibilité pour chaque zone.

Analyse des besoins des utilisateurs

Lorsque vous analysez les besoins des utilisateurs, tenez compte des éléments suivants :

- Besoins physiques du réseau, tels que les imprimantes ou l'espace de stockage des fichiers.

  Déterminez si les ressources sont partagées par des groupes d'utilisateurs au sein d'une même arborescence ou par des groupes d'utilisateurs issus de plusieurs conteneurs. Étudiez également les besoins en ressources physiques des utilisateurs distants.
- Besoins en services de Bindery des utilisateurs

  Déterminez les applications basées sur des services de Bindery et leurs utilisateurs.
- Besoins des applications.

  Déterminez les applications et les fichiers de données dont ont besoin les utilisateurs, les systèmes d'exploitation présents, et les groupes ou utilisateurs ayant besoin d'accéder à ces applications. Prenez en compte le lancement manuel ou automatique des applications partagées par des applications telles que ZENworks.

Création des instructions d'accessibilité

Une fois que vous avez rassemblé les informations concernant les besoins des utilisateurs, vous devez définir les objets eDirectory que vous allez utiliser pour créer les environnements des utilisateurs. Par exemple, si vous créez des ensembles de règles ou des objets Application, vous devez déterminer leur nombre et l'endroit où vous allez autoriser leur placement dans l'arborescence.

Vous devez également déterminer comment vous allez mettre en oeuvre les mesures de sécurité pour restreindre l'accès utilisateur. Vous devez identifier toutes les précautions de sécurité à prendre dans certains cas. Par exemple, vous pouvez avertir les administrateurs réseau de ne pas octroyer de droit Superviseur eDirectory sur des objets Serveur, car ce droit est hérité par le système de fichiers.

Conception d'eDirectory pour l'e-Business

Si vous utilisez eDirectory pour l'e-Business, que vous fournissiez un portail pour des services ou que vous partagiez des données avec d'autres entreprises, les recommandations mentionnées dans ce chapitre ne sont pas forcément applicables à votre cas.

Vous pouvez suivre les instructions de conception de e-Business eDirectory suggérées ci-après.

- Créez une arborescence avec un nombre limité de conteneurs.

  Cette instruction dépend des applications utilisées et de la mise en oeuvre des eDirectory. Par exemple, le déploiement global d'un serveur de messagerie requiert des instructions de conception d'eDirectory plus traditionnelles, telles que celles présentées plus haut dans ce chapitre. En outre, si vous vous apprêtez à distribuer l'administration des utilisateurs, vous pouvez créer une unité organisationnelle (OU) différente pour chaque zone de responsabilité administrative.
- Conservez au moins deux partitions.

  Maintenez la partition par défaut au niveau Arborescence et créez une partition pour le reste de l'arborescence. Si vous avez créé des unités organisationnelles à des fins administratives, créez une partition pour chacune d'entre elles.

  Si vous répartissez la charge sur plusieurs serveurs, essayez de limiter le nombre de partitions ; conservez-en toutefois au moins deux pour la sauvegarde et la récupération en cas de sinistre.

- Créez au moins trois répliques de votre arborescence pour garantir la tolérance aux pannes et assurer l'équilibrage des charges.

  N'oubliez pas que LDAP n'équilibre pas lui-même les charges. Pour équilibrer la charge sur LDAP, pensez à utiliser des commutateurs de niveau 4.

- Créez une autre arborescence pour l'e-Business. Limitez les ressources réseau, telles que les serveurs et les imprimantes, incluses dans cette arborescence. Envisagez la création d'une arborescence qui ne contiendrait que des objets Utilisateur.

  Vous pouvez utiliser NetIQ Identity Manager pour lier cette arborescence utilisateur à d'autres arborescences contenant des informations sur le réseau. Pour plus d'informations, reportez-vous au *NetIQ Identity Manager Setup Guide* (Guide de configuration de NetIQ Identity Manager).

- Utilisez des classes auxiliaires pour personnaliser le schéma.

  Si un client ou une application requièrent un objet Utilisateur différent du standard inetOrgPerson, utilisez les classes auxiliaires pour personnaliser le schéma. L'utilisation de classes auxiliaires permet aux concepteurs d'applications de modifier les attributs utilisés dans la classe sans avoir à recréer l'arborescence.

- Augmentez les performances d'importation au format LDIF.

  Lors de l'exécution de l'utilitaire d'importation/de conversion/d'exportation NetIQ, eDirectory indexe chaque objet pendant le processus. Cette opération risque de ralentir le processus d'importation au format LDIF. Pour améliorer les performances d'importation LDIF, interrompez tous les index à partir des attributs des objets créés, exécutez l'utilitaire d'importation/de conversion/d'exportation NetIQ, puis reprenez l'indexation des attributs.

- Mettez en oeuvre des noms communs (CN) globalement uniques.

  eDirectory autorise la présence d'un même nom commun dans plusieurs conteneurs. Toutefois, si vous utilisez des noms communs globalement uniques, vous pouvez effectuer des recherches sur ces noms, sans mettre en place de logique de gestion de réponses multiples.

Présentation de NetIQ Certificate Server

NetIQ Certificate Server permet de concevoir, d'émettre et de gérer des certificats numériques en créant un objet Conteneur de sécurité et un objet Autorité de certification organisationnelle. L'objet Autorité de certification organisationnelle garantit une transmission sécurisée des données et est requis pour les produits Web. Le premier serveur eDirectory SP4 crée automatiquement et stocke physiquement les objets Conteneur de sécurité et Autorité de certification organisationnelle pour l'ensemble de l'arborescence eDirectory. Ces deux objets sont créés au sommet de l'arborescence eDirectory et doivent y rester.

Une arborescence eDirectory ne peut comporter qu'un seul objet Autorité de certification organisationnelle. Une fois que l'objet Autorité de certification organisationnelle a été créé sur un serveur, il n'est pas possible de le déplacer vers un autre serveur. La suppression et le remplacement d'un objet Autorité de certificat organisationnelle annulent tout certificat associé auparavant à cet objet.

IMPORTANT : vérifiez que le premier serveur eDirectory est bien celui qui doit être l'hôte permanent de l'objet Autorité de certification organisationnelle. Vérifiez également qu'il est fiable, accessible et qu'il fait partie intégrante du réseau.

Si ce serveur n'est pas le premier serveur eDirectory sur le réseau, le programme d'installation recherche le serveur eDirectory qui contient l'objet Autorité de certification organisationnelle et fait référence à ce serveur. Le programme d'installation accède au conteneur de sécurité et crée un objet Certificat de serveur.

Si aucun objet Autorité de certificat organisationnelle n'est disponible sur le réseau, les produits Web ne peuvent pas fonctionner.

Droits requis pour exécuter des tâches sur NetIQ Certificate Server

Pour exécuter les tâches associées à la configuration de NetIQ Certificate Server, l'administrateur doit disposer des droits décrits dans le tableau suivant.

Tâche NetIQ Certificate Server	Droits requis
Configuration de la sécurité de base pour l'installation du premier serveur dans une nouvelle arborescence ou la mise à niveau du premier serveur dans une arborescence où aucun système de sécurité de base n'a été installé	Droit Superviseur au niveau de la racine Droit Superviseur sur le conteneur Sécurité
Configuration de la sécurité de base pour l'installation des autres serveurs	Droit Superviseur sur le conteneur du serveur Droit Superviseur sur l'objet W0 (situé à l'intérieur du conteneur de sécurité)
Création de l'autorité de certification organisationnelle	Droit Superviseur sur le conteneur Sécurité
Création d'objets Certificat de serveur	Droit Superviseur sur le conteneur du serveur Droit Lire sur l'attribut NDSPKI:Private Key de l'objet Autorité de certification organisationnelle

De plus, l'administrateur à la racine peut déléguer la responsabilité d'utiliser l'autorité de certification organisationnelle en assignant les droits suivants aux administrateurs de sous-conteneurs. Les administrateurs de sous-conteneurs doivent posséder les droits suivants pour pouvoir installer NetIQ eDirectory avec la sécurité SSL :

- Droit Lire sur l'attribut NDSPKI:Private Key de l'objet Autorité de certification organisationnelle situé dans le conteneur Sécurité.
- Droit Superviseur sur l'objet W0 situé dans le conteneur Sécurité, à l'intérieur de l'objet KAP.

Ces droits sont assignés à un groupe ou à un rôle dans le cadre duquel tous les utilisateurs administratifs sont définis. Pour obtenir une liste complète des droits requis pour exécuter des tâches spécifiques associées à NetIQ Certificate Server, reportez-au Chapitre 25, « Présentation du serveur de certificats », page 705.

Opérations eDirectory sécurisées sur des ordinateurs Linux

eDirectory inclut des services PKCS (Public Key Cryptography Services) lesquels contiennent NetIQ Certificate Server qui lui fournit les services d'infrastructure de clés publiques (PKI), d'infrastructure cryptographique internationale (NICI) ainsi que le serveur SAS-SSL.

Les sections suivantes fournissent des informations sur l'exécution d'opérations sécurisées eDirectory :

- « Vérification de l'installation et de l'initialisation de NICI sur le serveur » page 97
- « Initialisation du module NICI sur le serveur » page 97
- « Démarrage du serveur de certificats (services PKI) » page 98
- « Arrêt du serveur de certificats (services PKI) » page 98
- « Création d'un objet Autorité de certification organisationnelle » page 98
- « Création d'un objet Certificat de serveur » page 98
- « Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle » page 99

Pour plus d'informations sur l'utilisation de l'autorité de certification externe, reportez-vous au Chapitre 25, « Présentation du serveur de certificats », page 705.

Vérification de l'installation et de l'initialisation de NICI sur le serveur

Vérifiez les conditions suivantes, qui indiquent si le module NICI a été installé et initialisé correctement :

- Le fichier `/etc/nici.cfg` existe
- Le répertoire `/var/novell/nici` existe
- Le fichier `/var/novell/nici/primenici` existe

Si ces conditions ne sont pas remplies, suivez la procédure décrite à la section « Initialisation du module NICI sur le serveur » page 97.

Initialisation du module NICI sur le serveur

1. Arrêtez le serveur eDirectory.
   - Sur les systèmes Linux, entrez

     ```
     /etc/init.d/ndsd stop
     ```

   IMPORTANT : Nous vous recommandons d'utiliser ndsmanage pour démarrer ou arrêter ndsd.

2. Vérifiez si le progiciel NICI est installé.
   - Sur les systèmes Linux, entrez

     ```
     rpm -qa | grep nici
     ```

3. (Conditionnel) Si le progiciel NICI n'est pas installé, installez-le maintenant.

   Vous ne pourrez pas continuer si le progiciel NICI n'est pas installé.

4. Lancez le serveur eDirectory.
   - Sur les systèmes Linux, entrez :

     ```
     /etc/init.d/ndsd start
     ```

IMPORTANT : Nous vous recommandons d'utiliser ndsmanage pour démarrer ou arrêter ndsd.

Démarrage du serveur de certificats (services PKI)

Pour démarrer les services PKI, entrez la commande:

```
npki -1
```

Arrêt du serveur de certificats (services PKI)

Pour arrêter les services PKI, entrez la commande:

```
npki -u
```

Création d’un objet Autorité de certification organisationnelle

1. Lancez NetIQ iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la section Creating an Organizational Certificate Authority Object (https://www.netiq.com/documentation/edir88/crtadmin88/data/fbgccghh.html) (Création d'un objet Autorité de certification organisationnelle) du *NetIQ Certificate Server 3.3 Administration Guide* (Guide d'administration de NetIQ Certificate Server 3.3).
3. Cliquez sur le bouton **Rôles et tâches**  .
4. Cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   S'il n'existe aucun objet Autorité de certification organisationnelle, la boîte de dialogue de création d'un objet Autorité de certification organisationnelle s'ouvre, de même que l'Assistant correspondant qui crée l'objet. Suivez les instructions à l'écran pour créer l'objet. Pour obtenir des informations spécifiques sur la boîte de dialogue ou sur l'une des pages de l'Assistant, cliquez sur **Aide**.

REMARQUE : vous ne pouvez avoir qu'un seul objet Autorité de certification organisationnelle dans votre arborescence eDirectory. Pour plus d'informations sur la création d'une autorité de certification organisationnelle, reportez-vous à la section « Création d'une autorité de certification organisationnelle pour votre organisation » page 708.

Création d'un objet Certificat de serveur

Les objets Certificat de serveur sont créés dans le conteneur qui contient l'objet Serveur eDirectory. Selon vos besoins, vous pouvez créer un objet Certificat de serveur distinct pour chaque application prenant en charge la cryptographie sur le serveur, ou vous pouvez créer un objet Certificat de serveur pour toutes les applications utilisées sur ce serveur.

REMARQUE : les termes « objet Certificat de serveur » et « objet Matériel clé » (KMO – Key Material Object) sont synonymes. Le nom de schéma de l'objet eDirectory est NDSPKI:Key Material.

1. Lancez NetIQ iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Création d'un objet Certificat de serveur » page 720.
3. Cliquez sur le bouton **Rôles et tâches** .
4. Cliquez sur **Serveur de certificats NetIQ** > **Create Server Certificate** (Créer un certificat de serveur).

   L'assistant Créer un certificat de serveur apparaît. Suivez les instructions à l'écran pour créer l'objet. Pour des informations spécifiques sur l'une des pages de l'Assistant, cliquez sur **Aide**.

Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle

Un certificat auto-signé peut être utilisé pour vérifier l'identité de l'autorité de certification organisationnelle ainsi que la validité d'un certificat signé par cette autorité.

À partir de la page de propriétés de l'autorité de certification organisationnelle, vous pouvez afficher les certificats et les propriétés associés à cet objet. À partir de la page de propriétés du certificat auto-signé, vous pouvez exporter le certificat auto-signé dans un fichier qui pourra être utilisé dans des applications prenant en charge la cryptographie.

Le certificat auto-signé qui réside dans l'autorité de certification organisationnelle est identique au certificat de racine approuvée d'un objet Certificat de serveur qui, lui, est signé par l'autorité de certification organisationnelle. Tout service qui reconnaît le certificat auto-signé de l'autorité de certification organisationnelle en tant que racine approuvée accepte un certificat utilisateur ou un certificat de serveur valide signé par cette autorité.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
3. Spécifiez le nom et le contexte d'un objet Autorité de certification organisationnelle, puis cliquez sur **OK**.

   Les objets Autorité de certification organisationnelle se trouvent dans le conteneur Sécurité.
4. Cliquez sur l'onglet **Certificats**, puis sur **Self-Signed Certificate** (Certificat auto-signé).
5. Cliquez sur **Exporter**.

   L'assistant d'exportation du certificat apparaît. Suivez les instructions à l'écran pour exporter le certificat. Pour des informations spécifiques sur l'une des pages de l'Assistant, cliquez sur **Aide**.
6. Sur la page d'exportation du résumé du certificat, cliquez sur **Save the Exported Certificate to a File** (Enregistrer le certificat exporté dans un fichier).

   Une fois enregistré dans un fichier, le certificat peut être importé en tant que racine approuvée dans une application prenant en charge la cryptographie.
7. Cliquez sur **Fermer**.

Insérez ce fichier dans toutes les opérations de ligne de commande qui établissent des connexions sécurisées avec eDirectory.

Synchronisation des heures réseau

La synchronisation horaire est un service qui maintient la cohérence des heures sur les serveurs réseau. Elle est assurée par le système d'exploitation du serveur et non par eDirectory. eDirectory gère sa propre heure interne pour garantir l'ordre approprié des paquets eDirectory, mais il obtient cette heure à partir du système d'exploitation du serveur.

Si votre réseau utilise Windows ou Linux, vous devez employer le protocole NTP (Network Time Protocol) pour synchroniser les serveurs, car il s'agit d'un standard largement utilisé pour la synchronisation horaire.

NTP

NTP fait partie de la suite de protocole UDP, qui fait elle-même partie de la suite de protocole TCP/IP. Par conséquent, la suite protocole TCP/IP doit être chargée sur les ordinateurs utilisant NTP. Les ordinateurs de votre réseau bénéficiant d'un accès à Internet peuvent obtenir l'heure des serveurs NTP sur Internet.

NTP synchronise les horloges avec le temps universel (Universal Time Coordinated – UTC), qui est la norme horaire internationale.

NTP présente le concept de strate. Un serveur monostrate est relié à un appareil de mesure précise de l'heure, par exemple une horloge atomique. Un serveur monostrate donne l'heure à un serveur bistrate, et ainsi de suite.

Pour plus d'informations sur le logiciel de synchronisation horaire, consultez le site Web The Network Time Protocol (protocole NTP) (http://www.ntp.org).

Synchronisation horaire sur les ordinateurs Linux

Vous pouvez utiliser le daemon xntpd du protocole NTP (Network Time Protocol) pour synchroniser l'heure sur des serveurs Linux. xntpd est un daemon de système d'exploitation qui définit et gère l'heure système en synchronisation avec les serveurs horaires standard sur Internet.

Pour plus d'informations sur l'exécution de ntpd sur un système Linux, consultez le site Web ntpd - Network Time Protocol (NTP) Daemon (http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html) (Daemon ntpd du protocole NTP).

Vérification de la synchronisation horaire

Pour vérifier que l'heure est synchronisée dans l'arborescence, exécutez DSRepair à partir d'un serveur de l'arborescence qui dispose au moins de droits en lecture/écriture sur l'objet Arborescence.

Windows

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**.
2. Cliquez sur **dsrepair.dlm** > **Démarrer**.
3. Cliquez sur **Réparer** > **Synchronisation horaire**.

Linux

1. Exécutez la commande suivante :

   ```
   ndsrepair -T
   ```

3 Gestion des objets

NetIQ eDirectory comprend NetIQ iManager, une application de gestion réseau de type Web qui vous permet de gérer les objets de votre arborescence eDirectory. Pour comprendre les fonctionnalités et avantages de NetIQ iManager, reportez-vous au *Guide d'administration de NetIQ iManager*.

La gestion des objets eDirectory implique la création, la modification et la manipulation de ces objets. Par exemple, vous pouvez avoir besoin de créer des comptes utilisateur et de gérer les droits utilisateur. Avec NetIQ iManager, vous pouvez effectuer les opérations suivantes :

- Exécuter des opérations d'administration de base (par exemple, parcourir, créer, modifier et organiser les objets) ;
- Créer des comptes utilisateur (en spécifiant notamment le nom de connexion des utilisateurs ainsi que d'autres informations utilisées par eDirectory) ;
- Gérer des droits (assigner des droits, accorder des équivalences, bloquer des héritages et afficher des droits effectifs). Pour plus d'informations, reportez-vous à la section « Gestion des droits » page 75.
- Configurer une administration basée sur les rôles (définir les rôles de l'administrateur pour des applications d'administration spécifiques via l'objet RBS – services basés sur le rôle).

Ce chapitre contient des informations sur les rubriques suivantes :

- « Tâches d'objet générales » page 101
- « Gestion des comptes utilisateur » page 106
- « Configuration des services basés sur le rôle » page 114

Tâches d'objet générales

Cette section décrit les procédures des tâches de base impliquées dans la gestion de l'arborescence eDirectory :

- « Recherche dans l'arborescence eDirectory » page 102
- « Création d'un objet » page 105
- « Modification des propriétés d'un objet » page 105
- « Copie d'objets » page 105
- « Déplacement d'objets » page 105
- « Suppression d'objets » page 106
- « Attribution de nouveaux noms à des objets » page 106

Recherche dans l'arborescence eDirectory

Le bouton **Afficher les objets** ( ) dans iManager vous permet de rechercher ou d'atteindre des objets dans votre arborescence eDirectory. Vous pouvez afficher la structure de votre arborescence et cliquer avec le bouton droit sur des objets pour effectuer des tâches. Les tâches disponibles dépendent du type d'objet que vous sélectionnez.

La page Sélecteur d'objet eDirectory dans iManager vous permet également de rechercher ou d'atteindre des objets. Dans la plupart des champs d'entrée d'iManager, vous pouvez spécifier le nom de l'objet et son contexte ou cliquer sur le bouton **Sélecteur d'objet** pour rechercher ou atteindre l'objet désiré. En sélectionnant un objet sur la page Sélecteur d'objet eDirectory, vous insérez l'objet et son contexte dans le champ d'entrée de texte.

Ce chapitre comprend les informations suivantes :

- « Utilisation du bouton Afficher les objets » page 102
- « Utilisation du bouton Sélecteur d'objet » page 104

Utilisation du bouton Afficher les objets

Appliquez les méthodes décrites ci-dessous pour localiser les objets que vous désirez gérer.

- « Utilisation de la fonction Parcourir » page 102
- « Utilisation de la recherche » page 103

Utilisation de la fonction Parcourir

1. Dans iManager, cliquez sur le bouton **Afficher les objets** .
2. Cliquez sur **Parcourir**.
3. Utilisez les options suivantes pour rechercher un objet :

Option	Description
	Permet de descendre d'un niveau dans l'arborescence.
	Permet de monter d'un niveau dans l'arborescence.
Contexte	Permet de spécifier le nom du conteneur dont vous voulez afficher le contenu. Pour utiliser cette option, précisez le nom du conteneur souhaité, puis cliquez sur **Appliquer**.
Nom	Permet de spécifier le nom d'un objet. Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, `g*` permet de rechercher tous les objets qui commencent par la lettre g, comme Grèce ou Gilbert ; `*te` permet de rechercher tous les objets qui se terminent par te, comme Imprimante ou Colette. Pour utiliser cette option, saisissez le nom souhaité, puis cliquez sur **Appliquer**.
Type	Permet de spécifier le type d'objet à rechercher. La valeur par défaut est Tous les types disponibles. Pour utiliser cette option, sélectionnez un type d'objet dans la liste déroulante et cliquez sur **Appliquer**.

4 Après avoir trouvé l'objet recherché, cliquez avec le bouton droit sur cet objet et sélectionnez une tâche dans la liste des tâches disponibles.

Utilisation de la recherche

1 Dans NetIQ iManager, cliquez sur le bouton **Afficher les objets** .

2 Cliquez sur **Rechercher**.

3 Dans le champ **Contexte**, indiquez le nom du conteneur dans lequel vous souhaitez effectuer la recherche.

   Cliquez sur **Rechercher dans sous-conteneurs** pour élargir la recherche aux sous-conteneurs appartenant au conteneur en cours.

4 Dans le champ **Nom**, indiquez le nom de l'objet à rechercher.

   Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, `g*` permet de rechercher tous les objets qui commencent par la lettre g, comme Grèce ou Gilbert ; `*te` permet de rechercher tous les objets qui se terminent par te, comme Imprimante ou Colette.

5 Sélectionnez le type d'objet à rechercher dans la liste déroulante **Type**.

6 Cliquez sur **Rechercher**.

7 Après avoir trouvé l'objet recherché, cliquez avec le bouton droit sur cet objet et sélectionnez une tâche dans la liste des tâches disponibles.

Utilisation du bouton Sélecteur d'objet

Appliquez les méthodes décrites ci-dessous pour localiser les objets que vous désirez gérer.

- « Utilisation de la fonction Parcourir » page 104
- « Utilisation de la recherche » page 104

Utilisation de la fonction Parcourir

1. Cliquez sur le bouton **Sélecteur d'objet** sur une page de propriétés iManager.
2. Cliquez sur **Parcourir**.
3. Utilisez les options suivantes pour rechercher un objet :

Option	Description
	Permet de descendre d'un niveau dans l'arborescence.
	Permet de monter d'un niveau dans l'arborescence.
Rechercher dans	Indiquez le nom du conteneur dont vous souhaitez afficher le contenu, puis cliquez sur **Appliquer**.
Rechercher les objets nommés	Permet de spécifier le nom d'un objet. Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, `g*` permet de rechercher tous les objets qui commencent par la lettre g, comme Grèce ou Gilbert ; `*te` permet de rechercher tous les objets qui se terminent par te, comme Imprimante ou Colette. Pour utiliser cette option, saisissez le nom souhaité, puis cliquez sur **Appliquer**.

Utilisation de la recherche

1. Cliquez sur le bouton **Sélecteur d'objet** sur une page de propriétés iManager.
2. Cliquez sur **Rechercher**.
3. Dans le champ **Démarrer la recherche dans**, indiquez le nom du conteneur dans lequel vous souhaitez effectuer la recherche.

   Cliquez sur **Rechercher dans sous-conteneurs** pour élargir la recherche aux sous-conteneurs appartenant au conteneur en cours.
4. Dans le champ **Rechercher les objets nommés**, indiquez le nom de l'objet à rechercher.

   Vous pouvez utiliser l'astérisque (*) comme caractère générique dans ce champ. Par exemple, `g*` permet de rechercher tous les objets qui commencent par la lettre g, comme Grèce ou Gilbert ; `*te` permet de rechercher tous les objets qui se terminent par te, comme Imprimante ou Colette.
5. Cliquez sur **Rechercher**.

Création d'un objet

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration de l'annuaire** > **Créer un objet**.

3 Sélectionnez un objet dans la liste des classes d'objet disponibles, puis cliquez sur **OK**.

4 Précisez les informations recherchées, puis cliquez sur **OK**.

   Les informations recherchées dépendent du type d'objet que vous créez. Cliquez sur le ? pour plus d'informations.

5 Cliquez sur **OK**.

Modification des propriétés d'un objet

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

3 Spécifiez le nom et le contexte des objets à modifier, puis cliquez sur **OK**.

4 Editez les pages de propriétés souhaitées.

   Cliquez sur le ? pour plus d'informations sur des pages de propriétés spécifiques.

5 Cliquez sur **OK**.

Copie d'objets

Cette option vous permet de créer un nouvel objet avec les mêmes valeurs d'attribut qu'un objet existant ou de copier les valeurs d'attribut d'un objet vers un autre.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Copier un objet**.

3 Dans le champ **Copier à partir de cet objet**, spécifiez le nom et le contexte de l'objet à copier.

4 Sélectionnez l'une des options suivantes :

   - **Créer un objet et copier des valeurs d'attribut**
   - **Copier des valeurs d'attributs vers un objet existant**

5 Pour copier des droits Liste de contrôle d'accès (ACL) sur l'objet que vous créez/modifiez, sélectionnez **Copier les droits ACL**.

   Le processus de copie des droits ACL peut être plus ou moins long en fonction de votre environnement système et réseau.

6 Cliquez sur **OK**.

Déplacement d'objets

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Déplacer l'objet**.

3 Dans le champ **Nom de l'objet**, spécifiez le nom et le contexte des objets à déplacer.

4 Dans le champ **Déplacer vers**, spécifiez le conteneur vers lequel vous souhaitez déplacer le ou les objets.

5 Pour créer un alias à l'ancien emplacement de chaque objet déplacé, sélectionnez **Créer un alias à la place de l'objet déplacé**.

Si vous créez un alias, les opérations qui sont tributaires de l'ancien emplacement se poursuivent sans interruption tant que vous ne les modifiez pas afin de préciser le nouvel emplacement.

6 Cliquez sur **OK**.

Suppression d'objets

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Supprimer l'objet**.

3 Spécifiez le nom et le contexte du ou des objets à supprimer.

4 Cliquez sur **OK**.

Attribution de nouveaux noms à des objets

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Renommer un objet**.

3 Dans le champ **Nom de l'objet**, spécifiez le nom et le contexte de l'objet à renommer.

4 Dans le champ **Nouveau nom de l'objet**, spécifiez le nouveau nom de l'objet.

N'entrez pas le contexte de l'objet dans le champ **Nouveau nom de l'objet**.

5 Pour créer un alias de l'objet renommé, sélectionnez **Créer un alias à la place de l'objet renommé**.

Si vous créez un alias, les opérations qui dépendent de l'ancien nom de l'objet se poursuivent sans interruption jusqu'à ce que vous puissiez les mettre à jour pour qu'elles reflètent le nouveau nom.

6 Pour enregistrer l'ancien nom, sélectionnez **Enregistrer l'ancien nom**.

Ainsi, l'ancien nom est enregistré comme valeur supplémentaire (non officielle) de la propriété Nom. L'enregistrement de l'ancien nom permet aux utilisateurs de rechercher un objet à partir de son ancien nom. Après avoir renommé l'objet, vous pouvez afficher l'ancien nom dans le champ **Autre nom** sous l'onglet **General Identification** (Identification générale) pour cet objet.

7 Cliquez sur **OK**.

Gestion des comptes utilisateur

Pour configurer un compte utilisateur eDirectory, il convient de créer un objet Utilisateur et de définir des propriétés qui permettront de contrôler la connexion et l'environnement informatique réseau de cet utilisateur. Vous pouvez utiliser un objet Modèle pour faciliter ces tâches.

Vous pouvez créer des scripts de connexion pour connecter automatiquement des utilisateurs aux fichiers, imprimantes et autres ressources réseau dont ils ont besoin lorsqu'ils s'authentifient. Si plusieurs utilisateurs accèdent aux mêmes ressources, vous pouvez placer les commandes du script de connexion dans les scripts de connexion de profil et de conteneur.

Ce chapitre comprend les informations suivantes :

- « Création et modification des comptes utilisateur » page 107
- « Paramétrage de fonctions de compte facultatives » page 108
- « Configuration de scripts de connexion » page 111

- « Restrictions des heures de connexion pour les utilisateurs distants » page 112
- « Suppression de comptes utilisateur » page 113

Création et modification des comptes utilisateur

Un compte utilisateur est un objet Utilisateur dans l'arborescence eDirectory. Un objet Utilisateur indique le nom de connexion d'un utilisateur et fournit d'autres informations qui sont exploitées par eDirectory pour contrôler l'accès de cet utilisateur aux ressources réseau.

Ce chapitre comprend les informations suivantes :

- « Création d'un objet Utilisateur » page 107
- « Modification d'un compte utilisateur » page 107
- « Activation d'un compte utilisateur » page 108
- « Désactivation d'un compte utilisateur » page 108

Création d'un objet Utilisateur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Utilisateurs** > **Créer un utilisateur**.
3. Spécifiez un nom d'utilisateur et un nom de famille pour l'utilisateur.
4. Indiquez un conteneur dans lequel l'utilisateur sera créé.
5. Spécifiez éventuellement des informations supplémentaires et cliquez ensuite sur **OK**.

   Cliquez sur le ? pour plus d'informations sur des pages de propriétés spécifiques.
6. Cliquez sur **OK**.

Modification d'un compte utilisateur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Utilisateurs** > **Modifier un utilisateur**.
3. Spécifiez le nom et le contexte des utilisateurs à modifier, puis cliquez sur **OK**.
4. Editez les pages de propriétés souhaitées.

   Cliquez sur le ? pour plus d'informations sur des pages de propriétés spécifiques.
5. Cliquez sur **OK**.

Activation d'un compte utilisateur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Utilisateurs** > **Activer le compte**.
3. Spécifiez le nom et le contexte de l'utilisateur, puis cliquez sur **OK**.

Désactivation d'un compte utilisateur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Utilisateurs** > **Désactiver le compte**.
3. Spécifiez le nom et le contexte de l'utilisateur, puis cliquez sur **OK**.

Paramétrage de fonctions de compte facultatives

Après avoir créé un objet Utilisateur, vous pouvez configurer son environnement informatique réseau et implémenter des fonctions de sécurité supplémentaires pour la connexion.

Définition de l'environnement réseau d'un utilisateur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Utilisateurs** > **Modifier un utilisateur**.
3. Spécifiez le nom et le contexte des utilisateurs à modifier, puis cliquez sur **OK**.
4. Sous l'onglet **Général**, sélectionnez la page **Environnement**.
5. Complétez la page de propriétés.

   Cliquez sur le ? pour plus d'informations sur des pages de propriétés spécifiques.
6. Cliquez sur **OK**.

Configuration d'un paramètre de sécurité de connexion supplémentaire pour un utilisateur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Utilisateurs** > **Modifier un utilisateur**.
3. Spécifiez le nom et le contexte des utilisateurs à modifier, puis cliquez sur **OK**.
4. Sous l'onglet **Restrictions**, complétez les pages de propriétés souhaitées.

   Cliquez sur le ? pour plus d'informations.

Page	Description	Attribut LDAP
Restrictions de mot de passe	Définit un mot de passe de connexion.	passwordRequired
Restrictions de connexion	◆ Activation ou désactivation du compte. ◆ Limitation du nombre de sessions de connexion simultanées. ◆ Définition d'une date d'expiration et de verrouillage de la connexion.	loginDisabled loginMaximumSimultaneous loginExpirationTime ou loginGraceLimit
Restrictions de temps	Permet de restreindre les heures de connexion de l'utilisateur. Si vous définissez une restriction et que l'utilisateur est déjà connecté quand débute la période de restriction, le système affiche un message d'avertissement pendant cinq minutes puis, si l'utilisateur ne s'est toujours pas déconnecté, il le déconnecte automatiquement. Pour les utilisateurs distants, reportez-vous à la section « Restrictions des heures de connexion pour les utilisateurs distants » page 112.	loginAllowedTimeMap
Restrictions d'adresse	Restreint les emplacements réseau (postes de travail) à partir desquels l'utilisateur peut se connecter. Si vous ne définissez pas de restrictions sur cette page, l'utilisateur peut se connecter à partir de n'importe quel emplacement du réseau.	networkAddressRestriction
Solde de compte	Permet de définir la facturation de l'utilisation du serveur de cet utilisateur.	accountBalance
Verrouillage en cas d'intrus	Vous permet d'utiliser ce compte s'il a été verrouillé en raison de la détection d'un intrus. Pour gérer la configuration de la détection d'intrus, utilisez la page de propriétés Détection d'intrus du conteneur parent.	lockedByIntruder

5 Cliquez sur **OK**.

Configuration de la détection d'intrus pour tous les utilisateurs dans un conteneur

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

3 Spécifiez le nom et le contexte d'un objet Conteneur, puis cliquez sur **OK**.

4 Sous l'onglet **Général**, sélectionnez la page **Détection d'intrus**.

5 Sélectionnez l'une des options suivantes :

Option	Description
Détecter les intrus	Active le système de détection d'intrus pour les comptes utilisateur situés dans le conteneur.
Tentatives de connexion incorrectes	Indique le nombre d'échecs de connexion simultanés auquel l'utilisateur a droit avant l'activation de la détection d'intrus. Si une personne utilise l'un des comptes utilisateur du conteneur pour se connecter et qu'au bout du nombre de tentatives infructueuses spécifié elle n'y parvient toujours pas, la détection d'intrus est activée. Ce nombre est stocké dans la propriété Login Intruder Limit (Nombre maximum de tentatives d'intrusion) du conteneur.
Intervalle de réinitialisation après des tentatives d'intrusion	Précise l'intervalle pendant lequel les échecs de connexion consécutifs doivent survenir pour que soit activée la détection d'intrusion. Entrez le nombre de jours, d'heures et de minutes.
Verrouillage du compte après détection	Indique si la connexion doit être désactivée lorsque la détection d'intrus est activée sur un compte utilisateur de ce conteneur. Si vous ne cochez pas cette case, le système n'effectue aucune opération lorsque la détection d'intrus est activée. Si vous cochez cette case et si le système verrouille un compte utilisateur en raison de la détection d'un intrus, vous pouvez déverrouiller le compte en désélectionnant la case Compte verrouillé dans la page de propriétés Verrouillage en cas d'intrusion de l'objet Utilisateur.
Jours, Heures, Minutes	Ces trois champs indiquent la durée de désactivation de la connexion lorsque la détection d'intrus est activée sur un compte utilisateur de ce conteneur. Entrez le nombre de jours, d'heures et de minutes souhaité, ou acceptez la valeur par défaut, soit 15 minutes. Au bout du délai spécifié, le système active à nouveau la connexion pour le compte utilisateur. Le contenu de ces champs est stocké dans la propriété Délai de réinitialisation après intrusion du conteneur. Si les valeurs de ces trois champs sont définies sur zéro, le compte utilisateur est verrouillé indéfiniment.

6 Cliquez sur **OK**.

Configuration d'une durée pour l'absence de verrouillage en cas d'intrusion

Cette fonction permet de spécifier la durée pendant laquelle le compte n'est pas verrouillé si un utilisateur tente de se connecter en utilisant le mot de passe qui était applicable avant celui en cours. Si vous sélectionnez l'option *No Intruder Lock Out* (Aucun verrouillage en cas d'intrusion), la détection d'intrus n'est pas activée pendant la durée spécifiée, à partir du dernier changement de mot de passe.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **NMAS** > **NMAS Login Methods** (Méthodes de connexion NMAS) > **NDS**.
3 Sur la page NDS, indiquez la durée pendant laquelle le compte utilisateur n'est pas verrouillé, puis cliquez sur **OK**.

Désactivation de l'intervalle de mise à jour de l'heure de connexion

Vous pouvez spécifier une valeur d'intervalle pour désactiver la mise à jour de l'attribut Heure de connexion d'un utilisateur. Vous pouvez spécifier la valeur d'intervalle pour un utilisateur, un conteneur, un objet LPO (Login Policy Security Object) ou un serveur. Pour activer cette fonction, le schéma doit être étendu à l'aide du fichier `nmas.sch`.

Pour spécifier l'intervalle pour un utilisateur :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches**
2. Cliquez sur **NMAS Role** (Rôle NMAS) > **NMAS Users** (Utilisateurs NMAS).
3. Indiquez le nom et le contexte de l'objet dont vous souhaitez spécifier l'intervalle.
4. Sous l'onglet **Général**, sélectionnez **Autre**, puis choisissez **sasUpdateLoginTimeInterval** dans **Attributs non définis**.
5. Utilisez le bouton fléché pour déplacer **sasUpdateLoginTimeInterval** de la liste des attributs non définis vers la liste **Attributs définis**, selon les besoins, puis cliquez sur **Appliquer**.

Pour spécifier l'intervalle de mise à jour pour un conteneur et un objet LPO :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches**
2. Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
3. Spécifiez le nom et le contexte d'un objet Conteneur ou Stratégie de connexion, puis cliquez sur **OK**.
4. Sous l'onglet **Général**, sélectionnez **Autre**, puis sélectionnez **sasUpdateLoginTimeInterval** dans **Attributs non définis**.
5. Utilisez le bouton fléché pour déplacer **sasUpdateLoginTimeInterval** de la liste des attributs non définis vers la liste **Attributs définis**, selon les besoins, puis cliquez sur **Appliquer**.

Configuration de scripts de connexion

Un script de connexion est une liste de commandes qui s'exécutent lorsqu'un utilisateur se connecte. Il sert généralement à connecter l'utilisateur à des ressources réseau telles que des fichiers et des imprimantes. Les scripts de connexion s'exécutent sur le poste de travail de l'utilisateur dans l'ordre suivant :

1. Script de connexion de conteneur
2. Script de connexion de profil
3. Script de connexion utilisateur

Pendant le processus de connexion, si le système ne trouve pas l'un de ces scripts de connexion, il passe au suivant sur la liste. S'il n'en trouve aucun, il exécute un script par défaut qui assigne une unité de recherche à un dossier sur le serveur par défaut de l'utilisateur. Le serveur par défaut est défini dans la page de propriétés Environnement de l'objet Utilisateur.

Création d'un script de connexion

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

3 Spécifiez le nom et le contexte de l'objet dans lequel vous souhaitez créer le script de connexion.

Pour que le script de connexion s'applique à	Créez-le sur
Un seul utilisateur	L'objet Utilisateur
Un ou plusieurs utilisateurs non encore créés	Un objet Modèle
Tous les utilisateurs d'un conteneur	L'objet Conteneur
Un ensemble d'utilisateurs dans un ou plusieurs conteneurs	Un objet Profil

4 Cliquez sur **OK**.

5 Sous l'onglet **Général**, sélectionnez la page **Script de connexion**.

6 Entrez les commandes de script de connexion de votre choix.

Reportez-vous au *Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/data/front.html) (Guide de scripts de connexion) pour plus d'informations.

7 Cliquez sur **OK**.

Assignation d'un profil à un utilisateur

Si vous associez un profil à un objet Utilisateur, le script de connexion du profil s'exécutera lors de la connexion de l'utilisateur. Assurez-vous que l'utilisateur dispose du droit Parcourir sur l'objet Profil et du droit Lire sur la propriété Script de connexion de l'objet Profil.

Pour plus d'informations, reportez-vous à la section « Affichage des droits effectifs sur un objet ou une propriété eDirectory » page 79.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Utilisateur** > **Modifier un utilisateur**.

3 Spécifiez le nom et le contexte de l'objet Utilisateur dans lequel vous souhaitez créer le script de connexion.

4 Cliquez sur **OK**.

5 Sous l'onglet **Général**, sélectionnez la page **Script de connexion**.

6 Pour associer un objet Profil à cet objet, entrez le nom et le contexte de l'objet Profil dans le champ **Profil**.

7 Cliquez sur **OK**.

Restrictions des heures de connexion pour les utilisateurs distants

Dans la page de propriétés Restrictions horaires d'un objet Utilisateur, vous pouvez limiter les heures auxquelles l'utilisateur peut être connecté à eDirectory. Par défaut, aucune restriction n'est définie pour les heures de connexion.

Si vous définissez une restriction sur les heures de connexion et que l'utilisateur est déjà connecté quand débute la période de restriction, le système émet un avertissement l'invitant à se déconnecter dans les cinq minutes qui suivent. S'il est toujours connecté au terme des cinq minutes, il est automatiquement déconnecté et perd tout le travail qu'il n'a pas enregistré.

Si un utilisateur se connecte à distance à partir d'un fuseau horaire différent de celui du serveur qui traite la requête de connexion, les restrictions qui lui sont appliquées en termes de plages de connexion sont ajustées pour tenir compte du décalage horaire. Par exemple, si vous interdisez qu'un utilisateur se connecte les lundis entre 1 heure et 6 heures du matin et que celui-ci se connecte à distance depuis un fuseau horaire en avance d'une heure sur votre serveur, il ne pourra pas se connecter entre 2 heures et 7 heures du matin.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Utilisateurs** > **Modifier un utilisateur**.
3 Spécifiez le nom et le contexte des utilisateurs à modifier, puis cliquez sur **OK**.
4 Sous l'onglet **Restrictions**, cliquez sur **Restrictions horaires**.
5 Sélectionnez l'une des options suivantes :

Option	Description
Grille horaire	Chaque cellule de la grille horaire représente une demi-heure durant un jour de la semaine. Les cellules rouges représentent les périodes soumises à restriction (périodes auxquelles l'objet ne doit pas être connecté). Les cellules grises représentent les périodes non soumises à restriction (périodes auxquelles l'objet peut être connecté). Pour créer une restriction horaire, cliquez sur les heures de votre choix pour les rendre gris foncé. Vous pouvez aussi sélectionner plusieurs heures en maintenant la touche Maj enfoncée, en cliquant sur une cellule, puis en faisant glisser le curseur sur les cellules correspondantes. Les restrictions des heures de connexion que vous définissez sont stockées dans la propriété Plage horaire des connexions autorisées de cet objet.
Ajouter une restriction horaire	Pour ajouter une restriction horaire, sélectionnez une cellule grise, puis cochez cette option.
Supprimer une restriction horaire	Pour supprimer une restriction horaire, sélectionnez une cellule rouge, puis cochez cette option.
Mise à jour	Cliquez sur ce bouton pour activer la sélection.
Réinitialiser	Cliquez sur ce bouton pour que la grille horaire retrouve son état antérieur à l'ouverture de cette page de propriétés.

6 Cliquez sur **OK**.

Suppression de comptes utilisateur

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Utilisateurs** > **Supprimer un utilisateur**.
3 Spécifiez le nom et le contexte du ou des utilisateurs à supprimer.
4 Cliquez sur **OK**.

Configuration des services basés sur le rôle

iManager permet aux administrateurs d'assigner des responsabilités particulières aux utilisateurs et de leur présenter uniquement les outils (et les droits associés) nécessaires à l'exécution de celles-ci. Cette fonctionnalité s'appelle *Services basés sur le rôle (RBS).*

Les services basés sur le rôle permettent aux administrateurs de limiter l'utilisateur à un groupe spécifique de fonctions, appelées *tâches*, et à des d'objets déterminés par le regroupement de tâches, appelés *rôles*. Les tâches que voit un utilisateur à l'écran lorsqu'il accède à iManager dépendent de ses assignations de rôles dans eDirectory. Seules les tâches qui ont été assignées à cet utilisateur s'affichent. L'utilisateur n'a pas besoin de parcourir l'arborescence pour trouver un objet à gérer. Le plug-in iManager pour cette tâche présente les outils et l'interface nécessaires à sa réalisation.

Vous pouvez assigner plusieurs rôles à un même utilisateur. Inversement, vous pouvez assigner le même rôle à plusieurs utilisateurs.

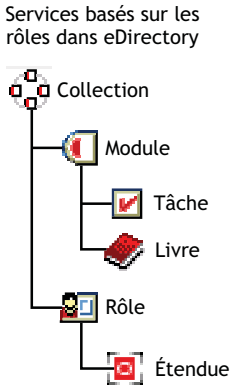
Les services basés sur le rôle sont représentés par des objets définis dans eDirectory. Le schéma eDirectory de base est étendu lors de l'installation d'iManager. Les types d'objet RBS sont listés dans le tableau ci-dessous :

Objet	Description
rbsCollection	Objet Conteneur qui contient tous les objets Rôle et Module RBS. Les objets rbsCollection sont les conteneurs du niveau le plus élevé pour tous les objets RBS. Une arborescence peut contenir autant d'objets rbsCollection que nécessaire. Ces objets ont des « propriétaires ». Il s'agit d'utilisateurs qui disposent de droits de gestion sur la collection. Les objets rbsCollection peuvent être créés dans l'un des conteneurs suivants : ◆ Pays ◆ Domaine ◆ Lieu ◆ Organisation ◆ Unité organisationnelle
rbsRole	Objet Conteneur qui précise les tâches que les utilisateurs (membres) sont autorisés à effectuer. Définir un rôle consiste à créer un objet rbsRole et à désigner les tâches que le rôle peut exécuter. Les membres d'un rôle peuvent être des utilisateurs, groupes, organisations ou unités organisationnelles et sont associés à un rôle dans une étendue spécifique de l'arborescence. Les objets rbsTask et rbsBook sont assignés à des objets rbsRole. Les objets rbsRole peuvent être créés uniquement dans des conteneurs rbsCollection.
rbsModule	Objet Conteneur qui renferme les objets rbsTask et rbsBook. Les objets rbsModule ont un attribut de nom de module qui représente le nom du produit définissant les tâches ou les livres (par exemple, Maintenance d'eDirectory, NMAS ou accès au certificat NetIQ). Les objets rbsModule ne peuvent être créés que dans des conteneurs rbsCollection.

Objet	Description
rbsTask	Objet Feuille qui représente une fonction spécifique, telle que par exemple la réinitialisation de mots de passe de connexion. Les objets rbsTask ne se trouvent que dans des conteneurs rbsModule.
rbsBook	Objet Feuille contenant une liste de pages assignées au livre. Un objet rbsBook peut être assigné à un ou plusieurs rôles et à un ou plusieurs types de classe d'objet. Les objets rbsBook se situent exclusivement dans des conteneurs rbsModule.
rbsScope	Objet Feuille utilisé pour les assignations ACL (à la place des assignations pour chaque objet Utilisateur). Les objets rbsScope représentent le contexte dans l'arborescence dans lequel un rôle sera exécuté et sont associés aux objets rbsRole. Ils héritent de la classe Groupe. Les objets Utilisateur sont assignés à un objet rbsScope. Ces objets ont une référence à l'étendue de l'arborescence à laquelle ils sont associés. Il est créé à la demande, puis automatiquement supprimé lorsqu'il n'est plus nécessaire. Ils sont situés exclusivement dans des conteneurs rbsRole. **AVERTISSEMENT :** ne modifiez jamais la configuration d'un objet Étendue. Vous pourriez rencontrer de graves problèmes et mettre le système en panne.

Les objets RBS sont situés dans l'arborescence eDirectory, comme l'indique le schéma suivant :

Figure 3-1 *Objets RBS dans l'arborescence eDirectory*



Définition des rôles RBS

Les rôles RBS définissent les tâches que des utilisateurs sont autorisés à exécuter. Définir un rôle RBS consiste à créer un objet rbsRole, puis à désigner les tâches que cet objet peut exécuter et les objets Utilisateur, Groupe ou Conteneur qui peuvent exécuter ces tâches. Dans certains cas, les plug-ins NetIQ iManager (livrés avec le produit) fournissent des rôles RBS prédéfinis que vous pouvez modifier.

Les tâches que les rôles RBS peuvent exécuter sont représentées par des objets rbsTask dans votre arborescence eDirectory. Ces objets sont automatiquement ajoutés durant l'installation des produits. Ils sont répartis dans un ou plusieurs objets rbsModule, c'est-à-dire des conteneurs qui correspondent aux divers modules fonctionnels du produit.

Pour toute information sur l'assignation d'un rôle à des membres, reportez-vous à la section « Assignation de l'adhésion et de l'étendue du rôle RBS » page 117.

- « Création d'un objet Rôle » page 116
- « Modification des tâches associées à un rôle » page 116
- « Assignation de l'adhésion et de l'étendue du rôle RBS » page 117
- « Suppression d'un objet Services basés sur le rôle » page 118

Création d'un objet Rôle

Utilisez l'Assistant Créer un rôle iManager pour créer un objet rbsRole. Il est recommandé de créer cet objet rbsRole dans le même conteneur rbsCollection que les autres objets rbsRole (par exemple, le conteneur Collection de services basés sur le rôle).

1. Dans iManager, cliquez sur le bouton **Configurer** .
2. Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.
3. Cliquez sur la collection dans laquelle vous souhaitez créer un rôle.
4. Cliquez sur l'onglet **Rôle**.
5. Cliquez sur **Nouveau** > **Rôle iManager**.
6. Suivez les instructions de l'Assistant Créer un rôle iManager.

Pour savoir comment ajouter des membres à des rôles, reportez-vous à la section « Définition de tâches RBS personnalisées » page 118.

Modification des tâches associées à un rôle

À chaque rôle RBS est associé un ensemble de tâches disponibles. Vous pouvez ajouter ou supprimer des tâches en fonction de vos besoins.

1. Dans iManager, cliquez sur le bouton **Configurer** .
2. Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.
3. Cliquez sur la collection dans laquelle vous souhaitez modifier un rôle.
4. Cliquez sur l'onglet **Rôle**.
5. Cliquez sur le rôle à modifier.

6 (Facultatif) Si vous souhaitez ajouter des tâches à un rôle, procédez comme suit :

   6a Cliquez sur **Ajouter**.

   6b Utilisez les boutons fléchés pour déplacer les tâches de la liste **Toutes les tâches** vers la liste **Tâches assignées**, en fonction des besoins.

   6c Cliquez sur **OK**, puis à nouveau sur **OK**.

7 (Facultatif) Si vous souhaitez supprimer des tâches d'un rôle, procédez comme suit :

   7a Sélectionnez les tâches à supprimer et cliquez sur **Retirer**.

   7b Cliquez sur **OK**, puis à nouveau sur **OK**.

8 Une fois l'opération terminée, cliquez sur **Fermer**.

Assignation de l'adhésion et de l'étendue du rôle RBS

Après avoir défini les rôles RBS nécessaires dans votre organisation, vous pouvez assigner des membres à chaque rôle. Ainsi, vous indiquez l'étendue de l'exercice des fonctions du rôle pour chaque membre. L'étendue est l'emplacement ou contexte de l'arborescence eDirectory auquel le rôle peut s'appliquer.

Vous pouvez assigner un utilisateur à un rôle de différentes manières :

- Directement
- Via des assignations de groupes et de groupes dynamiques. Si un utilisateur est membre d'un groupe ou d'un groupe dynamique assigné à un rôle, il a accès à ce rôle.
- Via des assignations de rôles organisationnels. Si un utilisateur est titulaire d'un rôle organisationnel assigné à un rôle, il a accès à ce rôle.
- Via des assignations de conteneurs. Un objet Utilisateur a accès à tous les rôles auxquels son conteneur parent est assigné. Cela concerne également d'autres conteneurs jusqu'à la racine de l'arborescence.

Un utilisateur peut être associé à un rôle plusieurs fois, chaque fois avec une étendue différente. Inversement, vous pouvez assigner la même tâche à plusieurs membres.

Pour assigner des membres à un rôle et définir une étendue, procédez comme suit :

1 Dans iManager, cliquez sur le bouton **Configurer** .

2 Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.

3 Cliquez sur la collection dans laquelle vous souhaitez modifier un rôle.

4 Cliquez sur l'onglet **Rôle**.

5 Sélectionnez le rôle à modifier.

6 Cliquez sur **Opérations** > **Associations de membres**.

7 (Facultatif) Si vous souhaitez ajouter un membre au rôle, procédez comme suit :

   7a Dans le champ **Nom**, spécifiez le nom de l'objet à ajouter (un objet Utilisateur, Groupe ou Conteneur) et le contexte.

   7b Dans le champ **Étendue**, spécifiez le nom et le contexte de l'objet Organisation ou Unité organisationnelle.

   7c Cliquez sur **Ajouter**.

8 (Facultatif) Si vous souhaitez supprimer un membre du rôle, procédez comme suit :

   8a Dans la liste des membres actuels du rôle, sélectionnez le membre à supprimer.

   8b Cliquez sur **Retirer**.

9 Une fois terminé, cliquez sur **OK**, puis à nouveau sur **OK**.

10 Cliquez sur **Fermer**.

Suppression d'un objet Services basés sur le rôle

1 Dans iManager, cliquez sur le bouton **Configurer** .

2 Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.

3 Cliquez sur la collection dans laquelle vous souhaitez supprimer un rôle RBS.

4 Cliquez sur l'onglet **Rôle**.

5 Sélectionnez le rôle à modifier.

6 Cliquez sur **Supprimer**.

7 Cliquez sur **OK**.

8 Dès que vous avez fini, cliquez sur **OK**.

9 Cliquez sur **Fermer**.

Définition de tâches RBS personnalisées

- « Création d'une tâche iManager » page 118
- « Modification de l'assignation des rôles » page 118
- « Suppression d'une tâche » page 119

Création d'une tâche iManager

1 Dans iManager, cliquez sur le bouton **Configurer** .

2 Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.

3 Cliquez sur la collection dans laquelle vous souhaitez créer une tâche.

4 Cliquez sur l'onglet **Tâche**.

5 Cliquez sur **Nouveau** > **Tâche iManager**.

6 Suivez les instructions du Générateur de tâches pour créer une tâche personnalisée.

Modification de l'assignation des rôles

1 Dans iManager, cliquez sur le bouton **Configurer** .

2 Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.

3 Cliquez sur la collection dans laquelle vous souhaitez modifier une tâche.

4 Cliquez sur l'onglet **Tâche**.

5 Sélectionnez la tâche à modifier.

6 Cliquez sur **Opérations** > **Assignation de rôle**.

7 Déplacez les rôles souhaités de la colonne **Rôles disponibles** vers la colonne **Rôles assignés**.

8 Cliquez sur **OK**, puis à nouveau sur **OK**.

9 Cliquez sur **Fermer**.

Suppression d'une tâche

1 Dans iManager, cliquez sur le bouton **Configurer** .

2 Cliquez sur **Services basés sur le rôle** > **Configuration RBS**.

3 Cliquez sur la collection dans laquelle vous souhaitez supprimer une tâche.

4 Cliquez sur l'onglet **Tâche**.

5 Sélectionnez la tâche à supprimer.

6 Cliquez sur **Supprimer**.

7 Cliquez sur **OK**.

8 Dès que vous avez fini, cliquez sur **OK**.

9 Cliquez sur **Fermer**.

4 Gestion des processus en arrière-plan

Pour prendre en charge des environnements dynamiques de grande envergure, eDirectory fournit des options de configuration et des processus en arrière-plan optimisés permettant d'adapter vos systèmes en fonction de votre environnement.

Ce chapitre comprend les sections suivantes :

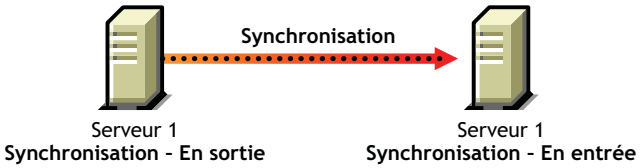
- « Synchronisation » page 121
- « Configuration des processus en arrière-plan » page 137

Synchronisation

La synchronisation est le transfert d'informations sur l'annuaire d'une réplique vers une autre, pour garantir la cohérence des deux partitions. eDirectory garde automatiquement les serveurs de l'anneau de répliques synchronisés.

La synchronisation peut être entrante ou sortante. Par exemple, si les modifications de données doivent être synchronisées à partir des serveurs 1 et 2, le terme *sortant* désigne le processus de synchronisation envoyé du serveur 1 au serveur 2, tandis que le terme *entrant* désigne le processus de synchronisation reçu du serveur 1 par le serveur 2.

Figure 4-1 *Synchronisations entrante et sortante*



Il existe deux types de synchronisation :

- Synchronisation normale ou synchronisation des répliques
- Synchronisation de priorité

Le tableau ci-dessous compare les synchronisations normale et de priorité :

Tableau 4-1 *Comparaison entre la synchronisation normale (ou des répliques) et la synchronisation de priorité*

Synchronisation normale ou synchronisation des répliques	Synchronisation de priorité
Se déclenche en cas de modifications de données sur n'importe quel serveur de l'anneau de répliques. Pour plus d'informations, reportez-vous à la « Synchronisation normale ou des répliques » page 124.	Se déclenche uniquement en cas de modifications des données identifiées comme essentielles. Pour plus d'informations, reportez-vous à la « Synchronisation de priorité » page 126.

Synchronisation normale ou synchronisation des répliques	Synchronisation de priorité
Une fois les données modifiées, les changements sont enregistrés dans la mémoire tampon. La synchronisation normale débute environ 30 secondes après l'enregistrement des modifications.	Les changements apportés aux données essentielles ne sont pas enregistrés dans la mémoire tampon. La synchronisation de priorité débute immédiatement après la modification des données.
Principale synchronisation dans eDirectory. Elle s'opère, que la synchronisation de priorité soit activée ou non.	Processus complémentaire à la synchronisation normale. Bien que les attributs essentiels soient synchronisés par la synchronisation de priorité, ils le sont à nouveau par la synchronisation normale.
Peut s'opérer entre serveurs eDirectory 8.8 ou avec des serveurs qui hébergent des versions antérieures d'eDirectory.	S'opère uniquement entre des serveurs eDirectory 8.8 et versions ultérieures contenant la même partition.
N'échoue jamais à cause de ses caractéristiques. Pour plus d'informations, reportez-vous à la « Caractéristiques de la synchronisation » page 122.	Si la synchronisation de priorité échoue, les modifications des données essentielles sont synchronisées par la synchronisation normale. Pour plus d'informations, reportez-vous à la « Situations d'échec de la synchronisation de priorité » page 134.

REMARQUE : les informations de synchronisation de priorité sont disponibles dans les balises SYDL ou Détails de synchronisation des écrans de trace d'iMonitor, dstrace ou ndstrace.

Caractéristiques de la synchronisation

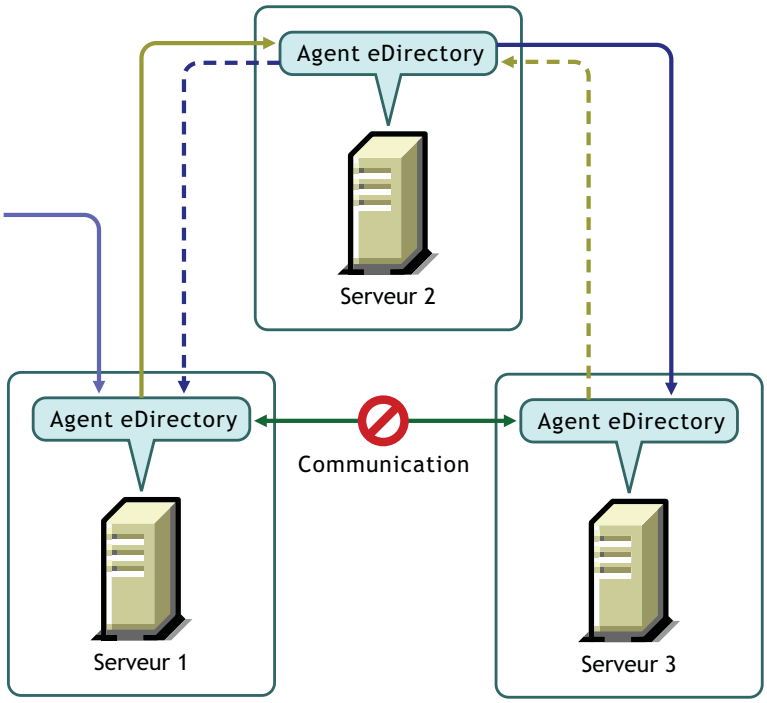
La synchronisation dans eDirectory :

- est transitive.
- gère le modèle de transactions d'objets.
- comporte des tampons horaires tels que le vecteur de transition (Transitive Vector), l'heure à laquelle les dernières modifications sont parvenues à la réplique locale (local received up to) et l'heure à laquelle elles sont parvenues à la réplique distante (remote received up to).

Synchronisation transitive

La synchronisation dans eDirectory est transitive. Cela signifie que eDirectory synchronise les modifications apportées aux données sans que l'agent eDirectory doive contacter directement tous les autres agents de l'anneau de répliques pour synchroniser les changements avec chacun d'entre eux.

Figure 4-2 *Synchronisation transitive*



Par exemple, si vous modifiez des données sur le serveur 1, les changements sont synchronisés du serveur 1 vers le serveur 2, puis du serveur 2 vers le serveur 3. Si le serveur 1 n'a pas pu entrer directement en contact avec le serveur 3 en raison d'un problème de communication, ce dernier reçoit malgré tout les modifications par le biais du serveur 2. Il le signale au serveur 2 qui, à son tour, indique au serveur 1 que le serveur 3 et lui-même sont synchronisés.

Modèle de transactions d'objets

La synchronisation dans eDirectory gère le modèle de transactions d'objets, une norme pour les annuaires compatibles X.500 et LDAP. Le modèle de transactions d'objets implique que toutes les transactions précédentes doivent être synchronisées avant que de nouvelles puissent l'être.

Imaginons, par exemple, que vous avez apporté les modifications D1, D2 et D3 aux données d'un serveur. En raison d'une défaillance réseau, ces modifications ne sont pas synchronisées sur les autres serveurs. Si vous apportez ensuite une modification D4 sur le serveur, celle-ci ne sera synchronisée qu'après la synchronisation de D1, D2 et D3 sur tous les serveurs de l'anneau de répliques.

Vecteur de transition

Un vecteur de transition est un tampon horaire pour une réplique. Ce tampon est constitué d'une représentation du nombre de secondes écoulées depuis un point de référence historique commun (1er janvier 1970), du numéro de réplique et du numéro d'événement en cours. Voici un exemple : s3D35F377 r02 e002

Pour plus d'informations, reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration » page 458.

Local Received Up To

Local Received Up To (LRUT) désigne l'heure à laquelle les dernières modifications sont parvenues à la réplique locale.

Pour plus d'informations, reportez-vous à la section « Exploration d'objets dans l'arborescence » page 257.

Remote Received Up To

Remote Received Up To (RRUT) désigne l'heure à laquelle les dernières modifications sont parvenues à la réplique distante.

Pour plus d'informations, reportez-vous à la section « Exploration d'objets dans l'arborescence » page 257.

Synchronisation normale ou des répliques

La synchronisation normale, également appelée synchronisation des répliques, désigne l'un des deux processus de synchronisation dans eDirectory. Elle synchronise toutes les modifications apportées aux données d'un serveur avec les autres serveurs de l'anneau de répliques.

La synchronisation normale s'opère sur tous les serveurs hébergeant une quelconque version d'eDirectory, qui possèdent la même partition.

Pour plus d'informations, reportez-vous à la « Gestion des répliques » page 155.

Vous pouvez activer ou désactiver la synchronisation normale en activant ou désactivant les synchronisations entrante et sortante dans NetIQ iMonitor. Par défaut, ces deux formes de synchronisation sont activées. Pour que les modifications apportées aux données soient synchronisées sur les différents serveurs par le biais de la synchronisation normale, vous devez configurer les paramètres de synchronisation dans iMonitor. Reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252 pour plus d'informations.

Avec la synchronisation normale, lorsque vous modifiez des données, les changements sont enregistrés dans la mémoire tampon avant d'être synchronisés sur les autres serveurs. Vous pouvez consulter l'état de synchronisation des serveurs de votre configuration dans iMonitor. Reportez-vous à la section « Exploration d'objets dans l'arborescence » page 257 pour plus d'informations.

La synchronisation normale est transitive et gère le modèle de transactions d'objets. Pour plus d'informations, reportez-vous aux sections “Synchronisation transitive” et “Modèle de transactions d'objets” à la page 101.

Configuration de la synchronisation normale

Vous pouvez configurer la synchronisation normale à l'aide de Configuration de l'agent sous Synchronisation de l'agent dans iMonitor.

Cette section contient les informations suivantes :

- « Activation/désactivation de la synchronisation normale » page 125
- « Activation/désactivation du cache en ligne » page 125
- « Threads de synchronisation » page 125
- « Méthode de synchronisation » page 125

Activation/désactivation de la synchronisation normale

Vous pouvez activer ou désactiver la synchronisation normale en activant ou désactivant les synchronisations entrante et sortante dans iMonitor. Reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252 pour plus d'informations.

La synchronisation sortante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données sur ce serveur ne seront pas synchronisées avec les autres serveurs. Vous pouvez indiquer, en heures, le délai pendant lequel la synchronisation sortante doit être désactivée. La valeur par défaut de ce paramètre est 24 heures, ce qui correspond également au délai maximal autorisé. Une fois le délai spécifié écoulé, les modifications apportées aux données sur ce serveur sont synchronisées avec les autres serveurs.

La synchronisation entrante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données sur d'autres serveurs ne seront pas synchronisées avec ce serveur.

Activation/désactivation du cache en ligne

Le cache de changement en ligne peut être activé ou désactivé pour un serveur. Cette option ne peut toutefois être désactivée que si la synchronisation sortante est elle-même désactivée. Si la synchronisation sortante est activée, le cache de changement en ligne l'est également.

La désactivation du cache de changement en ligne rend ce cache non valide pour cette réplique et affiche un drapeau non valide dans **Configuration de l'agent** > **Partitions**. Si le cache de changement en ligne est réactivé, le drapeau non valide est supprimé lors de la reconstruction du cache.

Threads de synchronisation

Pour la synchronisation sortante, vous devez configurer les threads de synchronisation. Dans iMonitor, vous pouvez spécifier le nombre de threads de synchronisation à l'aide de **Configuration de l'agent** sous **Synchronisation de l'agent**. Les valeurs possibles vont de 1 à 16. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252.

Méthode de synchronisation

En principe, eDirectory choisit automatiquement la méthode en fonction du nombre de répliques et de partenaires de réplication. Les différentes méthodes de synchronisation sont les suivantes :

- **Par partition :** les modifications apportées aux données sont synchronisées simultanément avec les autres répliques, à l'aide de plusieurs threads. Ainsi, si vous apportez les modifications D1, D2 et D3 aux données de la réplique R1 et que celles-ci doivent être synchronisées avec les répliques R2 et R3, elles le sont simultanément.
- **Par serveur:** les modifications apportées aux données sont synchronisées séquentiellement par le biais d'un seul thread. Si vous apportez les modifications D1, D2 et D3 aux données de la réplique R1 et que celles-ci doivent être synchronisées avec les répliques R2 et R3, D1 est d'abord synchronisée avec R2 et R3, puis D2, et ainsi de suite.
- **Par ajustement dynamique :** eDirectory choisit automatiquement la méthode de synchronisation en fonction des ressources système allouées.

Dans iMonitor, vous pouvez spécifier la méthode de synchronisation à l'aide de **Configuration de l'agent** sous **Synchronisation de l'agent**. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252.

REMARQUE : dans eDirectory 9.0 ou version ultérieure, le contrôleur de synchronisation (skulker) lance immédiatement la synchronisation sans délai dès que la transaction de données s'est terminée correctement. Ceci peut avoir une incidence sur les performances des opérations eDirectory. Pour optimiser les performances des opérations eDirectory, vous pouvez introduire un délai de synchronisation en exportant la variable d'environnement `NDSD_CC_SKULK_DELAY`. Les valeurs de cette variable ne peuvent être entrées qu'en secondes, comme illustré dans l'exemple ci-dessous :

```
NDSD_CC_SKULK_DELAY=<SECONDS>
NDSD_CC_SKULK_DELAY=5
```

Dans l'exemple ci-dessus, la synchronisation des données entre les serveurs eDirectory a été reportée de 5 secondes. La synchronisation immédiate n'affecte pas la planification si la synchronisation est déjà en cours.

Synchronisation de priorité

La synchronisation de priorité désigne l'un des deux processus de synchronisation dans eDirectory. Elle permet de synchroniser vos données critiques immédiatement sans attendre la synchronisation normale.

La synchronisation de priorité est complémentaire au processus de synchronisation normal dans eDirectory. Contrairement à cette dernière, pour la synchronisation de priorité, les changements ne sont pas enregistrés dans la mémoire tampon avant d'être synchronisés sur les autres serveurs, ce qui accélère le processus.

Vous pouvez synchroniser vos données critiques à l'aide de la synchronisation de priorité si vous ne pouvez pas attendre la synchronisation normale. La synchronisation de priorité est plus rapide que la synchronisation normale. Elle est prise en charge uniquement entre plusieurs serveurs eDirectory 8.8 (ou versions ultérieures) hébergeant la même partition.

Le tableau suivant liste les plates-formes prenant en charge la synchronisation de priorité :

Fonction	Linux	Windows
Synchronisation de priorité	✓	✓

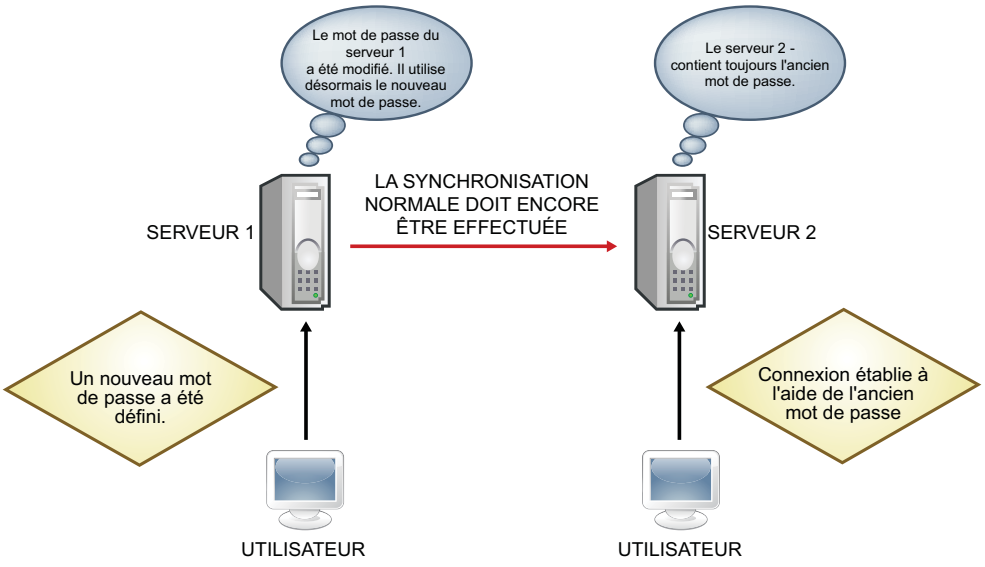
Cette section présente les informations suivantes :

- « Avantage de la synchronisation de priorité » page 126
- « Utilisation de la synchronisation de priorité » page 127

Avantage de la synchronisation de priorité

La synchronisation normale peut prendre un certain temps, pendant lequel les données modifiées ne sont pas disponibles sur d'autres serveurs. Supposons, par exemple, que votre configuration contienne différentes applications qui communiquent avec l'annuaire. Vous modifiez votre mot de passe sur le Server1. Avec la synchronisation normale, un certain temps s'écoule avant que ce changement ne soit synchronisé avec le Server2. Par conséquent, un utilisateur pourra toujours s'authentifier à l'annuaire via une application dialoguant avec le Server2, à l'aide de l'ancien mot de passe.

Figure 4-3 Avantage de la synchronisation de priorité



Dans les déploiements à grande échelle, lorsque les données critiques d'un objet sont modifiées, les changements doivent être synchronisés immédiatement. Le processus de synchronisation de priorité résout ce problème.

Utilisation de la synchronisation de priorité

Pour synchroniser des modifications de données via la synchronisation de priorité, vous devez procéder comme suit :

1. Activez la synchronisation de priorité, configurez le nombre de threads et la taille de la file d'attente de la synchronisation de priorité via iMonitor.
2. Définissez les règles de synchronisation de priorité en identifiant les attributs critiques via iManager.
3. Appliquez les règles de synchronisation de priorité aux partitions via iManager.

La synchronisation de priorité est activée par défaut. Reportez-vous à la section « Activation/désactivation de la synchronisation de priorité entrante/sortante » page 128 pour plus d'informations.

Pour synchroniser les modifications apportées aux données essentielles par le biais de la synchronisation de priorité :

1 Spécifiez le nombre de threads pour la synchronisation de priorité.

Pour plus d'informations, reportez-vous à la section « Synchronisation de priorité - Threads » page 128.

2 Spécifiez la taille de la file d'attente pour la synchronisation de priorité.

Pour plus d'informations, reportez-vous à la section « Synchronisation de priorité - Taille de la file d'attente » page 129.

3 Créez et définissez une règle de synchronisation de priorité en identifiant les attributs essentiels à synchroniser en priorité.

Pour plus d'informations, reportez-vous à la section « Création et définition d'une règle de synchronisation de priorité » page 131.

4 Appliquez la règle de synchronisation de priorité à une ou plusieurs partitions.

   Pour plus d'informations, reportez-vous à la section « Application d'une règle de synchronisation de priorité » page 132.

Le processus de synchronisation de priorité vise uniquement la synchronisation des modifications apportées aux attributs essentiels. La synchronisation de priorité gère le modèle de transactions d'objets. Dès lors, si des données non essentielles ont été modifiées et ne sont pas encore synchronisées et que des données essentielles sont changées pour la même entrée, les premières et les secondes sont synchronisées simultanément.

Par exemple, un utilisateur possède les attributs suivants : Salaire, N° employé, Adresse et N° unité. Vous identifiez Salaire et Adresse comme attributs essentiels. N° employé et N° unité ont été modifiés, mais ne sont pas encore synchronisés. Lorsque les modifications de Salaire et Adresse sont synchronisées par le biais de la synchronisation de priorité, N° employé et N° unité le sont également, bien qu'ils ne soient pas identifiés comme essentiels.

Cette section fournit les informations suivantes :

- « Activation/désactivation de la synchronisation de priorité entrante/sortante » page 128
- « Synchronisation de priorité - Threads » page 128
- « Synchronisation de priorité - Taille de la file d'attente » page 129
- « Gestion des règles de synchronisation de priorité » page 129
- « Situations d'échec de la synchronisation de priorité » page 134

Activation/désactivation de la synchronisation de priorité entrante/sortante

Dans eDirectory, vous pouvez activer ou désactiver la synchronisation de priorité entrante et/ou sortante à l'aide d'iMonitor. Reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252 pour plus d'informations.

La synchronisation de priorité entrante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données essentielles sur les autres serveurs ne sont pas synchronisées avec ce serveur par le biais de la synchronisation de priorité. Elles le sont toutefois par le processus de synchronisation normale.

La synchronisation de priorité sortante est activée par défaut. Si l'option est désactivée pour un serveur, les modifications apportées aux données essentielles sur ce serveur ne sont pas synchronisées avec les autres serveurs par le biais de la synchronisation de priorité. Elles le sont toutefois par le processus de synchronisation normale.

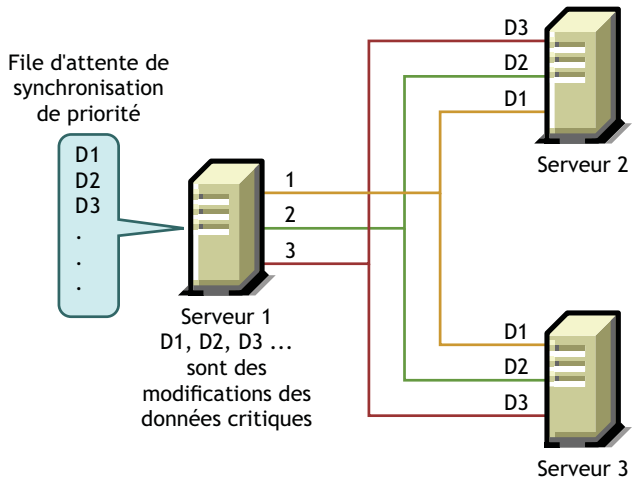
Synchronisation de priorité - Threads

Vous devez configurer le nombre de threads à utiliser pour la synchronisation de priorité sortante. Dans iMonitor, vous pouvez spécifier le nombre de threads de synchronisation de priorité à l'aide de **Configuration de l'agent** sous **Synchronisation de l'agent**. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252. Les valeurs prises en charges sont comprises entre 1 et 32. La valeur par défaut est 4.

Synchronisation de priorité - Taille de la file d'attente

Ce paramètre indique le nombre maximal d'entrées essentielles modifiées que la file d'attente peut contenir avant de les synchroniser. Dès que vous modifiez les entrées essentielles, elles s'ajoutent dans la file d'attente de la synchronisation de priorité et sont synchronisées l'une après l'autre. Imaginons, par exemple, que D1, D2 et D3 sont les entrées essentielles modifiées sur le serveur 1 et qu'elles doivent être synchronisées sur les serveurs 2 et 3 par la synchronisation de priorité. D1 est synchronisée avec les serveurs 2 et 3, puis D2 est synchronisée et enfin, D3. Si une entrée antérieure de la file d'attente n'est pas correctement synchronisée avec l'un des serveurs, cela n'affecte pas la synchronisation des autres entrées.

Figure 4-4 *File d'attente de la synchronisation de priorité*



Vous pouvez spécifier la taille de la file d'attente pour la synchronisation de priorité dans iMonitor à l'aide de **Configuration de l'agent** sous **Synchronisation de l'agent**. Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252.

Lors d'un processus de synchronisation de priorité, si plusieurs modifications sont apportées en peu de temps, la file d'attente risque d'atteindre sa taille maximale. Dans ce cas, elle expire et une nouvelle file d'attente est formée. Les modifications dans l'ancienne file d'attente qui n'ont pas encore été synchronisées le seront par la synchronisation normale.

La taille de la file d'attente pour la synchronisation de priorité peut être comprise entre 0 et 2^{32} - 1. Par défaut, elle est de 2^{32} -1. Si la taille de la file d'attente de la synchronisation de priorité est définie sur 0, les modifications ne sont pas synchronisées par cette synchronisation. Elles le sont toutefois par la synchronisation normale.

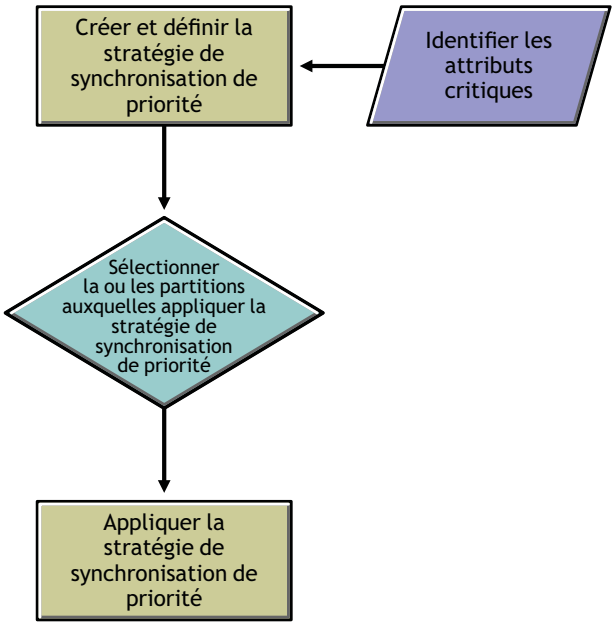
La valeur -1 implique une taille de file d'attente illimitée. -1 correspond à 2^{32} - 1. Si une valeur négative est spécifiée, -3 par exemple, cela signifie -3 = -1-2, ce qui correspond à 2^{32} - 1-2.

Gestion des règles de synchronisation de priorité

Pour gérer la synchronisation de priorité, vous pouvez créer et définir des règles et les appliquer à des partitions via iManager ou LDAP. Vous définissez une stratégie de synchronisation de priorité en identifiant les attributs qui sont essentiels.

REMARQUE : les plug-ins sont uniquement disponibles dans NetIQ iManager 2.6 et versions ultérieures.

Figure 4-5 *Processus de synchronisation de priorité*



Par exemple, si les attributs Mot de passe et Numéro de compte sont essentiels, vous pouvez créer une règle de synchronisation de priorité PS1 qui contient ces attributs. Vous pouvez ensuite appliquer cette règle à une partition P1. Si vous modifiez le mot de passe ou le numéro de compte d'une entrée sur un serveur, les changements sont immédiatement synchronisés avec les autres serveurs qui ont la partition P1.

Pour que la synchronisation de priorité s'effectue, vous devez vérifier que les synchronisations de priorité entrante et sortante sont activées dans iMonitor. Elles le sont par défaut. Si vous désactivez les synchronisations de priorité entrante et sortante, les modifications apportées aux données sont synchronisées par la synchronisation normale.

Pour plus d'informations, reportez-vous à la section « Contrôle et configuration de l'agent DS » page 252.

Cette section contient les informations suivantes :

- « Création et définition d'une règle de synchronisation de priorité » page 131
- « Édition d'une règle de synchronisation de priorité » page 131
- « Application d'une règle de synchronisation de priorité » page 132
- « Suppression d'une règle de synchronisation de priorité » page 133

Lorsque vous créez une partition enfant, la règle de synchronisation de priorité appliquée au parent est héritée par la partition enfant. Lorsque vous fusionnez des partitions, la stratégie de synchronisation de priorité du parent est conservée.

Création et définition d'une règle de synchronisation de priorité

Pour définir une règle de synchronisation de priorité, vous pouvez sélectionner les attributs directement ou par le biais d'une classe d'objet. Dans ce dernier cas, tous les attributs de la classe d'objet sont sélectionnés pour la synchronisation de priorité. Vous pouvez sélectionner les attributs obligatoires ou facultatifs pour cette synchronisation de priorité.

La règle de synchronisation de priorité peut être créée n'importe où dans l'arborescence eDirectory à l'aide d'iManager ou de LDAP.

À l'aide d'iManager :

1. Cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Stratégies de synchronisation de priorité**.
3. Dans l'Assistant de gestion des stratégies de synchronisation de priorité, sélectionnez **Créer, éditer et appliquer la stratégie**.
4. Cliquez sur **Suivant**.
5. Suivez les instructions de l'Assistant de création d'une règle de synchronisation de priorité pour créer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

À l'aide de LDAP :

Pour créer une règle de synchronisation de priorité vide :

```
dn:cn=policy1,o=policies

changetype:add

objectclass:prsyncpolicy
```

Pour définir la règle de synchronisation de priorité en marquant les attributs pour la synchronisation de priorité :

```
dn:cn=policy2,o=policies

changetype:add

objectclass:prsyncpolicy

prsyncattributes:description
```

Dans l'exemple ci-dessus, Description désigne l'attribut marqué pour la synchronisation de priorité.

Édition d'une règle de synchronisation de priorité

Vous pouvez éditer un objet Règle de synchronisation de priorité à l'aide d'iManager ou de LDAP.

À l'aide d'iManager :

1. Cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Stratégies de synchronisation de priorité**.
3. Dans l'Assistant de gestion des stratégies de synchronisation de priorité, sélectionnez **Éditer la stratégie**.
4. Cliquez sur **Suivant**.

5 Suivez les instructions de l'Assistant d'édition de la règle de synchronisation de priorité pour éditer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

À l'aide de LDAP :

Dans l'exemple suivant, la règle de synchronisation de priorité est modifiée en marquant Surname (Nom de famille) pour la synchronisation de priorité au lieu de Description.

```
dn:cn=policy2,o=policies

changetype:modify

add:prsyncattributes

prsyncattributes:surname
```

Pour supprimer de la règle de synchronisation de priorité un attribut marqué pour la synchronisation de priorité :

```
dn:cn=policy2,o=policies

changetype:modify

add:prsyncattributes

prsyncattributes:description
```

Dans l'exemple ci-dessus, l'attribut Description est supprimé de la règle de synchronisation de priorité.

Application d'une règle de synchronisation de priorité

Vous pouvez appliquer une stratégie de synchronisation de priorité à plusieurs partitions, mais une seule stratégie par partition.

Vous pouvez appliquer une règle de synchronisation de priorité à une partition à l'aide d'iManager ou de LDAP.

À l'aide d'iManager :

1 Cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Gestion des partitions et des répliques** > **Stratégies de synchronisation de priorité**.
3 Dans l'Assistant de gestion des stratégies de synchronisation de priorité, sélectionnez **Créer, éditer et appliquer la stratégie**.
4 Suivez les instructions de l'Assistant d'application de la règle de synchronisation de priorité pour appliquer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

À l'aide de LDAP :

Pour appliquer une règle de synchronisation de priorité à une partition racine :

```
dn:

changetype:modify

add:prsyncpolicydn

prsyncpolicydn:cn=policy2,o=policies
```

Dans l'exemple ci-dessus, la règle policy2 est appliquée à la partition racine.

Pour appliquer une règle de synchronisation de priorité à une partition non racine :

```
dn:o=org
changetype:modify
add:prsyncpolicydn
prsyncpolicydn:cn=policy2,o=policies
```

Dans l'exemple ci-dessus, la règle policy2 est appliquée à la partition non racine.

Pour remplacer une règle de synchronisation de priorité pour une partition non racine :

```
dn:o=org
changetype:modify
replace:prsyncpolicydn
prsyncpolicydn:cn=policy1,o=policies
```

Dans l'exemple ci-dessus, la règle policy2 est remplacée par la règle policy1.

Pour dissocier une règle de synchronisation de priorité d'une partition non racine :

```
dn:o=org
changetype:modify
delete:prsyncpolicydn
```

Dans l'exemple ci-dessus, la règle de synchronisation de priorité est dissociée de la partition non racine O=Org.

Suppression d'une règle de synchronisation de priorité

Vous pouvez supprimer une règle de synchronisation de priorité à l'aide d'iManager ou de LDAP.

À l'aide d'iManager :

1. Cliquez sur le bouton **Rôles et tâches**  .
2. Cliquez sur **Gestion des partitions et des répliques** > **Stratégies de synchronisation de priorité**.
3. Dans l'Assistant de gestion des stratégies de synchronisation de priorité, sélectionnez **Supprimer les stratégies**.
4. Suivez les instructions de l'Assistant de suppression de la règle de synchronisation de priorité pour supprimer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

À l'aide de LDAP :

```
dn:cn=policy1,o=policies
changetype:delete
```

REMARQUE : pour plus d'informations sur la création et la gestion des stratégies de synchronisation de priorité, reportez-vous à la « Utilisation des outils LDAP sous Linux » page 377 et à la « Utilitaire Importation/Conversion/Exportation NetIQ » page 165.

Situations d'échec de la synchronisation de priorité

La synchronisation de priorité peut échouer dans l'une des situations suivantes :

- Échec réseau : la synchronisation de priorité n'enregistre pas les modifications si elle ne parvient pas à les envoyer au serveur distant en raison d'un échec réseau.
- La taille de la file d'attente de la synchronisation de priorité atteint son maximum : la synchronisation de priorité ignore les changements dans la file d'attente de la synchronisation de priorité si le nombre d'entrées dépasse la taille de cette file d'attente.
- Échec de la synchronisation de schéma : si le schéma n'est pas synchronisé, le processus de synchronisation de priorité échoue.
- L'objet n'existe pas sur d'autres serveurs : si la création de l'objet à proprement parler n'est pas synchronisée, la synchronisation de priorité échoue.
- Mélange de serveurs dans l'anneau de répliques : si vous disposez à la fois de serveurs eDirectory 8.8 et versions antérieures, la synchronisation de priorité échoue.

Lorsque la synchronisation de priorité échoue pour l'une des raisons susmentionnées, les changements apportés aux données essentielles sont synchronisés par le processus normal.

Réplication basée sur des stratégies

La réplication dans eDirectory respecte une topologie en maille par défaut. Cela signifie que toutes les répliques d'un anneau de répliques peuvent être entrantes ou sortantes. Le modèle de maillage n'est pas forcément idéal dans tous les environnements. La *réplication basée sur des stratégies* permet aux administrateurs de configurer la topologie de réplication pour optimiser le trafic de réplication.

Pour configurer la topologie de réplication, créez un fichier de stratégie et spécifiez la stratégie pour toutes les partitions dans un seul fichier avant de le copier sur les serveurs requis.

Sous Linux

Créez le fichier de stratégie au format XML, nommez-le `selectivesync.xml` et stockez-le avec le fichier `nds.conf`.

Voici un exemple de définition XML d'une stratégie :

```
<?xml version="1.0" encoding="utf-8" ?>

<SelectiveSync   xmlns="http://www.novell.com/nds"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.novell.com/nds     file:/opt/novell/eDirectory/
lib64/nds-schema/xsd/selectivesync.xsd" config-version="0.1">

    <Partition DN=".novell.TREE.">

         <SourceServer DN=".server1.novell.TREE.">

                <SyncronizeTo>.server2.novell.TREE.</SyncronizeTo>

         </SourceServer>

         <SourceServer DN=".server2.novell.TREE.">

                <SyncronizeTo>.server3.novell.TREE.</SyncronizeTo>

         </SourceServer>
```

```
        <SourceServer DN=".server3.novell.TREE.">

                <SyncronizeTo>.server1.novell.TREE.</SyncronizeTo>

        </SourceServer>

    </Partition>

</SelectiveSync>
```

Sous Windows

Créez le fichier de stratégie au format XML et nommez-le `selectivesync.xml` à l'emplacement d'installation (par exemple, `C:\Novell\NDS`).

Voici un exemple de définition XML d'une stratégie :

```
<?xml version="1.0" encoding="utf-8" ?>

<SelectiveSync   xmlns="http://www.novell.com/nds"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.novell.com/nds
C:\Novell\NDS\selectivesync.xsd" config-version="0.1">

    <Partition DN=".novell.TREE.">

        <SourceServer DN=".server1.novell.TREE.">

                <SyncronizeTo>.server2.novell.TREE.</SyncronizeTo>

        </SourceServer>

        <SourceServer DN=".server2.novell.TREE.">

                <SyncronizeTo>.server3.novell.TREE.</SyncronizeTo>

        </SourceServer>

        <SourceServer DN=".server3.novell.TREE.">

                <SyncronizeTo>.server1.novell.TREE.</SyncronizeTo>

        </SourceServer>

    </Partition>

</SelectiveSync>
```

Notez que sous Windows, il n'existe pas de fichier spécifiant le chemin d'accès xsd.

Configuration manuelle des threads de synchronisation

Il est possible d'augmenter manuellement les threads créés pour la réplication simultanée sur plusieurs serveurs en configurant le nombre maximal de threads créés. Ce paramètre s'applique à toutes les partitions d'un serveur.

Pour configurer le nombre maximal de threads créés :

1. Connectez-vous à iMonitor.
2. Accédez à **Configuration de l'agent** > **Synchronisation de l'agent**.
3. Le cas échéant, dans la section **Méthode de synchronisation**, sélectionnez **par serveur**.

4 Dans la section **Threads de synchronisation système**, sélectionnez **désactivé**.

5 Dans la section **Nombre max. de threads de synchronisation des paramètres manuels**, définissez le nombre de threads désirés.

Synchronisation système

Dans la synchronisation système, le nombre de threads du contrôleur de synchronisation est calculé à l'aide des deux formules suivantes :

- **En mode partition** : nombre de threads du contrôleur de synchronisation = nombre de partitions sur ce serveur
- **En mode serveur** : nombre de threads du contrôleur de synchronisation = (nombre de serveurs connus sur le serveur + 1)/2

Si l'option **Nombre max. de threads de synchronisation système** est désactivée, les deux formules ci-dessus ne seront pas utilisées. La valeur spécifiée pour **Nombre max. de threads de synchronisation des paramètres manuels** sera utilisée à la place.

Par exemple, imaginons une configuration avec 5 serveurs et 3 partitions. Si vous activez **Nombre max. de threads de synchronisation système** : en mode partition, un serveur peut créer un maximum de 3 threads de contrôleur de synchronisation et également de 3 threads de contrôleur de synchronisation en mode serveur. Toutefois, s'il existe un maximum de 3 threads de contrôleur de synchronisation, un serveur ne peut pas envoyer de mises à jour aux 4 autres serveurs sur toutes les partitions en parallèle. Dans ce cas, désactivez **Nombre max. de threads de synchronisation système**, puis augmentez le nombre de threads de contrôleur de synchronisation dans **Nombre max. de threads de synchronisation des paramètres manuels**.

Nombre maximal de threads de contrôleur de synchronisation

Si vous définissez **Nombre max. de threads de synchronisation des paramètres manuels** sur 12, un seul serveur peut envoyer des mises à jour à tous les serveurs sur toutes les partitions en parallèle. Toutefois, cette configuration ne peut pas créer plus de 12 threads de contrôleur de synchronisation en mode serveur et 3 threads de contrôleur de synchronisation en mode partition même si **Nombre max. de threads de synchronisation des paramètres manuels** est défini sur une valeur supérieure à 12.

Configuration de la synchronisation sortante asynchrone

Dans les versions précédentes d'eDirectory, la synchronisation sortante d'un serveur vers un autre était effectuée séquentiellement par un seul thread, et la réplication des changements prenait du temps.

eDirectory inclut un thread qui analyse le cache de changement et prépare les paquets à envoyer à l'autre serveur, puis remplit une file d'attente de paquets. Un autre thread prélève les paquets et les envoie sur l'autre serveur un par un permettant ainsi une optimisation de la synchronisation et un gain de temps.

Pour configurer la synchronisation sortante d'un serveur vers un autre :

1 Connectez-vous à iMonitor.

2 Accédez à **Configuration de l'agent** > **Paramètres des processus en arrière-plan**.

3 Dans la section **Paramètres de synchronisation sortante asynchrones**, sélectionnez **Activer**.

REMARQUE : l'activation de la synchronisation sortante asynchrone peut entraîner une utilisation accrue du processeur et des E/S au niveau du serveur de réception. Pour éviter ce problème, vous pouvez définir un retard dans l'envoi des paquets en spécifiant un intervalle de retard dans **Délai de répartiteur asynchrone de threads**. Vous pouvez définir ce délai entre 0 et 999 millisecondes. La valeur par défaut est zéro milliseconde.

Configuration des processus en arrière-plan

Vous pouvez contrôler la vitesse des processus en arrière-plan du contrôleur de synchronisation, du purgeur et de la notice nécrologique à l'aide de l'un des paramètres suivants :

- UC : spécifie le pourcentage maximal de ressources informatiques et le délai entre deux exécutions du même processus (contrôleur de synchronisation, purgeur et notice nécrologique).
- Limite stricte : spécifie un paramètre de délai statique pour chacun des processus de contrôleur de synchronisation (skulker), purgeur et notice nécrologique.

Pour plus d'informations sur la configuration des processus en arrière-plan, reportez-vous à la section « Configuration des processus en arrière-plan » page 255.

Stratégie de limite stricte

La stratégie de limite stricte est activée par défaut. Les processus en arrière-plan traitent un certain nombre d'objets et se mettent ensuite en veille pour un intervalle de 100 millisecondes (valeur par défaut). Vous pouvez réduire le délai (de mise en veille) afin d'améliorer les performances du système. Vous pouvez augmenter l'utilisation du processeur, lorsque le délai est proche de 0 milliseconde et si un ou plusieurs de ces processus s'exécutent en arrière-plan. Vous devez la surveiller et l'ajuster en conséquence.

Stratégie dynamique basée sur l'UC

La stratégie basée sur l'UC permet au système d'ajuster dynamiquement le délai des trois processus en arrière-plan suivants pour limiter l'utilisation maximum de l'UC :

- Modifier le délai de traitement du cache (qui fait partie de la synchronisation sortante)
- Délai de la procédure Obit (processus de la notice nécrologique)
- Délai de l'outil de purge (nettoyage du cache de changement)

Le système réduit automatiquement l'utilisation de l'UC au niveau configuré. Une charge client élevée ralentit les processus en arrière-plan tandis qu'une charge client réduite augmente leur vitesse de traitement. Si vous ne souhaitez pas de ralentissement des processus en arrière-plan, vous pouvez configurer la limite maximale de délai en réduisant l'intervalle de mise en veille dans cette stratégie. Toutefois, la définition d'un intervalle de mise en veille réduit risque d'entraîner une violation des restrictions de l'UC.

Intervalle des processus en arrière-plan

Vous pouvez définir des valeurs d'intervalle pour les processus en arrière-plan suivants :

- Intervalle de lien en amont/DRL
- Intervalle de nettoyage

- Intervalle de synchronisation extérieure
- Intervalle de synchronisation des schémas
- Intervalle du nettoyeur
- Intervalle de l'outil de purge

Pour configurer les intervalles de processus en arrière-plan :

1. Connectez-vous à iMonitor.
2. Accédez à **Configuration de l'agent** > **Paramètres des processus en arrière-plan**.
3. Dans la section **Intervalle du processus en arrière-plan**, indiquez une valeur pour l'intervalle.

5 Gestion du schéma

Le schéma de votre arborescence NetIQ eDirectory définit les classes d'objet (par exemple, Utilisateurs, Groupes et Imprimantes) que peut contenir cette arborescence. Il désigne les attributs (propriétés) qui composent chaque type d'objet, à savoir ceux qui sont requis lors de la création de l'objet et ceux qui sont facultatifs.

Chaque objet eDirectory appartient à une classe d'objet qui spécifie les attributs qui peuvent être associés à l'objet. Tous les attributs sont basés sur un ensemble de types d'attribut, eux-mêmes basés sur un ensemble standard de syntaxes d'attribut.

Le schéma eDirectory contrôle non seulement la structure des différents objets, mais aussi les relations entre les objets dans l'arborescence eDirectory. Les règles de schéma autorisent des objets définis à contenir d'autres objets subordonnés. Le schéma définit ainsi la structure de l'arborescence eDirectory.

Vous pouvez avoir besoin de modifier votre schéma en fonction de l'évolution des besoins d'informations de votre entreprise. Par exemple, si vous avez besoin aujourd'hui d'un numéro de télécopie pour un objet Utilisateur, alors que vous n'en avez jamais demandé auparavant, vous pouvez créer une classe Utilisateur pour laquelle le numéro de télécopie est un attribut obligatoire, puis l'utiliser pour créer des objets Utilisateur.

Le rôle Gestion du schéma de NetIQ iManager vous permet, si vous disposez du droit Superviseur sur une arborescence, de personnaliser le schéma de cette arborescence et d'exécuter les tâches suivantes :

- Afficher la liste de toutes les classes et de tous les attributs du schéma
- Étendre le schéma par l'ajout d'une classe ou d'un attribut
- Créer une classe en lui attribuant un nom, et en définissant les attributs, indicateurs et conteneurs auxquels la classe peut être ajoutée, ainsi que les classes parent dont elle peut hériter les attributs.
- Créer un attribut en lui attribuant un nom et en spécifiant sa syntaxe et ses indicateurs
- Ajouter un attribut à une classe existante
- Supprimer une classe ou un attribut qui n'est pas utilisé ou qui est devenu obsolète.
- Identifier et résoudre les problèmes éventuels

Ce chapitre contient des informations sur les rubriques suivantes :

- « Extension du schéma » page 140
- « Affichage du schéma » page 144
- « Extension manuelle du schéma » page 145
- « Drapeaux de schéma ajoutés à eDirectory 8.7 et versions ultérieures » page 147
- « Utilisation du client pour effectuer des opérations sur le schéma » page 148

Pour plus d'informations sur les schémas, reportez-vous au *NetIQ eDirectory Schema Reference* (http://developer.novell.com/documentation/ndslib/schm_enu/data/h4q1mn1i.html) (Référence des schémas NetIQ eDirectory).

Extension du schéma

Vous pouvez étendre le schéma d'une arborescence en créant une nouvelle classe ou un nouvel attribut. Pour étendre le schéma de votre arborescence eDirectory, vous devez disposez du droit Superviseur pour l'ensemble de l'arborescence.

Les opérations suivantes permettent d'étendre le schéma :

- Création d'une classe
- Suppression d'une classe
- Création d'un attribut
- Ajout d'un attribut facultatif à une classe
- Suppression d'un attribut

Les opérations suivantes permettent d'étendre le schéma pour les attributs auxiliaires :

- Création d'une classe auxiliaire
- Extension d'un objet avec les propriétés d'une classe auxiliaire
- Modification des propriétés auxiliaires d'un objet
- Suppression des propriétés auxiliaires d'un objet

Création d'une classe

Vous pouvez ajouter une classe au schéma existant en fonction de l'évolution des besoins de votre organisation.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Schéma** > **Créer une classe**.
3. Suivez les instructions de l'Assistant de création de classes pour définir la classe d'objet.

   L'assistant fournit l'aide nécessaire tout au long de la procédure.

   Pour définir des propriétés personnalisées à ajouter à la classe d'objet, vous devez au préalable quitter l'assistant. Pour plus d'informations, reportez-vous à la section Création d'un attribut.

Suppression d'une classe

Vous pouvez supprimer les classes inutilisées qui ne font pas partie du schéma de base de l'arborescence eDirectory. iManager vous empêche uniquement de supprimer les classes en cours d'utilisation dans les partitions localement répliquées.

Vous pouvez également supprimer une classe du schéma dans les cas suivants :

- après la fusion de deux arborescences et la résolution des différences de classe ;
- chaque fois qu'une classe est devenue obsolète.

Pour supprimer une classe :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Schéma** > **Supprimer une classe**.
3. Sélectionnez la classe à supprimer.

Seules les classes dont la suppression est autorisée sont affichées.

4 Cliquez sur **Supprimer**.

Création d'un attribut

Vous pouvez définir des types d'attribut personnalisés et les ajouter en tant qu'attributs facultatifs aux classes d'objet existantes. Vous ne pouvez toutefois pas ajouter d'attributs obligatoires aux classes existantes.

REMARQUE : en raison d'un problème de réplication, les attributs dans eDirectory autres que le type d'attribut de flux ne peuvent pas contenir des valeurs supérieures à 60 Ko ou 30 000 caractères. Si un utilisateur ou une application définit la valeur d'un attribut binaire ou de chaîne et dépasse cette limite, eDirectory renvoie une erreur -649 indiquant que la valeur est trop longue.

Pour créer un nouvel attribut :

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Schéma** > **Créer un attribut**.

3 Suivez les instructions de l'Assistant de création d'attributs pour définir le nouvel attribut.

L'assistant fournit l'aide nécessaire tout au long de la procédure.

Ajout d'un attribut facultatif à une classe

Vous pouvez ajouter des attributs facultatifs aux classes existantes. Cette opération peut s'avérer nécessaire dans les cas suivants :

- Les besoins en information de votre entreprise changent.
- Vous vous préparez à fusionner les arborescences.

REMARQUE : Les attributs obligatoires ne peuvent être définis qu'au moment de la création d'une classe.

Pour ajouter un attribut facultatif à une classe :

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Schéma** > **Ajouter un attribut**.

3 Sélectionnez la classe à laquelle vous souhaitez ajouter un attribut, puis cliquez sur **OK**.

4 Dans la liste **Attributs facultatifs disponibles**, sélectionnez les attributs que vous voulez ajouter, puis cliquez sur ➡ pour les ajouter à la liste **Ajouter ces attributs facultatifs**.

Si vous ajoutez un attribut par erreur ou si vous changez d'avis, sélectionnez l'attribut dans la liste **Ajouter le ou les attributs facultatifs suivants**, puis cliquez sur ⬅ pour le supprimer de la liste des attributs à ajouter.

5 Cliquez sur **OK**.

Les objets de cette classe que vous créez possèdent maintenant les propriétés que vous avez ajoutées. Pour définir des valeurs pour les propriétés ajoutées, utilisez la page de propriétés générique Autre de l'objet.

SUGGESTION : vous pouvez modifier une classe existante en utilisant cette page pour faire des ajouts dans la liste **Attributs actuels**. Vous pouvez uniquement supprimer les attributs que vous avez ajoutés avant de cliquer sur **OK**. Vous ne pouvez pas supprimer les attributs qui ont déjà été ajoutés et enregistrés.

Suppression d'un attribut

Vous pouvez supprimer les attributs inutilisés qui ne font pas partie du schéma de base de l'arborescence eDirectory.

Vous pouvez également supprimer un attribut du schéma dans les cas suivants :

- Après la fusion de deux arborescences et la résolution des différences d'attribut
- chaque fois qu'un attribut est devenu obsolète.

Pour supprimer un attribut :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Schéma** > **Supprimer un attribut**.
3. Sélectionnez l'attribut à supprimer.

   Seuls les attributs dont la suppression est autorisée sont affichés.
4. Cliquez sur **Supprimer**.

Création d'une classe auxiliaire

Une classe auxiliaire est un ensemble de propriétés (attributs) ajouté à des instances d'objet eDirectory définies, et non à l'intégralité d'une classe d'objets. Par exemple, une application de messagerie pourrait étendre le schéma de votre arborescence eDirectory pour y inclure une classe auxiliaire Propriétés de messagerie, puis étendre chacun des objets avec ces propriétés, le cas échéant.

Grâce au Gestionnaire de schéma, vous pouvez définir vos propres classes auxiliaires. Vous pouvez ensuite étendre des objets distincts dotés des propriétés définies dans ces classes auxiliaires.

Pour créer une classe auxiliaire :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Schéma** > **Créer une classe**.
3. Spécifiez un nom de classe et un ID ASN1 (facultatif), puis cliquez sur **Suivant**.
4. Sélectionnez **Classe auxiliaire** lorsque vous définissez les drapeaux de classe, puis cliquez sur **Suivant**.
5. Suivez les instructions de l'Assistant de création de classes pour définir la nouvelle classe auxiliaire.

   L'assistant fournit l'aide nécessaire tout au long de la procédure.

Extension d'un objet avec les propriétés d'une classe auxiliaire

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Schéma** > **Extensions d'objet**.
3 Spécifiez le nom et le contexte de l'objet à étendre, puis cliquez sur **OK**.
4 Selon la présence ou non de la classe auxiliaire que vous souhaitez utiliser dans la liste **Extensions de classe auxiliaire actuelles**, effectuez l'action correspondante :

La classe auxiliaire apparaît-elle déjà dans la liste ?	Action :
Oui	Quittez cette procédure. Reportez-vous plutôt à la section « Modification des propriétés auxiliaires d'un objet » page 143.
Non	Cliquez sur **Ajouter**, sélectionnez la classe auxiliaire, puis cliquez sur **OK**.

5 Cliquez sur **Fermer**.

Modification des propriétés auxiliaires d'un objet

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
3 Spécifiez le nom et le contexte de l'objet à modifier, puis cliquez sur **OK**.
4 Sous l'onglet **Général**, cliquez sur la page **Autre**.
5 Dans l'écran qui apparaît, définissez les valeurs d'attributs de votre choix.
   - Double-cliquez sur un attribut non défini pour l'ajouter à la liste des attributs définis.
   - Sélectionnez un attribut défini, puis cliquez sur **Éditer** pour modifier l'attribut ou sur **Supprimer** pour le supprimer.
   - Vous devez connaître la syntaxe d'une propriété pour la définir correctement. Pour plus d'informations, reportez-vous au *NetIQ eDirectory Schema Reference* (http://developer.novell.com/documentation/ndslib/schm_enu/data/h4q1mn1i.html) (Référence des schémas NetIQ eDirectory).
6 Cliquez sur **Appliquer**, puis sur **OK**.

Suppression des propriétés auxiliaires d'un objet

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Schéma** > **Extensions d'objet**.
3 Spécifiez le nom et le contexte de l'objet à étendre, puis cliquez sur **OK**.
4 Dans la liste des extensions de classe auxiliaire actuelles, sélectionnez la classe auxiliaire dont vous souhaitez supprimer les propriétés.
5 Cliquez sur **Retirer**, puis sur **OK**.

Cette opération supprime la totalité des propriétés qui ont été ajoutées par la classe auxiliaire, à l'exception de celles que l'objet possède déjà de façon innée.

6 Cliquez sur **Fermer**.

Affichage du schéma

Vous pouvez afficher le schéma pour évaluer s'il répond bien aux besoins d'informations de la société. Plus votre entreprise est grande et sa structure complexe, plus la personnalisation du schéma est nécessaire. Cependant, même les petites entreprises peuvent avoir des besoins de suivi particuliers. Affichez le schéma pour vous aider à déterminer les éventuelles extensions à apporter au schéma de base.

Affichage des informations sur la classe

La page Informations sur la classe d'iManager fournit des informations sur la classe sélectionnée et vous permet d'ajouter des attributs. La plupart des informations figurant dans cette page ont été spécifiées lors de la création de la classe. Certains des attributs facultatifs peuvent avoir été ajoutés par la suite.

Au moment de la création de la classe, s'il a été spécifié que celle-ci devait hériter d'attributs d'une autre classe, ces attributs sont classés de la même façon que dans la classe parente. Si, par exemple, Classe d'objet est un attribut obligatoire de la classe parente, il apparaît à cet écran comme attribut obligatoire de la classe sélectionnée.

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Schéma** > **Informations sur la classe**.
3 Sélectionnez la classe pour laquelle vous souhaitez obtenir des informations, puis cliquez sur **Afficher**.

   Cliquez sur le pour plus d'informations.

Affichage des informations sur l'attribut

1 Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Schéma** > **Informations sur l'attribut**.
3 Sélectionnez l'attribut pour lequel vous souhaitez obtenir des informations, puis cliquez sur **Afficher**.

   Cliquez sur le pour plus d'informations.

Extension manuelle du schéma

Vous pouvez étendre manuellement le schéma eDirectory à l'aide des fichiers avec une extension `.sch`.

Ce chapitre comprend les informations suivantes :

- « Extension du schéma sous Windows » page 145
- « Extension du schéma sous Linux » page 145

Extension du schéma sous Windows

`NDSCons.exe` permet d'étendre le schéma sur les serveurs Windows. Les fichiers de schéma (`*.sch`) fournis avec eDirectory sont installés par défaut dans le répertoire `C:\Novell\NDS`.

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**.
2. Cliquez sur **install.dlm**, puis sur **Exécuter**
3. Cliquez sur **Installer d'autres fichiers de schéma**, puis cliquez sur **Suivant**.
4. Connectez-vous en tant qu'utilisateur doté de droits d'administrateur, puis cliquez sur **OK**.
5. Indiquez le nom du fichier de schéma et le chemin d'accès correspondant.
6. Cliquez sur **Terminer**.

Extension du schéma sous Linux

Les sections suivantes fournissent des informations relatives à l'extension de schéma sur les ordinateurs Linux :

- « Utilisation de l'utilitaire ndssch pour étendre le schéma sous Linux » page 145
- « Extension du schéma RFC 2307 » page 146

Utilisation de l'utilitaire ndssch pour étendre le schéma sous Linux

Outre NetIQ iManager, vous pouvez faire appel à ndssch, l'utilitaire d'extension de schéma eDirectory, pour étendre le schéma sur les ordinateurs Linux. Les attributs et les classes que vous spécifiez dans le fichier de schéma (`.sch`) sont utilisés pour modifier le schéma de l'arborescence. Les associations entre les attributs et les classes sont créées selon les indications du fichier `.sch`.

Utilisez la syntaxe suivante.

```
ndssch [-h hostname[:port]] [-t tree_name] [-F <logfile>] admin-FDN schemafile...
```

```
ndssch [-h hostname[:port]] [-t tree_name] [-d] admin_FDN schemafile
[schema_description]...
```

Paramètre ndssch	Description
`-h` *`nom_hôte`*	Nom ou adresse IP du serveur sur lequel le schéma doit être étendu. Le schéma de l'arborescence à laquelle appartient le serveur spécifié est étendu. Ce paramètre est facultatif si l'arborescence se situe sur l'hôte dont le schéma doit être étendu. Sinon, il est obligatoire.
`port`	Port du serveur.
`-t` *`nom_de_l'arborescence`*	Nom de l'arborescence sur laquelle le schéma doit être étendu. Ce paramètre est facultatif. Le nom d'arborescence par défaut est indiqué dans le fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Pour plus d'informations, reportez-vous à la section « Paramètres de configuration » du *Guide d'installation de NetIQ eDirectory*.
`-F` *`logfile`*	Indique le nom du chemin d'accès au fichier journal ndssch.
`FDN-admin`	Nom et contexte complet de l'utilisateur disposant de droits d'administrateur eDirectory sur l'arborescence.

Paramètre ndssch	Description
fichier_schéma	Nom du fichier qui contient des informations concernant le schéma à étendre.
-d, *description_schéma*	Si cette option est activée, chaque fichier de schéma doit être suivi de sa description.

Extension du schéma RFC 2307

Les attributs et les classes d'objets définis dans le fichier RFC 2307 (http://www.ietf.org/rfc/rfc2307.txt) sont liés à l'utilisateur ou au groupe, ainsi qu'aux NIS (Network Information Services - services d'information réseau). Les définitions associées à l'utilisateur ou au groupe sont compilées dans le fichier `/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.sch`. Les définitions liées aux NIS sont compilées dans le fichier `/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.sch`. Les fichiers correspondants au format LDIF sont également fournis (`/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-usergroup.ldif` et `/opt/novell/eDirectory/lib/nds-modules/schema/rfc2307-nis.ldif` respectivement).

Vous pouvez étendre le schéma RFC 2307 à l'aide de l'utilitaire ndssch ou de l'outil ldapmodify.

- « Utilisation de l'utilitaire ndssch » page 146
- « Utilisation de l'utilitaire ldapmodify » page 147

Utilisation de l'utilitaire ndssch

Entrez l'une des commandes suivantes :

```
ndssch -t tree_name admin-FDN /opt/novell/eDirectory/lib/nds-schema/rfc2307-usergroup.sch
```

ou

```
ndssch -t tree_name admin-FDN /opt/novell/eDirectory/lib/nds-schema/rfc2307-nis.sch
```

Paramètre	Description
-t	Nom de l'arborescence sur laquelle le schéma doit être étendu. Ce paramètre est facultatif. Si ce paramètre n'est pas spécifié, le nom de l'arborescence utilisé est extrait du fichier `/etc/opt/novell/eDirectory/conf/nds.conf`.

Utilisation de l'utilitaire ldapmodify

Entrez l'une des commandes suivantes :

```
ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/rfc2307-usergroup.ldif
```

ou

```
ldapmodify -h -D -w -f /opt/novell/eDirectory/lib/nds-schema/rfc2307-nis.ldif
```

Paramètre	Description
-h *ldaphost*	Définit un autre hôte sur lequel le serveur LDAP est exécuté.

Paramètre	Description
`-D` *`binddn`*	Utilise *`DN_liaison`* pour établir une liaison vers l'annuaire X.500. Doit être un nom distinctif représenté par une chaîne, comme le définit RFC 1779.
`-w` *`passwd`*	Utilise *`mot_de_passe`* comme mot de passe pour l'authentification simple.
`-f` *`file`*	Lit les informations de modification de l'entrée à partir du fichier et non de l'entrée standard.

Drapeaux de schéma ajoutés à eDirectory 8.7 et versions ultérieures

Les drapeaux de schéma READ_FILTERED et BOTH_MANAGED ont été ajoutés à partir de la version 8.7 d'eDirectory.

Le drapeau READ_FILTERED sert à préciser qu'un attribut est de type LDAP OPÉRATIONNEL. LDAP utilise ce drapeau lors des requêtes de lecture du schéma pour indiquer qu'un attribut est « opérationnel ». READ_FILTERED est activé pour certains attributs de schéma définis en interne. La définition de l'état « opérationnel » pour LDAP comprend trois drapeaux de schéma. Outre le nouveau drapeau READ_FILTERED, les autres qui servent à spécifier l'état « opérationnel » sont READ_ONLY et HIDDEN. Si l'un d'eux est activé dans une définition de schéma, LDAP considère l'attribut comme « opérationnel » et ne le renvoie pas, sauf demande contraire.

Le drapeau BOTH_MANAGED offre un nouveau mécanisme de renforcement de la sécurité des droits. Il n'est significatif que sur un attribut de syntaxe de nom distinctif. S'il est activé pour un tel attribut, la connexion qui fait une demande doit disposer des droits à la fois sur l'objet et l'attribut cible, ainsi que sur l'objet référencé par l'attribut cible. Il s'agit d'une extension de la fonctionnalité actuelle du drapeau WRITE_MANAGED. Il n'est actuellement activé sur aucun attribut de schéma de base. Ce nouveau comportement de sécurité est uniquement possible sur un serveur eDirectory 8.7.*x* ou version ultérieure. Pour bénéficier d'un comportement homogène, vous devez donc mettre à niveau l'ensemble de l'arborescence vers Directory 8.7 ou version ultérieure.

Étant donné que ces drapeaux ne sont reconnus que par un serveur eDirectory 8.7.*x*(ou version ultérieure), ils peuvent uniquement être activés sur une définition de schéma par un serveur eDirectory 8.7.*x* (ou version ultérieure) qui dispose d'une copie de la partition root (seuls les serveurs détenteurs de la racine ont en effet la possibilité de modifier le schéma). L'installation normale d'un nouveau serveur ou la mise à niveau d'un serveur existant qui ne détient pas la partition racine ne permet pas d'ajouter ces nouveaux drapeaux au schéma de votre arborescence.

Si vous voulez activer l'une ou l'autre des nouvelles fonctions dans votre arborescence, assurez-vous que le schéma est correctement étendu afin d'ajouter ces drapeaux. Vous pouvez effectuer cette tâche de deux manières. La première consiste à choisir un serveur qui possède une copie accessible en écriture de la partition racine à mettre à niveau vers eDirectory version 8.7 ou ultérieure. Le nouveau schéma est alors étendu automatiquement à l'aide des nouveaux drapeaux.

La seconde méthode est plus complexe et comprend deux étapes :

1. Installez un nouveau serveur 8.7.*x* (ou version ultérieure) ou mettez à niveau un serveur de l'arborescence. Il n'est pas nécessaire que ce serveur possède une copie de [Root].
2. Ajoutez manuellement une copie de la partition racine au nouveau serveur.
3. Réexécutez les fichiers d'extension de schéma appropriés sur ce serveur pour étendre le schéma :

Plate-forme	Instructions
Windows	Chargez le fichier `install.dlm`, puis cliquez sur **Installer d'autres fichiers de schéma**.
Linux	Utilisez l'utilitaire ndssch. Pour plus d'informations, reportez-vous à la section « Utilisation de l'utilitaire ndssch pour étendre le schéma sous Linux » page 145.

4 Installez les nouveaux fichiers de schéma de votre choix dont les nouveaux drapeaux sont activés.

5 (Facultatif) Une fois le schéma synchronisé, vous pouvez supprimer la réplique racine de ce serveur.

REMARQUE : Les nouveaux drapeaux de schéma activent des fonctions facultatives. Si vous n'en avez pas besoin, l'absence des nouveaux drapeaux sur les définitions de schéma ne perturbe pas le fonctionnement normal d'eDirectory dans votre arborescence. Le drapeau READ_FILTERED ne sera pas présent sur certaines définitions d'attributs. Dès lors, une requête de lecture LDAP de tous les attributs d'un objet peut renvoyer des données supplémentaires qu'elle n'aurait pas reçues dans le cas contraire. Certains attributs seront toujours traités comme étant opérationnels du fait de la présence des drapeaux READ_ONLY et/ou HIDDEN. Le drapeau BOTH_MANAGED doit uniquement être activé sur des arborescences entièrement mises à niveau, car il ne peut fonctionner de manière homogène que dans cet environnement.

Utilisation du client pour effectuer des opérations sur le schéma

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à distance aux opérations DSSchema. Vous pouvez utiliser l'outil eMTool DSSchema pour synchroniser le schéma, importer un schéma distant, déclarer une nouvelle période, réinitialiser le schéma local et réaliser une mise à jour du schéma (opérations normalement réalisées à l'aide de DSRepair. Pour plus d'informations, reportez-vous à la « Maintenance du schéma » page 350).

Le fichier `emboxclient.jar` est installé sur votre serveur dans le cadre de l'installation d'eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client, reportez-vous à la « Utilisation du client à ligne de commande » page 594.

Utilisation de l'outil eMTool DSSchema

1 Exécutez le client en mode interactif en entrant les éléments suivants dans la ligne de commande :

```
java -cp path_to_the_file/emboxclient.jar  -i
```

(Si le fichier `emboxclient.jar` figure déjà dans votre chemin d'accès à la classe, il vous suffit d'entrer la commande `java -i`.)

L'invite du client apparaît :

```
Client>
```

2 Connectez-vous au serveur à réparer en entrant la commande suivante :

```
login -sserver_name_or_IP_address -pport_number
-uusername.context -wpassword -n
```

Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option `-n` ouvre une connexion non sécurisée.

Le client indique si la connexion a abouti.

3 Entrez une commande de réparation à l'aide de la syntaxe suivante :

```
dsschema.options  tâche
```

Par exemple :

`dsschema.rst` invite la réplique maîtresse de la racine de l'arborescence à synchroniser son schéma avec ce serveur.

`dsschema.irs -nMonArborescence` importe le schéma distant de l'arborescence nommée MonArborescence.

Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

Le client indique la réussite ou l'échec de la réparation.

Pour plus d'informations sur les options de l'outil eMTool DSSchema, reportez-vous à la section « Options de l'outil EMTool DSSchema » page 150.

4 Déconnectez-vous du client en entrant la commande suivante :

```
logout
```

5 Quittez le client en entrant la commande suivante :

```
exit
```

Options de l'outil EMTool DSSchema

Les tableaux suivants répertorient les options de l'outil EMTool DSSchema. Vous pouvez également utiliser la commande `list -t dsschema` du client pour afficher les options DSSchema de manière détaillée. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services » page 597.

Option	Description
`rst`	Synchronise le schéma de la réplique maîtresse de la racine de l'arborescence avec le serveur.
`irs -nnom_arborescence`	Importe un schéma distant à partir d'une autre arborescence.
`dse`	Établit une nouvelle période de schéma sur le serveur qui contient la réplique maîtresse de la racine.
`rls`	Réinitialise le schéma local à l'aide d'une copie du serveur qui contient la réplique maîtresse de la partition de la racine.
`gsu`	Effectue une mise à jour globale du schéma.
`scc`	Ajoute des règles d'endiguement circulaire du schéma à la classe Domaine.

6 Gestion des partitions et des répliques

Les partitions sont des divisions logiques de la base de données NetIQ eDirectory qui forment une unité de données distincte dans l'arborescence eDirectory. Les administrateurs s'en servent pour stocker et répliquer des informations sur eDirectory. Chaque partition se compose d'un objet Conteneur, de tous les objets qu'il inclut et des informations concernant ces objets. Les partitions ne comprennent pas d'informations sur le système de fichiers, ni sur les répertoires et fichiers de ce système.

Plutôt que de stocker une copie de toute la base de données eDirectory sur chaque serveur, vous pouvez faire une copie de la partition eDirectory et la stocker sur plusieurs serveurs du réseau. Chaque copie de la partition constitue une réplique. Vous pouvez créer autant de répliques que vous le souhaitez pour chaque partition eDirectory et les stocker sur n'importe quel serveur. Les répliques peuvent être de type maîtresse, lecture/écriture, lecture seule, références subordonnées, lecture/écriture filtrée et lecture seule filtrée.

Le tableau suivant décrit les types de répliques.

Réplique	Description
Maîtresse, lecture-écriture et lecture seule	Contiennent tous les objets et attributs d'une partition.
Références subordonnées	Utilisées pour la connectivité de l'arborescence.
Répliques filtrées	Contiennent un sous-ensemble d'informations extraites de la partition entière, comprenant uniquement les classes et attributs souhaités définis par le filtre de réplication du serveur. Ce filtre permet d'identifier les classes et attributs autorisés à passer en cas de synchronisation entrante et de changements locaux. Les répliques filtrées permettent aux administrateurs de créer des répliques peu volumineuses et fractionnaires. ◆ Les répliques peu volumineuses contiennent uniquement les classes d'objets que vous indiquez. ◆ Les répliques fractionnaires contiennent uniquement les attributs que vous indiquez. La fonctionnalité des répliques filtrées permet d'obtenir des réponses rapides lorsque les données stockées dans eDirectory sont fournies par les applications. Les répliques filtrées permettent également de stocker davantage de répliques sur un seul serveur.
Répliques filtrées en lecture/écriture	Permettent d'apporter des modifications locales aux classes et aux attributs qui constituent un sous-ensemble du filtre de réplication du serveur. Cependant, ces répliques ne peuvent créer des objets que si tous les attributs obligatoires de la classe se trouvent dans le filtre de réplication.
Répliques filtrées Lecture seule	Ne permettent pas les modifications locales.

Ce chapitre explique comment gérer les partitions et les répliques.

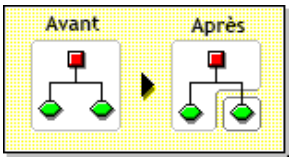
- « Création d'une partition » page 152
- « Fusion d'une partition » page 153
- « Déplacement de partitions » page 154
- « Annulation des opérations de création ou de fusion de partitions » page 155
- « Gestion des répliques » page 155
- « Configuration et gestion des répliques filtrées » page 158
- « Affichage des partitions et des répliques » page 161

Création d'une partition

Lorsque vous créez des partitions, vous effectuez des divisions logiques de votre arborescence. Ces divisions peuvent être répliquées et distribuées entre les différents serveurs eDirectory de votre réseau.

Lorsque vous créez une partition, vous divisez la partition parent afin d'obtenir deux partitions. La nouvelle partition devient une partition enfant, comme l'indique la figure ci-dessous.

Figure 6-1 *Avant et après la division d'une partition*



Par exemple, si vous choisissez une unité organisationnelle et la créez en tant que nouvelle partition, vous séparez l'unité organisationnelle et tous ses objets subordonnés de sa partition parent.

L'objet Unité organisationnelle choisi devient la racine de la nouvelle partition. Les répliques de la nouvelle partition se trouvent sur les mêmes serveurs que celles de la partition parent, et les objets de cette nouvelle partition sont placés dans l'objet Racine de la partition.

La création d'une partition peut prendre un certain temps, car toutes les répliques doivent être synchronisées avec les informations de cette nouvelle partition. Si vous tentez d'effectuer une autre opération de partition pendant la création d'une partition, vous recevez un message vous informant que la partition est occupée.

Affichez la liste des répliques de la nouvelle partition. Lorsque toutes les répliques sont activées, l'opération est terminée. Vous devez régulièrement rafraîchir cette vue manuellement car l'affichage des états n'est pas rafraîchi automatiquement.

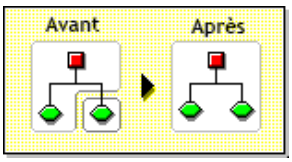
Pour créer une partition, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Créer une partition**.
3. Entrez le nom et le contexte du conteneur à partir duquel vous souhaitez créer une partition, puis cliquez sur **OK**.

Fusion d'une partition

Lorsque vous fusionnez une partition avec sa partition parent, la partition choisie et ses répliques sont combinées avec la partition parent. Aucune partition n'est supprimée ; il s'agit en fait de fusionner et de créer des partitions pour définir la méthode de division logique de l'arborescence Annuaire, comme l'indique la figure ci-dessous.

Figure 6-2 *Avant et après la fusion d'une partition*



Vous pouvez décider de fusionner une partition avec sa partition parent pour plusieurs raisons :

- Les informations de l'Annuaire dans les deux partitions sont étroitement liées.
- Vous souhaitez supprimer une partition subordonnée sans supprimer les objets qu'elle contient.
- Vous allez supprimer les objets de la partition.
- Vous voulez supprimer toutes les répliques de la partition. Fusionner une partition avec sa partition parent est le seul moyen de supprimer la réplique maîtresse de la partition.
- Vous avez déplacé un conteneur (il doit s'agir de la racine d'une partition sans partition subordonnée) et vous ne souhaitez plus que ce dernier soit une partition.
- L'organisation de votre entreprise subit des changements ; vous souhaitez donc revoir votre arborescence Annuaire et modifier la structure des partitions.

Il est conseillé de séparer les partitions si elles sont de grande taille et contiennent des centaines d'objets, car elles augmentent les temps de réponse sur le réseau.

La partition racine de l'arborescence ne peut pas être fusionnée puisqu'il s'agit de la partition la plus élevée et qu'elle ne peut donc pas fusionner avec une partition parent.

La partition est fusionnée lorsque le processus est achevé sur les serveurs. La durée de cette opération peut être plus ou moins longue selon la taille des partitions, le trafic réseau, la configuration du serveur, etc.

IMPORTANT : Avant de fusionner une partition, vérifiez la synchronisation des deux partitions et résolvez les erreurs éventuelles pour pouvoir continuer. Si vous résolvez les erreurs, les problèmes rencontrés dans l'Annuaire sont isolés ; ainsi, vous évitez la propagation des erreurs et l'apparition de nouvelles erreurs.

Assurez-vous que tous les serveurs ayant des répliques (y compris des références subordonnées) de la partition à fusionner sont sous tension avant de tenter de fusionner cette partition. Si un serveur est hors service, eDirectory ne peut pas lire ses répliques et l'opération ne peut donc pas être effectuée.

Si des erreurs apparaissent au cours du processus de fusion d'une partition, résolvez-les au fur et à mesure. N'essayez pas de résoudre l'erreur en poursuivant les opérations ; cela ne ferait que créer des erreurs supplémentaires.

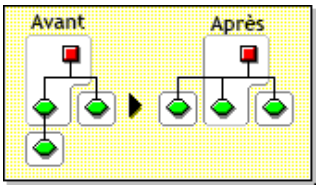
Pour fusionner une partition enfant avec sa partition parente, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Fusionner la partition**.
3. Spécifiez le nom et le contexte de la partition à fusionner avec sa partition parente, puis cliquez sur **OK**.

Déplacement de partitions

Si vous déplacez une partition, la sous-arborescence correspondante est déplacée dans l'arborescence Annuaire. Vous pouvez déplacer un objet racine de partition (c'est-à-dire un objet Conteneur) uniquement si aucune partition ne lui est subordonnée.

Figure 6-3 *Avant et après le déplacement d'une partition*



Lorsque vous déplacez une partition, vous devez respecter les règles d'endiguement d'eDirectory. Par exemple, vous ne pouvez pas déplacer un objet Unité organisationnelle qui se trouve directement sous la racine de l'arborescence en cours, car les règles d'endiguement de la racine autorisent uniquement le déplacement des objets Lieu, Pays et Organisation.

Lorsque vous déplacez une partition, eDirectory modifie toutes les références à son objet Racine. Le nom commun de l'objet reste inchangé ; cependant, le nom complet du conteneur (et de tous les objets qui lui sont subordonnés) est modifié.

Lorsque vous déplacez une partition, vous avez tout intérêt à créer un objet Alias pour remplacer le conteneur que vous déplacez. Ainsi, les utilisateurs pourront continuer à se connecter au réseau et retrouver les objets à leur emplacement d'origine dans l'Annuaire.

L'objet Alias créé porte le même nom commun que le conteneur que vous avez déplacé et fait référence à son nouveau nom complet.

IMPORTANT : si vous déplacez une partition sans la remplacer par un objet Alias, les utilisateurs qui ne connaissent pas le nouvel emplacement de la partition retrouvent difficilement les objets qu'elle contient dans l'arborescence Annuaire, puisqu'ils les recherchent à leur emplacement d'origine.

De plus, il se peut que la connexion échoue également sur les postes de travail client si le paramètre `NAME CONTEXT` a pour valeur l'emplacement d'origine du conteneur dans l'arborescence Annuaire.

Lorsque vous déplacez un objet, son contexte change. Les utilisateurs dont le contexte de nom fait référence à l'objet déplacé doivent donc mettre à jour le paramètre `NAME CONTEXT` de manière à ce que celui-ci mentionne le nouveau nom de l'objet.

Vous pouvez mettre à jour automatiquement le paramètre `NAME CONTEXT` des utilisateurs après avoir déplacé un objet Conteneur à l'aide de l'utilitaire NCUPDATE.

Si vous ne souhaitez pas que la partition, une fois déplacée, reste une partition, fusionnez-la avec sa partition parent.

Vérifiez que la synchronisation de l'arborescence Annuaire s'effectue correctement avant de déplacer une partition. Si la partition à déplacer ou la partition cible comporte des erreurs de synchronisation, n'effectuez pas le déplacement. Résolvez d'abord les erreurs de synchronisation.

Pour déplacer une partition, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Déplacer une partition**.
3. Dans le champ **Nom de l'objet**, indiquez le nom et le contexte de l'objet Partition à déplacer.
4. Dans le champ **Déplacer vers**, indiquez le nom et le contexte du conteneur vers lequel vous souhaitez transférer la partition.
5. Pour créer un alias à l'ancien emplacement de la partition déplacée, sélectionnez **Créer un alias à la place de l'objet déplacé**.

   Si vous créez un alias, les opérations qui sont tributaires de l'ancien emplacement se poursuivent sans interruption tant que vous ne les modifiez pas afin de préciser le nouvel emplacement.
6. Cliquez sur **OK**.

Annulation des opérations de création ou de fusion de partitions

Vous pouvez annuler la création ou la fusion d'une partition tant que la modification à part entière n'a pas été exécutée. Utilisez cette fonction pour annuler une opération, si votre réseau eDirectory renvoie des erreurs eDirectory ou s'il ne parvient pas à effectuer la synchronisation à la suite d'une opération de partition.

Si les répliques de votre arborescence Annuaire contiennent des erreurs de synchronisation, le problème n'est pas forcément résolu par l'opération d'annulation. Cependant, vous pouvez utiliser cette fonction comme première option de dépannage.

Si une opération de partition ne peut pas être effectuée parce qu'un serveur est hors tension (ou non disponible pour une autre raison), connectez le serveur au réseau pour que l'opération puisse être effectuée ou abandonnez l'opération. Si eDirectory ne peut pas effectuer la synchronisation car la base de données est altérée, vous devez annuler les partitions en cours.

La synchronisation complète des partitions sur le réseau peut demander un temps considérable, selon le nombre de répliques concernées, la visibilité des serveurs concernés et le trafic réseau existant.

Si vous recevez un message d'erreur vous informant que la partition est occupée, cela ne signifie pas que vous deviez annuler l'opération. Vous pouvez généralement vous attendre à ce que les opérations de partition s'effectuent sous 24 heures, en fonction de la taille de la partition, des problèmes de connexion, etc. Si l'exécution d'une opération particulière échoue dans ce laps de temps, vous devez alors essayer d'annuler l'opération en cours.

Gestion des répliques

Avant d'ajouter ou de supprimer une réplique, ou de modifier un type de réplique, planifiez soigneusement les emplacements des répliques cibles. Reportez-vous à la « Instructions concernant la réplication de votre arborescence » page 91.

Ajout d'une réplique

Ajouter une réplique à un serveur afin de doter votre répertoire des éléments suivants :

- Une tolérance aux pannes
- Un accès plus rapide aux données
- Un accès plus rapide via une liaison WAN
- Un accès aux objets dans un contexte défini (à l'aide des services de Bindery)

Pour ajouter une réplique, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte de la partition ou du serveur à répliquer, puis cliquez sur **OK**.
4. Cliquez sur **Ajouter une réplique**.
5. Spécifiez le nom et le contexte de la partition ou du serveur.
6. Choisissez l'un des types de réplique suivants :

Type de réplique	Description
Lecture/écriture	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique. Sélectionnez cette option si aucune réplique modifiable ne se trouve suffisamment près des utilisateurs qui gèrent les objets eDirectory de cette partition.
Lecture seule	Les utilisateurs peuvent lire le contenu de la nouvelle réplique, mais ne peuvent pas le modifier. Sélectionnez cette option si aucune réplique ne se trouve suffisamment près des utilisateurs qui lisent les objets eDirectory de cette partition mais ne peuvent pas les modifier.
Lecture/écriture filtrée	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique, qui est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.
Lecture seule filtrée	Les utilisateurs peuvent lire le contenu de la nouvelle réplique mais ne peuvent pas le modifier. Ce contenu est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.

7. Cliquez sur **OK**.

Pour plus d'informations, reportez-vous à la section « Types de réplique » page 62.

Suppression d'une réplique

Si vous supprimez une réplique de la partition, elle disparaît du serveur.

Pour retirer un serveur de l'arborescence Annuaire, vous pouvez supprimer ses répliques avant de retirer le serveur lui-même. Si vous supprimez les répliques, vous réduisez les risques de problèmes au moment du retrait du serveur.

Lorsque vous retirez les répliques, le trafic de synchronisation du réseau est également réduit. Notez qu'il est conseillé de ne pas utiliser plus de six répliques de chaque partition.

Vous ne pouvez pas supprimer une réplique maîtresse ni une référence subordonnée.

Si la réplique que vous souhaitez supprimer est une réplique maîtresse, vous pouvez effectuer l'une des deux opérations suivantes :

- Vous pouvez vous connecter à un serveur possédant une autre réplique de la partition et transformer cette réplique en nouvelle réplique maîtresse

  La réplique maîtresse initiale est automatiquement convertie en réplique en lecture/écriture et vous pouvez alors la supprimer.
- Vous pouvez fusionner la partition avec sa partition parent

  Les répliques de la partition sont alors fusionnées avec celles de la partition parent et retirées des serveurs sur lesquels elles se trouvaient. Le processus de fusion retire les limites des partitions, mais pas les objets. Les objets restent placés sur chacun des serveurs contenant une réplique de la partition « jointe ».

Lorsque vous supprimez des répliques, tenez compte des points suivants :

- Pour garantir la tolérance aux pannes, vous devez conserver au moins trois répliques de chaque partition sur des serveurs différents.
- Si vous supprimez une réplique, une copie d'une partie de la base de données Annuaire est supprimée sur le serveur cible.

  Vous pouvez toujours accéder à la base de données à partir des autres serveurs du réseau, et le serveur sur lequel était stockée la réplique fonctionne toujours dans eDirectory.

  Vous ne pouvez pas supprimer ni gérer de répliques de référence subordonnée. Elles sont automatiquement créées par eDirectory sur un serveur contenant une réplique d'une partition mais pas de réplique de sa partition enfant.

Pour supprimer une réplique, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à supprimer, puis cliquez sur **OK**.
4. Cliquez sur , à gauche de la réplique à supprimer.
5. Cliquez sur **OK**.

Changement du type d'une réplique

Modifiez le type d'une réplique pour contrôler l'accès aux informations de cette réplique. Par exemple, vous pouvez décider de convertir une réplique en lecture/écriture en réplique en lecture seule pour empêcher les utilisateurs d'écrire dans cette réplique et de modifier des données de l'Annuaire.

Vous pouvez modifier le type d'une réplique en lecture/écriture ou d'une réplique en lecture seule. Vous ne pouvez pas modifier le type d'une réplique maîtresse. En revanche, vous pouvez transformer une réplique Lecture/écriture ou Lecture seule en réplique maîtresse (la réplique maîtresse initiale devenant alors automatiquement une réplique Lecture/écriture).

La plupart des répliques doivent être en lecture/écriture. Vous pouvez écrire dans des répliques en lecture/écriture en effectuant des opérations sur les postes client. Elles envoient les informations à synchroniser lorsqu'une modification est effectuée. Vous ne pouvez pas écrire dans des répliques en lecture seule en effectuant des opérations sur les postes client. Cependant, elles sont mises à jour lors de la synchronisation des répliques.

Vous ne pouvez pas modifier le type d'une réplique de référence subordonnée. Pour placer une réplique d'une partition sur un serveur possédant une référence subordonnée, vous devez effectuer une opération d'ajout de réplique. Une réplique de référence subordonnée ne constitue pas une copie complète d'une partition. Les répliques de référence subordonnée sont placées et gérées par eDirectory. Elles sont automatiquement créées par eDirectory sur un serveur contenant une réplique d'une partition mais pas de réplique de sa partition enfant.

Pour modifier le type d'une réplique, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à modifier, puis cliquez sur **OK**.
4. Cliquez sur le type (dans la colonne Type) de la réplique à modifier.
5. Sélectionnez un nouveau type de réplique, puis cliquez sur **OK**.

Type de réplique	Description
Maîtresse	Les utilisateurs peuvent lire et modifier le contenu de cette réplique qui constitue le point de départ de toute activité ultérieure de partitionnement s'appliquant à cette partition, comme la création ou la fusion d'une sous-partition. Une seule réplique maîtresse par partition est autorisée.
Lecture/écriture	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique. Sélectionnez cette option si aucune réplique modifiable ne se trouve suffisamment près des utilisateurs qui gèrent les objets eDirectory de cette partition.
Lecture seule	Les utilisateurs peuvent lire le contenu de la nouvelle réplique, mais ne peuvent pas le modifier. Sélectionnez cette option si aucune réplique ne se trouve suffisamment près des utilisateurs qui lisent les objets eDirectory de cette partition mais ne peuvent pas les modifier.
Lecture/écriture filtrée	Les utilisateurs peuvent lire et modifier le contenu de la nouvelle réplique, qui est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.
Lecture seule filtrée	Les utilisateurs peuvent lire le contenu de la nouvelle réplique, mais ils ne peuvent pas le modifier. Ce contenu est limité aux types d'objets et de propriétés eDirectory spécifiés dans un filtre.

6. Cliquez sur **OK**.

Pour plus d'informations, reportez-vous à la section « Types de réplique » page 62.

Configuration et gestion des répliques filtrées

Les répliques filtrées gèrent un sous-ensemble filtré d'informations d'une partition eDirectory (objets ou classes d'objets et ensemble filtré d'attributs et de valeurs de ces objets).

Les administrateurs utilisent généralement la fonction de réplique filtrée pour créer un serveur eDirectory qui contient un ensemble de répliques filtrées constitué uniquement d'objets et d'attributs spécifiques qui seront synchronisés.

Pour ce faire, iManager fournit des outils qui permettent de créer une étendue de partition de réplique filtrée et un filtre. Une étendue est tout simplement l'ensemble des partitions dont les répliques doivent être placées sur un serveur, tandis qu'un filtre de réplication contient l'ensemble des classes et attributs eDirectory à héberger dans l'ensemble des répliques filtrées d'un serveur. Le serveur eDirectory peut alors héberger un ensemble de données bien défini provenant de nombreuses partitions de l'arborescence.

La description de l'étendue des partitions et des filtres de réplication du serveur est stockée dans eDirectory. Elle peut être gérée via l'objet Serveur ou le rôle Partition et répliques dans iManager.

- « Utilisation de l'Assistant de de réplique filtrée » page 159
- « Définition d'un statut de partition » page 159
- « Configuration d'un filtre de serveur » page 160

Utilisation de l'Assistant de de réplique filtrée

L'Assistant de de réplique filtrée vous guide tout au long de la configuration d'un filtre de réplication et d'un statut de partition de serveur.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Assistant de répliques filtrées**.
3. Indiquez le serveur sur lequel une réplique filtrée doit être configurée, puis cliquez sur **Suivant**.
4. Pour définir les classes et les attributs d'un ensemble de filtres de ce serveur, cliquez sur **Définir l'ensemble de filtres**.

   Le filtre de réplication contient l'ensemble des classes et attributs eDirectory à héberger sur l'ensemble de répliques filtrées de ce serveur. Pour plus d'informations sur la définition d'un ensemble de filtres, reportez-vous à la section « Configuration d'un filtre de serveur » page 160.
5. Cliquez sur **Suivant**.
6. Pour définir l'étendue de partition de ce serveur, cliquez sur **Définir l'étendue de la partition**.

   Pour plus d'informations sur les statuts de partition, reportez-vous à la section « Définition d'un statut de partition » page 159.
7. Cliquez sur **Suivant**, puis sur **Terminer**.

Définition d'un statut de partition

Une étendue de partition est un ensemble de partitions dont vous voulez placer les répliques sur un serveur. La page Affichage des répliques d'iManager offre une vue de la hiérarchie des partitions de l'arborescence eDirectory. Vous pouvez sélectionner les partitions une à une, un ensemble de partitions d'une branche donnée ou toutes les partitions de l'arborescence. Vous pouvez ensuite sélectionner le type de répliques de ces partitions à ajouter au serveur. Vous pouvez aussi modifier les types de répliques existants.

Un serveur peut contenir à la fois des répliques complètes et des répliques filtrées. Pour plus d'informations, reportez-vous à la section « Répliques filtrées » page 65.

Affichage des répliques sur un serveur eDirectory

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte du serveur à afficher, puis cliquez sur **OK** pour afficher la liste des répliques sur ce serveur.

Ajout d'une réplique filtrée à un serveur eDirectory

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte du serveur auquel vous voulez ajouter une partition filtrée, puis cliquez sur **OK**.
4. Cliquez sur **Ajouter une réplique**.
5. Spécifiez le nom et le contexte de la partition.
6. Cliquez sur **Lecture-écriture filtrée** ou sur **Lecture seule filtrée** puis cliquez sur **OK**.

Transformation d'une réplique complète en réplique filtrée

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à modifier, puis cliquez sur **OK**.
4. Cliquez sur le type de réplique à modifier (dans la colonne **Type**).
5. Cliquez sur **Lecture-écriture filtrée** ou sur **Lecture seule filtrée**, puis cliquez sur **OK**.

Configuration d'un filtre de serveur

Un filtre de réplication de serveur contient l'ensemble des classes et attributs eDirectory à héberger dans l'ensemble des répliques filtrées d'un serveur. Vous pouvez configurer un filtre depuis n'importe quel objet Serveur. Pour les répliques filtrées, vous disposez uniquement d'un filtre par serveur. En d'autres termes, tout filtre défini pour un serveur eDirectory s'applique à l'ensemble des répliques filtrées de ce serveur. Ce filtre ne s'applique cependant pas aux répliques complètes.

Un filtre de serveur peut être modifié si nécessaire, mais cette opération génère une resynchronisation de la réplique et risque donc de prendre du temps. Il est recommandé de planifier attentivement la fonction du serveur.

Vous pouvez configurer ou modifier un filtre de serveur de l'une des façons suivantes :

- « Utilisation de l'affichage de la réplique » page 161
- « Utilisation de l'objet Serveur » page 161

Utilisation de l'affichage de la réplique

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Spécifiez le nom et le contexte de la partition ou du serveur qui contient la réplique à modifier, puis cliquez sur **OK**.
4. Cliquez sur Éditer dans la colonne Filtre du serveur ou de la partition à modifier.
5. Ajoutez les classes et les attributs souhaités, puis cliquez sur **OK**.
6. Cliquez sur **Terminer**.

Utilisation de l'objet Serveur

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
3. Spécifiez le nom et le contexte du serveur qui contient la réplique à modifier, puis cliquez sur **OK**.
4. Cliquez sur l'onglet **Réplique**.
5. Si aucun filtre n'a été défini pour ce serveur, cliquez sur **Le filtre est vide** afin d'ouvrir la fenêtre Boîte de dialogue Éditer le filtre, puis ajoutez les classes et les attributs souhaités.

   ou

   Cliquez sur **Copier un filtre à partir de** pour rechercher un objet (un autre serveur, par exemple) dont vous voulez copier le filtre.
6. Pour éditer un filtre existant, cliquez sur un élément doté d'un hyperlien dans le filtre pour ouvrir la fenêtre Boîte de dialogue Éditer le filtre, puis ajoutez ou supprimez les classes et les attributs désirés.

Affichage des partitions et des répliques

Ce chapitre comprend les informations suivantes :

- « Affichage des partitions d'un serveur » page 162
- « Affichage des répliques d'une partition » page 162
- « Affichage des informations concernant une partition » page 162
- « Affichage de la hiérarchie des partitions » page 162
- « Affichage des informations concernant une réplique » page 163

Affichage des partitions d'un serveur

Vous pouvez afficher les partitions allouées à un serveur à l'aide de NetIQ iManager. Vous pouvez avoir besoin d'afficher les partitions stockées sur un serveur pour retirer un objet Serveur de l'arborescence Annuaire. Si tel est le cas, vous pouvez afficher les répliques à retirer avant de retirer l'objet.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Entrez le nom et le contexte d'un objet Serveur, puis cliquez sur **OK**.

Affichage des répliques d'une partition

Cette opération vous permet d'identifier les éléments suivants :

- Les serveurs sur lesquels se trouvent les répliques de la partition
- Le serveur qui héberge la réplique maîtresse de la partition
- Les serveurs qui hébergent des répliques en lecture/écriture, en lecture seule et de référence subordonnée de la partition
- L'état de chacune des répliques de la partition

Pour afficher les répliques d'une partition :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Entrez le nom et le contexte d'une partition, puis cliquez sur **OK**.

Affichage des informations concernant une partition

L'affichage des informations sur une partition permet principalement de contrôler sa synchronisation (dernière synchronisation réussie et dernière tentative de synchronisation).

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Afficher les informations sur la partition**.
3. Entrez le nom et le contexte d'une partition, puis cliquez sur **OK**.

Affichage de la hiérarchie des partitions

Vous pouvez facilement afficher la hiérarchie des partitions dans iManager. Il est possible de développer des objets Conteneur pour afficher les partitions parentes et les partitions enfants.

Chaque conteneur qui représente la racine d'une partition est marqué par l'icône suivante : .

Affichage des informations concernant une réplique

L'affichage des informations sur une réplique permet principalement de contrôler son état. Une réplique eDirectory peut avoir différents états selon les opérations de partition ou de réplication exécutées. Le tableau suivant décrit les différents états de réplique que vous pouvez rencontrer dans iManager.

État	Description
Actif	Ne subit pas actuellement d'opérations de partition ou de réplication.
Nouveau	Est actuellement ajoutée en tant que nouvelle réplique sur le serveur.
Expiration en cours	Est actuellement supprimée du serveur.
Morte	A été supprimée du serveur.
Démarrage	Est actuellement changée en réplique principale.
Fin	A été changée en réplique principale.
Changer type	Est actuellement changée en un type de réplique différent.
Verrouillée	Est verrouillée en vue d'un déplacement de partition ou d'une opération de réparation.
Déplacement de la transition	Est au début d'une opération de déplacement de partition.
Déplacer	Est au milieu d'une opération de déplacement de partition.
Séparation de la transition	Est au début d'une opération de fractionnement de partition (création d'une partition enfant).
Diviser	Est au milieu d'une opération de fractionnement de partition (création d'une partition enfant).
Rejoindre	Est fusionnée avec sa partition parent.
Activation de la transition	Est sur le point de revenir à l'état Actif.
Inconnu	Dans un état non connu d'iManager

Pour afficher des informations sur une réplique, procédez comme suit :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.
3. Entrez le nom et le contexte d'une partition ou d'un serveur, puis cliquez sur **OK**.

7 Utilitaires de gestion de NetIQ eDirectory

Ce chapitre contient des informations sur les utilitaires NetIQ eDirectory suivants :

- « Utilitaire Importation/Conversion/Exportation NetIQ » page 165
- « Gestionnaire d'index » page 205
- « Gestionnaire de services eDirectory » page 207
- « Utilitaire de chargement en bloc hors connexion » page 209
- « Fichiers LDIF » page 218

Utilitaire Importation/Conversion/Exportation NetIQ

L'utilitaire Importation/Conversion/Exportation NetIQ vous permet d'effectuer les opérations suivantes :

- Importer des données à partir de fichiers LDIF vers un annuaire LDAP.
- Exporter des données à partir de l'annuaire LDAP vers un fichier LDIF.
- Faire migrer des données entre des serveurs LDAP.
- effectuer une comparaison et une mise à niveau de schéma ;
- Charger des informations dans eDirectory à l'aide d'un modèle.
- importer un schéma à partir de fichiers SCH dans un annuaire LDAP.

L'utilitaire Importation/Conversion/Exportation NetIQ gère un ensemble de gestionnaires qui lisent ou écrivent des données dans différents formats. Les gestionnaires source lisent les données tandis que les gestionnaires cible les inscrivent. Un module exécutable unique peut être à la fois un gestionnaire source et un gestionnaire cible. Le moteur reçoit des données d'un gestionnaire source, les traite, puis les transmet à un gestionnaire cible.

Par exemple, si vous souhaitez importer des données LDIF dans un annuaire LDAP, le moteur Importation/Conversion/Exportation NetIQ utilise un gestionnaire source LDIF pour lire le fichier LDIF et un gestionnaire cible LDAP pour transmettre ces données au serveur d'annuaire LDAP. Pour plus d'informations sur la syntaxe, la structure et le débogage des fichiers LDIF, reportez-vous à l'Annexe J, « Dépannage », page 949.

Vous pouvez exécuter l'utilitaire Importation/Conversion/Exportation NetIQ à partir de la ligne de commande ou de l'assistant Importation/Conversion/Exportation de NetIQ iManager. Le gestionnaire de données séparées par une virgule n'est cependant disponible que dans l'utilitaire de ligne de commande et dans NetIQ iManager.

Vous pouvez exécuter l'utilitaire Importation/Conversion/Exportation NetIQ de l'une des manières suivantes :

- « Utilisation de l'assistant Importation/Conversion/Exportation de NetIQ iManager » page 166
- « Utilisation de l'interface de ligne de commande » page 174

L'assistant et l'interface de ligne de commande permettent d'accéder au moteur Importation/Conversion/Exportation NetIQ. L'interface de ligne de commande offre cependant des options supplémentaires pour combiner des gestionnaires source et cible.

L'utilitaire Importation/Conversion/Exportation NetIQ remplace à la fois les utilitaires BULKLOAD et ZONEIMPORT inclus dans les versions précédentes de NDS et eDirectory.

Utilisation de l'assistant Importation/Conversion/ Exportation de NetIQ iManager

L'assistant Importation/Conversion/Exportation permet d'effectuer les opérations suivantes :

- « Ajout d'un schéma manquant » page 166
- « Importation de données à partir d'un fichier » page 167
- « Exportation de données vers un fichier » page 168
- « Migration de données entre des serveurs LDAP » page 169
- « Mise à jour d'un schéma à partir d'un fichier » page 170
- « Ajout d'un schéma à partir d'un serveur » page 171
- « Comparaison de fichiers de schéma » page 172
- « Comparaison de schéma à partir d'un serveur et d'un fichier » page 172
- « Génération d'un fichier d'ordre » page 173

Pour plus d'informations sur l'accès à NetIQ iManager et sur son utilisation, reportez-vous au *Guide d'administration de NetIQ iManager.*

Ajout d'un schéma manquant

iManager intègre des options permettant d'ajouter un schéma manquant au schéma d'un serveur. Ce processus implique une comparaison d'une source et d'une cible. Si le schéma source contient un schéma supplémentaire, ce dernier est ajouté au schéma cible. La source peut être un fichier ou un serveur LDAP, et la destination doit être un serveur LDAP.

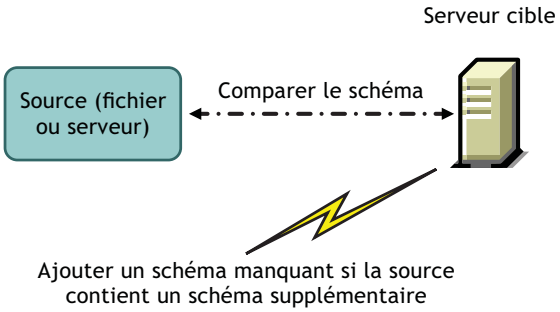
L'Assistant ICE dans iManager permet d'ajouter le schéma manquant à l'aide des options suivantes :

- Ajouter un schéma depuis un fichier
- Ajouter un schéma depuis un serveur

Ajouter un schéma depuis un fichier

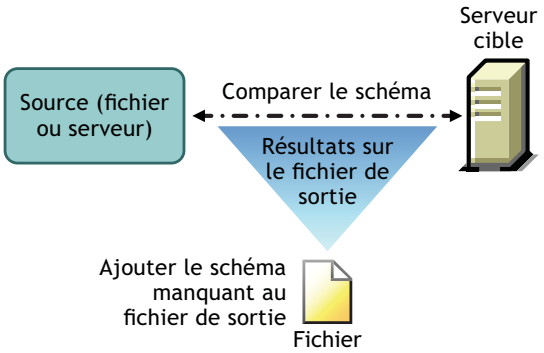
ICE peut comparer le schéma dans la source et la cible. La source est un fichier ou serveur LDAP ; la cible, un serveur LDAP. Le fichier du schéma source peut être au format LDIF ou SCH.

Figure 7-1 *Comparaison et ajout du schéma depuis un fichier*



Si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur de destination, sélectionnez l'option **Ne pas ajouter mais comparer le schéma**. Dans ce cas, le schéma supplémentaire n'est pas ajouté au serveur cible, mais les différences de schéma peuvent être affichées en cliquant sur le lien disponible à la fin de l'opération.

Figure 7-2 *Comparaison du schéma et consignation des résultats dans un fichier de sortie*



Ajouter un schéma depuis un serveur

La source et la cible sont des serveurs LDAP.

Si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur de destination, sélectionnez l'option **Ne pas ajouter mais comparer le schéma**. Dans ce cas, le schéma supplémentaire n'est pas ajouté au serveur cible, mais les différences de schéma peuvent être affichées en cliquant sur le lien disponible à la fin de l'opération.

Importation de données à partir d'un fichier

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Importer les données depuis un fichier du disque**, puis sur **Suivant**.
4. Sélectionnez le type de fichier à importer.
5. Entrez le nom du fichier qui contient les données à importer, spécifiez les options appropriées, puis cliquez sur **Suivant**.

   Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.
6. Spécifiez le serveur LDAP dans lequel importer les données.
7. Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8 Cliquez sur **Suivant**, puis sur **Terminer**.

Exportation de données vers un fichier

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Exporter les données vers un fichier du disque**, puis sur **Suivant**.

4 Spécifiez le serveur LDAP comportant les entrées à exporter.

Les **paramètres avancés** permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP source
Port	Numéro de port (nombre entier) du serveur LDAP source
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6 Cliquez sur **Suivant**.

7 Spécifiez les critères de recherche (décrits ci-dessous) relatifs aux entrées à exporter.

Option	Description
DN de base	Nom distinctif de base pour la requête de recherche Si vous laissez ce champ vide, la valeur par défaut du nom distinctif de base est “” (chaîne vide).
Étendue	Étendue de la requête de recherche
Filtre	Filtre de recherche conforme à la convention RFC 1558 La valeur par défaut est objectclass=*.
Attributs	Attributs qui doivent vous être renvoyés pour chaque entrée de la recherche

8 Cliquez sur **Suivant**.

9 Sélectionnez le type de fichier d'exportation.

Le fichier exporté est enregistré à un emplacement temporaire. Vous pouvez le télécharger à la fin de l'exécution de l'Assistant.

10 Cliquez sur **Suivant**, puis sur **Terminer**.

Migration de données entre des serveurs LDAP

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Migrer les données entre les serveurs**, puis sur **Suivant**.

4 Sélectionnez le serveur LDAP comportant les entrées à migrer.

Les **paramètres avancés** permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP source
Port	Numéro de port (nombre entier) du serveur LDAP source
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6 Cliquez sur **Suivant**.

7 Spécifiez les critères de recherche (décrits ci-dessous) relatifs aux entrées à migrer :

Option	Description
DN de base	Nom distinctif de base pour la requête de recherche Si vous laissez ce champ vide, la valeur par défaut du nom distinctif de base est "" (chaîne vide).
Étendue	Étendue de la requête de recherche
Filtre	Filtre de recherche conforme à la convention RFC 2254 La valeur par défaut est objectclass=*.
Attributs	Attributs qui doivent vous être renvoyés pour chaque entrée de la recherche

8 Cliquez sur **Suivant**.

9 Spécifiez le serveur LDAP vers lequel les données doivent migrer.

10 Cliquez sur **Suivant**, puis sur **Terminer**.

REMARQUE : vérifiez que le schéma est cohérent pour l'ensemble des services LDAP.

Mise à jour d'un schéma à partir d'un fichier

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Ajouter un schéma depuis un fichier** > **Suivant**.

4 Sélectionnez le type de fichier à ajouter.

Vous avez le choix entre les types Fichier LDIF et Fichier de schéma.

5 Entrez le nom du fichier qui contient le schéma à ajouter, spécifiez les options appropriées, puis cliquez sur **Suivant**.

Sélectionnez **Ne pas ajouter mais comparer le schéma** si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur cible. Dans ce cas, le schéma supplémentaire n'est pas ajouté au serveur cible, mais les différences de schéma peuvent être affichées en cliquant sur le lien disponible à la fin de l'opération.

Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

6 Spécifiez le serveur LDAP dans lequel importer le schéma.

7 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8 Cliquez sur **Suivant** > **Terminer**.

Ajout d'un schéma à partir d'un serveur

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Ajouter un schéma depuis un serveur** > **Suivant**.

4 Spécifiez le serveur LDAP à partir duquel ajouter le schéma.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

Sélectionnez **Ne pas ajouter mais comparer le schéma** si vous souhaitez simplement comparer le schéma sans ajouter de schéma supplémentaire au serveur cible. Dans ce cas, le schéma supplémentaire n'est pas ajouté au serveur cible, mais les différences de schéma peuvent être affichées en cliquant sur le lien disponible à la fin de l'opération.

6 Spécifiez le serveur LDAP dans lequel ajouter le schéma.

7 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8 Cliquez sur **Suivant** > **Terminer**.

Comparaison de fichiers de schéma

L'option **Comparer les fichiers de schéma** compare le schéma d'un fichier source à celui d'un fichier de destination, puis consigne le résultat dans un fichier de sortie. Pour ajouter le schéma manquant au fichier cible, appliquez-lui les enregistrements du fichier de sortie.

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Comparer les fichiers de schéma** > **Suivant**.

4 Sélectionnez le type de fichier à comparer.

   Vous avez le choix entre les types Fichier LDIF et Fichier de schéma.

5 Entrez le nom du fichier qui contient le schéma à comparer, spécifiez les options appropriées, puis cliquez sur **Suivant**.

   Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

6 Spécifiez le fichier de schéma avec lequel le comparer.

   Vous pouvez uniquement sélectionner un fichier LDIF.

7 Cliquez sur **Suivant** > **Terminer**.

Pour afficher les différences entre les deux fichiers de schéma, cliquez sur le lien disponible à la fin de l'opération.

Comparaison de schéma à partir d'un serveur et d'un fichier

L'option **Comparer un schéma entre serveur et fichier** compare le schéma d'un serveur source et celui d'un fichier de destination, puis consigne le résultat dans un fichier de sortie. Pour ajouter le schéma manquant au fichier cible, appliquez-lui les enregistrements du fichier de sortie.

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Comparer un schéma entre serveur et fichier** > **Suivant**.

4 Spécifiez le serveur LDAP à partir duquel comparer le schéma.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6 Sélectionnez le type de fichier avec lequel effectuer la comparaison.

7 Entrez le nom du fichier qui contient les données à comparer, spécifiez les options appropriées, puis cliquez sur **Suivant**.

   Les options de cette page dépendent du type de fichier que vous avez sélectionné. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

8 Cliquez sur **Suivant** > **Terminer**.

Pour afficher les différences entre le schéma du serveur et le fichier de schéma, cliquez sur le lien disponible à la fin de l'opération.

Génération d'un fichier d'ordre

Cette option crée un fichier d'ordre à utiliser avec le gestionnaire DELIM pour l'importation de données à partir d'un fichier de données séparées par une virgule. L'Assistant vous aide à créer ce fichier d'ordre qui contient une liste des attributs pour une classe d'objet spécifique.

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.

3 Cliquez sur **Créer un fichier d'ordre**, puis sur **Suivant**.

4 Sélectionnez la classe pour laquelle vous souhaitez générer le fichier d'ordre et cliquez sur **Afficher**.

   Sélectionnez les attributs à ajouter à la liste **Attributs en séquence**.

   Sélectionnez la classe auxiliaire et ajoutez-la à la liste **Classes auxiliaires sélectionnées**.

   Pour plus d'informations sur les listes Attributs en séquence et Classes auxiliaires, consultez l'aide en ligne d'iMonitor.

   Cliquez sur Suivant.

5 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Contexte	Contexte auquel les objets créés sont associés
Sélectionner le fichier de données	Emplacement du fichier de données
Sélectionner le séparateur dans le fichier de données	Séparateur à utiliser dans le fichier de données. Le séparateur par défaut est une virgule (,)
Sélectionner l'attribut d'assignation de nom	Attributs d'assignation de nom de la liste des attributs disponibles pour la classe sélectionnée

Les **paramètres avancés** permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

Sélectionnez les enregistrements à traiter dans le fichier de données à l'aide de l'option **Enregistrements à traiter**. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

6 Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

Les **paramètres avancés** permettent de configurer des options supplémentaires pour le gestionnaire source LDAP. Pour plus d'informations sur les options disponibles, cliquez sur **Aide**.

7 Cliquez sur **Suivant**, puis sur **Terminer**.

Utilisation de l'interface de ligne de commande

Vous pouvez faire appel à la version de ligne de commande de l'utilitaire Importation/Conversion/Exportation NetIQ pour effectuer les opérations suivantes :

- Importations LDIF
- Exportations LDIF
- importer des données séparées par une virgule ;
- exporter des données séparées par une virgule ;
- Migration de données entre des serveurs LDAP
- comparer et mettre à jour des schémas ;
- charger des informations dans eDirectory à l'aide d'un modèle ;
- importer des schémas.

L'assistant Importation/Conversion/Exportation NetIQ s'installe simultanément avec NetIQ iManager. Une version de Windows (`ice.exe`) est comprise dans l'installation. Sur les ordinateurs Linux, l'utilitaire Importation/Exportation est inclus dans le paquetage `NOVLice`.

Syntaxe d'importation, de conversion et d'exportation NetIQ

Pour lancer l'utilitaire Importation/Conversion/Exportation NetIQ, utilisez la syntaxe suivante :

```
ice general_options
-S[LDIF | LDAP | DELIM | LOAD | SCH] source_options
-D[LDIF | LDAP | DELIM] destination_options
```

ou, si vous utilisez le cache de schéma :

```
ice -C schema_options
-S[LDIF | LDAP] source_options
-D[LDIF | LDAP] destination_options
```

Un fichier LDIF ne représente pas une destination valide en cas de mise à jour au moyen du cache de schéma.

Les options générales sont facultatives ; elles doivent toutefois être définies avant toute option source ou de destination. L'ordre des sections du gestionnaire `-S` (source) et `-D (cible)` est indifférent.

Voici la liste des gestionnaires source et cible disponibles :

- « Options du gestionnaire source LDIF » page 177
- « Options du gestionnaire de destination LDIF » page 178
- « Options du gestionnaire source LDAP » page 178
- « Options du gestionnaire de destination LDAP » page 181
- « Options du gestionnaire source DELIM » page 182
- « Options du gestionnaire cible DELIM » page 184
- « Options du gestionnaire source SCH » page 185
- « Options du gestionnaire source LOAD » page 185

Options générales

Les options générales ont une incidence sur l'ensemble du traitement effectué par le moteur Importation/Conversion/Exportation NetIQ.

Option	Description
`-C`	Indique que vous utilisez le cache de schéma pour procéder à la comparaison et à la mise à jour de schémas.
`-l` *`fichier_journal`*	Indique le nom du fichier dans lequel les messages de sortie (notamment les messages d'erreur) sont consignés. Si vous n'utilisez pas cette option, les messages d'erreur sont enregistrés dans le fichier `ice.log`. Si vous omettez cette option sur les ordinateurs Linux, les messages d'erreur ne seront pas enregistrés.
`-o`	Écrase le fichier journal existant. Si cet indicateur n'est pas défini, les messages sont ajoutés au fichier journal.

Option	Description
`-e` *`fichier_journal_erreurs_ LDIF`*	Indique le nom du fichier dans lequel les entrées qui échouent sont consignées au format LDIF. Vous pouvez consulter ce fichier, le modifier afin de corriger les erreurs et l'appliquer de nouveau au répertoire.
`-p` *`URL`*	Indique l'emplacement de la règle de placement XML que le moteur doit utiliser. Les règles de placement permettent de modifier le placement d'une entrée. Pour plus d'informations, reportez-vous à la section « Règles de conversion » page 193.
`-c URL`	Indique l'emplacement de la règle de création XML que le moteur doit utiliser. Les règles de création vous permettent de fournir les informations manquantes dont peut dépendre la réussite de la création d'une entrée lors d'une importation. Pour plus d'informations, reportez-vous à la section « Règles de conversion » page 193.
`-s` *`URL`*	Indique l'emplacement de la règle d'assignation de schéma XML que le moteur doit utiliser. Les règles d'assignation de schéma vous permettent d'assigner un élément de schéma d'un serveur source à un élément de schéma différent mais équivalent sur un serveur cible. Pour plus d'informations, reportez-vous à la section « Règles de conversion » page 193.
`-h` ou `-?`	Affiche l'aide relative à la ligne de commande.

Options de schéma

Les options de schéma vous permettent d'utiliser le cache de schéma pour effectuer des comparaisons et des mises à jour de schémas.

Option	Description
`-C -a`	Met à jour le schéma cible (ajoute le schéma manquant).
`-C -c` *`nom_fichier`*	Génère le schéma cible dans le fichier spécifié.
`-C -n`	Désactive la pré-vérification du schéma.

Options du gestionnaire source

L'option du gestionnaire source (`-S`) détermine la source des données d'importation. Vous ne pouvez spécifier qu'une seule des options suivantes sur la ligne de commande.

Option	Description
`-SLDIF`	Indique que la source est un fichier LDIF. Pour obtenir la liste des options LDIF prises en charge, reportez-vous à la section « Options du gestionnaire source LDIF » page 177.
`-SLDAP`	Indique que la source est un serveur LDAP. Pour obtenir la liste des options LDAP prises en charge, reportez-vous à la section « Options du gestionnaire source LDAP » page 178.

Option	Description
`-SDELIM`	Indique que la source est un fichier de données séparées par une virgule. **REMARQUE :** pour de meilleures performances, importez les données à l'aide de l'utilitaire Importation/Conversion/Exportation NetIQ avec le fichier LDIF au lieu de DELIM. Vous pouvez utiliser un script PERL personnalisé pour générer la sortie au format souhaité. Pour obtenir la liste des options DELIM prises en charge, reportez-vous à la section « Options du gestionnaire source DELIM » page 182.
`-SSCH`	Indique que la source est un fichier de schéma. Pour obtenir la liste des options SCH prises en charge, reportez-vous à la section « Options du gestionnaire source SCH » page 185.
`-SLOAD`	Indique que la source est un modèle DirLoad. Pour obtenir la liste des options LOAD prises en charge, reportez-vous à la section « Options du gestionnaire source LOAD » page 185.

Options du gestionnaire cible

L'option du gestionnaire cible (`-D`) permet de définir la cible des données d'exportation. Vous ne pouvez spécifier qu'une seule des options suivantes sur la ligne de commande.

Option	Description
`-DLDIF`	Indique que la destination est un fichier LDIF. Pour obtenir la liste des options prises en charge, reportez-vous à la section « Options du gestionnaire de destination LDIF » page 178.
`-DLDAP`	Indique que la destination est un serveur LDAP. Pour obtenir la liste des options prises en charge, reportez-vous à la section « Options du gestionnaire de destination LDAP » page 181.
`-DDELIM`	Indique que la destination est un fichier de données séparées par une virgule. Pour obtenir la liste des options prises en charge, reportez-vous à la section « Options du gestionnaire cible DELIM » page 184.

Options du gestionnaire source LDIF

Le gestionnaire source LDIF lit les données à partir d'un fichier LDIF, puis les transmet au moteur Importation/Conversion/Exportation NetIQ.

Option	Description
`-f` *`fichier_LDIF`*	Indique le nom du fichier qui contient les enregistrements LDIF que le gestionnaire source LDIF lit et transmet au moteur. Si vous omettez cette option sur les ordinateurs Linux, l'entrée standard est reprise.
`-a`	Si les enregistrements du fichier LDIF sont des enregistrements de contenu (c'est-à-dire qu'ils ne contiennent aucun type de modification), ils sont traités comme des enregistrements dont le type de modification est Ajouter (Add).

Option	Description
`-c`	Empêche le gestionnaire source LDIF de s'arrêter sur les erreurs. Cela comprend aussi bien les erreurs survenues au cours de l'analyse LDIF que celles renvoyées par le gestionnaire cible. Lorsque cette option est activée et qu'une erreur se produit, le gestionnaire source LDIF la signale, recherche l'enregistrement suivant dans le fichier LDIF et continue.
`-n`	N'exécute pas les opérations de mise à jour, mais imprime les résultats qui seraient obtenus. Lorsque cette option est définie, le gestionnaire source LDIF analyse le fichier LDIF, mais n'envoie aucun enregistrement au moteur Importation/Conversion/Exportation NetIQ (ou au gestionnaire cible).
`-m`	Si les enregistrements du fichier LDIF sont des enregistrements de contenu (c'est-à-dire qu'ils ne contiennent aucun type de modification), ils sont traités comme des enregistrements dont le type de modification est Modifier (Modify).
`-x`	Si les enregistrements du fichier LDIF sont des enregistrements de contenu (c'est-à-dire qu'ils ne contiennent aucun type de modification), ils sont traités comme des enregistrements dont le type de modification est Supprimer (Delete).
`-R` *`valeur`*	Indique la plage d'enregistrements à traiter.
`-v`	Active le mode verbeux du gestionnaire.
`-e` *`valeur`*	Modèle à utiliser pour déchiffrer les valeurs des attributs présents dans le fichier LDIF. [des/3des].
`-E` *`valeur`*	Mot de passe pour le déchiffrement des attributs. Vous pouvez utiliser la variable `ADM_E_SRC_PASSWD` pour chiffrer le gestionnaire source LDIF.

Options du gestionnaire de destination LDIF

Le gestionnaire cible LDIF reçoit les données du moteur Importation/Conversion/Exportation NetIQ et les inscrit dans un fichier LDIF.

Option	Description
`-f` *`fichier_LDIF`*	Indique le nom du fichier dans lequel les enregistrements LDIF peuvent être écrits. Si vous omettez cette option sur les ordinateurs Linux, la sortie est envoyée vers stdout.
`-B`	Indique de ne pas supprimer l'impression des valeurs binaires.
`-b`	Indique de ne pas coder au format base64 les données LDIF.
`-e` *`valeur`*	Modèle à utiliser pour chiffrer les valeurs d'attribut provenant du serveur LDAP.[des/3des].
`-E` *`valeur`*	Mot de passe de chiffrement des attributs. Vous pouvez utiliser la variable `ADM_E_DEST_PASSWD` pour chiffrer le gestionnaire cible LDIF.

Options du gestionnaire source LDAP

Le gestionnaire source LDAP lit les données d'un serveur LDAP en lui envoyant une requête de recherche. Il envoie ensuite au moteur Importation/Conversion/Exportation NetIQ les entrées résultant de cette opération de recherche.

Option	Description
`-s` *`nom_serveur`*	Indique le nom DNS ou l'adresse IP du serveur LDAP auquel le gestionnaire envoie une requête de recherche. L'hôte local est paramétré par défaut. **REMARQUE :** si vous utilisez eDirectory 9.1 ou une version ultérieure, indiquez le nom de domaine complet du serveur LDAP pour cette option.
`-p` *`port`*	Désigne le numéro de port (nombre entier) du serveur LDAP indiqué par *`nom_serveur`*. Le numéro de port par défaut est 389. Pour les opérations sécurisées, le numéro de port par défaut est 636. Lorsque ICE communique avec un serveur LDAP sur le port SSL (636 par défaut) sans certificat, il choisit d'accepter n'importe quel certificat de serveur et suppose que celui-ci est approuvé. Cette option doit être uniquement utilisée dans des environnements contrôlés où une communication codée entre serveurs et clients est souhaitée mais la vérification serveur superflue.
`-d` *`DN`*	Indique le nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur.
`-w` *`mot de passe`*	Indique l'attribut de mot de passe de l'entrée spécifiée par *`DN`*. `Vous pouvez utiliser la variable ADM_SRC_PASSWD` pour fournir des mots de passe au gestionnaire source LDAP.
`-M`	Invite à entrer le mot de passe de l'entrée spécifiée par *`DN`*. Cette option s'applique uniquement à Linux.
`-F` *`filtre`*	Indique un filtre de recherche conforme à la convention RFC 1558. Si vous omettez cette option, la valeur par défaut utilisée par le filtre est `objectclass=*`.
`-n`	N'exécute pas réellement la recherche, mais affiche un aperçu des résultats qui seraient obtenus.
`-a` *`liste_attributs`*	Indique la liste des attributs, séparés par une virgule, à récupérer au cours de la recherche. En plus des noms d'attribut, trois autres valeurs sont disponibles : ◆ N'obtient aucun attribut `(1.1)` ◆ Tous les attributs utilisateur `(*)` ◆ Une liste vide permet d'obtenir tous les attributs non opérationnels Si vous ne définissez pas cette option, la liste des attributs est par défaut une liste vide.
`-o` *`liste_attributs`*	Indique la liste des attributs, séparés par une virgule, à omettre des résultats de la recherche transmis par le serveur LDAP avant l'envoi au moteur. Cette option est pratique lorsque vous souhaitez utiliser un caractère joker avec l'option `–a` afin d'obtenir tous les attributs d'une classe donnée, puis de retirer certains d'entre eux des résultats de la recherche avant de transférer les données au moteur. Par exemple, `-a* -o telephoneNumber` recherche tous les attributs de niveau utilisateur et filtre les numéros de téléphone dans les résultats.
`-R`	Indique de ne pas suivre automatiquement les renvois. Le paramétrage par défaut consiste à suivre les renvois avec le nom et le mot de passe précisés dans les options `-d` et `-w`.

Option	Description
`-e` *`valeur`*	Précise les indicateurs de débogage à activer dans le kit de développement (SDK) client LDAP. Pour plus d'informations, reportez-vous à la section « Utilisation des drapeaux de débogage SDK LDAP ».
`-b` *`DN_base`*	Indique le nom distinctif de base de la requête de recherche. Si cette option n'est pas définie, la valeur par défaut du nom distinctif de base est une chaîne vide (« »).
`-c` *`étendue_recherche`*	Définit l'étendue de la requête de recherche. Les valeurs valides sont les suivantes : ◆ `One` : effectue la recherche uniquement dans les enfants immédiats de l'objet de base. ◆ `Base` : effectue la recherche uniquement dans l'entrée de l'objet de base proprement dit. ◆ `Sub` : effectue la recherche dans la sous-arborescence LDAP située à la racine de l'objet de base et dans l'objet de base proprement dit. Si cette option n'est pas définie, la valeur par défaut utilisée est `Sub`.
`-r` *`suppr_réf_alias`*	Indique le mode de suppression des références aux alias au cours de l'opération de recherche. Les valeurs sont les suivantes : ◆ `Never` (Jamais) : empêche le serveur de supprimer les références aux alias. ◆ `Always` (Toujours) : entraîne la suppression des références aux alias lors de la localisation de l'objet de base de la recherche et de l'évaluation des entrées correspondant au filtre de recherche. ◆ `Search` (Rechercher) : entraîne la suppression des références aux alias lors de l'application du filtre aux entrées dans l'étendue de la recherche après la localisation de l'objet de base, mais pas lors de la localisation de l'objet de base proprement dite. ◆ `Find` (Trouver) : entraîne la suppression des références aux alias lors de la localisation de l'objet de base de la recherche, mais pas lors de l'évaluation des entrées correspondant au filtre de la recherche. Si cette option n'est pas définie, la suppression des références aux alias prend par défaut la valeur `Never` (Jamais).
`-l` *`limite_temps`*	Indique la limite temporelle (en secondes) de la recherche.
`-z` *`limite_taille`*	Indique le nombre maximal d'entrées que la recherche peut renvoyer.
`-V` *`version`*	Indique la version du protocole LDAP à utiliser pour la connexion. Cette valeur doit être définie sur 2 ou 3. Si cette option n'est pas définie, elle est paramétrée par défaut sur 3.
`-v`	Active le mode verbeux du gestionnaire.
`-L` *`nom_fichier`*	Indique un fichier au format PEM qui contient une clé de serveur utilisée pour l'authentification SSL avec la valeur par défaut `/var/opt/novell/eDirectory/data/SSCert.pem`. **REMARQUE :** si le serveur LDAP utilise des certificats CE, vous devez transmettre `SSECCert.pem` avec cette option.

Option	Description
`-A`	Récupère uniquement le nom des attributs. L'opération de recherche ne renvoie pas les valeurs des attributs.
`-t`	Empêche le gestionnaire LDAP de s'arrêter sur les erreurs.
`-m`	Les opérations LDAP seront des modifications.
`-x`	Les opérations LDAP seront des suppressions.
`-k`	Cette option n'est plus prise en charge. Pour utiliser SSL, spécifiez un certificat valide à l'aide de l'option `-L`.
`-M`	Active la commande Gérer DSA IT.
`-MM`	Active la commande Gérer DSA IT et la rend prioritaire.

Options du gestionnaire de destination LDAP

Le gestionnaire cible LDAP reçoit des données du moteur Importation/Conversion/Exportation NetIQ et les renvoie à un serveur LDAP sous forme d'opérations de mise à jour que le serveur doit exécuter.

Pour des informations sur le mot de passe haché dans un fichier LDIF, reportez-vous à la section « Représentation du mot de passe haché dans les fichiers LDIF ».

Option	Description
`-s` *`nom_serveur`*	Indique le nom DNS ou l'adresse IP du serveur LDAP auquel le gestionnaire envoie une requête de recherche. L'hôte local est paramétré par défaut.
`-p` *`port`*	Désigne le numéro de port (nombre entier) du serveur LDAP indiqué par *`nom_serveur`*. Le numéro de port par défaut est 389. Pour les opérations sécurisées, le numéro de port par défaut est 636.
`-d` *`DN`*	Indique le nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur.
`-w` *`mot de passe`*	Indique l'attribut de mot de passe de l'entrée spécifiée par *`DN`*. Vous pouvez utiliser la variable `ADM_DEST_PASSWD` pour fournir des mots de passe au gestionnaire cible LDAP.
`-M`	Invite à entrer le mot de passe de l'entrée spécifiée par *`DN`*. Cette option s'applique uniquement à Linux.
`-B`	Sélectionnez cette option si vous ne voulez pas utiliser les requêtes asynchrones LDAP Bulk Update/Replication Protocol (LBURP) pour transférer les mises à jour vers le serveur. À la place, utilisez des requêtes d'opération de mise à jour LDAP synchrones standard. Pour plus d'informations, reportez-vous à la section « Protocole LBURP (LDAP Bulk Update/Replication Protocol) » page 202.
`-F`	Autorise la création de références en aval. Lorsqu'une entrée doit être créée avant son parent, une marque de réservation appelée **référence en aval** est ajoutée pour le parent de cette entrée afin d'en assurer la création correcte. Si une opération ultérieure crée le parent, la référence en aval se transforme en entrée normale.

Option	Description
`-l`	Stocke les valeurs de mot de passe à l'aide de la méthode de mot de passe simple du service NMAS (Modular Authentication Service) NetIQ. Les mots de passe sont conservés dans un emplacement sécurisé de l'annuaire ; les paires de clés ne sont pas générées tant qu'elles ne sont pas réellement requises pour l'authentification entre les serveurs.
`-e` *`valeur`*	Précise les indicateurs de débogage à activer dans le kit de développement (SDK) client LDAP. Pour plus d'informations, reportez-vous à la section « Utilisation des drapeaux de débogage SDK LDAP ».
`-V` *`version`*	Indique la version du protocole LDAP à utiliser pour la connexion. Cette valeur doit être définie sur 2 ou 3. Si cette option n'est pas définie, elle est paramétrée par défaut sur 3.
`-L` *`nom_fichier`*	Indique un fichier au format PEM qui contient une clé de serveur utilisée pour l'authentification SSL avec la valeur par défaut `/var/opt/novell/eDirectory/data/SSCert.pem`. **REMARQUE :** si le serveur LDAP utilise des certificats CE, vous devez transmettre `SSECCert.pem` avec cette option.
`-k`	Cette option n'est plus prise en charge. Pour utiliser SSL, spécifiez un certificat valide à l'aide de l'option `-L`.
`-M`	Active la commande Gérer DSA IT.
`-MM`	Active la commande Gérer DSA IT et la rend prioritaire.
`-P`	Active le traitement LBURP concurrent. Cette option n'est activée que si toutes les opérations dans LDIF sont des ajouts (add). Lorsque vous utilisez l'option `-F`, `-P` est activé par défaut.
`-Z`	Indique le nombre de requêtes asynchrones. Cette option indique le nombre d'entrées que le client ICE peut envoyer au serveur LDAP en mode asynchrone avant d'attendre l'envoi des résultats par le serveur.

Options du gestionnaire source DELIM

Le gestionnaire source DELIM lit des données provenant d'un fichier de données séparées par une virgule, avant de les envoyer au gestionnaire cible.

Option	Description
`-f` *`nom_fichier`*	Indique le nom d'un fichier qui contient des enregistrements séparés par une virgule que le gestionnaire source DELIM lit et transmet au gestionnaire cible.
`-F` *`valeur`*	Précise le nom du fichier contenant l'ordre des données d'attribut pour le fichier spécifié par `-f`. Le nombre de colonnes pour un attribut dans le fichier délimité correspond par défaut au nombre maximal de valeurs pour l'attribut. En cas de répétition de l'attribut, le nombre de colonnes est égal au nombre de fois que l'attribut se répète dans le modèle. Si cette option n'est pas définie, saisissez directement cette information en utilisant `-t`. Pour plus d'informations, reportez-vous à la section « Importation de données séparées par une virgule » page 188.

Option	Description
`-t` *`valeur`*	Liste des attributs séparés par une virgule qui précise l'ordre des données d'attribut pour le fichier spécifié par l'option `-f`. Le nombre de colonnes pour un attribut dans le fichier délimité correspond par défaut au nombre maximal de valeurs pour l'attribut. En cas de répétition de l'attribut, le nombre de colonnes est égal au nombre de fois que l'attribut se répète dans le modèle. Cette option ou l'option `-F` doit être définie. Pour plus d'informations, reportez-vous à la section « Importation de données séparées par une virgule » page 188.
`-c`	Empêche le gestionnaire source DELIM de s'arrêter sur les erreurs. Cela comprend aussi bien les erreurs survenues au cours de l'analyse de fichiers de données séparées par une virgule que celles renvoyées par le gestionnaire cible. Lorsque cette option est définie et qu'une erreur se produit, le gestionnaire source DELIM la signale, recherche l'enregistrement suivant dans le fichier de données séparées par une virgule et continue.
`-n` *`valeur`*	Indique l'attribut d'assignation LDAP du nouvel objet. Cet attribut doit être contenu dans les données d'attribut définies à l'aide des options `-F` ou `-t`.
`-l` *`valeur`*	Indique le chemin d'accès auquel le RDN doit être annexé (par exemple, `o=myCompany`). En cas de transmission du DN, cette valeur est facultative.
`-o` *`valeur`*	Liste des classes d'objet (si aucune ne figure dans votre fichier d'entrée) ou des classes d'objet supplémentaires, telles que les classes auxiliaires, séparées par une virgule. La valeur par défaut est `inetorgperson`.
`-i` *`valeur`*	Liste des colonnes à ignorer, séparées par des virgules. Cette valeur est un nombre entier correspondant au numéro de la colonne à ignorer. Par exemple, pour ignorer les troisième et cinquième colonnes, entrez `i3,5`.
`-d` *`valeur`*	Indique le séparateur. Le séparateur par défaut est une virgule (,). Les valeurs ci-dessous sont des séparateurs spéciaux : ◆ `[q]` = guillemets (un seul caractère " comme séparateur) ◆ `[t]` = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier `-d[t]`.
`-q` *`valeur`*	Indique le séparateur secondaire. Les guillemets simples (' ') sont utilisés comme séparateur secondaire par défaut. Les valeurs ci-dessous sont des séparateurs spéciaux : ◆ `[q]` = guillemets (un seul caractère " comme séparateur) ◆ `[t]` = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier `-q[t]`.
`-v`	Exécution en mode verbeux.
`-k` *`valeur`*	Indique que la première ligne dans le fichier délimité constitue le modèle. Si cette option est utilisée avec `-t` ou `-F` , le modèle spécifié est vérifié afin qu'il soit cohérent avec celui du fichier délimité.

Options du gestionnaire cible DELIM

Le gestionnaire cible DELIM reçoit les données provenant d'un gestionnaire source et les écrit dans un fichier de données séparées par une virgule.

Option	Description
`-f nom_fichier`	Indique le nom du fichier dans lequel des enregistrements séparés par une virgule peuvent être écrits.
`-F valeur`	Précise le nom du fichier contenant l'ordre des données d'attribut pour le fichier spécifié par `-f`. Le nombre de colonnes pour un attribut dans le fichier délimité correspond par défaut au nombre maximal de valeurs pour l'attribut. En cas de répétition de l'attribut, le nombre de colonnes est égal au nombre de fois que l'attribut se répète dans le modèle. Si cette option n'est pas définie, saisissez directement cette information en utilisant `-t`.
`-t valeur`	Liste des attributs séparés par une virgule qui précise l'ordre des données d'attribut pour le fichier spécifié par l'option `-f`. Le nombre de colonnes pour un attribut dans le fichier délimité correspond par défaut au nombre maximal de valeurs pour l'attribut. En cas de répétition de l'attribut, le nombre de colonnes est égal au nombre de fois que l'attribut se répète dans le modèle. Cette option ou l'option `-F` doit être définie.
`-l valeur`	Peut être soit RDN ou DN. Indique si le pilote doit placer le DN entier, ou seulement le RDN, dans les données. Le RDN est la valeur par défaut.
`-d valeur`	Indique le séparateur. Le séparateur par défaut est une virgule (,). Les valeurs ci-dessous sont des séparateurs spéciaux : ◆ `[q]` = guillemets (un seul caractère " comme séparateur) ◆ `[t]` = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier `-d[t]`.
`-q valeur`	Indique le séparateur secondaire. Les guillemets simples (' ') sont utilisés comme séparateur secondaire par défaut. Les valeurs ci-dessous sont des séparateurs spéciaux : ◆ `[q]` = guillemets (un seul caractère " comme séparateur) ◆ `[t]` = tabulation Par exemple, pour indiquer qu'une tabulation est un séparateur, vous devez spécifier `-q[t]`.
`-n valeur`	Indique un attribut d'assignation de nom à ajouter au cours de l'importation, par exemple, `cn`.

Options du gestionnaire source SCH

Le gestionnaire SCH lit les données à partir d'un fichier de schéma NDS ou eDirectory hérité (fichiers avec l'extension `*.sch`), puis les envoie au moteur Importation/Conversion/Exportation NetIQ. Vous pouvez utiliser ce gestionnaire pour mettre en oeuvre des opérations liées au schéma sur un serveur LDAP, par exemple des extensions avec un fichier `*.sch` en entrée.

Le gestionnaire SCH est uniquement un gestionnaire source. Vous pouvez l'utiliser pour importer des fichiers `*.sch` dans un serveur LDAP, mais pas pour exporter des fichiers `*.sch`.

Les options prises en charge par le gestionnaire SCH sont indiquées dans le tableau suivant.

Option	Description
-f nom_fichier	Indique le chemin d'accès complet au fichier `*.sch`.
`-v`	(Facultatif) Exécution en mode verbeux.

Options du gestionnaire source LOAD

Le gestionnaire DirLoad génère les informations eDirectory à partir des commandes d'un modèle. Ce fichier de modèle est spécifié avec l'argument `-f` et contient les informations de spécification d'attribut et les informations de contrôle de programme.

Option	Description
-f nom_fichier	Indique le fichier modèle qui contient toutes les spécifications d'attribut et toutes les informations de contrôle pour exécuter le programme.
`-c`	Continue l'exécution sur l'enregistrement suivant si une erreur est signalée.
`-v`	Exécution en mode verbeux.
`-r`	Transforme la requête en requête de suppression : les données sont supprimées au lieu d'être ajoutées. Cette option permet de supprimer des enregistrements ajoutés à l'aide d'un modèle DirLoad.
`-m`	Indique que le fichier modèle contient des demandes de modification.

Les spécifications d'attributs déterminent le contexte des nouveaux objets.

Reportez-vous à l'exemple suivant de fichier de spécification d'attributs :

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last)
dn:cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn),ou=dev,ou=ds,o=novell
objectclass: inetorgperson
telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)
title: $R(titles)
locality: Our location
```

Le format du fichier de spécification d'attributs est semblable à celui d'un fichier LDIF. Cependant, il permet d'exploiter des structures performantes pour fournir des informations supplémentaires et définir des relations entre les attributs.

La valeur numérique unique insère dans une valeur d'attribut une valeur numérique unique pour un objet donné.

```
Syntax: $C[(<format)]
```

La variable facultative *<format* indique le format d'impression à appliquer à la valeur. Notez que si aucun format n'est spécifié, il est également impossible d'utiliser les parenthèses :

```
$C
$C(%d)
$C(%04d)
```

La séquence simple `$C` insère la valeur numérique courante dans une valeur d'attribut. Elle équivaut à `$C(%d)`, car « `%d` » est le format par défaut utilisé par le programme si aucun autre format n'est spécifié. La valeur numérique est incrémentée après chaque objet : si vous utilisez `$C` à plusieurs reprises dans la spécification d'attribut, la valeur est identique pour un même objet. La valeur initiale peut être spécifiée dans le fichier de paramètres à l'aide de la syntaxe `!COUNTER=valeur`.

La valeur numérique aléatoire insère une valeur numérique aléatoire dans une valeur d'attribut, conformément à la syntaxe suivante :

```
$N(<low-<high[,<format])]
```

Les variables *<bas* et *<haut* fixent respectivement les limites inférieure et supérieure employées pour générer un nombre aléatoire. La variable facultative *<format* indique le format d'impression à appliquer à une valeur de la liste.

```
$N(1-999)
$N(1-999,%d)
$N(1-999,%03d)
```

La valeur de chaîne aléatoire provenant d'une liste insère dans une valeur d'attribut une chaîne sélectionnée de façon aléatoire dans une liste spécifiée, conformément à la syntaxe suivante :

```
$R(<filename[,<format])]
```

La variable *<nom_fichier* désigne un fichier qui contient une liste de valeurs. Il peut s'agir du chemin absolu ou relatif d'un fichier. Divers fichiers contenant les listes sont inclus avec ce paquetage. Les valeurs doivent être séparées par un caractère de retour à la ligne.

La variable facultative *<format* indique le format d'impression à appliquer à une valeur de la liste.

```
$A(givenname)
$A(givenname,%s)
$A(givenname,%.1s)
```

Notez que les références en aval ne sont pas autorisées. Tout attribut dont vous prévoyez d'utiliser la valeur doit précéder l'attribut actuel dans le fichier de spécification d'attributs. Dans l'exemple suivant, le cn en tant que partie du DN est constitué à partir de givenname, initial et sn. Par conséquent, ces attributs doivent précéder le DN dans le fichier de paramètres.

```
givenname: $R(first)
initial: $R(initial)
sn: $R(last) dn:o=novell,ou=dev,ou=ds,cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn)
```

Le DN reçoit un traitement particulier dans le fichier LDIF : quel que soit l'emplacement du DN dans les paramètres, il sera écrit en premier (conformément à la syntaxe LDIF) dans le fichier LDIF. Tous les autres attributs sont écrits dans l'ordre dans lequel ils apparaissent.

Les paramètres de contrôle fournissent des contrôles supplémentaires pour la création d'objets. Pour tous les contrôles, un point d'exclamation (!) figure en début de ligne et permet de les distinguer des paramètres d'attribut. Les contrôles peuvent apparaître n'importe où dans le fichier.

```
!COUNTER=300
!OBJECTCOUNT=2
!CYCLE=title
!UNICYCLE=first,last
!CYCLE=ou,BLOCK=10
```

- Compteur

  Fournit la valeur initiale pour la valeur de compteur unique. La valeur du compteur est insérée dans un attribut quelconque avec la syntaxe `$C`.

- Object Count (Nombre d'objets)

  `Le paramètre OBJECTCOUNT détermine le nombre d'objets créés à partir du modèle.`

- Cycle

  `Le paramètre CYCLE peut servir à modifier le mode d'extraction des valeurs aléatoires à partir des fichiers (syntaxe $R).` Il peut présenter trois valeurs.

  `!CYCLE=title`

  Dès que la liste nommée « title » (titre) est utilisée, le système extrait la valeur suivante de la liste au lieu de sélectionner une valeur de façon aléatoire. Une fois toutes les valeurs utilisées dans l'ordre, la liste reprend au début.

  `!CYCLE=ou,BLOCK=10`

  Chaque valeur de la liste « ou » doit être utilisée 10 fois avant de passer à la valeur suivante.

  La variante la plus intéressante du paramètre de contrôle `CYCLE` est `UNICYCLE`. Elle indique une liste de sources qui sont parcourues de façon cyclique de gauche à droite, permettant ainsi de créer, si nécessaire, des valeurs dont l'unicité est garantie. En cas d'emploi de ce contrôle, le contrôle `OBJECTCOUNT` sert uniquement à limiter le nombre d'objets au nombre maximum d'objets uniques pouvant être créés à partir des listes. En d'autres termes, si les listes désignées dans `UNICYCLE` peuvent produire 15 000 objets, `OBJECTCOUNT` peut servir à réduire ce nombre, mais pas à l'augmenter.

  Par exemple, supposons que le fichier `givenname` contienne deux valeurs (Doug et Karl) et que le fichier `sn` en contienne trois (Hoffman, Schultz et Grieger). Avec le paramètre de contrôle `!UNICYCLE=givenname,sn` et la définition d'attribut `cn: $R(givenname) $R(sn)`, les CN suivants sont créés :

  `cn: Doug Hoffmancn cn: Karl Hoffmancn cn: Doug Schultzcn cn: Karl Schultzcn cn: Doug Griegercn cn: Karl Grieger`

Exemples

Voici des exemples de commandes que vous pouvez utiliser avec l'utilitaire de ligne de commande Importation/Conversion/Exportation NetIQ pour les fonctions suivantes :

- « Exécution d'une importation LDIF » page 188
- « Exécution d'une exportation LDIF » page 188
- « Importation de données séparées par une virgule » page 188
- « Exportation de données séparées par une virgule » page 189
- « Exécution d'une migration de données entre des serveurs LDAP » page 189
- « Exécution d'une importation de schéma » page 190
- « Exécution d'une importation de fichier LOAD » page 190

- « Exécution d'une exportation LDIF à partir d'un serveur LDAP contenant des attributs chiffrés » page 192
- « Exécution d'une importation LDIF comportant des attributs chiffrés » page 192

Exécution d'une importation LDIF

Pour effectuer une importation LDIF, associez le gestionnaire source LDIF et le gestionnaire de destination LDAP de la manière suivante :

```
ice -S LDIF -f entries.ldif -D LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w
secret
```

Cette commande permet de lire les données LDIF à partir du fichier `entries.ldif` et de les envoyer au serveur LDAP server1.acme.com sur le port 389 à l'aide de l'identité cn=admin,c=us et du mot de passe « secret ».

Exécution d'une exportation LDIF

Pour effectuer une exportation LDIF, associez le gestionnaire source LDAP et le gestionnaire cible LDIF. Par exemple :

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDIF -f server1.ldif
```

Cette commande permet de rechercher dans une sous-arborescence tous les objets situés sur le serveur server1.acme.com au niveau du port 389, à l'aide de l'identité cn=admin,c=us et du mot de passe « password », ainsi que de générer les données au format LDIF dans le fichier `server1.ldif`.

Importation de données séparées par une virgule

Pour exécuter une importation délimitée par des virgules, utilisez une commande similaire à la suivante :

```
ice -S DELIM -f/tmp/in.csv -F /tmp/order.csv -ncn -lo=acme -D LDAP -s
server1.acme.com -p389 -d cn=admin,c=us -w secret
```

Cette commande lit les données séparées par une virgule du fichier `/tmp/in.csv`, ainsi que l'ordre des attributs, défini dans le fichier `/tmp/order.csv`. Pour chaque entrée d'attribut du fichier `in.csv`, le type d'attribut est spécifié dans le fichier `order.csv`. Par exemple, si le fichier `in.csv` contient

```
pat,pat,engineer,john
```

alors le fichier `order.csv` contient

```
dn,cn,title,sn
```

Les informations du fichier `order.csv` peuvent être saisies directement à l'aide de l'option `-t`.

Les données sont ensuite envoyées au serveur LDAP `server1.acme.com` sur le port 389 à l'aide de l'identité `cn=admin,c=us` et du mot de passe « `secret` ».

Cet exemple indique que cn doit devenir le nouveau DN pour cet à en utilisant l'option `-n` et cet objet a été ajouté au conteneur Organisation acme à l'aide de l'option `-l`.

Le modèle utilisé pour générer des fichiers séparés par une virgule créés à l'aide de l'utilitaire Importation/Conversion/Exportation NetIQ figure à la première ligne. Pour spécifier que la première ligne du fichier délimité est le modèle, utilisez l'option `-k`. Si `F -` ou `-t` est utilisé avec `-k`, le modèle spécifié doit être cohérent avec celui dans le fichier délimité, dans lequel les deux possèdent exactement les mêmes attributs. Toutefois, le nombre d'occurrences et l'ordre d'apparition de chaque attribut peuvent différer. Dans l'exemple ci-dessus, le fichier `in.csv` contient

`dn,cn,title,title,title,sn` à la première ligne. Les modèles suivants sont cohérents et peuvent être utilisés avec l'option -t ou -F lorsque -k est utilisé :

`dn,cn,title,sn` (le nombre de répétitions du titre de l'attribut diffère)

`dn,sn,titre cn` (l'ordre des attributs diffère)

Toutefois, les éléments suivants ne sont pas compatibles avec le modèle `in.csv` et ne peuvent donc pas être spécifiés avec l'option -t ou -F lorsque -k est utilisé :

`dn,cn,title,sn,objectclass` (nouvel attribut de classe d'objet)

`dn,cn,title` (attribut `sn` manquant)

Exportation de données séparées par une virgule

Pour exécuter une exportation délimitée par des virgules, utilisez une commande similaire à la suivante :

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D DELIM -f /tmp/server1.csv -F order.csv
```

Cette commande permet de rechercher dans une sous-arborescence tous les objets situés sur le serveur server1.acme.com au niveau du port 389, à l'aide de l'identité cn=admin,c=us et du mot de passe « password » et compile les données séparées par une virgule, dans le fichier `/tmp/server1.csv`.

Si un attribut dans le fichier `order.csv` a plusieurs valeurs, `/tmp/server1.csv`, le nombre de colonnes pour cet attribut correspond au nombre maximal de valeurs pour l'attribut. Si un attribut se répète dans le fichier `order.csv`, le nombre de colonnes pour cet attribut correspond au nombre de répétitions de l'attribut.

Par exemple, si le fichier `order.csv` contient `dn, sn,objectclass` et que `objectclass` possède 4 valeurs, alors que `dn` et `sn` ont uniquement 1 valeur pour toutes les entrées exportées, `dn` et `sn` auraient 1 colonne tandis que `objectclass` compterait 4 colonnes. Si vous ne voulez que 2 valeurs pour `objectclass` dans le fichier délimité, le fichier `order.csv` doit contenir `dn,sn,objectclass,objectclass`.

Dans les deux cas, les attributs sont écrits dans le fichier `/tmp/server1.csv` sur la première ligne. Dans le premier cas, la première ligne du fichier `/tmp/server1.csv` sera `dn,sn,objectclass,objectclass,objectclass,objectclasss`, et dans le second cas, elle contiendra `dn,sn,objectclass,objectclass`.

Pour éviter que la première ligne soit considérée comme une succession d'attributs lors d'une importation ultérieure, utilisez l'option `-k`. Pour plus d'informations, reportez-vous à la section « Importation de données séparées par une virgule » page 188.

Exécution d'une migration de données entre des serveurs LDAP

Pour effectuer une migration de données entre des serveurs LDAP, associez les gestionnaires source et cible LDAP. Par exemple :

```
ice -S LDAP -s server1.acme.com -p 389 -d cn=admin,c=us -w password -F
objectClass=* -c sub -D LDAP -s server2.acme.com -p 389 -d cn=admin,c=us -w secret
```

Cette commande permet de rechercher dans une sous-arborescence tous les objets situés sur le serveur server1.acme.com au niveau du port 389, sous l'identité cn=admin,c=us et à l'aide du mot de passe « password » et envoie les données au serveur LDAP server2.acme.com sur le port 389 sous l'identité cn=admin,c=us à l'aide du mot de passe « secret ».

Exécution d'une importation de schéma

Pour exécuter une importation de schéma, utilisez une commande similaire à la suivante :

```
ice -S SCH -f $HOME/myfile.sch -D LDAP -s myserver -d cn=admin,o=novell -w passwd
```

Cette commande lit les données de schéma à partir du fichier `myfile.sch` et les envoie au serveur LDAP myserver sous l'identité `cn=admin,o=novell` et à l'aide de du mot de passe « `passwd` ».

Exécution d'une importation de fichier LOAD

Pour exécuter une importation de fichier LOAD, utilisez une commande similaire à la suivante :

```
ice -S LOAD -f attrs -D LDIF -f new.ldf
```

Dans cet exemple, le contenu du fichier d'attributs `attrs` est le suivant :

```
#=====================================================================

#  DirLoad 1.00
#=====================================================================

!COUNTER=300

!OBJECTCOUNT=2
#---------------------------------------------------------------------

#  ATTRIBUTE TEMPLATE
# -------------------------------------------------------------------

objectclass: inetorgperson

givenname: $R(first)

initials: $R(initial)

sn: $R(last)

dn: cn=$A(givenname,%.1s)$A(initial,%.1s)$A(sn),ou=$R(ou),ou=dev,o=novell,

telephonenumber: 1-800-$N(1-999,%03d)-$C(%04d)

title: $R(titles)
```

L'exécution de la commande précédente à partir de l'invite de commande génère le fichier LDIF suivant :

```
version: 1

dn: cn=JohnBBill,ou=ds,ou=dev,o=novell

changetype: add

objectclass: inetorgperson

givenname: John

initials: B

sn: Bill

telephonenumber: 1-800-290-0300

title: Amigo
```

```
dn: cn=BobJAmy,ou=ds,ou=dev,o=novell

changetype: add

objectclass: inetorgperson

givenname: Bob

initials: J

sn: Amy

telephonenumber: 1-800-486-0301

title: Pomo
```

L'exécution de la commande suivante à partir de l'invite de commande entraîne l'envoi des données à un serveur LDAP via le gestionnaire LDAP :

```
ice -S LOAD -f attrs -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

Si le fichier de modèle précédent est utilisé avec la commande suivante, tous les enregistrements ajoutés via la commande ci-dessus sont supprimés.

```
ice -S LOAD -f attrs -r -D LDAP -s www.novell.com -d cn=admin,o=novell -w admin
```

L'exemple ci-dessous illustre la façon de modifier des enregistrements à l'aide du paramètre –m :

```
# ====================================================================

#  DirLoad 1.00

# ====================================================================
!COUNTER=300

!OBJECTCOUNT=2

#--------------------------------------------------------------------

#  ATTRIBUTE TEMPLATE

# --------------------------------------------------------------------

dn: cn=$R(first),%.1s)($R(initial),%.1s)$R(last),ou=$R(ou),ou=dev,o=novell

delete: givenname

add: givenname

givenname: test1

replace: givenname

givenname: test2

givenname: test3
```

Si le fichier `attrs` contient les données ci-dessus et que vous utilisez la commande suivante :

```
ice -S LOAD -f attrs -m -D LDIF -f new.ldf
```

les données LDIF suivantes sont générées :

```
version: 1
```

```
dn: cn=BillTSmith,ou=ds,ou=dev,o=novell

changetype: modify

delete: givenname

-

add: givenname

givenname: test1

-

replace: givenname

givenname: test2

givenname: test3

-

dn: cn=JohnAWilliams,ou=ldap,ou=dev,o=novell

changetype: modify

delete: givenname

-

add: givenname

givenname: test1

-

replace: givenname

givenname: test2

givenname: test3

-
```

Exécution d'une exportation LDIF à partir d'un serveur LDAP contenant des attributs chiffrés

Pour effectuer une exportation LDIF à partir d'un serveur LDAP comportant des attributs chiffrés, associez le gestionnaire source LDAP et le gestionnaire cible LDIF, ainsi que le modèle et le mot de passe de chiffrement. Par exemple :

```
ice -S LDAP -s server1.acme.com -p 636 -L cert-server1.pem -d cn=admin,c=us -w
password -F objectClass=* -c sub -D LDIF -f server1.ldif -e des -E secret
```

Exécution d'une importation LDIF comportant des attributs chiffrés

Pour effectuer une importation LDIF d'un fichier dont les attributs ont été précédemment chiffrés par ICE, associez la source LDIF au modèle et mot de passe utilisés précédemment pour l'exportation du fichier et au gestionnaire cible LDAP. Par exemple :

```
ice -S LDIF -f server1.ldif -e des -E secret -D LDAP -s server2.acme.com -p 636 -L
cert-server2.pem -d cn=admin,c=us -w password
```

Règles de conversion

Le moteur Importation/Conversion/Exportation NetIQ vous permet de définir un ensemble de règles qui décrivent les opérations de traitement à réaliser sur chaque enregistrement reçu du gestionnaire source, avant sa transmission au gestionnaire cible. Ces règles sont définies au format XML (sous la forme soit d'un fichier XML, soit de données XML stockées dans l'annuaire) et résolvent les problèmes suivants lors de l'importation d'entrées à partir d'un annuaire LDAP dans un autre :

- Informations manquantes
- Différences hiérarchiques
- Différences de schémas

Trois types de règle de conversion sont disponibles :

Règle	Description
Placement	Modifie le placement d'une entrée. Par exemple, si vous importez un groupe d'utilisateurs vers le conteneur l=San Francisco, c=États-Unis et que vous souhaitez ensuite placer ces utilisateurs dans le conteneur l=Los Angeles, c=États-Unis une fois l'importation terminée, vous pouvez le faire en utilisant une règle de placement. Pour plus d'informations sur le format de ces règles, reportez-vous à la section « Règles de placement » page 198.
Création	Fournit les informations manquantes qui peuvent s'avérer nécessaires à la création d'une entrée lors de l'importation. Par exemple, supposons que vous ayez exporté des données LDIF à partir d'un serveur dont le schéma requiert uniquement l'attribut cn (commonName) pour les entrées utilisateur, mais que le serveur dans lequel vous importez ces données LDIF nécessite à la fois les attributs cn et sn (surname). Vous pouvez alors utiliser la règle de création pour fournir une valeur sn par défaut (telle que « ») pour chacune des entrées lors de leur traitement par le moteur. Lorsque ces entrées sont envoyées au serveur cible, elles contiennent l'attribut sn requis et leur ajout peut s'effectuer correctement. Pour plus d'informations sur le format de ces règles, reportez-vous à la section « Règles de création » page 196.
Assignation de schéma	Si, lors du transfert de données entre des serveurs (directement ou via LDIF), il existe des différences entre les schémas des serveurs, vous pouvez utiliser la règle Assignation de schéma pour effectuer les opérations suivantes : ◆ Étendre le schéma sur le serveur cible afin d'intégrer les classes d'objet et les types d'attribut dans des entrées provenant du serveur source. ◆ assigner un élément de schéma du serveur source à un élément de schéma différent mais équivalent sur le serveur cible. Pour plus d'informations sur le format de ces règles, reportez-vous à la section « Règles d'assignation de schéma » page 195.

Vous pouvez activer les règles de conversion dans l'assistant Importation/Exportation NetIQ eDirectory, ainsi que dans l'interface de ligne de commande. Pour plus d'informations sur les règles XML, reportez-vous à la section « Utilisation des règles XML » page 194.

Utilisation de l'Assistant d'importation, de conversion et d'exportation NetIQ eDirectory

1. Dans iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Sélectionnez la tâche à exécuter.
4. Dans **Paramètres avancés**, sélectionnez l'une des options suivantes :

Option	Description
Règles de schéma	Indique l'emplacement de la règle d'assignation de schéma XML que le moteur doit utiliser.
Règles de placement	Indique l'emplacement de la règle de placement XML que le moteur doit utiliser.
Règles de création	Indique l'emplacement de la règle de création XML que le moteur doit utiliser.

5. Cliquez sur **Suivant**.
6. Suivez les instructions en ligne pour terminer la tâche sélectionnée.

Utilisation de l'interface de ligne de commande

Vous pouvez activer les règles de conversion à l'aide des options générales `-p`, `-c` et `-s` dans le fichier exécutable d'importation, de conversion et d'exportation NetIQ. Pour plus d'informations, reportez-vous à la section « Options générales » page 175.

Option	Description
`-p` *URL*	Emplacement de la règle de placement XML que le moteur doit utiliser.
`-c` *URL*	Emplacement de la règle de création XML que le moteur doit utiliser.
`-s` *URL*	Emplacement de la règle d'assignation de schéma XML que le moteur doit utiliser.

Pour ces trois options, la variable *URL* doit se présenter comme suit :

- URL au format suivant :

  `file://[path/]filename`

  Le fichier doit se trouver sur le système de fichiers local.
- URL LDAP conforme à la convention RFC 2255 qui spécifie une recherche de niveau de base et une liste d'attributs comportant la description d'un seul attribut pour un type d'attribut à valeur unique.

Utilisation des règles XML

Les règles de conversion de l'utilitaire Importation/Conversion/Exportation NetIQ utilisent le même format XML que NetIQ Identity Manager. Pour plus d'informations sur NetIQ Identity Manager, rendez-vous sur le *site de documentation de NetIQ Identity Manager*.

Règles d'assignation de schéma

L'élément `<attr-name-map>` est l'élément le plus élevé pour les règles d'assignation de schéma. Les règles d'assignation déterminent comment le schéma d'importation interagit avec le schéma d'exportation. Elles associent les définitions et les attributs de classe d'importation indiqués aux définitions correspondantes dans le schéma d'exportation.

Les règles d'assignation peuvent être définies pour les noms d'attribut ou les noms de classe.

- Pour une assignation d'attribut, la règle doit spécifier qu'il s'agit d'une assignation d'attribut, mais elle doit également indiquer un espace de noms (`nds-name` est la balise pour le nom source), le nom dans l'espace de noms eDirectory, puis l'autre espace de noms (`app-name` est la balise pour le nom cible) et le nom dans ce dernier. Elle peut spécifier que l'assignation s'applique à une classe particulière ou à toutes les classes comportant l'attribut.
- Pour une assignation de classe, la règle doit spécifier qu'il s'agit d'une assignation de classe, mais elle doit également indiquer un espace de nom (eDirectory ou l'application), le nom dans cet espace de nom, puis l'autre espace de nom et le nom dans cet espace de nom.

Voici la définition formelle des DTD concernant les règles d'assignation de schéma:

```
<!ELEMENT attr-name-map (attr-name | class-name)*>

<!ELEMENT attr-name (nds-name, app-name)>
<!ATTLIST attr-name
          class-name    CDATA    #IMPLIED>

<!ELEMENT class-name (nds-name, app-name)>

<!ELEMENT nds-name (#PCDATA)>

<!ELEMENT app-name (#PCDATA)>
```

Vous pouvez avoir plusieurs éléments d'assignation dans un fichier. Chaque élément est traité dans l'ordre où il apparaît dans le fichier. Si vous assignez la même classe ou le même attribut plusieurs fois, la première assignation est prioritaire.

Les exemples suivants illustrent la création d'une règle d'assignation de schéma.

Règle de schéma 1 : La règle suivante assigne l'attribut nom de source à l'attribut sn de destination pour la classe inetOrgPerson.

```
<attr-name-map>
   <attr-name class-name="inetOrgPperson">
      <nds-name>surname</nds-name>
      <app-name>sn</app-name>
   </attr-name>
</attr-name-map>
```

Règle de schéma 2 : La règle suivante assigne la définition de classe inetOrgPerson source à la définition de classe Utilisateur de destination.

```
<attr-name-map>
   <class-name>
      <nds-name>inetOrgPerson</nds-name>
      <app-name>User</app-name>
   </class-name>
</attr-name-map>
```

Règle de schéma 3 : L'exemple suivant contient deux règles. La première règle assigne l'attribut nom de source à l'attribut sn de destination pour toutes les classes qui utilisent ces attributs. La deuxième règle assigne la définition de classe inetOrgPerson source à la définition de classe Utilisateur de destination.

```
<attr-name-map>
   <attr-name>
      <nds-name>surname</nds-name>
      <app-name>sn</app-name>
   </attr-name>
   <class-name>
      <nds-name>inetOrgPerson</nds-name>
      <app-name>User</app-name>
   </class-name>
</attr-name-map>
```

Exemple de commande : Si les règles d'assignation de schéma sont enregistrées dans un fichier `sr1.xml`, la commande suivante indique à l'utilitaire de les exploiter lors du traitement du fichier `1entry.ldf` et d'envoyer les résultats à un fichier cible, `outt1.ldf`.

```
ice -o -sfile://sr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

Règles de création

Les règles de création précisent les conditions de création d'une nouvelle entrée dans le répertoire de destination. Elles prennent en charge les éléments suivants :

- **Attributs requis** indique qu'un enregistrement d'ajout doit avoir des valeurs pour tous les attributs requis, faute de quoi l'ajout échoue. La règle peut fournir une valeur par défaut pour un attribut requis. Si un enregistrement n'a pas de valeur pour l'attribut, l'entrée se voit attribuer la valeur par défaut. Si l'enregistrement possède une valeur, celle-ci est utilisée.
- **Attributs de concordance :** spécifie qu'un enregistrement d'ajout doit avoir les attributs spécifiés et doit correspondre aux valeurs indiquées, faute de quoi l'ajout échoue.
- **Modèles** indique le nom distinctif d'un objet Modèle dans eDirectory. Actuellement, l'utilitaire Importation/Conversion/Exportation NetIQ ne prend pas en charge la spécification de modèles dans les règles de création.

Voici la définition formelle des DTD concernant les règles de création :

```
<!ELEMENT create-rules (create-rule)*>

<!ELEMENT create-rule (match-attr*,
                       required-attr*,
                       template?) >
<!ATTLIST create-rule
          class-name    CDATA   #IMPLIED
          description   CDATA   #IMPLIED>

<!ELEMENT match-attr    (value)+ >
<!ATTLIST match-attr
          attr-name      CDATA    #REQUIRED>

<!ELEMENT required-attr (value)*>
<!ATTLIST required-attr
          attr-name     CDATA   #REQUIRED>

<!ELEMENT template EMPTY>
<!ATTLIST template
          template-dn   CDATA   #REQUIRED>
```

Vous pouvez avoir plusieurs éléments de règle de création dans un fichier. Chaque règle est traitée dans l'ordre où elle apparaît dans le fichier. Si un enregistrement ne correspond à aucune des règles, il est ignoré sans pour autant générer un message d'erreur.

Les exemples suivants montrent comment formater les règles de création.

Règle de création 1 : La règle suivante pose trois conditions sur les enregistrements d'ajout qui appartiennent à la classe inetOrgPerson. Ces enregistrements doivent posséder les attributs givenName et Surname. Ils doivent posséder un attribut L, mais si ce n'est pas le cas, la règle de création fournit une valeur par défaut de Provo pour eux.

```
<create-rules>
   <create-rule class-name="inetOrgPerson">
      <required-attr attr-name="givenName"/>
      <required-attr attr-name="surname"/>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

Règle de création 2 : La règle de création suivante pose trois conditions sur tous les enregistrements d'ajout, quelle que soit leur classe de base :

- L'enregistrement doit contenir un attribut givenName. Si ce n'est pas le cas, l'ajout échoue.
- L'enregistrement doit contenir un attribut Surname. Si ce n'est pas le cas, l'ajout échoue.
- L'enregistrement doit contenir un attribut L. Si ce n'est pas le cas, l'attribut se voit assigner la valeur de Provo.

```
<create-rules>
   <create-rule>
      <required-attr attr-name="givenName"/>
      <required-attr attr-name="Surname"/>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

Règle de création 3 : La règle de création suivante pose deux conditions sur tous les enregistrements, quelle que soit leur classe de base :

- La règle vérifie si l'enregistrement contient un attribut uid avec une valeur de ratuid. Si ce n'est pas le cas, l'ajout échoue.
- La règle vérifie si l'enregistrement possède un attribut L. S'il ne possède pas cet attribut, l'attribut L se voit attribuer la valeur de Provo.

```
<create-rules>
   <create-rule>
      <match-attr attr-name="uid">
         <value>cn=ratuid</value>
      </match-attr>
      <required-attr attr-name="L">
         <value>Provo</value>
      </required-attr>
   </create-rule>
</create-rules>
```

Exemple de commande : Si les règles de création sont enregistrées dans un fichier `crl.xml`, la commande suivante indique à l'utilitaire de les employer lors du traitement du fichier `1entry.ldf` et d'envoyer les résultats à un fichier cible (`outt1.ldf`).

```
ice -o -cfile://cr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

Règles de placement

Les règles de placement déterminent l'endroit où une entrée est créée dans le répertoire de destination. Elles prennent en charge les conditions suivantes pour déterminer si la règle doit être utilisée pour placer une entrée :

- **Classe de concordance :** Si la règle contient des éléments match-class, un attribut objectClass indiqué dans l'enregistrement doit correspondre à l'attribut class-name de la règle. Si la correspondance échoue, la règle de placement n'est pas utilisée pour cet enregistrement.
- **Attribut de concordance :** Si la règle contient des éléments match-attr, l'enregistrement doit contenir une valeur d'attribut pour chacun des attributs spécifiés dans l'élément match-attr. Si la correspondance échoue, la règle de placement n'est pas utilisée pour cet enregistrement.
- **Chemin de concordance :** Si la règle contient des éléments match path, une partie du dn de l'enregistrement doit correspondre au préfixe indiqué dans l'élément match path. Si la correspondance échoue, la règle de placement n'est pas utilisée pour cet enregistrement.

Le dernier élément de la règle indique où placer l'entrée. La règle de placement peut utiliser aucun ou plusieurs des éléments suivants :

- **PCDATA** utilise des données de caractère analysées pour préciser le DN d'un conteneur pour les entrées.
- **Copier le nom :** indique que l'attribut d'assignation de nom de l'ancien DN est utilisé dans le nouveau DN de l'entrée.
- **Copier l'attribut :** indique l'attribut d'assignation de nom à utiliser dans le nouveau DN de l'entrée. L'attribut de dénomination indiqué doit être un attribut de dénomination valide pour la classe de base de l'entrée.
- **Copier le chemin :** indique que le DN source doit être utilisé comme DN cible.

- **Copier le suffixe du chemin :** indique que le DN source, ou une partie de son chemin, doit être utilisé comme DN cible. Si un élément match path est spécifié, seule la partie de l'ancien DN qui ne correspond pas à l'attribut de préfixe (prefix) de cet élément est utilisée comme composant du DN de l'entrée.

Voici la DTD formelle de la règle de placement :

```
<!ELEMENT placement-rules (placement-rule*)>
<!ATTLIST placement-rules
          src-dn-format    (%dn-format;)   "slash"
          dest-dn-format   (%dn-format;)   "slash"
          src-dn-delims    CDATA           #IMPLIED
          dest-dn-delims   CDATA           #IMPLIED>

<!ELEMENT placement-rule (match-class*,
                          match-path*,
                          match-attr*,
                          placement)>
<!ATTLIST placement-rule
          description      CDATA            #IMPLIED>

<!ELEMENT match-class      EMPTY>
<!ATTLIST match-class
          class-name       CDATA            #REQUIRED>

<!ELEMENT match-path       EMPTY>
<!ATTLIST match-path
          prefix           CDATA            #REQUIRED>

<!ELEMENT match-attr       (value)+ >
<!ATTLIST match-attr
          attr-name        CDATA            #REQUIRED>

<!ELEMENT placement        (#PCDATA |
                           copy-name |
                           copy-attr |
                           copy-path |
                           copy-path-suffix)* >
```

Vous pouvez avoir plusieurs éléments de règle de placement dans un fichier. Chaque règle est traitée dans l'ordre où elle apparaît dans le fichier. Si un enregistrement ne correspond à aucune des règles, il est ignoré sans pour autant générer un message d'erreur.

Les exemples suivants montrent comment formater les règles de placement. Les attributs `scr-dn-format="ldap"` et `dest-dn-format="ldap"` définissent la règle de façon à ce que l'espace de noms du DN de la source et de la cible se présente au format LDAP.

L'utilitaire Importation/Conversion/Exportation NetIQ ne prend en charge que les noms sources et cibles au format LDAP.

Exemple de placement 1 : La règle de placement suivante requiert que l'enregistrement ait une classe de base de inetOrgPerson. Si l'enregistrement remplit cette condition, l'entrée est immédiatement subordonnée au conteneur test et le composant le plus à gauche de son DN source est utilisé comme partie de son DN.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-class class-name="inetOrgPerson"></match-class>
       <placement>cn=<copy-name/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

Avec cette règle, un enregistrement avec une classe de base de inetOrgPerson et avec le DN suivant :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
```

aurait le DN suivant dans le répertoire cible :

```
dn: cn=Kim Jones, o=test
```

Exemple de placement 2 : La règle de placement suivante requiert que l'enregistrement ait un attribut sn. Si l'enregistrement remplit cette condition, l'entrée est immédiatement subordonnée au conteneur test et le composant le plus à gauche de son DN source est utilisé comme partie de son DN.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement>cn=<copy-name/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

Avec cette règle, un enregistrement avec le dn et l'attribut sn suivants :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

aurait le DN suivant dans le répertoire cible :

```
dn: cn=Kim Jones, o=test
```

Exemple de placement 3 : La règle de placement suivante requiert que l'enregistrement ait un attribut sn. Si l'enregistrement remplit cette condition, l'entrée est immédiatement subordonnée au conteneur test et son attribut sn est utilisé comme composant de son DN. L'attribut indiqué dans l'élément copy-attr doit être un attribut de dénomination de la classe de base de l'entrée.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
  <placement-rule>
    <match-attr attr-name="sn"></match-attr>
    <placement>cn=<copy-attr attr-name="sn"/>,o=test</placement>
  </placement-rule>
</placement-rules>
```

Avec cette règle, un enregistrement avec le dn et l'attribut sn suivants :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

aurait le DN suivant dans le répertoire cible :

```
dn: cn=Jones, o=test
```

Exemple de placement 4 : La règle de placement suivante requiert que l'enregistrement ait un attribut sn. Si l'enregistrement remplit cette condition, le DN source est utilisé comme DN cible.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement><copy-path/></placement>
    </placement-rule>
 </placement-rules>
```

Exemple de placement 5 : La règle de placement suivante requiert que l'enregistrement ait un attribut sn. Si l'enregistrement remplit cette condition, le DN entier de l'entrée est copié vers le conteneur test.

```
<placement-rules src-dn-format="ldap" dest-dn-format="ldap">
    <placement-rule>
       <match-attr attr-name="sn"></match-attr>
       <placement><copy-path-suffix/>,o=test</placement>
    </placement-rule>
 </placement-rules>
```

Avec cette règle, un enregistrement avec le dn et l'attribut sn suivants :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ
sn: Jones
```

aurait le DN suivant dans le répertoire cible :

```
dn: cn=Kim Jones, ou=English, ou=Humanities, o=UofZ, o=test
```

Exemple de placement 6 : La règle de placement suivante requiert que l'enregistrement ait un attribut sn. Si l'enregistrement remplit cette condition, le DN entier de l'entrée est copié dans le conteneur NewOrganization.

```
<placement-rules>
 <placement-rule>
  <match-path prefix="o=engineering"/>
  <placement><copy-path-suffix/>o=neworg</placement>
 </placement-rule>
</placement-rules>
```

Par exemple :

```
dn: cn=bob,o=engineering
```

devient

```
dn: cn=bob,o=neworg
```

Exemple de commande : si les règles de placement sont enregistrées dans un fichier `pr1.xml`, la commande suivante demande à l'utilitaire de les employer lors du traitement du fichier `1entry.ldf` et d'envoyer les résultats au fichier cible (`foutt1.ldf`).

```
ice -o -pfile://pr1.xml -SLDIF -f1entry.ldf -c -DLDIF
-foutt1.ldf
```

Protocole LBURP (LDAP Bulk Update/Replication Protocol)

L'utilitaire Importation/Conversion/Exportation NetIQ utilise le protocole LBURP (LDAP Bulk Update/Replication Protocol) pour envoyer des requêtes asynchrones à un serveur LDAP. Cela garantit que les requêtes seront traitées dans l'ordre indiqué par le protocole et non pas dans un ordre arbitraire influencé par les interactions des multiprocesseurs ou le planificateur du système d'exploitation.

Le protocole LBURP permet également à l'utilitaire Importation/Conversion/Exportation NetIQ d'envoyer plusieurs mises à jour dans une seule requête et de recevoir la réponse de toutes ces mises à jour sous la forme d'une réponse unique. Ce protocole permet d'optimiser l'efficacité du réseau.

Le protocole LBURP fonctionne de la manière suivante :

1. L'utilitaire Importation/Conversion/Exportation NetIQ établit une liaison avec un serveur LDAP.
2. Le serveur envoie une réponse de liaison au client.
3. Le client envoie une requête étendue LBURP de début au serveur.
4. Le serveur envoie une réponse étendue LBURP de début au client.
5. Le client envoie ou non des requêtes étendues d'opération LBURP au serveur.

   Ces requêtes peuvent être envoyées en mode asynchrone. Chaque requête contient un numéro séquentiel identifiant sa place par rapport aux autres requêtes envoyées par le client sur la même connexion. Chaque requête contient également au moins une opération de mise à jour LDAP.
6. Le serveur traite chacune des requêtes étendues d'opération LBURP dans l'ordre défini par le numéro séquentiel et envoie une réponse étendue d'opération LBURP pour chaque requête.
7. Une fois que toutes les mises à jour ont été envoyées au serveur, le client envoie une requête étendue LBURP de fin au serveur.
8. Le serveur envoie une réponse étendue LBURP de fin au client.

Le protocole LBURP permet à l'utilitaire Importation/Conversion/Exportation NetIQ de présenter des données au serveur aussi rapidement que la connexion réseau le permet. Si la connexion réseau est suffisamment rapide, le serveur peut traiter les opérations de mise à jour en continu, car il n'a jamais besoin de s'interrompre parce que l'utilitaire Importation/Conversion/Exportation NetIQ lui donne d'autres tâches à réaliser.

Le processeur LBURP dans les eDirectory effectue également des opérations de mise à jour sur la base de données dans des groupes afin d'optimiser l'efficacité du traitement des opérations de mise à jour. Le protocole LBURP peut augmenter nettement l'efficacité des importations LDIF par rapport à une approche synchrone traditionnelle.

Le protocole LBURP est activé par défaut, mais vous pouvez le désactiver au cours d'une importation LDIF.

Pour activer ou désactiver le protocole LBURP au cours d'une importation LDIF :

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Importer les données depuis un fichier du disque**, puis sur **Suivant**.
4. Sélectionnez **LDIF** dans la liste déroulante **Type de fichier**, puis indiquez le nom du fichier LDIF contenant les données à importer.
5. Cliquez sur **Suivant**.
6. Spécifiez le serveur LDAP sur lequel les données seront importées, ainsi que le type de connexion (anonyme ou authentifiée).

7 Sous **Paramètres avancés**, sélectionnez **Utiliser LBURP**.

8 Cliquez sur **Suivant**, puis suivez les instructions en ligne pour exécuter les autres opérations de l'assistant d'importation LDIF.

IMPORTANT : le protocole LBURP étant relativement récent, les serveurs eDirectory antérieurs à la version 8.5 (ainsi que la plupart des serveurs non-eDirectory) ne le prennent pas en charge. Si vous utilisez l'assistant Importation/Exportation NetIQ eDirectory pour importer un fichier LDIF vers l'un de ces serveurs, vous devez désactiver l'option LBURP pour que l'importation LDIF fonctionne.

Vous pouvez utiliser l'option de ligne de commande pour activer ou désactiver LBURP pendant une importation LDIF. Pour plus d'informations, reportez-vous à l'option « -B » page 181.

Amélioration de la vitesse des importations LDIF

Dans les cas où le fichier LDIF que vous importez contient à lui seul des milliers voire des millions d'enregistrements, pensez à effectuer les opérations suivantes :

- « Importation directe vers un serveur avec une réplique en lecture/écriture » page 203
- « Utilisation du protocole LBURP » page 203
- « Configuration du cache de base de données » page 204
- « Utilisation de mots de passe simples » page 204
- « Utilisation appropriée des index » page 204

Importation directe vers un serveur avec une réplique en lecture/écriture

Si cela est possible, sélectionnez pour l'importation LDIF un serveur de destination qui comporte des répliques en lecture/écriture contenant toutes les entrées répertoriées dans le fichier LDIF. Cette opération permet d'optimiser l'efficacité du réseau.

Pour les mises à jour, évitez que le serveur cible soit chaîné à d'autres serveurs eDirectory. Cela risque de réduire nettement les performances. Toutefois, si certaines des entrées à mettre à jour se trouvent uniquement sur des serveurs eDirectory qui n'exécutent pas LDAP, vous serez peut-être obligé d'autoriser le chaînage pour importer le fichier LDIF.

Pour plus d'informations sur la gestion des répliques et des partitions, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

Utilisation du protocole LBURP

L'utilitaire Importation/Conversion/Exportation NetIQ optimise le réseau et l'efficacité de traitement du serveur eDirectory en utilisant le protocole LBURP pour transférer des données entre l'assistant et le serveur. L'utilisation du protocole LBURP au cours d'une importation LDIF améliore nettement la vitesse d'exécution de cette opération.

Pour plus d'informations sur le protocole LBURP, reportez-vous à la section « Protocole LBURP (LDAP Bulk Update/Replication Protocol) » page 202.

Configuration du cache de base de données

La taille du cache de base de données que eDirectory peut utiliser a un impact direct sur la vitesse d'exécution des importations LDIF, notamment lorsque le nombre total d'entrées sur le serveur augmente. Lorsque vous effectuez une importation LDIF, vous pouvez allouer, pendant cette opération, le maximum de mémoire possible à eDirectory. Une fois que l'importation est terminée et que le serveur gère une charge moyenne, vous pouvez restaurer les paramètres de mémoire précédents. Cela est particulièrement important si l'importation est la seule activité réalisée sur le serveur eDirectory.

Pour plus d'informations sur la configuration du cache de base de données eDirectory, reportez-vous au Chapitre 19, « Maintenance de NetIQ eDirectory », page 561.

Utilisation de mots de passe simples

NetIQ eDirectory utilise des paires de clé publique et privée pour l'authentification. La génération de ces clés est un processus qui requiert d'énormes ressources UC. À partir de la version 8.7.3 d'eDirectory, vous pouvez envisager de stocker les mots de passe à l'aide de la fonction de mot de passe simple du service NMAS (NetIQ Modular Authentication Service). Lorsque vous choisissez cette option, les mots de passe sont conservés dans un emplacement sécurisé dans le répertoire et les paires de clés ne sont pas générées tant qu'elles ne sont pas réellement requises pour l'authentification entre les serveurs. Cela permet d'augmenter considérablement la vitesse de chargement d'un objet qui contient des informations de mot de passe.

Pour activer des mots de passe simples au cours d'une importation LDIF :

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Importer les données depuis un fichier du disque**, puis sur **Suivant**.
4. Sélectionnez **LDIF** dans la liste déroulante **Type de fichier**, puis entrez le nom du fichier LDIF contenant les données à importer.
5. Cliquez sur **Suivant**.
6. Spécifiez le serveur LDAP sur lequel les données seront importées, ainsi que le type de connexion (anonyme ou authentifiée).
7. Sous **Paramètres avancés**, sélectionnez **Stocker les mots de passe simples NMAS/hachés**.
8. Cliquez sur **Suivant**, puis suivez les instructions en ligne pour exécuter les autres opérations de l'assistant d'importation LDIF.

Si vous choisissez de stocker les mots de passe à l'aide de la fonction Mot de passe simple, vous devez utiliser un logiciel Novell Client compatible avec NMAS afin de vous connecter à l'arborescence eDirectory et accéder aux services de fichier et d'impression traditionnels. Le service NMAS doit également être installé sur le serveur. Les applications LDAP créant des liaisons avec un nom et un mot de passe fonctionnent de manière transparente avec la fonction de mot de passe simple.

Pour plus d'informations sur NMAS, reportez-vous au Chapitre 24, « Présentation de l'infrastructure d'authentification d'eDirectory », page 673.

Utilisation appropriée des index

La présence d'index inutiles risque de ralentir l'importation LDIF : en effet, chaque index défini requiert un traitement supplémentaire pour chaque entrée dont les valeurs d'attribut sont stockées dans cet index. Avant d'effectuer une importation LDIF, vous devez supprimer tout index inutile ; vous

pouvez ensuite envisager de recréer certains de ces index une fois que vous avez terminé le chargement des données et passé en revue les statistiques de prédicat afin de vérifier où ces index sont réellement nécessaires.

Pour plus d'informations sur le réglage des index, reportez-vous à la « Gestionnaire d'index » page 205.

Gestionnaire d'index

Le gestionnaire d'index est un attribut de l'objet Serveur qui vous permet de gérer les index des bases de données. Ces index sont utilisés par eDirectory pour optimiser les performances des requêtes.

NetIQ eDirectory est livré avec un ensemble d'index offrant des fonctionnalités de recherche élémentaire. Ces index par défaut s'appliquent aux attributs suivants :

CN	Nom d'objet en alias
dc	Notice nécrologique
Prénom	Member
Nom	Référence
uniqueID	Équivalent à moi
GUID	NLS : certificat commun
cn_SS	Revision
uniqueID_SS	extensionInfo
ldapAttributeList	ldapClassList

Vous pouvez également créer des index personnalisés afin d'améliorer les performances d'eDirectory dans votre environnement. Par exemple, si votre entreprise a mis en oeuvre une nouvelle application LDAP qui recherche un attribut qui n'est pas indexé par défaut, il peut s'avérer nécessaire de créer un index pour cet attribut.

REMARQUE : bien que les index améliorent les performances en matière de recherche, l'ajout d'index supplémentaires risque d'augmenter le temps nécessaire à la mise à jour de l'annuaire. En règle générale, créez des index uniquement si vous pensez que les problèmes de performance résultent d'une recherche spécifique dans l'annuaire.

NetIQ iManager vous permet de créer ou de supprimer des index. Vous pouvez également afficher et gérer les propriétés de chaque index, comme son nom, son état, son type, sa règle et l'attribut indexé.

Création d'un index

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Gestion de l'index**.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Sur la page Modifier les index, cliquez sur **Créer**.
5. Saisissez le nom de l'index.

Si vous ne saisissez aucun nom pour cet index, l'attribut lui est automatiquement assigné comme nom.

IMPORTANT : le caractère $ sert de séparateur pour les valeurs d'attribut. Si vous souhaitez utiliser ce caractère dans le nom de l'index, vous devez le faire précéder d'une barre oblique inverse (\) afin de désactiver son effet lors de la manipulation des index via LDAP.

---

6 Sélectionnez un attribut.

7 Sélectionnez la règle d'index.

- **Valeur** (value) recherche la valeur complète ou la première partie de la valeur d'un attribut. Par exemple, la concordance de valeur peut être utilisée pour rechercher les entrées dont l'attribut « LastName » (nom de famille) est « Jensen » et celles dont l'attribut « LastName » commence par « Jen ».
- **Présence** (presence) exige uniquement la présence d'un attribut et non des valeurs d'attribut spécifiques. Une requête visant à rechercher toutes les entrées comportant un attribut Script de connexion utiliserait un index de présence.
- **Sous-chaîne** (substring) recherche une sous-chaîne de la chaîne de valeurs d'un attribut. Par exemple, une requête visant à rechercher les entrées dont l'attribut « LastName » (nom de famille) comporte « der » renverrait aussi bien « Derington », que « Anderson » et « Lauder ».

  Un index de sous-chaînes est le type d'index dont la création et la gestion exigent le plus de ressources système.

8 Cliquez sur **OK** pour mettre à jour la table des index.

9 Cliquez sur **Appliquer** pour redémarrer en arrière-plan le contrôleur de connectivité (limber) et prendre en compte la modification.

Suppression d'un index

Certains index peuvent devenir inutiles. Dans ce cas, qu'ils soient définis par l'utilisateur ou créés automatiquement, vous pouvez les supprimer.

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Gestion de l'index**.

3 Sélectionnez un serveur dans la liste des serveurs disponibles.

4 Dans la page Modifier les index, sélectionnez l'index défini par l'utilisateur ou ajouté automatiquement que vous souhaitez supprimer.

5 Cliquez sur **Supprimer** pour mettre à jour la table des index.

6 Cliquez sur **Appliquer** pour redémarrer en arrière-plan le contrôleur de connectivité et prendre en compte la modification.

Mise hors ligne d'un index

Pendant les périodes d'activité intensive, vous pouvez optimiser les performances en mettant temporairement hors ligne certains index. Par exemple, pour accélérer les opérations de chargement par lot, il est possible que vous souhaitiez suspendre tous les index définis par l'utilisateur. Dans la mesure où l'ajout et la modification d'objets impliquent la mise à jour des index définis, l'activation

simultanée de tous les index peut ralentir considérablement les opérations de chargement par lot des données. Une fois les opérations de chargement par lot terminées, vous pouvez remettre en ligne les index.

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Gestion de l'index**.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Sur la page Modifier les index, sélectionnez les index à mettre hors ligne, puis cliquez sur **Changer l'état**.

   L'état de l'index passe de En ligne à Hors ligne dans la table d'affichage. Un index peut présenter l'un des états suivants :

   - **En ligne** : en cours d'exécution.
   - **Hors ligne** : mis en attente. L'index peut être relancé en cliquant sur **Mettre en ligne**.
   - **Nouveau** : Index en attente de passage à l'état En ligne.
   - **Supprimé** : Index en attente de suppression de la table des index.
5. Cliquez sur **Appliquer**.

Gestion des index sur d'autres serveurs

Si vous pensez qu'un index utilisé sur un serveur peut être utile sur un autre serveur, vous pouvez copier la définition de cet index d'un serveur vers un autre. En examinant les données de prédicat, vous pourriez également constater le cas de figure inverse : un index qui répondait à un besoin sur plusieurs serveurs n'est plus utile sur l'un de ces serveurs. Dans ce cas, vous pouvez supprimer l'index inutile de ce serveur.

Le gestionnaire d'index permet de cibler une instance spécifique d'un index sans incidence sur les autres instances.

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Gestion de l'index**.
3. Sélectionnez un serveur dans la liste des serveurs disponibles.
4. Pour copier une définition d'index vers un autre serveur de la même arborescence, cliquez sur **Modifier l'emplacement de l'index**.
5. Sélectionnez la définition d'index à copier.

   Lorsque vous choisissez un index, les serveurs de l'arborescence contenant cet index sont listés.
6. Utilisez les colonnes disponibles pour déplacer une copie de l'index vers le serveur de votre choix.
7. Cliquez sur **Appliquer**.

Gestionnaire de services eDirectory

Le gestionnaire de services eDirectory fournit des informations sur les services eDirectory disponibles et leur état. Il permet également de démarrer et d'arrêter ces services.

Le gestionnaire de services gère uniquement les services eDirectory. Pour ce faire, il utilise le fichier de configuration `dsservcfg.xml` qui fournit une liste des services à gérer sur les différentes plates-formes. Il permet également d'ajouter ou de supprimer des services dans la liste.

Pour accéder au Gestionnaire de services eDirectory, procédez comme suit :

- « Utilisation de l'outil Service Manager eMTool du client » page 208
- « Utilisation du plug-in du Gestionnaire de services pour NetIQ iManager » page 209

Utilisation de l'outil Service Manager eMTool du client

Le client eDirectory Management Toolbox (eMBox) est un client Java de ligne de commande qui permet d'accéder à distance à l'outil Service Manager eMTool d'eDirectory. Le fichier `emboxclient.jar` est installé sur votre serveur dans le cadre de l'installation d'eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client, reportez-vous à la « Utilisation du client à ligne de commande » page 594.

Utilisation du Gestionnaire de services eMTool du client

1. Exécutez le client en mode interactif en entrant les éléments suivants dans la ligne de commande :

   ```
   java -cp path_to_the_file/emboxclient.jar  -i
   ```

   (Si le fichier `emboxclient.jar` figure déjà dans votre chemin d'accès à la classe, il vous suffit d'entrer la commande `java -i`.)

   L'invite du client apparaît :

   ```
   Client>
   ```

2. Pour vous connecter au serveur qui exécutera le gestionnaire de services, entrez la commande suivante :

   ```
   login -s server_name_or_IP_address -p port_number
   -u username.context -w password -n
   ```

   Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option `-n` ouvre une connexion non sécurisée.

   Le client indique si la connexion a abouti.

3. Entrez l'une des commandes suivantes du Gestionnaire de services :

Commande	Description
`service.serviceList`	Liste les services eDirectory disponibles.
`service.serviceStart -n`*`nom_module`*	Démarre le service eDirectory indiqué.
`service.serviceStop -n`*`nom_module`*	Arrête le service eDirectory indiqué.
`service.serviceInfo -n`*`nom_module`*	Affiche les informations relatives au service indiqué.

   Vous pouvez également utiliser la commande `list -tservice` du client pour obtenir une liste détaillée des options du Gestionnaire de services. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services » page 597.

4. Déconnectez-vous du client en entrant la commande suivante :

   ```
   logout
   ```

5 Quittez le client en entrant la commande suivante :

```
exit
```

Utilisation du plug-in du Gestionnaire de services pour NetIQ iManager

1 Dans NetIQ iManager, cliquez sur **Rôles et tâches**.

2 Cliquez sur **Maintenance** > **Gestionnaire de services**.

3 Indiquez le serveur à gérer, puis cliquez sur **OK**.

4 Authentifiez-vous auprès du serveur sélectionné, puis cliquez sur **OK**.

5 Utilisez les icônes suivantes pour vérifier l'état d'un service eDirectory quelconque ou pour démarrer ou arrêter un service :

Icône	Description
	Un service est en cours d'exécution.
	Un service est arrêté.
	Démarre un service.
	Arrête un service.
	Un service est en cours d'exécution, mais vous ne pouvez pas l'arrêter.

Utilitaire de chargement en bloc hors connexion

L'utilitaire ldif2dib permet de charger en bloc des données à partir des fichiers LDIF vers la base de données NetIQ eDirectory (DIB), lorsque le serveur eDirectory est hors ligne. eDirectory prend en charge cet utilitaire sur les plates-formes Linux et Windows. Cet outil hors ligne réalise des chargements en bloc plus rapidement que les autres outils en ligne. L'utilitaire utilise le répertoire existant et ne crée pas de nouvelle base de données lors de l'importation d'entrées d'un fichier LDIF vers la DIB.

L'utilitaire ldif2dib est nécessaire lorsque vous avez besoin de remplir une grande base de données utilisateur avec les entrées d'un fichier LDIF. Les outils en ligne tels que ICE ou ldapmodify sont plus lents que ldif2dib en raison des surcharges associées au chargement en bloc et en ligne, telles que la vérification du schéma, la traduction du protocole et les vérifications du contrôle d'accès. ldif2dib permet d'accélérer le temps de fonctionnement lorsqu'une base de données utilisateur volumineuse doit être remplie et que le temps d'arrêt initial n'est pas un problème.

Amélioration des performances de chargement par lots

eDirectory propose de nouvelles options pour accroître les performances de chargement en bloc. Voici les paramètres vous permettant d'ajuster les performances de chargement en bloc à l'aide de l'utilitaire Importation/Conversion/Exportation (ICE) NetIQ.

- « Paramètres du cache eDirectory » page 210
- « Définition de la taille de transaction LBURP » page 210
- « Augmentation du nombre de requêtes asynchrones dans ICE » page 211
- « Augmentation du nombre de threads d'écriture LDAP » page 211
- « Désactivation de la validation de schéma dans ICE » page 212
- « Processus de liaison en amont » page 212
- « Désactivation des modèles ACL » page 212
- « Activation/désactivation du cache en ligne » page 214
- « Augmentation du timeout de LBURP » page 214

Reportez-vous également aux différents paramètres réglables de votre système d'exploitation.

Paramètres du cache eDirectory

Pour optimiser les performances de bulkload, allouez un pourcentage supérieur de cache eDirectory pour le cache de bloc. Pour plus d'informations, reportez-vous à la section Optimisation des sous-systèmes eDirectory du Guide d'optimisation NetIQ eDirectory.

Définition de la taille de transaction LBURP

La taille de transaction LBURP définit le nombre d'enregistrements qui sont envoyés au serveur LDAP par l'utilitaire ICE, durant une même transaction. En augmentant cette valeur, vous pouvez améliorer les performances du chargement par lot, en partant du principe que vous avez défini une mémoire suffisante et que l'augmentation n'entraîne pas de conflit d'entrées/sorties. La taille de transaction par défaut est 25, ce qui est suffisant pour les petits fichiers LDIF (moins de 100 000 opérations), mais non pour un nombre important d'enregistrements. La taille de transaction LBURP peut être définie entre 1 et 350.

Modification de la taille de transaction

Pour modifier la taille de transaction, changez la valeur requise dans le paramètre n4u.ldap.lburp.transize du fichier `/etc/opt/novell/eDirectory/conf/nds.conf`. Dans l'idéal, une taille de transaction plus élevée assure des performances plus rapides. Cependant, la taille de transaction ne doit pas être définie de façon arbitraire sur des valeurs élevées pour les raisons suivantes :

- Une taille de transaction plus élevée exige que le serveur alloue plus de mémoire pour effectuer la transaction. Si le système commence à manquer de mémoire, cela peut provoquer un ralentissement dû aux permutations.
- Le fichier LDIF doit être exempt d'erreurs et toutes les entrées préexistantes dans eDirectory doivent être mises en commentaire. Si la transaction présente ne serait-ce qu'une seule erreur (y compris les cas où l'objet à ajouter existe déjà dans l'annuaire), eDirectory ne tient pas compte du paramètre de la transaction LBURP et effectue une validation après chaque opération pour garantir l'intégrité des données.

Pour plus d'informations, reportez-vous à la section Dépannages des fichiers LDIF du Guide de dépannage de NetIQ eDirectory.

- L'optimisation LBURP ne fonctionne que pour les objets Feuille. Si la transaction renferme à la fois un conteneur et les objets qui lui sont subordonnés, eDirectory la traite comme une erreur. Pour éviter ce problème, nous recommandons de charger les objets Conteneur d'abord à l'aide d'un fichier LDIF distinct ou d'activer l'utilisation des références en aval.

  Pour plus d'informations, reportez-vous à la section Activation des références en aval du Guide de dépannage de NetIQ eDirectory.

Augmentation du nombre de requêtes asynchrones dans ICE

Cette option définit le nombre d'entrées que le client ICE peut envoyer au serveur LDAP en mode asynchrone avant de patienter pour obtenir les résultats renvoyés par le serveur. Le nombre de requêtes asynchrones peut être défini sur un nombre compris entre 10 et 200. La valeur par défaut est 100. Toute valeur inférieure au minimum (10) est ramenée à la valeur par défaut. La valeur minimale est suffisante pour les petits fichiers LDIF. Idéalement, une taille de fenêtre plus élevée assure de meilleures performances. Vous ne devez toutefois pas attribuer des valeurs arbitrairement élevées à la taille de fenêtre car une taille de fenêtre élargie oblige le client à allouer plus de mémoire au traitement des entrées dans le fichier LDIF. Si le système vient à manquer de mémoire, cela peut provoquer un ralentissement dû aux échanges. Vous pouvez modifier le nombre de requêtes asynchrones dans ICE à l'aide de l'option de ligne de commande ICE ou iManager.

Avec l'option de ligne de commande ICE

Il est possible de spécifier le nombre de requêtes asynchrones à l'aide de l'option de ligne de commande -Z de ICE. Elle est disponible dans le gestionnaire cible LDAP.

Pour définir 50 comme nombre de requêtes asynchrones envoyées au client ICE, entrez la commande suivante :

```
ice -SLDIF -f LDIF_file -a -c -DLDAP -d cn_of_admin -Z50 -w password
```

Avec l'Assistant ICE d'iManager

Pour définir le nombre de requêtes asynchrones envoyées par le client ICE via iManager, procédez comme suit :

1. Cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance > Assistant Importation/Conversion/Exportation**.
3. Entrez la valeur dans le champ Taille de la fenêtre LBURP dans les écrans du gestionnaire cible LDAP à la fois pour les tâches d'importation de données à partir d'un fichier et de migration de données entre les tâches des serveurs LDAP.
4. Cliquez sur **Suivant**.

   Pour plus d'informations, consultez l'aide de l'Assistant.

Augmentation du nombre de threads d'écriture LDAP

Le serveur LDAP comporte désormais plusieurs threads d'écriture. Utilisez l'option de ligne de commande -F de ICE pour activer les références en aval afin d'éviter toute erreur possible due à un traitement concurrent, en entrant la commande suivante :

```
ice -SLDIF -f LDIF_file -a -c -DLDAP -d cn_of_admin -w password  -F
```

Désactivation de la validation de schéma dans ICE

Utilisez les options de ligne de commande -C et -n de ICE pour désactiver la validation de schéma au niveau du client ICE en entrant la commande suivante :

```
ice -C -n -SLDIF -f LDIF_file -a -c -DLDAP -d cn_of_admin -w password
```

Processus de liaison en amont

La liaison en amont est un processus d'arrière-plan qui vérifie notamment l'intégrité référentielle dans le cadre des vérifications effectuées 50 minutes après l'activation du serveur eDirectory. Cette vérification s'effectue de nouveau après 13 heures. Veillez à ce que la liaison en amont ne s'exécute pas pendant le chargement par lots, qui risquerait alors d'être perturbé selon la durée du chargement et le nombre d'objets chargés

Désactivation des modèles ACL

Vous pouvez désactiver les modèles ACL (Access Control List - liste de contrôle d'accès) pour accroître les performances de chargement par lots. Certaines ACL risquent alors d'être manquantes, mais vous pouvez résoudre ce problème en ajoutant les ACL nécessaires au fichier LDIF ou en les appliquant ultérieurement.

1. Exécutez la commande suivante :

   ```
   ldapsearch -D cn_of_admin -w password -b cn=schema -s base
   objectclasses=inetorgperson
   ```

   Le résultat de cette commande sera similaire au suivant :

   ```
   dn: cn=schema
   objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
    organizationalPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
    $ loginAllowedTi meMap $ loginDisabled $ loginExpirationTime $
    loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
    loginIntruderAttempts $ loginIntruderResetTim e $
    loginMaximumSimultaneous $ loginScript $ loginTime $
    networkAddressRestri ction $ networkAddress $ passwordsUsed $
    passwordAllowChange $ passwordExpirationInterval $
    passwordExpirationTime $passwordMinimumLength $ passwordRequired $
    passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
    publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
    minimum AccountBalance $ messageServer $ Language $ UID $
    lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
    higherPrivileges $ printerControl $ securityFlags $ profileMembership $
    Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
    sASSecretStoreData $ sASPKIStoreKeys $ userCertificate
    $nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
   ```

```
 rADIUS AttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory
 $ rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
 $ rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
 carLicense $ departmentNumbe r $ employeeNumber $ employeeType $
 givenName $ homePhone $ homePostalAddress  $ initials $ jpegPhoto $
 labeledUri $ mail $ manager $ mobile $ pager $ ldap Photo $
 preferredLanguage $ roomNumber $ secretary $ uid $ userSMIMECertifica te
 $ x500UniqueIdentifier $ displayName $ userPKCS12 ) X-NDS_NAME 'User' X
-NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1' X-NDS_ACL_TEMPLATES (
'2#subtree#[Self]#[All Attributes Rights]' '6#entry#[Self]#loginScript'
'1#subtree#[Root Template]#[Entry Rights]' '2#entry#[Public]#messageServer'
'2#entry#[Root Template]#groupMembership'
'6#entry#[Self]#printJobConfiguration' '2#entry#[Root
Template]#networkAddress') )
```

2 Dans le résultat obtenu à l'étape précédente, supprimez les informations figurant en gras.

3 Enregistrez le résultat révisé sous la forme d'un fichier LDIF.

4 Ajoutez les informations suivantes dans le nouveau fichier LDIF :

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113730.3.2.2 )-add:objectclasses
```

Votre fichier LDIF devrait à présent ressembler à ceci :

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: ( 2.16.840.1.113730.3.2.2)
-
add:objectclasses
objectClasses: ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' SUP
 organization alPerson STRUCTURAL MAY ( groupMembership $ ndsHomeDirectory
 $ loginAllowedTimeMap $ loginDisabled $ loginExpirationTime $
 loginGraceLimit $ loginGraceRem aining $ loginIntruderAddress $
 loginIntruderAttempts $ loginIntruderResetTime $
 loginMaximumSimultaneous $ loginScript $ loginTime $
 networkAddressRestri ction $ networkAddress $ passwordsUsed $
 passwordAllowChange $ passwordExpirationInterval $
 passwordExpirationTime $ passwordMinimumLength $ passwordRequired
 $passwordUniqueRequired $ printJobConfiguration $ privateKey $ Profile $
 publicKey $ securityEquals $ accountBalance $ allowUnlimitedCredit $
 minimum AccountBalance $ messageServer $ Language $ UID $
 lockedByIntruder $ serverHolds $ lastLoginTime $ typeCreatorMap $
 higherPrivileges $ printerControl $ securityFlags $ profileMembership $
 Timezone $ sASServiceDN $ sASSecretStore $ sASSecretStoreKey $
 sASSecretStoreData $ sASPKIStoreKeys $ userCertificate $
 nDSPKIUserCertificateInfo $ nDSPKIKeystore $ rADIUSActiveConnections $
 rADIUSAttributeLists $ rADIUSConcurrentLimit $ rADIUSConnectionHistory $
 rADIUSDefa ultProfile $ rADIUSDialAccessGroup $ rADIUSEnableDialAccess
 $rADIUSPassword $ rADIUSServiceList $ audio $ businessCategory $
 carLicense
 $ departmentNumbe r $ employeeNumber $ employeeType $ givenName $
 homePhone $ homePostalAddress  $ initials $ jpegPhoto $ labeledUri $ mail
 $ manager $ mobile $ pager $ ldap Photo $ preferredLanguage $ roomNumber
 $ secretary $ uid $ userSMIMECertifica te $ x500UniqueIdentifier $
 displayName $ userPKCS12 ) X-NDS_NAME 'User' X-ND S_NOT_CONTAINER '1' X
-NDS_NONREMOVABLE '1')
```

5 Saisissez la commande suivante :

```
ldapmodify -D cn_of_admin -w password -f LDIF_file_name
```

Pour plus d'informations sur l'utilisation des ACL, reportez-vous au Guide d'optimisation NetIQ eDirectory.

Activation/désactivation du cache en ligne

Le cache de changement en ligne peut être activé ou désactivé pour un serveur. Cette option ne peut toutefois être désactivée que si la synchronisation sortante est elle-même désactivée. L'activation de la synchronisation sortante active également le cache de changement en ligne. La désactivation de ce cache de changement en ligne le marque comme non valide pour cette réplique et lui attribue un drapeau invalide dans **Configuration de l'agent > Partitions**. Si le cache de changement en ligne est réactivé, le drapeau non valide est supprimé lors de la reconstruction du cache.

Augmentation du timeout de LBURP

Par défaut, le timeout pour un client est de 20 minutes (1 200 secondes). Mais pendant le chargement par lots, lorsque la taille de la transaction LBURP est de l'ordre de 250, que les objets comportent un grand nombre d'attributs dont les valeurs sont élevées et qu'un traitement LBURP est activé simultanément sur le serveur, le serveur est occupé à traiter les données provenant du client ICE sans lui répondre dans le délai imparti entraînant ainsi l'expiration de ce dernier

Dès lors, nous vous recommandons d'augmenter le timeout. Pour ce faire, exportez la variable d'environnement LBURP_TIMEOUT avec des valeurs élevées (en secondes). Par exemple, pour exporter la variable LBURP_TIMEOUT avec 1 200 secondes, entrez la commande suivante : `export ICE_LBURP_TIMEOUT=1200`

Utilisation de ldif2dib pour le chargement en bloc

Vous pouvez spécifier le fichier LDIF qui contient les données à importer et le chemin d'accès aux fichiers de base de données dans laquelle les données doivent être importées via l'interface de ligne de commande. Pour utiliser ldif2dib afin de charger des données en bloc, procédez comme suit :

1 Réalisez une sauvegarde de la DIB.

Pour plus d'informations sur la procédure de sauvegarde et de restauration, reportez-vous au Chapitre 15, « Sauvegarde et restauration de NetIQ eDirectory », page 443.

2 Arrêtez le serveur eDirectory.

3 Pour démarrer le chargement en bloc à partir du fichier LDIF, entrez la commande suivante :

```
ldif2dib <LDIF File Name> [Options]
```

Où

- **LDIF File Name :** indique le nom de fichier LDIF permettant le chargement en bloc.
- **Options :** elles sont facultatives et indiquent les différents paramètres que vous pouvez utiliser pour l'optimisation de cet utilitaire. Les options prises en charge par l'utilitaire ldif2dib sont répertoriées ci-dessous :

Par exemple, si vous souhaitez définir des options permettant de spécifier le mode de traitement par lots et la taille du cache, ainsi que des options de pourcentage du cache de blocs, entrez la commande suivante :

```
ldif2dib 1MillionUsers.ldif -b/novell/log/logfile.txt -c314572800 -p90
```

SUGGESTION : vous pouvez suspendre provisoirement le chargement en bloc en appuyant sur la touche s ou S. La touche d'échappement (ÉCHAP) peut être utilisée pour arrêter le chargement en bloc.

Instances multiples

ldif2dib peut être utilisé pour les entrées de chargement en bloc à partir des fichiers LDIF vers une instance spécifique d'eDirectory (DIB), en indiquant l'emplacement de son fichier nds.db à l'aide de l'option -n. Si l'emplacement du fichier nds.db n'est pas spécifié avec l'option -n et s'il existe une seule instance d'eDirectory configurée sur le système, ldif2dib détecte automatiquement l'emplacement de ses fichiers de base de données. Toutefois, s'il existe plusieurs instances, ldif2dib affiche un menu contenant toutes les instances configurées et vous permet de choisir une instance pour le chargement en bloc.

Pour plus d'informations sur les instances multiples d'eDirectory, reportez-vous à la section Utilisation de ndsconfig pour configurer plusieurs instances d'eDirectory 9.2 du guide d'installation de NetIQ eDirectory.

Optimisation de ldif2dib

Cette section contient des informations sur les paramètres permettant d'ajuster ldif2dib :

- « Optimisation du cache » page 215
- « Taille de la transaction » page 215
- « Index » page 216
- « Pourcentage de cache de blocs » page 216
- « Intervalle de point de contrôle » page 216

Optimisation du cache

Le paramètre du cache de base de données est l'un des paramètres les plus importants qui affecte les performances d'eDirectory. S'il est trop faible, les opérations eDirectory ralentissent, car les informations doivent être récupérées à partir du disque plus souvent. S'il est trop élevé, la mémoire disponible ne suffit plus pour exécuter d'autres processus et l'ensemble du système ralentit. Pour plus d'informations sur le cache, reportez-vous à la section Modification des paramètres de cache FLAIM du Guide d'optimisation de NetIQ eDirectory.

En règle générale, les performances de chargement en bloc augmentent lorsque la taille du cache augmente. Toutefois, aucune amélioration des performances n'a été observée en augmentant la taille du cache au-delà d'une valeur correspondant à 3,8 fois la taille du fichier LDIF.

Taille de la transaction

La taille de la transaction définit la taille de la tranche exprimée en nombre d'objets par transaction. Si la taille de transaction est élevée, un petit nombre de tranches de grande taille consigne le résultat et lorsqu'elle est faible, un grand nombre de petites tranches consigne le résultat.

Les performances de chargement en bloc augmentent lorsque les tailles de transaction sont plus grandes. Une taille de transaction égale à zéro entraîne un cas spécial qui permet un nombre illimité d'objets par transaction. Lorsque la taille de transaction est de zéro, les performances sont élevées,

car la validation est effectuée à la fin du chargement en bloc. Toutefois, nous vous déconseillons de définir la taille de transaction sur 0 pour les fichiers LDIF très volumineux (supérieurs à un million d'objets). Vous pouvez définir la taille de transaction sur 4 000 pour les fichiers LDIF très volumineux.

Index

Bien que l'utilisation des index améliore les performances de recherche, elle ralentit aussi le chargement en bloc, car les index doivent être mis à jour pour tous les objets chargés dans la DIB. Ceci est d'autant plus vrai pour les index de sous-chaîne. Par conséquent, lorsque vous chargez en bloc un grand nombre d'objets, vous pouvez mettre en attente les index afin d'accélérer le chargement en bloc. Les index sont automatiquement repris lorsque le serveur eDirectory est mis en service. Utilisez l'option-x pour désactiver les index avant de charger des entrées à l'aide de ldif2dib.

Pourcentage de cache de blocs

Si les index de sous-chaîne sont activés pour les attributs, il est recommandé de définir le pourcentage de cache de blocs sur 50 %. Toutefois, si les index de sous-chaîne sont désactivés pour les attributs, vous pouvez définir le pourcentage de cache de blocs sur 90 %.

Intervalle de point de contrôle

L'intervalle de point de contrôle est le délai pendant lequel la base de données patiente avant de lancer le thread d'arrière-plan de point de contrôle visant à uniformiser l'état de la version sur disque de la base de données avec celui de la base de données en mémoire (en cache). Ce thread de point de contrôle vide le dirty cache sur le disque, puis nettoie le fichier journal de transaction individuelle. Étant donné que le chargement en bloc est momentanément interrompu pendant l'exécution du thread de point de contrôle, nous vous recommandons de définir une valeur élevée pour l'intervalle de point de contrôle afin d'accélérer les chargements en bloc.

Limites

Cette section détaille les limites de l'utilitaire ldif2dib :

- « Schéma » page 216
- « Modèles ACL » page 217
- « Options » page 217
- « Mot de passe simple et LDIF » page 217
- « Classes personnalisées » page 217
- « Répliques filtrées » page 217

Schéma

- Le fichier LDIF doit mentionner toutes les classes d'objet auxquelles appartient une entrée. Une entrée peut appartenir à plusieurs classes d'objet en raison d'un héritage. Par exemple, une entrée du type inetOrgPerson doit respecter la syntaxe suivante dans le fichier LDIF :

  ```
  objectclass: inetorgperson
  objectclass: organizationalPerson
  objectclass: person
  objectclass: top
  ```

- Les syntaxes suivantes ne sont actuellement pas prises en charge :

Modèles ACL

Les ACL spécifiées dans les modèles ACL pour une classe d'objet ne sont pas ajoutées automatiquement pour les objets chargés en bloc à l'aide de ldif2dib.

Options

Sous Linux, si l'option -b est utilisée, l'écran d'affichage des statistiques disparaît une fois le chargement en bloc terminé. Les dernières statistiques, cependant, sont inscrites dans le fichier journal pour référence.

Mot de passe simple et LDIF

Sous Windows, pendant le téléchargement de LDIF associé à un mot de passe simple, ldif2dib risque d'échouer si les clés NICI des dossiers Système et Administrateur ne sont pas synchronisées. Pour résoudre ce problème, accédez aux clés du dossier `nici/system` comme suit :

1. Allez dans le dossier `C:\Windows\system32\novell\nici\`.
2. Sauvegardez les fichiers du dossier de l'**administrateur**.
3. Accédez au dossier Système et à ses fichiers en procédant comme suit :
   - **3a** Accédez à l'onglet **Sécurité** dans la fenêtre Propriétés du dossier System.
   - **3b** Sélectionnez **Options avancées** et accédez à l'onglet **Propriétaire**.
   - **3c** Sélectionnez **Administrateur**.
   - **3d** Retournez à l'onglet **Sécurité** et ajoutez Administrateur à la liste.

     Répétez la procédure pour obtenir un accès en lecture à tous les fichiers du dossier Système.
4. Remplacez les fichiers du dossier **Administrator** par ceux du dossier system.
5. Une fois le téléchargement terminé, copiez les fichiers sauvegardés dans le dossier de l'**administrateur**.
6. Rétablissez l'accès Administrateur au dossier Système et aux fichiers qu'il contient.

Classes personnalisées

Le chargement en bloc d'un fichier LDIF incluant un grand nombre d'objets Conteneur à l'aide de ldif2dib peut provoquer une saturation de la mémoire entraînant une erreur -150.

Répliques filtrées

eDirectory ne prend pas en charge les opérations de chargement en bloc pour les répliques filtrées.

Avertissements

Le comportement de ldif2dib n'est pas défini dans les scénarios suivants :

- « Entrées en double » page 218
- « Aucune vérification de schéma » page 218
- « Espace insuffisant sur le disque dur » page 218

- « Arrêt forcé » page 218
- « Redimensionnement du terminal » page 218

Entrées en double

Le téléchargement de fichiers LDIF qui possèdent des entrées en double ou qui possèdent des entrées déjà présentes dans la DIB, sans l'option -u, provoque l'ajout répété de l'entrée menant ainsi à un état incohérent de la DIB. Dès lors, si vous n'êtes pas certain que les entrées soient répétées dans le fichier LDIF ou qu'elles étaient présentes dans la DIB avant le chargement en bloc, utilisez l'option -u pendant le chargement en bloc.

Aucune vérification de schéma

ldif2dib n'effectue aucune vérification de schéma. Vous pouvez ainsi ajouter un attribut à un objet même si l'attribut n'appartient pas au schéma de cet objet. Cette opération entraîne l'incohérence de l'état de la base de données DIB. N'utilisez ldif2dib que lorsque vous êtes certain que ces données LDIF ne nécessitent pas de vérification de schéma.

Espace insuffisant sur le disque dur

Le comportement de ldif2dib est indéfini lorsque l'espace sur le disque dur est insuffisant pour tous les objets chargés. Vous devez vous assurer que l'espace est suffisant pour accueillir tous les objets avant de démarrer le chargement en bloc.

Arrêt forcé

L'arrêt forcé du processus ldif2dib peut entraîner un état incohérent de la DIB. Utilisez la touche ÉCHAP pour quitter sans problème le chargement en bloc.

Redimensionnement du terminal

Le redimensionnement du terminal pendant le chargement en bloc peut fausser les statistiques dans l'interface utilisateur. Il est déconseillé de redimensionner le terminal pendant le chargement en bloc.

Fichiers LDIF

L'utilitaire d'importation, de conversion et d'exportation NetIQ permet d'importer et d'exporter facilement des fichiers LDIF vers et depuis eDirectory. Pour plus d'informations, reportez-vous à la section « Utilitaire Importation/Conversion/Exportation NetIQ » du *Guide d'administration de NetIQ eDirectory*.

Pour qu'une importation LDIF se déroule convenablement, vous devez commencer avec un fichier LDIF que l'utilitaire d'importation, de conversion et d'exportation NetIQ peut lire et traiter. Cette section décrit le format et la syntaxe des fichiers LDIF, et propose des exemples de fichiers LDIF corrects.

- « Comprendre LDIF » page 219
- « Débogage des fichiers LDIF » page 227
- « Utilisation de LDIF pour étendre le schéma » page 232
- « Limitations ldif2dib » page 236

Comprendre LDIF

LDIF est un format de fichier très répandu qui décrit des informations de répertoire ou des opérations de modification pouvant être réalisées sur un répertoire. LDIF est totalement indépendant du format de stockage utilisé au sein d'une implémentation de répertoire spécifique, et est typiquement utilisé pour exporter des informations de répertoire depuis des serveurs LDAP et pour importer des données vers des serveurs LDAP.

D'une façon générale, la génération de LDIF est simple. Elle vous permet d'utiliser des outils tels que awk ou perl, pour déplacer des données d'un format propriétaire dans un annuaire LDAP. Vous pouvez également écrire des scripts permettant de générer des données de test au format LDIF.

Format de fichier LDIF

L'utilitaire d'importation/de conversion/d'exportation NetIQ requiert des fichiers au format LDIF 1. Voici les règles de base applicables à un fichier LDIF 1 :

- La première ligne (autre qu'un commentaire) doit correspondre à la version 1.
- Une série d'un ou de plusieurs enregistrements suit la version.
- Chaque enregistrement se compose de champs (un champ par ligne).
- Les lignes sont séparées par un saut de ligne ou par une paire retour chariot/saut de ligne.
- Les enregistrements sont séparés par au moins une ligne vide.
- Il existe deux types d'enregistrements LDIF : enregistrements de contenu et enregistrements de modification. Un fichier LDIF peut comporter un nombre illimité d'enregistrements, mais ceux-ci doivent tous être du même type. Vous ne pouvez pas mélanger des enregistrements de contenu et des enregistrements de changement dans le même fichier LDIF.
- Toute ligne commençant par le signe dièse (#) est un commentaire et est par conséquent ignorée lors du traitement du fichier LDIF.

Enregistrements de contenu LDIF

Un enregistrement de contenu LDIF représente le contenu de l'ensemble d'une entrée. L'exemple de fichier LDIF ci-après comprend quatre enregistrements de contenu :

```
 1  version: 1
 2  dn: c=US
 3  objectClass: top
 4  objectClass: country
 5
 6  dn: l=San Francisco, c=US
 7  objectClass: top
 8  objectClass: locality
 9  st: San Francisco
10
11 dn: ou=Artists, l=San Francisco, c=US
12 objectClass: top
13 objectClass: organizationalUnit
14 telephoneNumber: +1 415 555 0000
15
16 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
17 sn: Michaels
18 givenname: Peter
19 objectClass: top
20 objectClass: person
21 objectClass: organizationalPerson
22 objectClass: iNetOrgPerson
23 telephonenumber: +1 415 555 0001
24 mail: Peter.Michaels@aaa.com
25 userpassword: Peter123
26
```

Ce fichier LDIF comprend les parties suivantes :

Composant	Description
Spécificateur de version	La première ligne d'un fichier LDIF comporte la version. Vous pouvez ajouter ou non des espaces entre les deux points et le numéro de version, actuellement défini sur 1. Si la ligne de version est manquante, toute application traitant le fichier LDIF peut supposer que le fichier est de version 0. Il est aussi possible que le fichier LDIF soit rejeté comme étant syntaxiquement incorrect. Les utilitaires NetIQ traitant les fichiers LDIF considèrent que le fichier est de la version 0 en cas d'absence de la ligne de version.
Spécificateur de nom distinctif	La première ligne de chaque enregistrement de contenu (lignes 2, 6, 11 et 16 de l'exemple précédent) spécifie le DN de l'entrée qu'il représente. Le spécificateur de DN doit revêtir l'une des deux formes suivantes : ◆ dn: *nom_distinctif_UTF-8_protégé* ◆ dn: *nom_distinctif_codé_Base64*
Séparateurs de lignes	Le séparateur de ligne peut être un saut de ligne ou une paire retour chariot/saut de ligne. Cela permet de résoudre une incompatibilité fréquente entre fichiers texte Linux et Solaris, qui utilisent un saut de ligne comme séparateur de ligne, et fichiers texte MS-DOS* et Windows, qui pour ce faire utilisent une paire retour chariot/saut de ligne.

Composant	Description
Séparateurs d'enregistrements	Les lignes vides (lignes 5, 10, 15 et 26 de l'exemple précédent) sont utilisées comme séparateurs d'enregistrements. Chaque enregistrement d'un fichier LDIF, y compris le dernier, doit se terminer par un séparateur d'enregistrement (une ou plusieurs lignes vides). Si certaines implémentations acceptent un fichier LDIF sans séparateur d'enregistrement final, il est impératif pour la spécification LDIF.
Spécificateur de valeur d'attribut	Toutes les autres lignes d'un enregistrement de contenu sont des spécificateurs de valeurs. Les spécificateurs de valeurs doivent revêtir l'une des trois formes suivantes : ◆ Description d'attribut : *valeur* ◆ Description d'attribut : *valeur_Base64_codée* ◆ Description d'attribut : < *URL*

Enregistrements de changement LDIF

Les enregistrements de changement LDIF comportent les modifications à apporter à un répertoire. Toutes les opérations de mise à jour LDAP (add, delete, modify et modify DN) peuvent être représentées dans un enregistrement de changement LDIF.

Les enregistrements de changement LDIF utilisent pour le spécificateur de nom distinctif, le spécificateur de valeur d'attribut et le séparateur d'enregistrement le même format que les enregistrements de contenu LDIF. (Reportez-vous à la section « Enregistrements de contenu LDIF » page 219 pour plus d'informations.) La présence d'un champ `changetype` est ce qui différencie un enregistrement de changement LDIF d'un enregistrement de contenu LDIF. Le champ `changetype` identifie l'opération spécifiée par l'enregistrement de changement.

Le champ `changetype` peut revêtir l'une des cinq formes suivantes :

Formulaire	Description
changetype:ajout	Mot-clé indiquant que l'enregistrement de changement spécifie une opération LDAP d'ajout.
changetype:suppression	Mot-clé indiquant que l'enregistrement de changement spécifie une opération LDAP de suppression.
changetype: moddn	Mot-clé indiquant que l'enregistrement de changement spécifie une opération LDAP de modification du DN si le processeur LDIF est lié au serveur LDAP en tant que client version 3 ou une opération de modification du RDN si le processeur LDIF est lié au serveur LDAP en tant que client version 2.
changetype: modrdn	Synonyme du type de changement moddn.
changetype:modification	Mot-clé indiquant que l'enregistrement de changement spécifie une opération LDAP de modification.

Changement de type add

Un enregistrement de changement de type add ressemble à un enregistrement de changement de contenu (reportez-vous à la section « Enregistrements de contenu LDIF » page 219) ; le champ changetype: add figure immédiatement avant les champs de valeur d'attribut.

Tous les enregistrements doivent être de même type. Vous ne pouvez pas mélanger des enregistrements de contenu et des enregistrements de changement.

```
 1 version: 1
 2 dn: c=US
 3 changetype: add
 4 objectClass: top
 5 objectClass: country
 6
 7 dn: l=San Francisco, c=US
 8 changetype: add
 9 objectClass: top
10 objectClass: locality
11 st: San Francisco
12
14 dn: ou=Artists, l=San Francisco, c=US
15   changetype: add
16 objectClass: top
17 objectClass: organizationalUnit
18 telephoneNumber: +1 415 555 0000
19
20 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
21 changetype: add
22 sn: Michaels
23 givenname: Peter
24 objectClass: top
25 objectClass: person
26 objectClass: organizationalPerson
27 objectClass: iNetOrgPerson
28 telephonenumber: +1 415 555 0001
29 mail: Peter.Michaels@aaa.com
30 userpassword: Peter123
31
```

Changement de type delete

Étant donné qu'un enregistrement de changement de type delete indique la suppression d'une entrée, les seuls champs nécessaires à ce type d'enregistrement sont le spécificateur de nom distinctif et le changement de type delete.

L'exemple de fichier LDIF suivant est utilisé pour supprimer les quatre entrées créées par le fichier LDIF présenté dans la section « Changement de type add » page 222.

IMPORTANT : Pour supprimer des entrées précédemment ajoutées, inversez l'ordre des entrées. Si vous n'effectuez pas cette opération, la suppression échoue, car les entrées de conteneur ne sont pas vides.

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: delete
 4
 5 dn: ou=Artists, l=San Francisco, c=US
 8   changetype: delete
 9
10 dn: l=San Francisco, c=US
11 changetype: delete
12
13 dn: c=US
14 changetype: delete
15
```

Changement de type modify

Le changement de type modify permet de spécifier l'ajout, la suppression et le remplacement de valeurs d'attribut pour une entrée déjà existante. Les modifications revêtent l'une des trois formes suivantes :

Élément	Description
add: type d'attribut	Mot-clé indiquant que les spécificateurs de valeur d'attribut suivants correspondant au type d'attribut doivent être ajoutés à l'entrée.
delete: attribute type	Mot-clé indiquant que les valeurs correspondant au type d'attribut doivent être supprimées. Si des spécificateurs de valeur d'attribut suivent le champ delete, les valeurs correspondantes sont supprimées. Si aucun spécificateur de valeur d'attribut ne suit le champ delete, toutes les valeurs sont supprimées. Si aucune valeur n'est associée à l'attribut, cette opération échoue, mais l'effet désiré est quand même obtenu, étant donné que l'attribut n'est associé à aucune valeur à supprimer.
replace: attribute type	Mot-clé indiquant que les valeurs correspondant au type d'attribut doivent être remplacées. Tous les spécificateurs de valeur d'attribut qui suivent le champ replace deviennent les nouvelles valeurs de ce type d'attribut. Si aucun spécificateur de valeur d'attribut ne suit le champ replace, le jeu de valeurs actuel est remplacé par un jeu de valeurs vide (ce qui entraîne le retrait de l'attribut). À la différence du spécificateur de modification delete, si aucune valeur n'est associée à l'attribut, le remplacement réussira tout de même. L'effet net est le même dans les deux cas.

L'exemple suivant illustre un changement de type modify qui permet d'ajouter un numéro de téléphone supplémentaire à l'entrée `cn=Peter Michaels`.

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: modify
 4 # add the telephone number to cn=Peter Michaels
 4 add: telephonenumber
 5 telephonenumber: +1 415 555 0002
 6
```

De même que vous pouvez combiner un mélange de modifications dans une requête de modification LDAP unique, vous pouvez spécifier plusieurs modifications dans un enregistrement LDIF unique. Une ligne contenant uniquement le caractère tiret (-) est utilisée pour marquer la fin des indications de valeur d'attribut pour chaque spécificateur de modification.

Le fichier LDIF exemple suivant comprend un mélange de modifications :

```
 1 version: 1
 2
 3 # An empty line to demonstrate that one or more
 4 # line separators between the version identifier
 5 # and the first record is legal.
 6
 7 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 8 changetype: modify
 9 # Add an additional telephone number value.
10 add: telephonenumber
11 telephonenumber: +1 415 555 0002
12 -
13 # Delete the entire fascimiletelephonenumber attribute.
14 delete: facsimileTelephoneNumber
15 -
16 # Replace the existing description (if any exists)
17 # with two new values.
18 replace: description
19 description: guitar player
20 description: solo performer
21 -
22 # Delete a specific value from the telephonenumber
23 # attribute.
24 delete: telephonenumber
25 telephonenumber: +1 415 555 0001
26 -
27 # Replace the existing title attribute with an empty
28 # set of values, thereby causing the title attribute to
29 # be removed.
30 replace: title
31 -
32
```

Changement de type modify DN

Le changement de type modify DN permet de renommer une entrée, de la déplacer, ou d'effectuer les deux opérations. Ce type de changement se compose de deux champs obligatoires et d'un champ facultatif.

Champ	Description
newrdn (obligatoire)	Indique le nouveau nom de l'entrée qui sera assignée lors du traitement de cet enregistrement. Le spécificateur « new RDN » doit revêtir l'une des deux formes suivantes : ◆ newrdn : *nom_distinctif_relatif_UTF-8_sécurisé* ◆ newrdn : *nom_distinctif_relatif_codé_Base64* Le spécificateur « new RDN » est obligatoire dans tous les enregistrements LDIF comportant un changement de type modify DN.

Champ	Description
deleteoldrdn (obligatoire)	Le spécificateur delete « old RDN » spécifie si l'ancien RDN doit être remplacé par la valeur newrdn ou s'il doit être conservé. Il revêt l'une des deux formes suivantes : ◆ deleteoldrdn: 0 Indique que l'ancienne valeur RDN doit être conservée dans l'entrée une fois renommée. ◆ deleteoldrdn: 1 Indique que l'ancienne valeur RDN doit être supprimée une fois l'entrée renommée.
newsuperior (facultatif)	Le spécificateur « new superior » indique le nom du nouveau parent qui sera assigné à l'entrée lors du traitement de l'enregistrement modify DN. Le spécificateur new « superior » doit revêtir l'une des deux formes suivantes : ◆ newsuperior: *nom_distinctif_UTF-8_protégé* ◆ newsuperior: *nom_distinctif_codé_Base64* Le spécificateur « new superior » est facultatif dans les enregistrements LDIF comportant un changement de type modify DN. Il n'est fourni que si vous souhaitez attribuer un autre parent à l'entrée.

L'exemple suivant illustre un changement de type modify DN et montre comment renommer une entrée :

```
 1 version: 1
 2
 3 # Rename ou=Artists to ou=West Coast Artists, and leave
 4 # its old RDN value.
 5 dn: ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: ou=West Coast Artists
 8 deleteoldrdn: 1
 9
```

L'exemple suivant illustre un changement de type modify DN et montre comment déplacer une entrée :

```
 1 version: 1
 2
 3 # Move cn=Peter Michaels from
 4 # ou=Artists,l=San Francisco,c=US to
 5 # ou=Promotion,l=New York,c=US and delete the old RDN.
 5 dn: cn=Peter Michaels,ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: cn=Peter Michaels
 8 deleteoldrdn: 1
 9 newsuperior: ou=Promotion,l=New York,c=US
10
```

L'exemple suivant illustre un changement de type modify DN et montre comment déplacer une entrée et la renommer en même temps :

```
 1 version: 1
 2
 3 # Move ou=Promotion from l=New York,c=US to
 4 # l=San Francisco,c=US and rename it to
 5 # ou=National Promotion.
 5 dn: ou=Promotion,l=New York,c=US
 6 changetype: moddn
 7 newrdn: ou=National Promotion
 8 deleteoldrdn: 1
 9 newsuperior: l=San Francisco,c=US
10
```

IMPORTANT : L'opération de modification RDN de LDAP 2 ne prend pas en charge le déplacement des entrées. Si vous tentez de déplacer une entrée en utilisant la syntaxe LDIF `newsuperior` avec un client LDAP 2, la requête échoue.

Retour à la ligne dans les fichiers LDIF

Pour retourner à la ligne dans un fichier LDIF, il suffit d'insérer un séparateur de ligne (saut de ligne ou paire retour chariot/saut de ligne), suivi d'un espace à l'emplacement auquel vous souhaitez retourner à la ligne. Lorsque l'analyseur syntaxique LDIF rencontre un espace en début de ligne, il sait concaténer le reste des données de la ligne avec les données de la ligne précédente. Il supprime alors l'espace en tête.

Vous ne devez pas aller à la ligne au milieu d'un caractère multi-octets UTF-8.

L'exemple de fichier LDIF suivant illustre une ligne avec retour à la ligne (voir lignes 13 et 14) :

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 sn: Michaels
 4 givenname: Peter
 5 objectClass: top
 6 objectClass: person
 7 objectClass: organizationalPerson
 8 objectClass: iNetOrgPerson
 9 telephonenumber: +1 415 555 0001
10 mail: Peter.Michaels@aaa.com
11 userpassword: Peter123
12 description: Peter is one of the most popular music
13  ians recording on our label. He's a big concert dr
14  aw, and his fans adore him.
15
```

Représentation du mot de passe haché dans les fichiers LDIF

Un mot de passe haché est représenté au format de données base64 dans le fichier LDIF. Le nom d'attribut `userpassword` doit être suivi du nom du codage utilisé pour le hachage du mot de passe. Ce nom doit être précédé et suivi d'accolades (« { » et « } »), comme l'illustrent les exemples suivants :

Exemple 1

Pour les mots de passe codés SHA :

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SHA}xcbdh46ngh37jsd0naSFDedjAS30dm5 objectclass:
inetOrgPerson
```

Exemple 2

Pour les mots de passe codés SSHA :

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SSHA}sGs948DFGkakdfkasdDF34DF4dS3skl5DFS5 objectclass:
inetOrgPerson
```

Exemple 3

Pour les mots de passe codés Digest MD5 :

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {MD5}a45lkSDF234SDFG62dsfsf2DG2QEvgdmnk4305 objectclass:
inetOrgPerson
```

Débogage des fichiers LDIF

- « Activation des références en aval » page 227
- « Contrôle de la syntaxe des fichiers LDIF » page 230
- « Utilisation du fichier d'erreurs LDIF » page 231
- « Utilisation des indicateurs de débogage SDK LDAP » page 231

Si vous rencontrez des problèmes avec un fichier LDIF, tenez compte des points suivants :

Activation des références en aval

Il peut arriver de rencontrer des fichiers LDIF dans lesquels un enregistrement permettant d'ajouter une entrée se trouve avant l'enregistrement permettant d'ajouter ses parents. Le cas échéant, une erreur est générée car le parent de la nouvelle entrée n'existe pas au moment où le serveur LDAP tente d'ajouter l'entrée.

Pour résoudre ce problème, il suffit d'activer l'utilisation de références en aval. Lorsque vous activez la création de références en aval et qu'une entrée va être créée alors que son parent n'existe pas encore, une marque de réservation appelée référence en aval est créée pour le parent de l'entrée afin de permettre la création de l'entrée. Si une opération ultérieure crée le parent, la référence en aval se transforme en entrée normale.

Il est possible qu'il reste une ou plusieurs références en aval une fois l'importation LDIF terminée (si le fichier LDIF n'a, par exemple, jamais créé de parent pour cette entrée). Dans ce cas, la référence en aval apparaît en tant qu'objet Inconnu dans iManager. Vous pouvez certes effectuer une recherche sur une entrée de référence en aval, mais vous ne pouvez pas lire les attributs (à l'exception de l'attribut objectClass) depuis l'entrée de référence en aval car elle n'est associée à aucun attribut et à aucune valeur d'attribut. Cependant, toutes les opérations LDAP fonctionnent normalement sur les entrées d'objet situées sous la référence en aval.

Identification des entrées de référence en aval

Les entrées de référence en aval sont associées à une classe d'objet Inconnu et ont également un indicateur d'entrée EF_REFERENCE NDS interne. Dans iManager, les entrées associées à une classe d'objet Inconnu sont représentées par une icône jaune circulaire au centre de laquelle se

trouve un point d'interrogation. Vous pouvez utiliser LDAP pour rechercher des objets dont la classe d'objet est Inconnu, bien qu'il n'existe actuellement aucun moyen d'accéder via LDAP aux paramètres de l'indicateur pour vérifier qu'il s'agit bien d'entrées de référence en aval.

Changement des entrées de référence en aval en objets normaux

Vous pouvez changer une entrée de référence en aval en un objet normal en créant ce dernier (à l'aide, par exemple, d'un fichier LDIF ou d'une requête client LDAP). Lorsque vous demandez à eDirectory de créer une entrée qui existe déjà en tant que référence en aval, il remplace l'entrée de référence en aval existante par l'objet dont vous avez demandé la création.

Utilisation de l'Assistant d'importation, de conversion et d'exportation NetIQ eDirectory

Pour activer les références en aval lors d'une importation LDIF :

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Importer les données** depuis un **fichier du disque**, puis sur **Suivant**.
4. Sélectionnez le type de fichier à importer **LDIF**.
5. Entrez le nom du fichier qui contient les données à importer, spécifiez les options appropriées, puis cliquez sur **Suivant**.
6. Spécifiez le serveur LDAP dans lequel importer les données.
7. Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

8. Dans **Paramètres avancés**, cliquez sur **Autoriser les références en aval**.
9. Cliquez sur **Suivant**, puis sur **Terminer**.

Pour activer les références en aval lors d'une migration de données entre serveurs :

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Migrer les données entre les serveurs**, puis sur **Suivant**.
4. Sélectionnez le serveur LDAP comportant les entrées à migrer.
5. Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP source
Port	Numéro de port (nombre entier) du serveur LDAP source
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

6 Dans **Paramètres avancés**, cliquez sur **Autoriser les références en aval**.

7 Cliquez sur **Suivant**.

8 Spécifiez les critères de recherche (décrits ci-dessous) relatifs aux entrées à migrer :

Option	Description
DN de base	Nom distinctif de base pour la requête de recherche Si vous laissez ce champ vide, la valeur par défaut du nom distinctif de base est "" (chaîne vide).
Étendue	Étendue de la requête de recherche
Filtre	Filtre de recherche conforme à la convention RFC 2254 La valeur par défaut est `objectclass=*`.
Attributs	Attributs qui doivent vous être renvoyés pour chaque entrée de la recherche

9 Cliquez sur **Suivant**.

10 Spécifiez le serveur LDAP vers lequel les données doivent migrer.

11 Cliquez sur **Suivant**, puis sur **Terminer**.

REMARQUE : vérifiez que le schéma est cohérent dans tous les services LDAP.

Utilisation de l'interface de ligne de commande de l'utilitaire d'importation, de conversion et d'exportation NetIQ

Pour activer les références en aval dans l'interface de ligne de commande, utilisez l'option -F du gestionnaire cible LDAP.

Pour plus d'informations, reportez-vous à la section « Options du gestionnaire de destination LDIF » du *Guide d'administration de NetIQ eDirectory*.

Contrôle de la syntaxe des fichiers LDIF

Vous pouvez vérifier la syntaxe d'un fichier LDIF avant de traiter les enregistrements qu'il contient en utilisant l'option du gestionnaire source LDIF Afficher les opérations sans les exécuter.

Le gestionnaire de source LDIF vérifie systématiquement la syntaxe des enregistrements d'un fichier LDIF lorsqu'il les traite. Utilisez cette option pour désactiver le traitement des enregistrements et vérifier la syntaxe.

Utilisation de l'Assistant d'importation, de conversion et d'exportation NetIQ eDirectory

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Importer les données** depuis un **fichier du disque**, puis sur **Suivant**.
4. Sélectionnez le type de fichier à importer **LDIF**.
5. Entrez le nom du fichier qui contient les données à importer et sélectionnez les options appropriées.
6. Dans **Paramètres avancés**, cliquez sur **Afficher les opérations sans les exécuter**, puis sur **Suivant**.
7. Spécifiez le serveur LDAP dans lequel importer les données.
8. Ajoutez les options appropriées, décrites dans le tableau ci-dessous :

Option	Description
Nom/Adresse IP du serveur DNS	Nom DNS ou adresse IP du serveur LDAP cible
Port	Numéro de port (nombre entier) du serveur LDAP cible
Fichier DER	Nom du fichier DER qui contient une clé de serveur utilisée pour l'authentification SSL
Méthode de connexion	Connexion authentifiée ou anonyme (pour l'entrée spécifiée dans le champ DN utilisateur)
DN utilisateur	Nom distinctif de l'entrée à utiliser lors de la liaison à l'opération de liaison définie sur le serveur
Mot de passe	Attribut de mot de passe de l'entrée spécifiée dans le champ DN utilisateur

9. Cliquez sur **Suivant**, puis sur **Terminer**.

Utilisation de l'interface de ligne de commande de l'utilitaire d'importation, de conversion et d'exportation NetIQ

Pour vérifier la syntaxe d'un fichier LDIF dans l'interface de ligne de commande, utilisez l'option -n du gestionnaire de source LDIF.

Pour plus d'informations, reportez-vous à la section « Options du gestionnaire source LDIF » du *Guide d'administration de NetIQ eDirectory*.

Utilisation du fichier d'erreurs LDIF

L'utilitaire d'importation/de conversion/d'exportation NetIQ crée automatiquement un fichier LDIF qui recense tous les enregistrements dont le traitement par le gestionnaire de destination a échoué. Vous pouvez éditer le fichier d'erreurs LDIF généré par l'utilitaire, corriger les erreurs et le réappliquer au serveur pour terminer une importation ou une migration de données contenant des enregistrements erronés.

Utilisation de l'Assistant d'importation/d'exportation NetIQ eDirectory

1. Dans NetIQ iManager, cliquez sur **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Assistant Importation/Conversion/Exportation**.
3. Cliquez sur **Importer les données** depuis un **fichier du disque**, puis sur **Suivant**.
4. Dans les Paramètres avancés, sélectionnez l'option **Consigner les enregistrements ayant échoué**, puis cliquez sur **Suivant**.
5. Sélectionnez le type de fichier à importer **LDIF**.
6. Entrez le nom du fichier qui contient les données à importer, spécifiez les options appropriées, puis cliquez sur **Suivant**.
7. Spécifiez le serveur LDAP dans lequel importer les données.
8. Ajoutez les options appropriées, décrites dans le tableau précédent :
9. Cliquez sur **Suivant**. Le fichier ice.log est créé. Il s'agit du fichier dans lequel sont consignés les messages de sortie (notamment les messages d'erreur). Les entrées qui échouent sont consignées au format LDIF.
10. Cliquez sur **Terminer**.

Utilisation de l'interface de ligne de commande de l'utilitaire d'importation, de conversion et d'exportation NetIQ

Utilisez l'option générale `-l` pour configurer des options de journal d'erreurs dans l'utilitaire de ligne de commande.

Pour plus d'informations, reportez-vous à la section « Options générales » du *Guide d'administration de NetIQ eDirectory*.

Utilisation des indicateurs de débogage SDK LDAP

Pour comprendre certains problèmes LDIF, vous devez connaître le fonctionnement du client LDAP SDK. Vous pouvez définir les indicateurs de débogage suivants pour le gestionnaire de source LDAP, le gestionnaire de destination LDAP, ou les deux.

Valeur	Description
0x0001	Effectue le suivi des appels de fonction LDAP.
0x0002	Imprimez des informations sur les paquets.
0x0004	Imprimez des informations sur les arguments.
0x0008	Imprime des informations sur les connexions.
0x0010	Imprime des informations sur le codage et le décodage BER.
0x0020	Imprime des informations sur les filtres de recherche.

Valeur	Description
0x0040	Imprime des informations sur la configuration.
0x0080	Imprime des informations sur l'ACL.
0x0100	Imprime des informations sur les statistiques.
0x0200	Imprime des informations supplémentaires sur les statistiques.
0x0400	Imprime des informations sur le shell.
0x0800	Imprime des informations sur l'analyse syntaxique.
0xFFFF (-1 Decimal)	Active toutes les options de débogage.

Pour activer cette fonction, utilisez l'option `-e` pour les gestionnaires de source et de destination LDAP. Le nombre entier correspondant à l'option `-e` est un masque binaire qui active différents types d'informations de débogage dans le SDK LDAP.

Pour plus d'informations, reportez-vous aux sections « Options du gestionnaire source LDAP » et « Options du gestionnaire de destination LDAP » du *Guide d'administration de NetIQ eDirectory*.

Utilisation de LDIF pour étendre le schéma

LDIF pouvant représenter des opérations de mise à jour LDAP, vous pouvez l'utiliser pour modifier le schéma.

Ajout d'une nouvelle classe d'objet

Pour ajouter une classe, il suffit d'ajouter une valeur d'attribut correspondant à la spécification de `NDSObjectClassDescription` à l'attribut `objectClasses` de `subschemaSubentry`.

```
NDSObjectClassDescription = "(" whsp
   numericoid whsp
   [ "NAME" qdescrs ]
   [ "DESC" qdstring ]
   [ "OBSOLETE" whsp ]
   [ "SUP" oids ]
   [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
   [ "MUST" oids ]
   [ "MAY" oids ]
   [ "X-NDS_NOT_CONTAINER" qdstrings ]
   [ "X-NDS_NONREMOVABLE" qdstrings ]
   [ "X-NDS_CONTAINMENT" qdstrings ]
   [ "X-NDS_NAMING" qdstrings ]
   [ "X-NDS_NAME" qdstrings ]
   whsp ")"
```

L'exemple de fichier LDIF suivant ajoute la classe d'objet `person` (personne) au schéma :

```
 1 version: 1
 2 dn: cn=schema
 3 changetype: add
 4 objectClasses: ( 2.5.6.6 NAME 'person' DESC 'Standard
 5   ObjectClass' SUP ndsLoginProperties STRUCTURAL MUST
 6   (cn $ sn) MAY (description $ seeAlso $ telephoneNum
 7  ber $ fullName $ givenName $ initials $ uid $ userPa
 8  ssword) X-NDS_NAMING ('cn' 'uid') X-NDS_CONTAINMENT
 9  ('organization' 'organizationalUnit' 'domain') X-NDS
10  _NAME 'Person' X-NDS_NOT_CONTAINER '1' X-NDS_NONREMO
11  VABLE '1')
12
```

Attributs obligatoires

Les attributs obligatoires sont listés dans la section `MUST` de la description de la classe d'objet. Pour la classe d'objet Personne, les attributs obligatoires sont `cn` et `sn`.

Attributs facultatifs

Les attributs facultatifs sont répertoriés dans la section `MAY` de la description de la classe d'objet. Les attributs facultatifs de la classe d'objet `Personne` sont : `description`, `seeAlso`, `telephoneNumber`, `fullName`, `givenName`, `initials`, `uid` et `userPassword`.

REMARQUE : l'attribut `userPassword` ne peut pas être utilisé comme attribut facultatif (`MAY`). Si vous essayez de l'employer comme attribut obligatoire (`MUST`) dans la nouvelle `classe d'objet` en utilisant ce format LDIF pour étendre le schéma, l'opération échoue.

Règles d'endiguement

Les classes d'objet qui peuvent contenir la classe d'objet définie sont indiquées dans la section `X-NDS_CONTAINMENT` de la description de la classe d'objet. La classe d'objet `person` peut être contenue dans les classes d'objets `organization` (organisation), `organizationalUnit` (unité organisationnelle) et `domain` (domaine).

Ajout d'un nouvel attribut

Pour ajouter un attribut, il suffit d'ajouter une valeur d'attribut qui correspond à la spécification de `NDSAttributeTypeDescription` sur l'attribut attributes de `subschemaSubentry`.

```
NDSAttributeTypeDescription = "(" whsp
  numericoid whsp  ; AttributeType identifier
  [ "NAME" qdescrs ]  ; name used in AttributeType
  [ "DESC" qdstring ]  ; description
  [ "OBSOLETE" whsp ]
  [ "SUP" woid ]  ; derived from this other AttributeType
  [ "EQUALITY" woid]  ; Matching Rule name
  [ "ORDERING" woid]  ; Matching Rule name
  [ "SUBSTR" woid ]  ; Matching Rule name
  [ "SYNTAX" whsp noidlen whsp ] ;  Syntax OID
  [ "SINGLE-VALUE" whsp ]  ; default multi-valued
  [ "COLLECTIVE" whsp ]  ; default not collective
  [ "NO-USER-MODIFICATION" whsp ] ;  default user modifiable
  [ "USAGE" whsp AttributeUsage ] ;  default userApplications
  [ "X-NDS_PUBLIC_READ" qdstrings ]
                             ; default not public read ('0')
  [ "X-NDS_SERVER_READ" qdstrings ]
```

```
                            ; default not server read ('0')
  [ "X-NDS_NEVER_SYNC" qdstrings ]
                             ; default not never sync ('0')
  [ "X-NDS_NOT_SCHED_SYNC_IMMEDIATE" qdstrings ]
                           ;  default sched sync immediate ('0')
  [ "X-NDS_SCHED_SYNC_NEVER" qdstrings ]
                                ;  default schedule sync ('0')
  [ "X-NDS_LOWER_BOUND" qdstrings ]
                            ;  default no lower bound('0')
                                  ;(upper is specified in SYNTAX)
  [ "X-NDS_NAME_VALUE_ACCESS" qdstrings ]
                       ; default not name value access ('0')
  [ "X-NDS_NAME" qdstrings ]  ; legacy NDS name
  whsp ")"
```

L'exemple de fichier LDIF suivant ajoute le type d'attribut `title` au schéma :

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} X-NDS_NAME 'Title' X-NDS_NOT_SCHED_SYNC_IMMEDIA
7  TE '1' X-NDS_LOWER_BOUND '1')
8
```

Valeur unique et valeurs multiples

Par défaut, un attribut est à valeurs multiples sauf s'il est explicitement défini comme étant à valeur unique. Dans l'exemple de fichier LDIF suivant, title est un attribut à valeur unique, car le mot-clé `SINGLE-VALUE` est ajouté à la suite de la section `SYNTAX` :

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} SINGLE-VALUE X-NDS_NAME 'Title' X-NDS_NOT_SCHED
7  _SYNC_IMMEDIATE '1' X-NDS_LOWER_BOUND '1')
8
```

Ajout d'un attribut facultatif à une classe d'objet existante

Bien que l'ajout de nouveaux éléments de schéma soit une pratique courante, la modification ou l'extension d'éléments de schéma existants est généralement une opération dangereuse. Étant donné que chaque élément de schéma est identifié de façon unique par un OID, lors d'une extension d'un élément de schéma standard, vous créez en fait une seconde définition pour l'élément, bien que celui-ci utilise toujours l'OID d'origine. Ceci peut engendrer des problèmes d'incompatibilité.

Il est parfois approprié de modifier des éléments du schéma. Vous pouvez par exemple avoir besoin d'étendre ou de modifier de nouveaux éléments de schéma à mesure que vous les définissez au cours du développement. Plutôt que d'ajouter de nouveaux attributs à une classe, vous devriez utiliser généralement des classes auxiliaires uniquement pour effectuer les opérations suivantes :

- Ajouter de nouveaux attributs à une classe d'objet existante.
- Diviser une classe d'objet existante en sous-classes.

Ajout ou suppression de classes auxiliaires

L'exemple de fichier LDIF suivant crée deux nouveaux attributs, une classe auxiliaire à partir de ceux-ci, puis ajoute une entrée `inetOrgPerson` ayant comme classe d'objet la classe `auxiliaire` et fournit des valeurs pour les attributs de la classe `auxiliaire`.

```
version: 1
# Add an attribute to track a bear's hair. The attribute is
# multi-valued, uses a case ignore string syntax,
# and has public read rights
# Values may include: long hair, short, curly, straight,
# none, black, and brown
# X-NDS_PUBLIC_READ '1' The 1 allows public read,
# 0 denies public read
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.10 NAME
'bearHair' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
X-NDS_PUBLIC_READ '1' )

# add an attribute to store a bear's picture
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.11 NAME
'bearPicture' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE )

# create an Auxiliary class for the bearfeatures
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (2.16.840.1.113719.1.186.6.101 NAME
'bearFeatures' MAY (bearHair $ bearPicture) AUXILIARY)

# now create a user named bobby
dn: cn=bobby,o=bearcave
changetype: add
cn: bobby
sn: bear
givenName: bobby
bearHair: Short
bearHair: Brown
bearHair: Curly
bearPicture:< file:///c:/tmp/alien.jpg
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: bearFeatures

# now create a person named john that will later be changed
# into a bear when bearFeatures is added to its objectClass
# list
dn: cn=john,o=bearcave
changetype: add
cn: John
sn: bear
givenName: john
objectClass: top
```

```
objectClass: person
objectClass: inetOrgPerson

# now morph john into a bear by adding bearFeatures
dn: cn=john,o=bearcave
changetype: modify
add: objectClass
objectClass: bearFeatures
-
add: bearHair
bearHair: long
bearHair: black
#bearPicture:< file:///c:/tmp/john.jpg>
-

# to morph john back to a person, simply delete the
# objectClass bearFeatures
dn: cn=john,o=bearcave
changetype: modify
delete: objectClass
objectClass: bearFeatures
```

Lorsque vous supprimez une classe `auxiliaire` de la liste objectClass, il n'est pas nécessaire de supprimer toutes les valeurs qui y sont associées. eDirectory effectue cette opération automatiquement.

Si la classe `auxiliaire` possédait des attributs `MUST`, ils doivent tous être spécifiés dans l'opération de modification qui ajoute la classe `auxiliaire` à la liste objectClass. Dans le cas contraire, la modification échoue.

Problèmes connus lors de l'analyse XML

Le traitement XML de tout enregistrement LDIF (format LDIF ou enregistrements générés à partir du serveur LDAP) échoue si des enregistrements ne satisfont pas à toutes les règles XML définies dans le fichier XML.

Limitations ldif2dib

- « Mot de passe simple et LDIF » page 236
- « Schéma » page 237
- « Modèles ACL » page 237
- « Gestionnaire de signal » page 237

Mot de passe simple et LDIF

Sous Windows, lors du téléchargement de LDIF avec un mot de passe simple, ldif2dib risque d'échouer si les clés NICI des dossiers `system` et *`administrator`* ne sont pas synchronisées.

Pour éviter ce problème, accédez aux clés dans le dossier `nici/system` comme suit :

1. Accédez au dossier `C:\Windows\system32\novell\nici\` (pour NICI 32 bits).

   ou

   Accédez au dossier `C:\Windows\SysWOW64\novell\nici\` (pour NICI 64 bits).
2. Sauvegardez les fichiers du dossier *`Administrator`*.

3 Accédez à l'onglet **Sécurité** dans la fenêtre Propriétés du dossier `System`.

4 Sélectionnez **Options avancées** et accédez à l'onglet **Propriétaire**.

5 Sélectionnez **Administrateur**.

6 Retournez à l'onglet **Sécurité** et ajoutez Administrateur à la liste.

7 Répétez la procédure de l'Étape 3 à l'Étape 6 pour obtenir un accès en lecture à tous les fichiers du dossier system.

8 Remplacez les fichiers du dossier *`Administrator`* par ceux du dossier system.

9 Une fois le téléchargement terminé, copiez les fichiers sauvegardés dans le dossier *`Administrator`*.

10 Rétablissez l'accès de l'administrateur au dossier `system` et aux fichiers qu'il contient.

Schéma

Le fichier LDIF doit mentionner toutes les classes d'objet auxquelles appartient une entrée. Vous devez également inclure les classes auxquelles une entrée appartient en raison d'un héritage. Par exemple, une entrée du type `inetOrgPerson` a la syntaxe suivante dans le fichier LDIF :

- `objectclass: inetorgperson`
- `objectclass: organizationalPerson`
- `objectclass: person`
- `objectclass: top`

Modèles ACL

Les objets chargés en bloc à l'aide de l'utilitaire `ldif2dib` ne sont pas ajoutés aux listes de contrôle d'accès spécifiées dans les modèles ACL de la classe de l'objet.

Gestionnaire de signal

Vous pouvez suspendre provisoirement l'opération de chargement en bloc hors ligne en appuyant sur la touche s ou S. Vous pouvez utiliser la touche d'échappement (Échap) pour arrêter l'opération de chargement en bloc.

8 Surveillance d'eDirectory

eDirectory fournit des fonctionnalités multi plate-formes de surveillance et de diagnostic pour tous les serveurs de votre arborescence eDirectory. Cette fonction vous permet de surveiller les serveurs à partir de n'importe quel emplacement, en reprenant plusieurs interfaces de différents gestionnaires d'outils/protocole ou en utilisant votre réseau lorsqu'un navigateur Web est disponible. Les utilitaires eDirectory (notamment ndscheck, iMonitor et ndsrepair) et les recherches LDAP rootDSE vous aident à rassembler les données de surveillance.

eDirectory propose également une méthode de recherche LDAP pour la récupération des statistiques en temps réel des sous-systèmes eDirectory et des processus en arrière-plan. Dans le cadre de cette méthode, eDirectory enregistre l'état des processus et des opérations eDirectory en tant qu'entrée avec comme DN de base `cn=monitor`. À l'aide de cette interface, un administrateur eDirectory peut surveiller l'état des modules et des opérations eDirectory. eDirectory prend en charge cette fonction sur le protocole LDAP et seul un client LDAP peut placer des requêtes pour surveiller les données.

- « Utilisation de NetIQ iMonitor » page 239
- « Utilisation de cn=monitor pour la surveillance » page 271
- « Utilisation de DSTrace » page 281
- « Messages DSTrace » page 289
- « Filtrage des messages d'iMonitor » page 293
- « Filtrage des messages de SAL » page 293

Utilisation de NetIQ iMonitor

L'utilitaire NetIQ iMonitor offre des fonctionnalités multi plate-formes de surveillance et de diagnostic pour tous les serveurs de votre arborescence eDirectory. Cet utilitaire permet de contrôler les serveurs à partir de tout emplacement du réseau où un navigateur Web est disponible.

iMonitor est utile pour effectuer un examen complet de l'environnement eDirectory, en fonction des partitions, des répliques ou des serveurs. Vous pouvez également savoir quelles tâches sont en cours de réalisation, le moment de leur exécution, les résultats qu'elles génèrent et leur durée.

iMonitor propose une alternative Web à de nombreux outils NetIQ eDirectory utilisant traditionnellement un serveur, tels que DSBrowse, DSTrace, DSDiag ainsi qu'aux fonctionnalités de diagnostic disponibles dans DSRepair. Ainsi, les fonctionnalités d'iMonitor sont principalement « orientées serveur », c'est-à-dire qu'elles se concentrent sur l'état de santé de différents agents eDirectory (exécutant des instances du service d'annuaire), et non à l'arborescence eDirectory dans son intégralité.

iMonitor offre les fonctions suivantes :

- Résumé de l'état de santé
  - Informations concernant la synchronisation
  - Serveurs connus
  - Configuration des agents
- Vérifications de l'état de santé

- Suivi des DS par lien hypertexte
- Configuration des agents
- Activité de l'agent et statistiques du verbe
- Rapports
- Informations sur les agents
- Informations sur les erreurs
- Navigateur d'objet/de schéma
- Surveillance de NetIQ Identity Manager
- Rechercher
- Liste des partitions
- État d'avancement des agents
- Planification des processus en arrière-plan
- DSRepair
- Surveillance des connexions

Les informations que vous pouvez visualiser dans iMonitor dépendent des facteurs suivants :

- Votre identité

  Les droits eDirectory associés à votre identité s'appliquent à l'ensemble des requêtes que vous lancez dans iMonitor. Par exemple, vous devez vous connecter en tant qu'administrateur du serveur ou en tant qu'opérateur de la console du serveur sur lequel vous tentez d'accéder à la page DSRepair.
- Version de l'agent eDirectory faisant l'objet de la surveillance

  Les versions plus récentes de NDS et d'eDirectory comprennent des fonctions et des options qui n'étaient pas disponibles dans les versions antérieures.

Les informations que vous affichez dans iMonitor reflètent instantanément les opérations qui ont lieu sur le serveur.

Ce chapitre procure des informations sur les sujets suivants :

- « Configuration système requise » page 240
- « Accès à iMonitor » page 241
- « Architecture iMonitor » page 242
- « Caractéristiques d'iMonitor » page 247
- « Opérations iMonitor sécurisées » page 268
- « Configuration d'un objet Serveur HTTP » page 269
- « Configuration des paramètres de la pile HTTP à l'aide de ndsconfig » page 270

Configuration système requise

Pour utiliser iMonitor, vous avez besoin des éléments suivants :

- NetIQ eDirectory 8.7.1 ou version ultérieure
- Un navigateur Web pris en charge, notamment Microsoft Internet Explorer ou Firefox

Plates-formes

L'utilitaire iMonitor fonctionne sur les plates-formes suivantes :

- Serveurs Windows 2000 et 2003 (non-SSL)
- Linux

Sous Windows, iMonitor se charge automatiquement au moment de l'exécution d'eDirectory. Sous Linux, iMonitor peut être chargé à l'aide de la commande `ndsimonitor -l`. Il peut aussi être chargé automatiquement en ajoutant `[ndsimonitor]` dans le fichier `/etc/opt/novell/eDirectory/conf/ndsimon.conf` avant de démarrer le serveur eDirectory.

L'utilitaire iMonitor s'exécute sur les navigateurs Web suivants :

- Microsoft Internet Explorer 10 et versions ultérieures
- Firefox* 40 et versions ultérieures

Versions d'eDirectory compatibles

iMonitor permet de surveiller les versions suivantes des services NDS et :

- Toutes les versions des services NDS et eDirectory pour Windows
- Toutes les versions des logiciels NDS et eDirectory pour Linux

Accès à iMonitor

1. Vérifiez que le fichier exécutable iMonitor est exécuté sur le serveur eDirectory.
2. Ouvrez votre navigateur Web.
3. Dans le champ Adresse (URL), tapez

   `http://server's_TCPIP_address:httpstack_port/nds`

   Par exemple :

   `http://137.65.135.150:8028/nds`

   Vous pouvez utiliser les noms DNS chaque fois que l'adresse IP ou IPX ou encore le nom distinctif d'un serveur peuvent être utilisés dans iMonitor. Par exemple, une fois DNS configuré,

   `http://prv-gromit.provo.novell.com/nds?server=prv-igloo.provo.novell.com`

   est équivalent à

   `http://prv-gromit.provo.novell.com/nds?server=IP_or_IPX address`

   ou

   `http://prv-gromit.provo.novell.com/nds?server=/cn=prv-igloo,ou=ds,ou=dev,o=novell,t=novell_inc`

   Si une pile HTTPS eDirectory est disponible, vous pouvez utiliser iMonitor via HTTPS.
4. Indiquez un nom d'utilisateur, un contexte et un mot de passe. Par exemple, `login cn=admin.o=novell`

   Pour avoir accès à toutes les fonctions, connectez-vous en tant qu'administrateur avec un nom distinctif complet ou avec des droits équivalents.
5. Cliquez sur **Connexion**.

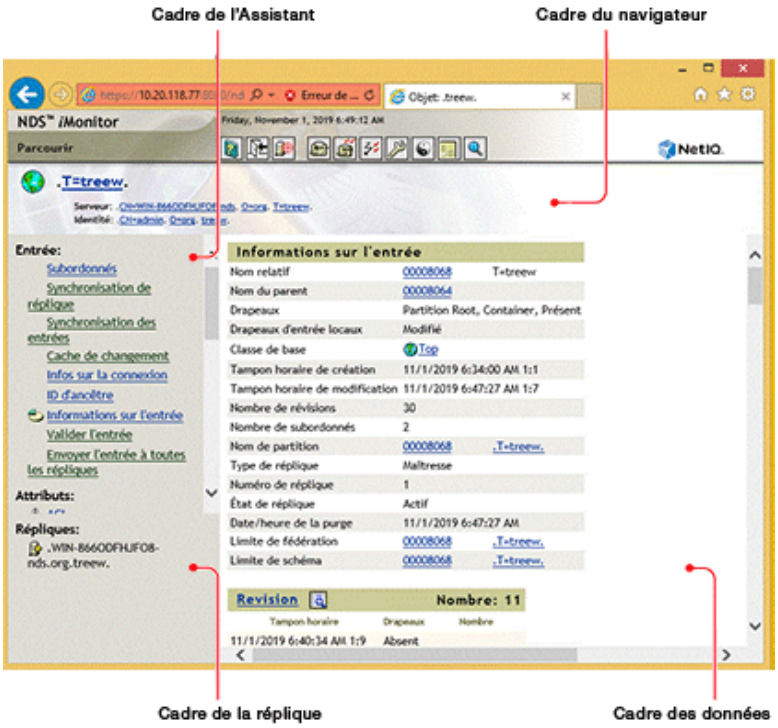
Architecture iMonitor

- « Anatomie d'une page dans iMonitor » page 242
- « Modes de fonctionnement » page 243
- « Fonctions d'iMonitor disponibles sur chaque page » page 244
- « Fichiers de configuration » page 245

Anatomie d'une page dans iMonitor

Dans iMonitor, chaque page est divisée en quatre cadres ou sections : le cadre du navigateur, le cadre de l'Assistant, le cadre des données et le cadre de la réplique.

Figure 8-1 *Cadres d'iMonitor*



Cadre du navigateur : situé dans la partie supérieure de la page. Ce cadre affiche le nom du serveur à partir duquel les données sont lues, votre identité, et les icônes sur lesquelles vous pouvez cliquer pour accéder à d'autres écrans, notamment ceux de l'aide en ligne, de connexion, du portal du serveur et d'autres pages iMonitor.

Cadre de l'Assistant : situé dans la partie gauche de la page. Ce cadre contient des aides à la navigation supplémentaires, telles que des liens vers d'autres pages, des éléments qui vous permettent de naviguer dans le cadre de données, ou d'autres éléments qui vous aident à obtenir ou à interpréter les données d'une page donnée.

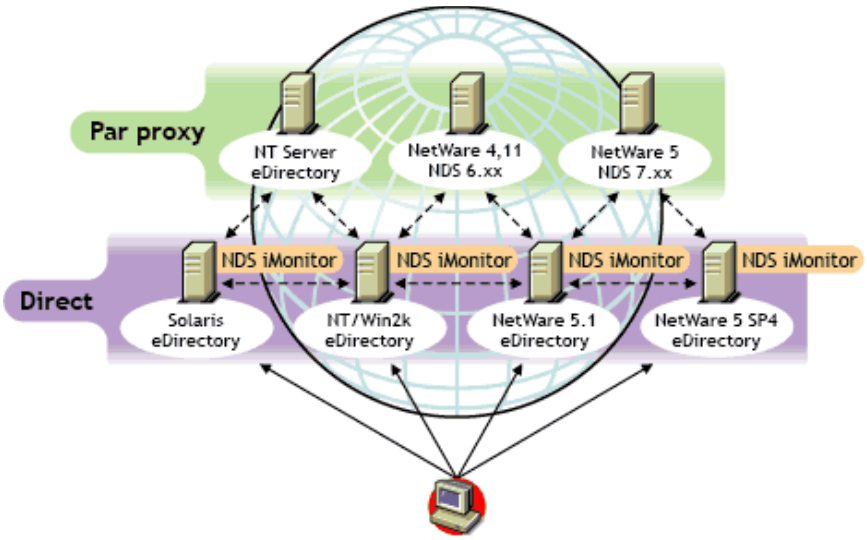
Cadre des données : affiche les informations détaillées sur les serveurs, que vous obtenez en cliquant sur l'un des liens indiqués ci-dessus. Il s'agit de la seule page que vous affichez si votre navigateur Web ne prend pas en charge les cadres.

Cadre de la réplique : permet de déterminer la réplique actuellement affichée et propose des liens servant à afficher les mêmes informations du point de vue d'une autre réplique ou d'un autre serveur. Ce cadre n'apparaît que lorsque vous affichez des pages sur lesquelles figure une autre réplique des données concernées ou une autre réplique qui présente une vue différente des informations affichées dans le cadre des données.

Modes de fonctionnement

NetIQ iMonitor peut être utilisé dans deux modes de fonctionnement différents : le mode Direct et le mode Proxy. Aucune modification de configuration n'est nécessaire pour passer d'un mode à l'autre. NetIQ iMonitor passe automatiquement d'un mode à l'autre. Il est toutefois préférable de comprendre le fonctionnement de ces deux modes afin de parcourir l'arborescence eDirectory de manière optimale.

Figure 8-2 *Modes de fonctionnement*



Mode Direct : utilisez ce mode lorsque votre navigateur Web pointe directement sur l'adresse ou le nom DNS d'une machine qui utilise le fichier exécutable iMonitor et lit uniquement les informations situées dans la DIB eDirectory locale de cette machine.

Certaines fonctions d'iMonitor sont centrées sur le serveur et ne sont accessibles que par le biais de l'utilitaire iMonitor exécuté sur cette machine. Ces fonctions utilisent des ensembles API locaux qui ne sont pas accessibles à distance. Parmi les fonctions d'iMonitor centrées sur le serveur figurent les pages DSTrace, DSRepair et Planification des processus à l'arrière-plan. Lorsque vous utilisez le mode direct, toutes les fonctions d'iMonitor sont disponibles sur cette machine.

Principales fonctions du mode direct :

- Ensemble complet de fonctions centrées sur le serveur
- Réduction de la largeur de bande réseau (accès plus rapide)
- accès par proxy toujours possible pour toutes les versions d'eDirectory.

Mode Proxy : utilisez ce mode lorsque votre navigateur Web pointe sur un utilitaire iMonitor exécuté sur une machine, mais collecte les informations d'une autre machine. Étant donné que iMonitor utilise des protocoles traditionnels non centrés sur le serveur eDirectory pour des fonctions non centrées

sur le serveur, toutes les versions d'eDirectory antérieures à la version NDS 6.*x* peuvent être surveillées et diagnostiquées. Toutefois, les fonctions centrées sur le serveur utilisent des API auxquelles il est impossible d'accéder à distance.

Il est possible de passer du mode proxy au mode direct pour un autre serveur à condition que la version d'eDirectory installée sur ce dernier soit une version avec laquelle iMonitor est livré. Si le serveur sur lequel vous rassemblez des informations par proxy exécute iMonitor, une icône supplémentaire apparaît dans le cadre du navigateur. Lorsque vous placez le pointeur de la souris sur cette icône, un lien vers l'utilitaire iMonitor du serveur distant apparaît. Si le serveur sur lequel vous collectez des informations par proxy exécute une ancienne version d'eDirectory, aucune icône supplémentaire n'apparaît ; vous devrez toujours recueillir des informations sur ce serveur par proxy jusqu'à ce qu'il soit mis à niveau vers une version d'eDirectory comprenant iMonitor.

Principales fonctions du mode proxy :

- Les serveurs de l'arborescence ne doivent pas tous obligatoirement exécuter iMonitor afin d'utiliser la plupart des fonctions iMonitor
- Un seul serveur doit être mis à niveau.
- Un point d'accès unique est offert pour les connexions à distance
- Vous pouvez accéder à iMonitor via une liaison à débit moins élevé alors que iMonitor accède aux informations eDirectory via des liaisons à plus haut débit.
- Un accès aux informations des versions précédentes des NDS est offert
- Les fonctions centrées sur le serveur ne sont disponibles qu'aux emplacements où iMonitor est installé.

Fonctions d'iMonitor disponibles sur chaque page

Vous pouvez accéder aux pages Résumé de l'agent, Informations sur les agents, Configuration de l'agent, Configuration de Trace, DSRepair, Rapports et Recherche à partir de n'importe quelle page iMonitor, à l'aide des icônes du cadre du navigateur. Vous pouvez également vous connecter ou accéder à la page Web du support NetIQ par le biais d'un lien situé sur n'importe quelle page iMonitor.

Connexion/déconnexion : le bouton **Connexion** n'est disponible que si vous n'êtes pas connecté. Un bouton **Déconnexion** qui ferme la fenêtre de votre navigateur, apparaît si vous êtes connecté. Tant que toutes les fenêtres de navigateur ne sont pas fermées, votre session iMonitor reste ouverte et vous n'aurez pas besoin de vous reconnecter pour y accéder. Vous pouvez consulter l'état de votre connexion sur n'importe quelle page, dans la zone Identité du cadre Navigateur.

Lien de connexion au support : le logo NetIQ situé dans le coin supérieur droit est un lien vers la page Web de connexion au support de NetIQ. Il fournit un lien direct vers le site Web de NetIQ sur lequel vous pouvez obtenir des mises à jour et des correctifs de serveur, ainsi qu'un support technique propre à chaque produit.

Fichiers de configuration

Des fichiers de configuration sont livrés avec iMonitor afin de vous permettre de modifier ou de définir le comportement ou les valeurs par défaut de l'utilitaire.

Les fichiers de configuration sont des fichiers texte qui contiennent des étiquettes de paramètres de configuration associées aux valeurs requises. Ces fichiers sont situés dans le même répertoire que le fichier exécutable d'iMonitor (qui se trouve généralement au même emplacement que les fichiers exécutables de NetIQ eDirectory) sous Windows, et dans le répertoire `/etc` sous Linux.

- « ndsimon » page 245
- « ndsimonhealth » page 246

ndsimon

Le fichier de configuration ndsimon permet de modifier les paramètres des fichiers de trace, de contrôler l'accès au serveur, de définir le nombre maximal d'objets à afficher lors du listage d'un conteneur ou de l'affichage de résultats de recherche, mais aussi de spécifier le nombre de minutes d'inactivité autorisé avant qu'une connexion soit coupée.

Serveur	Fichier de configuration
Windows	*répertoire_installation*`\novell\NDS\ndsimon.ini`
Linux	`/etc/opt/novell/eDirectory/conf/ndsimon.conf`

Le fichier de configuration ndsimon permet de définir deux groupes de paramètres, à savoir :

- Paramètres relatifs au mode d'exécution du fichier exécutable d'iMonitor

  Lors du chargement du fichier exécutable d'iMonitor, il tentera d'écouter sur le port 80, à savoir le port HTTP habituel. Si ce port est déjà utilisé, iMonitor basculera momentanément vers le port 8028. Si ce port est également utilisé, iMonitor basculera vers un autre port et effectuera une nouvelle tentative en ajoutant chaque fois 2 (8010, 8012, etc.) jusqu'à 8078.

  Lorsque le protocole SSL est configuré et disponible, le même schéma de tentative de liaison est appliqué. Dans un premier temps, une tentative est effectuée sur le port 81, puis sur les ports 8009, 8011, 8013 etc.

  Ainsi, iMonitor peut coexister avec un serveur Web qui s'exécute sur le même serveur. Il se peut toutefois que, sur certaines plates-formes, iMonitor se charge avant le serveur Web installé ou que vous souhaitiez que iMonitor se lie à un port de votre choix. Les ports habituels et SSL peuvent être configurés respectivement à l'aide des paramètres `HttpPort` et `HttpsPort`.

- Paramètres applicables à des fonctionnalités ou à des pages spécifiques

  Le fichier de configuration fourni avec iMonitor contient des exemples de paramètres que vous pouvez modifier. Ces paramètres sont précédés du caractère #. Il permet d'indiquer que ces paramètres sont mis en commentaires et qu'ils ne sont pas utilisés lorsque iMonitor analyse le fichier de configuration. S'agissant du fichier de configuration d'origine, iMonitor utilise l'ensemble des valeurs par défaut liées en interne pour ces paramètres. Pour activer l'un de ces paramètres, ou pour en ajouter, il suffit de supprimer le caractère # au début de la ligne.

ndsimonhealth

Le fichier de configuration ndsimonhealth vous permet de modifier les paramètres par défaut de la page d'informations sur l'état de santé de l'agent. Vous pouvez activer ou désactiver les options relatives à l'état de santé de l'agent, définir les niveaux de génération de rapports et les plages des options, ainsi qu'établir les niveaux de génération de rapports des serveurs.

Serveur	Fichier de configuration
Windows	*répertoire_installation*\novell\NDS\ndsimonhealth.ini
Linux	/etc/opt/novell/eDirectory/conf/ndsimonhealth.conf

Le fichier de configuration ndsimonhealth permet de définir trois types d'options.

- Options à activer/désactiver uniquement

  Pour désactiver une option, supprimez le signe # qui la précède et remplacez le niveau indiqué après le signe deux-points (:) par OFF. Pour définir le niveau de génération de rapports de ces options, supprimez le signe # qui les précède et indiquez un niveau de génération de rapports après le signe deux-points. Les niveaux autorisés sont WARN, MARGINAL et SUSPECT. Vous ne pouvez définir qu'un seul niveau de génération de rapports pour ces options.

- Options générales acceptant une plage de valeurs

  Ces options peuvent être activées ou désactivées, ou encore se voir affecter un niveau de génération de rapports avec les plages correspondantes.

  Pour définir le niveau de génération de rapports pour l'une de ces options, utilisez le nom de cette dernière suivi de « -active: », et le niveau de génération de rapports souhaité. Ainsi, pour activer time_delta (delta horaire), ajoutez la ligne suivante au fichier de configuration :

  ```
  time_delta-active: WARN
  ```

  Pour désactiver delta_horaire, ajoutez la ligne suivante au fichier de configuration :

  ```
  time_delta-active: OFF
  ```

  Lors de la saisie de plages, la plage indiquée est celle pour laquelle le niveau de génération de rapports ne doit pas être affiché.

  L'exemple de time_delta ci-dessous montre comment activer une option pour les trois niveaux de génération de rapports et définir les plages associées. Dans cet exemple, tout ce qui ne figure pas dans la plage -2 à 2 est au minimum marginal, tout ce qui n'est pas compris entre -5 et +5 est au moins suspect et tout ce qui ne figure pas entre -10 et 10 est un avertissement.

  ```
  time_delta-active: WARN | SUSPECT | MARGINAL
  time_delta-Min_Warn:      -10
  time_delta-Min_Suspect:    -5
  time_delta-Min_Marginal:   -2
  time_delta-Max_Marginal:    2
  time_delta-Max_Suspect:     5
  time_delta-Max_Warn:        10
  ```

  Pour obtenir de l'aide sur l'une de ces options, entrez l'URL suivante dans iMonitor :

  http://*XXX.XXX.XXX.XXX*:*PORT*/nds/help?hbase=/nds/health/OPTION_NAME

  XXX.XXX.XXX.XXX:*PORT* correspond à l'adresse IP et au port auxquels iMonitor peut être contacté, et *NOM_OPTION* est le nom de l'option sur laquelle vous souhaitez obtenir de l'aide (par exemple, time_delta).

Pour afficher les niveaux et plages actuellement définis, ouvrez avec votre navigateur la page d'état de santé qui contient l'option qui vous intéresse, puis ajoutez ce qui suit à la fin de la ligne d'URL :

```
&op=setup
```

- Options qui impliquent des paramètres personnalisés ou complexes

  Trois niveaux différents de génération de rapports du serveur peuvent être définis :

  - WARN détecte les serveurs qui exécutent une version d'eDirectory devant être mise à niveau dès que possible.
  - SUSPECT détecte les serveurs exécutant une version d'eDirectory dont la mise à niveau doit être planifiée.
  - MARGINAL détecte les serveurs exécutant une version d'eDirectory qui n'est pas à jour.

  Ces options définissent le niveau de génération de rapports lorsque la version du serveur appartient à la plage spécifiée.

Caractéristiques d'iMonitor

Cette section décrit brièvement les fonctions d'iMonitor.

Pour obtenir des informations détaillées sur chaque fonction, accédez à l'aide en ligne fournie dans chaque section d'iMonitor.

- « Affichage de l'état de santé des serveurs eDirectory » page 248
- « Affichage de l'état de synchronisation des partitions » page 248
- « Affichage de l'état des processus de la notice nécrologique et le nombre de caches de changement » page 249
- « Affichage des informations de connexion au serveur » page 250
- « Affichage des serveurs connus » page 251
- « Affichage des informations relatives aux répliques » page 251
- « Contrôle et configuration de l'agent DS » page 252
- « Configuration des paramètres Trace » page 253
- « Affichage des informations relatives à l'état des processus » page 254
- « Affichage de l'activité de l'agent » page 254
- « Affichage des modèles de trafic » page 255
- « Affichage des processus arrière-plan » page 255
- « Configuration des processus en arrière-plan » page 255
- « Affichage des erreurs relatives aux serveurs eDirectory » page 256
- « Affichage des informations DSRepair » page 256
- « Affichage d'informations sur l'état de santé de l'agent » page 257
- « Exploration d'objets dans l'arborescence » page 257
- « Affichage des entrées à synchroniser ou à purger » page 257
- « Affichage des détails de NetIQ Identity Manager » page 258
- « Affichage de l'état de synchronisation d'une réplique » page 258
- « Configuration et affichage de rapports » page 258
- « Affichage des définitions d'un schéma, d'une classe et d'un attribut » page 260

- « Recherche d'objets » page 261
- « Utilisation de la visionneuse de flux » page 261
- « Cloner l'ensemble DIB » page 262

Affichage de l'état de santé des serveurs eDirectory

La page Résumé de l'agent permet d'afficher des informations sur l'état de santé des serveurs eDirectory, notamment sur la synchronisation, l'état des processus de l'agent et le nombre total de serveurs reconnus par votre base de données.

1. Dans iMonitor, cliquez sur **Résumé de l'agent**  .
2. Choisissez parmi les options suivantes :

   Résumé de synchronisation de l'agent : permet d'afficher le type et le nombre de répliques que vous possédez, ainsi que le temps écoulé depuis leur dernière synchronisation. Vous pouvez également afficher le nombre d'erreurs pour chaque type de réplique. S'il n'y a qu'une réplique ou partition à afficher, le titre est le suivant : **État de synchronisation des partitions**.

   Si le résumé de synchronisation de l'agent n'apparaît pas, votre identité ne vous permet d'afficher aucune réplique.

   Ensemble des serveurs connus par la base de données permet d'afficher le type et le nombre de serveurs que la base de données reconnaît, qu'ils soient actifs ou non.

   L'option **Ensemble des états de processus de l'agent** affiche l'état des processus exécutés sur un agent sans intervention de l'administrateur. En cas de problème ou d'ajout d'informations, un état est enregistré. La table augmente ou diminue en fonction du nombre d'états enregistrés.

Affichage de l'état de synchronisation des partitions

La page Synchronisation de l'agent vous permet d'afficher l'état de synchronisation de vos partitions. Vous pouvez filtrer ces informations à l'aide des options répertoriées dans le cadre de l'Assistant dans la partie gauche de la page.

1. Dans iMonitor, cliquez sur **Synchronisation de l'agent** dans le cadre de l'assistant.
2. Choisissez parmi les options suivantes :

   État de la synchronisation des partitions permet d'afficher la partition, le nombre d'erreurs, la dernière synchronisation réussie et le delta d'anneau maximal.

   Partition affiche les liens vers la page de synchronisation des répliques de chaque partition.

   Dernière synchronisation réussie permet d'afficher le temps écoulé depuis la dernière synchronisation de toutes les répliques d'une partition à partir du serveur.

   Delta d'anneau maximal indique la quantité de données susceptibles de ne pas être synchronisées correctement par rapport à toutes les répliques de l'anneau. Par exemple, si un utilisateur a modifié son script de connexion au cours des 30 dernières minutes et que le delta d'anneau maximal est de 45 minutes, la synchronisation de son script de connexion risque d'échouer, et il est fort probable qu'il récupère l'ancien script de connexion lorsqu'il tentera de se connecter. Si toutefois l'utilisateur a modifié son script plus de 45 minutes auparavant, il devrait obtenir le nouveau script de connexion sur toutes les répliques.

   Si la valeur **Inconnu** apparaît dans la liste **Delta d'anneau maximal**, le vecteur de transition synchronisé est incohérent et le delta d'anneau maximal ne peut pas être calculé en raison d'opérations de réplique/partition en cours ou d'autres problèmes.

Affichage de l'état des processus de la notice nécrologique et le nombre de caches de changement

Pour afficher l'état des processus de la notice nécrologique et le nombre de caches de changement d'une partition donnée, accédez à l'objet racine de cette partition. Les données sont affichées pour les trois différents types de notices nécrologiques :

- OBIT_DEAD : créé lorsqu'un objet est supprimé.
- OBIT_NEWRDN : créé lorsqu'un objet est renommé.
- OBIT_MOVED : créé lorsqu'un objet est déplacé d'un emplacement vers un autre.

Lorsque les objets sont traités, ils peuvent se trouver dans quatre états distincts. Ils passent d'un état ÉMIS à un état PURGEABLE, avant d'être finalement purgés. Voici les quatre états distincts :

- ÉMIS
- NOTIFIÉ
- OK_TO_PURGE
- PURGEABLE

Il existe 12 combinaisons différentes pour un objet donné. Voici les différentes combinaisons :

- OBIT_DEAD_ISSUED
- OBIT_DEAD_NOTIFIED
- OBIT_DEAD_OK_TO_PURGE
- OBIT_DEAD_PURGEABLE
- OBIT_NEWRDN_ISSUED
- OBIT_NEWRDN_NOTIFIED
- OBIT_NEWRDN_OK_TO_PURGE
- OBIT_NEWRDN_PURGEABLE
- OBIT_MOVED_ISSUED
- OBIT_MOVED_NOTIFIED
- OBIT_MOVED_OK_TO_PURGE
- OBIT_MOVED_PURGEABLE

Un nombre s'affiche en face de chacune de ces combinaisons et indique le nombre total d'objets qui se trouvent dans un état particulier à la fin du dernier cycle de traitement de la notice nécrologique.

L'option Change cache count affiche le nombre d'objets présents dans le cache de changement de la partition sur le serveur actuel. Les chiffres suivants montrent le nombre de notices nécrologiques et le nombre de caches de changement pour un objet Racine de partition particulier de cette partition.

Figure 8-3 Informations sur le nombre de caches de changement et de notices nécrologiques

Obit and Change Cache Count Information	
OBIT_DEAD_ISSUED	8318
OBIT_DEAD_NOTIFIED	0
OBIT_DEAD_OK_TO_PURGE	1682
OBIT_DEAD_PURGEABLE	0
OBIT_NEWRDN_ISSUED	0
OBIT_NEWRDN_NOTIFIED	0
OBIT_NEWRDN_OK_TO_PURGE	0
OBIT_NEWRDN_PURGEABLE	0
OBIT_MOVED_ISSUED	0
OBIT_MOVED_NOTIFIED	0
OBIT_MOVED_OK_TO_PURGE	0
OBIT_MOVED_PURGEABLE	0
Obit Count from database index	10000
Change Cache Count	10002

Affichage des informations de connexion au serveur

La page Informations sur les agents vous permet d'afficher les informations de connexion relatives à votre serveur.

1. Dans iMonitor, cliquez sur **Informations sur l'agent** dans le cadre de l'assistant.
2. Choisissez parmi les options suivantes :

   Infos sur le ping indique que iMonitor a essayé un ping IP pour l'ensemble des adresses annoncées pour le serveur. Lorsque l'opération réussit, vous en êtes informé de la manière indiquée.

   Nom DNS indique que iMonitor a tenté d'inverser les adresses IP gérées par le serveur et précise le nom DNS associé.

   En fonction du transport, de la configuration et de la plate-forme que vous utilisez, cette information peut ne pas apparaître.

   L'option Infos sur la connexion permet d'afficher les informations de connexion relatives au serveur, notamment les adresses de renvoi du serveur, le delta horaire, la réplique maîtresse la plus proche de la racine et la profondeur de la réplique.

   En fonction du transport, de la configuration et de la plate-forme que vous utilisez, cette information peut ne pas apparaître.

   L'option Adresses de renvoi du serveur permet d'afficher l'ensemble des adresses utilisables pour atteindre votre serveur.

   L'option Heure synchronisée indique que le temps synthétique ou ultérieur n'est utilisé que si le dernier tampon horaire émis par une réplique est ultérieur à l'heure actuelle.

   eDirectory considère que l'heure est suffisamment bien synchronisée pour émettre des tampons horaires en fonction de l'heure actuelle du serveur. Le protocole de synchronisation horaire peut ou non être dans l'état synchronisé.

Delta horaire précise la différence horaire (en secondes) entre iMonitor et le serveur à distance. Un entier négatif indique que l'heure d'iMonitor avance par rapport à celle du serveur tandis qu'un entier positif indique plutôt un retard.

l'option Maîtresse la plus proche de la racine indique que la réplique la plus élevée ou la plus proche de la racine de l'arborescence de dénomination est une réplique maîtresse.

Profondeur de la réplique permet d'afficher la profondeur de la réplique la plus proche de la racine (c'est-à-dire le nombre de niveaux qui séparent la réplique la plus proche de la racine et la racine de l'arborescence).

Affichage des serveurs connus

La liste **Serveurs connus** indique les serveurs connus par la base de données du serveur source. Vous pouvez appliquer un filtre à la liste pour afficher tous les serveurs connus de la base de données ou tous les serveurs de l'anneau de réplique. Si une icône apparaît à côté d'un serveur, celui-ci fait partie d'un anneau de répliques.

1. Dans iMonitor, cliquez sur **Serveurs connus** dans le cadre de l'assistant.
2. Choisissez parmi les options suivantes :

   ID de l'entrée liste l'identificateur d'un objet sur le serveur local. Les ID d'entrée ne peuvent pas être utilisés sur plusieurs serveurs.

   Révision NDS indique le numéro de révision ou de version d'eDirectory mise en cache ou stockée sur le serveur avec lequel vous communiquez.

   État indique si le serveur est inconnu, actif ou inactif. L'état Inconnu signifie que le serveur n'a jamais eu besoin de communiquer avec le serveur signalé comme étant inconnu.

   Dernière mise à jour indique la dernière fois où ce serveur a tenté de communiquer avec le serveur et a détecté qu'il était inactif. Si cette colonne n'apparaît pas, tous les serveurs sont en service.

Affichage des informations relatives aux répliques

La page Partitions vous permet d'afficher des informations concernant les répliques du serveur avec lequel vous communiquez. Vous pouvez appliquer un filtre à cette page à l'aide des options du cadre de l'Assistant dans la partie gauche de la page.

L'option **Informations sur la partition** du serveur permet notamment d'afficher l'ID d'entrée, l'état de la réplique, l'heure de la purge et celle de la dernière modification de la partition du serveur.

Partition permet d'afficher des informations relatives à l'objet Arborescence de la partition sur le serveur.

Heure de la purge indique l'heure à laquelle vous pouvez retirer les données supprimées précédemment de la base de données car ces suppressions ont déjà été répercutées sur toutes les répliques.

Date/heure de la dernière modification permet d'afficher le dernier tampon horaire émis des données écrites dans la base de données pour la réplique. Vous pouvez ainsi savoir si l'horloge avance et si l'heure synthétique est utilisée.

Synchronisation des répliques permet d'afficher la page de résumé de synchronisation de réplique qui se rapporte à cette partition. La page Synchronisation de réplique contient des informations sur l'état de synchronisation de la partition et l'état de la réplique. Vous pouvez également afficher les listes des partitions et des répliques.

Contrôle et configuration de l'agent DS

La page Configuration de l'agent permet de contrôler et de configurer l'agent DS. Les fonctions accessibles sur cette page dépendent des droits de l'identité actuelle et de la version d'eDirectory utilisée.

1. Dans iMonitor, cliquez sur **Configuration de l'agent** .
2. Choisissez parmi les options suivantes :
   - **L'option** Informations sur les agents permet d'afficher les informations de connexion relatives à votre serveur.
   - **L'option** Partitions permet d'afficher les répliques du serveur avec lequel vous communiquez.
   - **Filtres de réplication** permet d'afficher les filtres de réplication configurés pour l'agent eDirectory spécifié. NDS eDirectory 8.5 (version de build 85.*xx*) était la première version d'eDirectory à implémenter une fonction dite de répliques filtrées. Pour plus d'informations sur la définition, l'utilisation et la configuration des répliques filtrées, reportez-vous à la section « Répliques filtrées » page 65.
   - **Déclencheurs d'agent** permet de lancer des processus d'arrière-plan. Ces déclencheurs ont la même fonction que la commande `SET DSTRACE=*option`.
   - **Paramètres des processus en arrière-plan** permet de modifier l'intervalle de lancement de certains processus à l'arrière-plan. Ces paramètres ont la même fonction que la commande `SET DSTRACE=!option`.
   - **Synchronisation de l'agent** permet de désactiver ou d'activer la synchronisation entrante ou sortante. Vous pouvez indiquer, en heures, le délai pendant lequel la synchronisation doit être désactivée.
   - **Cache de base de données** permet de configurer la quantité de mémoire cache de base de données utilisée par le moteur de base de données DS. Diverses statistiques de cache sont également disponibles pour vous aider à déterminer si la quantité de mémoire cache disponible est suffisante. Les performances du système peuvent être significativement ralenties si la quantité de mémoire cache disponible est insuffisante.
   - **Paramètres de connexion** vous permet d'indiquer si eDirectory met à jour les attributs de connexion lorsque les utilisateurs se connectent. Les options suivantes contrôlent le mode de réponse d'eDirectory lorsqu'un utilisateur se connecte :
     - **Délai de mise à jour de la connexion** indique la durée (en secondes) entre les mises à jour. Par exemple, si un ou plusieurs utilisateurs se connectent pendant le délai, eDirectory ajoute toutes les modifications à une file d'attente. À la fin du délai, eDirectory applique toutes les modifications mises en file d'attente.
     - **Intervalle de mise à jour de la connexion** indique l'intervalle (en secondes) au cours duquel les attributs de connexion d'un utilisateur spécifique ne seront pas mis à jour. L'intervalle type est de 3 600 secondes (1 heure). Par exemple, lorsqu'un utilisateur se connecte pour la première fois à 8h00, eDirectory met les attributs à jour et l'intervalle démarre. Si l'utilisateur se reconnecte avant 9h00, eDirectory n'effectue aucune mise à jour des attributs. La valeur par défaut est 0, ce qui signifie qu'aucun intervalle de désactivation n'est défini.

Configuration des paramètres Trace

Pour accéder aux informations de la page Configuration de Trace, vous devez être assimilé à l'administrateur sur le serveur ou à un opérateur sur la console. Pour que vous puissiez accéder aux informations sur cette page, le système vous invite à entrer votre nom d'utilisateur et votre mot de passe afin de vérifier vos références.

Vous pouvez configurer les paramètres de trace dans la page Configuration de Trace. DSTrace de NetIQ iMonitor est une fonction centrée sur le serveur. Cela signifie qu'elle ne peut être lancée que sur un serveur qui exécute iMonitor. Si vous tentez d'accéder à cette fonction sur un autre serveur, vous devez basculer sur l'application iMonitor exécutée sur ce serveur.

1. Dans iMonitor, cliquez sur **Configuration de Trace** .
2. Choisissez parmi les options suivantes :
   - **Mettre à jour** permet de soumettre des modifications aux options de Trace et aux préfixes de la ligne Trace. Si DSTrace est désactivé, cliquez sur **Activer Trace** pour le mettre en fonction. Si DSTrace est déjà activé, cliquez sur **Mettre à jour** pour soumettre les modifications apportées à la trace actuelle.
   - **Trace activée/Trace désactivée** active ou désactive DSTrace. Le texte du bouton change en fonction de l'état de DSTrace. **Si DSTrace est activé, le texte du bouton s'intitule Désactiver Trace**. Cliquez sur ce bouton pour activer ou désactiver DSTrace. Lorsque DSTrace est désactivé, l'option **Activer Trace** a la même fonction que l'option **Mettre à jour**.
   - **L'option** Préfixes de la ligne Trace permet de choisir les éléments de données à ajouter au début des lignes Trace.
   - **L'option intitulée** Options de Trace DS s'applique aux événements de l'agent DS local où l'opération Trace est lancée. Ces options affichent les erreurs, les problèmes éventuels et d'autres informations relatives à eDirectory sur votre serveur local. L'activation des options de DSTrace peut augmenter l'utilisation de l'UC et réduire les performances du système. Par conséquent, vous devez utiliser DSTrace pour effectuer des diagnostics, et non de manière courante. Ces options sont équivalentes à la commande `SET DSTRACE=+`*`option`*, mais en plus pratique.
   - **Configuration d'événement** répertorie les options d'événement eDirectory et NMAS à activer ou désactiver pour la surveillance dans DSTrace. Le système d'événements génère des événements pour les activités locales telles que l'ajout et la suppression d'objets, ou la modification de valeurs d'attributs. Pour chaque type d'événement, une structure contenant les informations qui lui sont propres est renvoyée.
   - **Historique de Trace** permet d'afficher la liste des précédentes exécutions de Trace. Les journaux de suivi antérieurs sont identifiés par la période de temps sur laquelle les données de suivi ont été collectées.
   - **Déclencheurs de Trace** permet d'afficher les drapeaux Trace qui doivent être définis pour pouvoir afficher les informations souhaitées sur l'agent DS dans DSTrace. Ces déclencheurs peuvent écrire de très grandes quantités d'informations sur Trace. En règle générale, nous vous recommandons d'activer ces déclencheurs à la demande du support NetIQ uniquement.
3. Cliquez sur **Activer Trace** pour activer DSTrace et soumettre d'éventuelles modifications.
4. Cliquez sur ou sur **Trace Live** pour faire apparaître DS Trace dans iMonitor.

Affichage des informations relatives à l'état des processus

La page État du processus de l'agent permet d'afficher les erreurs d'état des processus en arrière-plan, ainsi que des informations complémentaires sur chaque erreur survenue. Certaines options proposées dans le cadre de l'Assistant à gauche de cette page permettent de filtrer les informations de cette page.

Dans iMonitor, cliquez sur **État des processus de l'agent** dans le cadre de l'assistant. Les états des processus en arrière-plan actuellement signalés sont les suivants :

- Synchronisation des schémas
- Traitement des notices nécrologiques
- Référence externe/DRL
- Limber
- Réparer

Affichage de l'activité de l'agent

La page Activité de l'agent permet de déterminer des modèles de trafic et les éventuels goulots d'étranglement système. Cette page permet d'afficher les requêtes et les verbes actuellement gérés par eDirectory. Vous pouvez également connaître les requêtes qui tentent d'obtenir des verrous DIB afin d'écrire dans la base de données et leur nombre.

Si vous affichez un serveur qui exécute NetIQ eDirectory 8.6 ou version ultérieure, vous verrez également la liste des partitions et des serveurs de l'anneau de répliques, le serveur étant spécifié dans le cadre du navigateur. Depuis l'introduction de NetIQ eDirectory 8.6, la synchronisation n'utilise plus un seul thread. Tout serveur utilisant eDirectory 8.6 ou version ultérieure est susceptible de transmettre plusieurs partitions simultanément à un ou plusieurs partenaires de réplication. La page Activité de synchronisation a par conséquent été créée pour vous permettre de surveiller plus facilement cette stratégie de synchronisation parallèle.

1. Dans iMonitor, cliquez sur **Activité de l'agent** dans le cadre de l'assistant.
2. Choisissez parmi les options suivantes :
   - **Activité et statistiques du verbe** permet de connaître le nombre total de verbes appelés et de requêtes effectuées depuis la dernière initialisation d'eDirectory. Ces pages indiquent en outre le nombre de requêtes actuellement actives ainsi que la durée minimale, maximale et moyenne (en millisecondes) de traitement de ces requêtes.
   - **Synchronisation en cours et planifiée** liste les heures des différentes synchronisations entrantes et sortantes. Si une synchronisation entrante ou sortante est en cours, une icône indiquant que le processus est actif apparaît. Des informations sur l'heure de début de la synchronisation ainsi que sur le serveur concerné sont également affichées.

     Si les synchronisations entrantes et sortantes sont désactivées, une icône vous en informe ; elle vous indique également l'heure prévue pour leur réactivation. Pour les synchronisations sortantes, l'heure de la prochaine synchronisation planifiée est également indiquée.
   - **Événements** affiche une liste des événements actifs, ainsi que des statistiques sur les gestionnaires d'événements, un résumé des statistiques d'événements et les fonctions actuelles des droits d'événements qui ont été appelées.
   - **Planification des processus à l'arrière-plan** permet d'afficher les processus d'arrière-plan planifiés ainsi que leur état actuel et l'heure planifiée de leur prochaine exécution.

Affichage des modèles de trafic

La page Statistiques du verbe permet de déterminer des modèles de trafic et les éventuels goulots d'étranglement système. Cette page permet d'afficher un décompte de tous les verbes appelés et de toutes les requêtes effectuées depuis le dernier lancement d'eDirectory. Elle indique également le nombre de requêtes actuellement actives ainsi que les durées minimale, maximale et moyenne (en millisecondes) de leur traitement. Le suivi concerne tous les processus en arrière-plan et toutes les requêtes de Bindery et les requêtes eDirectory standard.

Si vous affichez cette page à l'aide d'une ancienne version d'eDirectory, toutes les informations qui apparaissent dans eDirectory version 8.5 ou ultérieure risquent de ne pas être disponibles.

Affichage des processus arrière-plan

La page Planification des processus à l'arrière-plan permet d'afficher les processus en arrière-plan planifiés, ainsi que leur état actuel et l'heure prévue pour leur prochaine exécution. La fonction de planification des processus en arrière-plan de NetIQ iMonitor est une fonction centrée sur le serveur. Cela signifie qu'elle ne peut être affichée que sur un serveur qui exécute iMonitor. Si vous tentez d'accéder à la planification des processus à l'arrière-plan sur un autre serveur, vous devez basculer vers l'application iMonitor exécutée sur ce serveur. Au fur et à mesure que vous mettez à niveau des serveurs vers eDirectory 8.5 ou version ultérieure, vous augmentez le nombre de fonctions centrées sur le serveur d'iMonitor disponibles. Les pages DSTrace et DSRepair comprennent d'autres fonctions centrées sur le serveur.

Pour accéder aux informations de la page Planification des processus à l'arrière-plan, vous devez être assimilé à l'administrateur sur le serveur ou à un opérateur sur la console. Pour que vous puissiez accéder aux informations de cette page, le système vous invite à vous connecter afin de vérifier vos références.

Configuration des processus en arrière-plan

Pour réduire la durée d'exécution des cycles de processus en arrière-plan, les administrateurs peuvent configurer une des stratégies suivantes pour les paramètres de délai des processus en arrière-plan dans la fenêtre Paramètres des processus en arrière-plan dans iMonitor :

- UC
- Limite stricte
- Délai de l'outil de purge

Pour configurer le processus en arrière-plan :

1. Connectez-vous à iMonitor.
2. Accédez à **Configuration de l'agent** > **Paramètres des processus en arrière-plan**.
3. Faites défiler jusqu'à la section **Paramètres du délai des processus en arrière-plan** et définissez l'intervalle de délai sur n'importe quelle valeur comprise entre 0 et 100 millisecondes ;

   Par défaut, la stratégie **Limite stricte** est activée avec les trois processus mis en veille pour 100 millisecondes.

   ou

   Sélectionnez la stratégie **UC** et configurez-la en fonction de vos besoins.

   Le pourcentage d'`utilisation maximum de l'UC` est par défaut 80 % et la `limite maximum de délai` est définie sur 100 millisecondes.

4 Entrez l'intervalle souhaité dans le champ **Intervalle de l'outil de purge**.

   Par défaut, cette propriété est définie sur 30 minutes. Vous pouvez modifier cet intervalle selon vos besoins.

Affichage des erreurs relatives aux serveurs eDirectory

La page Index des erreurs permet d'afficher des informations concernant les erreurs détectées sur les serveurs eDirectory. Les erreurs sont classées en deux catégories : erreurs propres à eDirectory et autres erreurs pouvant être à vérifier. Chaque erreur répertoriée est dotée d'un hyperlien qui mène à sa description : vous avez alors accès à une explication, à la cause possible de l'erreur et à des actions de dépannage.

1 Dans iMonitor, cliquez sur **Index des erreurs** dans le cadre de l'assistant.

   La page Index des erreurs permet d'accéder à la documentation NetIQ la plus récente, qui traite des erreurs et présente des informations techniques ainsi que des livres blancs.

Affichage des informations DSRepair

La page DSRepair permet d'afficher les problèmes et de sauvegarder ou de nettoyer les ensembles DIB. La fonction DSRepair de NetIQ iMonitor est centrée sur le serveur. Cela signifie qu'elle ne peut être lancée que sur un serveur qui exécute iMonitor. Si vous devez accéder aux informations DSRepair sur un autre serveur, il vous faut basculer vers l'application iMonitor exécutée sur ce serveur. Au fur et à mesure que vous mettez à niveau des serveurs vers des versions plus récentes d'eDirectory, le nombre de fonctions centrées sur le serveur d'iMonitor disponibles augmente. Les pages DSTrace et Planification des processus à l'arrière-plan comprennent d'autres fonctions centrées sur le serveur.

Pour accéder aux informations de cette page, vous devez être assimilé à l'administrateur sur le serveur ou à un opérateur sur la console. Pour que vous puissiez accéder aux informations de cette page, le système vous invite à vous connecter afin de vérifier vos références.

1 Dans iMonitor, cliquez sur **DSRepair**  .

2 Choisissez parmi les options suivantes :

   - **Téléchargements** permet de récupérer des fichiers liés aux réparations sur le serveur de fichiers. Si l'utilitaire DSRepair est en cours d'exécution ou si vous avez lancé une réparation à partir de la page DSRepair d'iMonitor, vous ne pouvez pas accéder au fichier `dsrepair.log` tant que l'opération n'est pas terminée.
   - L'option **Supprimer les anciens ensembles DIB** permet de supprimer un ancien ensemble DIB en cliquant sur la croix rouge **X**.

     AVERTISSEMENT : Cette action est irréversible. Lorsque vous sélectionnez cette option, l'ancien ensemble de DIB est purgé du système de fichiers.

   - **Paramètres avancés de réparation NDS** permet de rechercher les problèmes, de les résoudre ou de créer une sauvegarde de la base de données. Vous pouvez laisser le champ **Options de support** vide à moins que le support technique de NetIQ vous ait demandé de le compléter.

3 Cliquez sur **Lancer la réparation** pour exécuter DS Repair sur ce serveur.

Affichage d'informations sur l'état de santé de l'agent

La page État de santé de l'agent permet d'afficher des informations sur l'état de santé de l'agent eDirectory spécifié, ainsi que sur les partitions et les anneaux de répliques auxquels il participe.

1. Dans iMonitor, cliquez sur **État de santé de l'agent** dans le cadre de l'assistant.
2. Cliquez sur les liens pour afficher des informations détaillées.

Exploration d'objets dans l'arborescence

La page Parcourir vous permet d'accéder à des objets de votre arborescence. La barre de navigation située dans la partie supérieure de la page vous permet de savoir à quel serveur appartient l'objet que vous visualisez et d'afficher le chemin d'accès à cet objet. Le cadre Réplique situé dans la partie gauche de la page permet d'afficher un objet ou d'y accéder sur n'importe quelle partition réelle. Cliquez sur un objet souligné dans la page afin d'afficher plus d'informations à son sujet. Vous pouvez également cliquer sur n'importe quelle portion du nom dans le cadre du navigateur afin de parcourir l'arborescence en amont.

Les informations affichées sur cette page dépendent des droits eDirectory avec lesquels vous vous êtes connecté, du type d'objet que vous parcourez, ainsi que de la version NDS ou eDirectory utilisée. Cette page affiche des objets XRef si vous êtes connecté avec des droits Superviseur. La liste des répliques permet d'atteindre une copie réelle de la réplique. Si vous recherchez des objets dans des groupes dynamiques, le tampon horaire n'est pas affiché pour les membres dynamiques.

Synchronisation des répliques affiche l'état de synchronisation de la réplique qui contient cet objet.

Synchronisation des entrées affiche les attributs qui, selon ce serveur, doivent être synchronisés.

Infos sur la connexion permet de savoir où iMonitor a obtenu les informations sur cet objet.

Informations sur les entrées affiche les informations relatives aux noms, aux drapeaux, à la classe de base, au tampon horaire de modification et au résumé des données de connexion de l'objet.

Envoyer l'entrée à toutes les répliques permet de renvoyer les attributs de cette entrée à toutes les autres répliques. ²Ce processus peut s'avérer très long si l'objet possède de nombreuses valeurs d'attribut. Il n'a pas pour effet de rendre toutes les copies de l'objet identiques. Il permet simplement aux autres répliques de reconsidérer chaque attribut.

Tout envoyer (visible uniquement si l'objet parcouru est une racine de partition et si l'option Mode avancé est activée) renvoie toutes les entrées de cette partition à l'ensemble des serveurs qui possèdent des répliques de la partition. Ce processus n'a pas pour effet de rendre toutes les copies de l'objet identiques. Il permet simplement aux autres répliques de reconsidérer chaque objet et ses attributs.

Affichage des entrées à synchroniser ou à purger

La page Cache de changement permet d'afficher une liste d'entrées que ce serveur doit prendre en considération lors des opérations de synchronisation ou de purge. Cette option n'est disponible que si le serveur auquel vous accédez exécute eDirectory 8.6 ou version ultérieure et que l'objet affiché est une racine de partition. Vous devez disposer de droits Superviseur sur le serveur eDirectory pour afficher cette page.

Synchronisation des entrées permet de déterminer les raisons pour lesquelles une entrée doit être synchronisée.

REMARQUE : iMonitor ne dresse la liste que d'un nombre limité d'objets sur la page Cache de changement. Si vous souhaitez afficher tous les objets du cache de changement, pour une partition spécifique ou pour toutes les partitions d'un serveur, vous pouvez exécuter un rapport du vidage des changements du cache à la page Rapports. Reportez-vous à la section « Configuration et affichage de rapports » page 258 pour plus d'informations sur la configuration et l'exécution de rapports dans iMonitor.

Affichage des détails de NetIQ Identity Manager

La page DirXML - Résumé permet d'afficher la liste des pilotes DirXML exécutés sur votre serveur, l'état et les détails de chacun d'entre eux, ainsi que les associations en attente.

1. Dans iMonitor, cliquez sur **DirXML - Résumé** .
2. Choisissez parmi les options suivantes :

   État affiche l'état actuel du pilote spécifié. Les états possibles sont : Arrêté, Démarrage, En cours d'exécution, Arrêt en attente et Obtention du schéma.

   Option de démarrage affiche l'option de démarrage actuelle spécifiée pour le pilote sélectionné.

   En attente affiche le nombre d'associations qui n'ont pas encore été réalisées.

   L'icône Détail du pilote affiche des détails relatifs à l'abonné et à l'éditeur, les règles XML, les filtres ainsi que les listes d'associations en attente pour les pilotes DirXML qui s'exécutent sur votre serveur. Elle affiche également des informations détaillées sur les 50 premiers objets en attente. Les détails relatifs aux règles XML fournis sur cette page peuvent être utilisés pour définir le contenu des recherches dans les objets en attente afin de permettre que leur création se poursuive avec le pilote DirXML spécifié.

Affichage de l'état de synchronisation d'une réplique

La page Synchronisation des répliques permet d'afficher l'état de synchronisation d'une réplique.

1. Dans iMonitor, cliquez sur **Synchronisation de l'agent** dans le cadre de l'Assistant.
2. Cliquez sur **Synchronisation de réplique** pour la partition à afficher.
3. Utilisez les liens figurant sur cette page et sur la barre de navigation située à gauche pour accéder à d'autres partitions et vous déplacer dans l'anneau de répliques.

Configuration et affichage de rapports

La page Rapports permet d'afficher et de supprimer les rapports exécutés directement sur ce serveur. L'exécution de certains rapports peut être longue et exiger une grande quantité de ressources système.

Les rapports planifiés s'exécutent à l'aide de l'identité [Public], sans nécessiter d'authentification de l'utilisateur. Tous les rapports que vous exécutez portent votre identité. Toutes les données de rapport sont stockées sur le serveur à partir duquel vous exécutez le rapport. iMonitor stocke par défaut les données de rapport dans les répertoires suivants, en fonction du système d'exploitation :

Plate-forme	Répertoire
Windows	`C:\Novell\NDS\ndsimon\dsreports\`
Linux	`/var/opt/novell/eDirectory/data/dsreports`

La page Configuration du rapport permet d'afficher la liste des rapports préconfigurés, personnalisés et planifiés. Elle permet également de modifier, d'exécuter des rapports et peut servir à créer des rapports personnalisés pour des pages iMonitor. Le tableau suivant présente les rapports préconfigurés inclus dans iMonitor.

Rapport	Description
Informations sur le serveur	Parcourt l'intégralité de l'arborescence, communique avec tous les serveurs NCP détectés et signale les erreurs trouvées. Utilisez ce rapport pour diagnostiquer les problèmes liés à la synchronisation horaire et au contrôle de connectivité (limber) ou pour savoir si le serveur actuel peut communiquer avec tous les autres serveurs. S'il a été sélectionné dans la page de configuration, ce serveur peut également générer des informations sur l'état de santé de l'agent NDS pour chaque serveur de l'arborescence.
Liste des notices nécrologiques	Liste les notices nécrologiques de ce serveur.
Statistiques d'objet	Évalue les objets sous un angle particulier, puis génère les listes d'objets répondant aux critères demandés. Ces critères peuvent être l'heure future, les objets inconnus, les objets renommés, le nombre de classes de base, les conteneurs, les alias ou les références externes.
Vidage du cache de changement	Répertorie tous les objets contenus dans le cache de changement pour la partition sélectionnée ou pour toutes les partitions sur le serveur. Ce rapport génère également un vidage XML des objets dans le cache de changement, ainsi qu'une liste des attributs et des valeurs à synchroniser entre les serveurs. Le rapport fournit des informations permettant d'analyser tous les objets du cache de changement. **REMARQUE :** iMonitor stocke les vidages des changements du cache dans le même répertoire que le rapport du vidage des changements du cache, tel qu'il apparaît dans le tableau ci-dessus.
Annonce du service	Liste les annuaires et les serveurs connus du serveur actuel via SLP ou SAP.
État de santé de l'agent	Recueille des informations sur l'état de santé du serveur actuel.
Nombre de valeurs	Liste les objets avec des attributs dont le nombre de valeurs est supérieur à une valeur spécifiée par vos soins.

Affichage et suppression de rapports

1. Dans iMonitor, cliquez sur **Rapports** .
2. Cliquez sur pour supprimer un rapport et sur pour le visualiser.

Exécution d'un rapport

1. Dans iMonitor, cliquez sur **Rapports** > **Configuration du rapport**.
2. Cliquez sur pour exécuter le rapport.

Configuration ou planification d'un rapport

1. Dans iMonitor, cliquez sur **Rapports** > **Configuration du rapport**.
2. Cliquez sur pour configurer et planifier un rapport.

3 Choisissez les options souhaitées, puis cliquez sur **Enregistrer les valeurs par défaut** pour enregistrer les options sélectionnées.

4 (Facultatif) Configurez le rapport pour une exécution périodique ou ultérieure.

   4a Indiquez une fréquence, ainsi qu'un jour et une heure de début.

   4b Cliquez sur **Planifier**.

5 Cliquez sur **Exécuter le rapport** pour démarrer le rapport.

Création d'un rapport personnalisé

Les rapports personnalisés vous permettent de lancer n'importe quelle page iMonitor en tant que rapport.

1 Dans iMonitor, cliquez sur **Rapports** > **Configuration du rapport**.

2 Dans la **liste des rapports pouvant être exécutés**, cliquez sur **Rapports personnalisés**.

3 Nommez le rapport, puis entrez l'URL de la page iMonitor que vous souhaitez lancer sous forme de rapport.

   Lors de l'exécution d'un rapport personnalisé, entrez l'URL de la manière suivante :

   `/nds/page requise`

4 Dans le champ **Rapports enregistrés**, indiquez le nombre de versions du rapport que vous souhaitez conserver.

5 (Facultatif) Cliquez sur **Enregistrer** pour sauvegarder le rapport.

6 (Facultatif) Configurez le rapport pour une exécution périodique ou ultérieure.

   6a Indiquez une fréquence, ainsi qu'un jour et une heure de début.

   6b Cliquez sur **Planifier**.

7 Cliquez sur **Exécuter le rapport** pour démarrer le rapport.

Affichage des définitions d'un schéma, d'une classe et d'un attribut

La page Schéma permet d'afficher les définitions relatives à un schéma, une classe ou un attribut. Vous pouvez visualiser le schéma chargé dans votre arborescence, ses éventuelles extensions, ainsi que les informations qui lui sont spécifiques, telles que les modifications ou extensions effectuées.

1 Dans iMonitor, cliquez sur **Schéma** dans le cadre de l'assistant.

2 Choisissez parmi les options suivantes :

   Liste des synchronisations liste les serveurs avec lesquels ce serveur sera synchronisé. Cette option n'est disponible que pour les serveurs qui exécutent NDS eDirectory 8.5 ou version ultérieure. Vous devez disposer de droits Superviseur sur le serveur pour afficher ces informations.

   Racine du schéma affiche des informations sur la réplique du schéma la plus proche de la racine de l'arborescence dans ce contexte.

   Chaque serveur eDirectory stocke une réplique du schéma dans sa totalité. Celle-ci est stockée séparément des partitions qui contiennent les objets Annuaire. Les modifications apportées à une réplique du schéma sont répercutées sur les autres répliques. Vous ne pouvez apporter des modifications au schéma que via un serveur qui stocke une réplique accessible en écriture de la partition racine. Les serveurs qui stockent des répliques de la partition racine en lecture seule peuvent lire les informations du schéma, mais pas les modifier.

Définitions des attributs établit, pour chaque attribut, une liste répertoriant son nom, sa syntaxe ainsi que ses contraintes de fonctionnement. Utilisez la fenêtre de navigation située à gauche pour rechercher des attributs et y accéder.

Définitions de classe répertorie le nom de chaque classe, ses règles et ses attributs. Utilisez la fenêtre de navigation située à gauche pour rechercher des attributs et y accéder.

Recherche d'objets

Utilisez la page de recherche pour rechercher des objets à l'aide de différents filtres et options d'interrogation. Les options et les filtres de recherche sont regroupés en deux niveaux de formulaires de recherche : basique et avancé. Les requêtes de recherche élémentaires sont destinées aux utilisateurs ordinaires d'eDirectory souhaitant effectuer des recherches simples. En revanche, les requêtes de recherche complexes s'adressent plus particulièrement aux utilisateurs expérimentés et s'utilisent pour des recherches élaborées. Actuellement, seules les recherches au niveau du serveur sont prises en charge.

Toutes les options de recherche et tous les filtres des quatre sections sont conjonctifs. Les champs vierges (à l'exception de Nom distinctif relatif) seront ignorés. Utilisez la touche Ctrl pour désélectionner un élément ou sélectionner plusieurs éléments dans des listes autorisant les sélections multiples. Les listes autorisant les sélections multiples désélectionnées seront également ignorées.

1. Dans NetIQ iMonitor, cliquez sur **Rechercher**  .
2. Choisissez parmi les options suivantes :
   - Les **Options d'étendue** permettent de spécifier l'étendue de la recherche.
   - Les **Filtres d'entrée** permettent d'indiquer les filtres de requête de recherche liés aux informations entrées.
   - Les **Filtres d'attribut et de valeur** permettent d'indiquer les filtres de requête de recherche liés aux attributs et aux valeurs.
   - Les **Options d'affichage** permettent de spécifier les options qui contrôlent le format d'affichage des résultats de la recherche.

     REMARQUE : les paramètres **Options d'affichage** ne sont disponibles que si vous cliquez sur **Avancé** pour afficher toutes les options de recherche avancée.
3. Cliquez sur le bouton **Aide** situé dans la partie inférieure du formulaire de recherche pour afficher des informations succinctes sur le formulaire, à l'intérieur même de ce dernier.

   Cliquez sur **Recharger** ou sur **Rafraîchir** pour effacer les informations d'aide.

Utilisation de la visionneuse de flux

La page Visionneuse de flux permet d'afficher le flux actuel dans l'un des formats suivants :

- Texte brut
- HTML
- GIF
- JPEG
- BMP
- WAV

- Hex Dump
- Autre

Si vous souhaitez systématiquement afficher certains attributs de flux dans un format donné, vous pouvez utiliser la visionneuse de flux pour définir les paramètres d'affichage par défaut.

Configuration de l'attribut de flux NDS modifie le format d'affichage par défaut des flux dans votre navigateur. L'affichage correct du flux dépend exclusivement de votre navigateur ; il est donc possible que les paramètres que vous avez choisis ne soient pas toujours appliqués.

Vous devez être authentifié auprès du serveur pour pouvoir valider les modifications que vous avez apportées aux paramètres par défaut. Vos modifications sont consignées dans le fichier `streams.ini` (pour les serveurs Windows) ou `streams.conf` (pour les serveurs Linux). Il est donc également possible de modifier manuellement les paramètres par défaut.

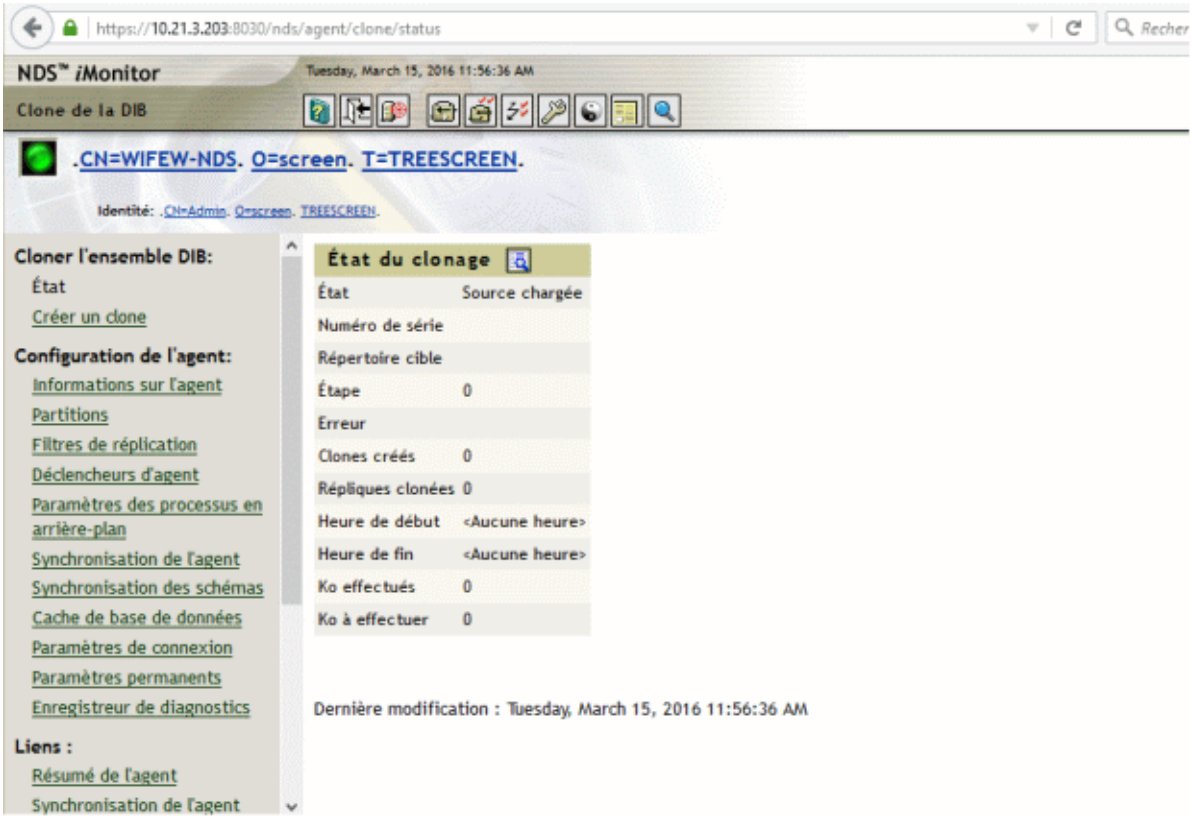
Cloner l'ensemble DIB

Cette option permet de dupliquer un ensemble complet de fichiers DIB d'une base de données eDirectory stockée sur un seul serveur (le serveur source). Le Clone de la DIB doit être extrait du serveur source qui contient toutes les répliques maîtresses dans l'arborescence. Ce clone peut ensuite être placé sur un autre serveur (le serveur cible). Lorsque le serveur cible lance eDirectory, il charge l'ensemble de fichiers DIB, accède à la réplique maîtresse de l'objet Serveur, résout son nom, puis synchronise les modifications éventuelles apportées à l'ensemble de fichiers DIB après la création du clone.

Vous devez placer le clone d'un ensemble DIB eDirectory sur un serveur qui exécute le même système d'exploitation que le serveur sur lequel le clone a été créé. Par exemple, si vous souhaitez restaurer un ensemble de fichiers DIB clonés sur un serveur Linux, créez le clone sur un serveur Linux, et non sur un serveur Windows.

Bien que l'interface dorsale de cette fonction ait été livrée avec eDirectory 8.7, elle n'est prise en charge que depuis eDirectory 8.7.1 avec iMonitor 2.4 ou une version ultérieure. Cette fonction ne s'applique pas aux versions de NetIQ eDirectory ou de NDS antérieures à 8.7.

Figure 8-4 *Page Cloner l'ensemble DIB dans iMonitor*



Cette section présente les informations suivantes :

- « Cas d'emploi de l'option Cloner l'ensemble DIB » page 263
- « Création d'un clone » page 264

Cas d'emploi de l'option Cloner l'ensemble DIB

L'option Cloner l'ensemble DIB est employée dans les cas suivants :

- Création d'un serveur avec des partitions dont l'état est déjà « actif »

  Les avantages sont les suivants :

  - Tous les serveurs de l'anneau de doivent pas être en cours d'exécution pour pouvoir leur ajouter un nouveau serveur dans l'anneau de répliques.
  - Tout nouveau serveur disposera automatiquement de toutes les partitions sans qu'aucune synchronisation ne soit nécessaire.
  - Le temps de fonctionnement est plus élevé.
- Récupération après sinistre

Avantages	Inconvénients
◆ Une seule copie de la partition est nécessaire à une exécution correcte. ◆ Temps d'arrêt réduit sur des serveurs de grande taille comprenant plusieurs partitions.	◆ Au moins une copie correcte des partitions en question est nécessaire. ◆ Ne traitera pas les sauvegardes SSL ou de sécurité. ◆ Le système de fichiers n'est pas pris en compte.

- Sauvegarde et restauration.

Avantages	Inconvénients
◆ Délai de récupération réduit notamment pour les bases de données volumineuses.	◆ Seuls les composants eDirectory de base sont ajoutés. Les composants LDAP, SNMP, SSL, etc. ne sont ni installés ni configurés. ◆ Les dernières modifications ne sont pas récupérées. Seul un instantané est réalisé. Aucun fichier de transaction individuelle n'est exécuté.

En raison des inconvénients cités ci-dessus, nous vous déconseillons d'utiliser l'option Cloner l'ensemble DIB pour des opérations de sauvegarde et de restauration.

Création d'un clone

Vous pouvez créer un ensemble de fichiers DIB cloné alors que le serveur d'origine est en ligne ou hors ligne. La méthode hors ligne nécessite la mise hors service d'eDirectory. Si vous utilisez le mode en ligne, eDirectory est actif et non verrouillé.

- « Méthode en ligne » page 264
- « Méthode hors ligne » page 266

AVERTISSEMENT : n'employez pas l'utilitaire de clonage de la DIB sur un serveur de gestion des identités pour cloner un autre serveur, car cela génère des fichiers inutiles de TAO sur le serveur cloné.

Méthode en ligne

1 Chargez le module ndsclone sur le serveur source.

Plate-forme	Pour étendre le schéma
Windows	À partir de `NDSCons.exe`, sélectionnez **dsclone.dll**, puis cliquez sur **Démarrer**.
Linux	Ajoutez une entrée `ndsclone` au fichier `ndsmodules.conf`, puis utilisez la page `http://adresse_IP:port/dhost` pour charger l'agent de clonage de l'annuaire. **REMARQUE :** le module `ndsclone` peut aussi être chargé à l'aide de la commande `ndstrace -c "load ndsclone"`.

2 Désactivez la synchronisation entrante à partir de la page de configuration de l'agent d'iMonitor avant de démarrer le processus de clonage de la DIB sur le serveur source.

3 Créez l'ensemble de fichiers DIB cloné.

   3a Lancez Cloner la configuration du DIB dans iMonitor.

   Cliquez sur **Configuration de l'agent** > **Cloner l'ensemble DIB** > **Créer un clone**.

   3b Indiquez le nom complet du serveur cible et le chemin des fichiers DIB clonés, puis cochez les cases **Créer un objet Clone** et **Cloner la DIB en ligne**.

   Le nom du serveur NCP (Objet Clone) du serveur cible doit correspondre au nom de serveur cible.

   3c Cliquez sur **Submit** (Soumettre).

   L'objet Clone NDS est créé et le jeu de fichiers DIB est copié vers la destination spécifiée.

4 Installez et configurez eDirectory sur le serveur cible et mettez le serveur hors service.

5 Copiez le répertoire DIB contenant l'ensemble de fichiers DIB clonés sur le serveur cible.

   Par ailleurs, sur un système Linux, copiez le fichier`/etc/opt/novell/eDirectory/conf/nds.conf` à partir du serveur source sur le serveur cible et mettez à jour les références suivantes sur le serveur cible :

   - Modifiez l'adresse IP pour les paramètres suivants :
     - n4u.server.interfaces
     - http.server.interfaces
     - https.server.interfaces
   - Indiquez le nom du serveur NCP créé à l'étape 3b dans le paramètre `n4u.NDS.nom-serveur`.
   - Indiquez le nom du serveur préféré dans le paramètre `n4u.NDS.serveur-préféré`. Généralement, le nom d'hôte du serveur cible est considéré comme le nom du serveur préféré.

6 Supprimez le fichier `nicisdi.key` des répertoires `/var/opt/novell/nici/0` et `/var/opt/novell/nici/0/backup` sur le serveur cible.

7 À présent, démarrez le serveur cible et exécutez la commande `ndsconfig upgrade`.

REMARQUE : sous Windows, vous devez exécuter la commande `EConfig.ps1` pour mettre à niveau le serveur eDirectory à l'aide du programme d'installation en mode silencieux. Lors de la mise à niveau, vous devez mentionner le nom de l'arborescence, le nom du serveur et les références de l'administrateur de la DIB clonée dans le fichier de réponse `upgrade.ni`. Vous devez également mentionner l'adresse IP du serveur existant contenant l'adresse IP des autres serveurs de l'arborescence. Pour plus d'informations, reportez-vous à la section Mise à niveau sans surveillance d'eDirectory sous Windows du *guide d'installation de NetIQ eDirectory*.

---

8 Assurez-vous que la réplique maîtresse de l'objet Serveur cible exécute eDirectory et qu'elle est disponible. Lors de son initialisation sur le serveur cible, eDirectory communique avec la réplique maîtresse sur laquelle le nom final du serveur cible est résolu.

9 Assurez-vous que la valeur de l'attribut de réplique du serveur cible est synchronisée sur tous les serveurs. Une fois que les modifications de l'attribut sont disponibles sur tous les serveurs, réactivez la synchronisation entrante sur le serveur source. La synchronisation entrante peut être activée sur la page de configuration de l'agent d'iMonitor ou via DSTrace.

10 Pour terminer la configuration d'eDirectory, reportez-vous à la section « Fin de la configuration d'eDirectory » page 267.

Méthode hors ligne

1 Créez l'ensemble de fichiers DIB cloné.

   1a Lancez Cloner la configuration du DIB dans iMonitor.

   Cliquez sur **Configuration de l'agent** > **Cloner l'ensemble DIB** > **Créer un clone**.

   1b Indiquez le nom complet du serveur cible, cochez la case **Créer un objet Clone** et désélectionnez la case **Cloner la DIB en ligne**.

   Le nom du serveur NCP du serveur cible doit correspondre au nom de serveur cible.

   1c Cliquez sur **Submit** (Soumettre).

   L'objet Clone NDS est créé, la DIB est verrouillée sur le serveur source et un message d'erreur indique qu'eDirectory est verrouillé.

2 Installez et configurez eDirectory sur le serveur cible et mettez le serveur hors service.

3 Copiez manuellement les fichiers `*.nds`, `nds*`, et `nds.rfl/*.*`à partir du répertoire DIB du serveur source vers un emplacement ou un support sur le serveur cible qui permet de déplacer l'ensemble vers le répertoire DIB du serveur cible. Par ailleurs, sur un système Linux, transférez le fichier `/etc/opt/novell/eDirectory/conf/nds.conf` sur le serveur cible et mettez à jour les références suivantes sur le serveur cible :

   - Modifiez l'adresse IP pour les paramètres suivants :
     - n4u.server.interfaces
     - http.server.interfaces
     - https.server.interfaces
   - Indiquez le nom du serveur NCP créé à l'étape 1b dans le paramètre `n4u.nds.nom-serveur`.
   - Indiquez le nom du serveur préféré dans le paramètre `n4u.NDS.serveur-préféré`. Généralement, le nom d'hôte du serveur cible est considéré comme le nom du serveur préféré.

4 Supprimez le fichier `nicisdi.key` des répertoires `/var/opt/novell/nici/0` et `/var/opt/novell/nici/0/backup` sur le serveur cible.

5 Exporter la variable d'environnement NDSD_DISABLE_INBOUND=Y, puis démarrez `ndsd` pour désactiver la synchronisation entrante sur le serveur source.

6 Redémarrez eDirectory sur le serveur source.

   Le clone n'est pas valide si vous redémarrez eDirectory sur le serveur source avant que les fichiers soient copiés. Vous devrez alors supprimer l'objet Serveur NCP et recréer le clone.

7 À présent, démarrez le serveur cible et exécutez la commande `ndsconfig upgrade`.

   REMARQUE : sous Windows, vous devez exécuter le fichier de configuration d'eDirectory. Vous devez également sélectionner l'arborescence eDirectory et vous y connecter pendant l'exécution du fichier de configuration pour mettre à niveau votre serveur eDirectory.

8 Assurez-vous que la valeur de l'attribut de réplique du serveur cible est synchronisée sur tous les serveurs. Une fois que les modifications de l'attribut sont disponibles sur tous les serveurs, réactivez la synchronisation entrante sur le serveur source. La synchronisation entrante peut être activée sur la page de configuration de l'agent d'iMonitor ou via DSTrace.

9 Installez eDirectory et démarrez le serveur sur le serveur cible, avec le répertoire DIB contenant l'ensemble de fichiers DIB clonés.

Assurez-vous que la réplique maîtresse du nouvel objet Serveur cible exécute eDirectory et qu'elle est disponible. Lors de son initialisation sur le serveur cible, eDirectory communique avec la réplique maîtresse sur laquelle le nom final du serveur cible est résolu.

10 Pour terminer la configuration d'eDirectory, reportez-vous à la section « Fin de la configuration d'eDirectory » page 267.

Fin de la configuration d'eDirectory

- SIDKEY à la page 237
- Configuration des services SAS, LDAP et SNMP à la page 237

SDIKEY

1 Mettez eDirectory hors service sur le serveur cible.

2 Déplacez ou renommez les fichiers `/var/opt/novell/nici/0/nicisdi.key` et `/var/opt/novell/nici/0/backup/nicisdi.key` sur le système de fichiers du serveur cible.

Plate-forme	Répertoire
Windows	`C:\Windows\SysWOW64\novell\nici\nicisdi.key`
Linux	`/var/opt/novell/nici/0/nicisdi.key`
	`/var/opt/novell/nici/0/backup/nicisdi.key`

3 Démarrez eDirectory sur le serveur cible.

Configuration des services SAS, LDAP, HTTP et SNMP

Linux : vous pouvez configurer les services SAS, LDAP, SNMP et HTTP en une seule opération en entrant la commande suivante sur la ligne de commande :

`ndsconfig upgrade [-a FDN_admin]`

Windows : exécutez le programme d'installation d'eDirectory et terminez la configuration des services SAS, LDAP, SNMP et HTTP.

Lorsque la configuration est terminée, HTTP écoute par défaut sur les ports 80 et 443. eDirectory stocke la configuration du port HTTP dans l'objet Serveur HTTP. Au besoin, vous pouvez modifier la configuration du port en tant qu'administrateur.

Pour procéder à une configuration individuelle des services, reportez-vous aux tableaux suivants :

SAS

Plate-forme	Commande ou outil
Windows	Créez un objet Service SAS et des certificats à l'aide d'iManager.

LDAP

Plate-forme	Commande ou outil
Windows	Créez des objets Groupe et Serveur LDAP à l'aide d'iManager.

SNMP

Plate-forme	Commande ou outil
Windows	rundll32 snmpinst, snmpinst **-c createobj -a FDN_utilisateur -p mot_de_passe -h nom_hôte_ou_adresse_IP**

Opérations iMonitor sécurisées

La sécurisation des accès à votre environnement iMonitor implique la procédure de protection suivante :

1. Utilisez un pare-feu et fournissez un accès VPN (cela s'applique également à NetIQ iManager et aux autres services Web dont l'accès doit être restreint).
2. Qu'un pare-feu soit ou non en place, limitez le type d'accès autorisé via iMonitor pour améliorer la protection contre les attaques de refus de service.

   Bien que des efforts considérables aient été entrepris pour s'assurer que iMonitor valide les données reçues via des requêtes d'URL, il est pratiquement impossible de garantir le rejet de toutes les entrées non valides éventuelles. Pour réduire le risque d'attaques de refus de service par le biais d'URL non valides, il existe trois niveaux d'accès que vous pouvez contrôler au moyen du fichier de configuration d'iMonitor à l'aide de l'option LockMask.

Niveau d'accès	Description
0	Pas d'authentification requise avant le traitement des URL par iMonitor. Dans ce cas, les droits eDirectory de l'identité [Public] sont appliqués à toutes les requêtes et les informations affichées par iMonitor sont limitées aux droits de l'utilisateur [Public]. Cependant, étant donné qu'aucune authentification n'est requise pour l'envoi d'URL à iMonitor, ce dernier peut être vulnérable aux attaques de refus de service basées sur la transmission d'informations incohérentes dans les URL.
1 (par défaut)	Authentification requise sous une identité eDirectory avant le traitement des URL par iMonitor. Dans ce cas, les droits eDirectory de cette identité sont appliqués à toutes les requêtes et sont donc restreints. Il existe une vulnérabilité aux attaques de refus de service identique à celle du niveau 0, à cette exception près que l'attaque doit être lancée par une personne qui s'est réellement authentifiée sur le serveur. En l'absence de toute authentification, iMonitor, lorsqu'il est configuré dans cet état, répond aux demandes d'URL par l'affichage d'une boîte de dialogue de connexion afin de rester protégé contre les attaques lancées par des utilisateurs non authentifiés.
2	Avant le traitement des URL par iMonitor, authentification requise sous une identité eDirectory disposant de droits équivalents à ceux d'un superviseur sur le serveur auprès duquel iMonitor s'authentifie. Il existe une vulnérabilité aux attaques de refus de service identique à celle du niveau 1, à cette exception près que l'attaque doit être lancée par une personne qui s'est réellement authentifiée en tant que superviseur du serveur. En l'absence de toute authentification, iMonitor, lorsqu'il est configuré dans cet état, répond aux demandes d'URL par l'affichage d'une boîte de dialogue de connexion afin de rester protégé contre les attaques lancées tant par des utilisateurs non authentifiés que par des utilisateurs authentifiés qui ne sont pas superviseurs.

Le niveau 1 est le niveau par défaut car de nombreux administrateurs n'ont pas d'accès Superviseur à chaque serveur de l'arborescence mais peuvent avoir besoin d'utiliser le service iMonitor sur un serveur qui interagit avec les leurs.

REMARQUE : plusieurs fonctions d'iMonitor telles que Repair et Trace requièrent une équivalence de superviseur pour les accès, quel que soit le paramètre LockMask.

Configuration d'un objet Serveur HTTP

Un objet Serveur HTTP est créé dans le cadre de l'installation d'eDirectory. La configuration par défaut des services HTTP se trouve dans le répertoire de cet objet. Toutefois, vous pouvez modifier la configuration par défaut à l'aide de NetIQ iManager. L'objet Serveur HTTP représente des données de configuration propres au serveur.

Les attributs de l'objet Serveur HTTP sont les suivants :

- **httpDefaultTLSPort :** indique le port sécurisé sur lequel écoute le serveur HTTP.
- **httpDefaultClearPort :** indique le port en texte clair sur lequel écoute le serveur HTTP.
- **httpAuthRequiresTLS :** indique si la requête acheminée via le port en texte clair doit être redirigée vers un port sécurisé.
- **httpTraceLevel :** indique le niveau de débogage du serveur HTTP dans DSTrace.
- **httpKeyMaterialObject :** indique le nom distinctif de l'objet Certificat que le serveur HTTP doit utiliser lors de la gestion de la connexion sécurisée. Pour configurer les interfaces d'iMonitor en mode SuiteB, activez le mode SuiteB souhaité en définissant la valeur de httpBindRestrictions en mode SuiteB, puis associez un certificat de serveur ECDSA approprié à httpKeyMaterialObject. httpkeyMaterialObject est configuré par défaut pour utiliser le certificat RSA.
- **httpSessionTimeout :** indique le timeout des sessions HTTP. La valeur par défaut est de 900 secondes.
- **httpKeepAliveRequestTimeout :** indique le timeout de maintien en activité de chaque requête HTTP. La valeur par défaut est de 15 secondes.
- **httpRequestTimeout :** indique le timeout de chaque requête HTTP. La valeur par défaut est de 300 secondes.
- **httpIOBufferSize :** indique la taille du tampon d'entrée et de sortie du serveur HTTP. La valeur par défaut est 8192 octets.
- **httpThreadsPerCPU :** indique les threads HTTP qui doivent être générés par unité centrale. La valeur par défaut est de 2 threads.
- **httpHostServerDN :** indique le nom distinctif de l'objet Serveur NCP auquel il est associé.
- **httpBindRestrictions :** vous permet de définir le niveau de chiffrement Cipher.
  - **RSA :** vous pouvez utiliser les valeurs suivantes pour restreindre l'utilisation du chiffrement :
    - 0 - accepte les chiffrements définis sur ÉLEVÉ, MOYEN, FAIBLE et EXPORTER
    - 1 - accepte uniquement les chiffrements définis sur ÉLEVÉ, MOYEN ou FAIBLE
    - 2 - accepte uniquement les chiffrements définis sur ÉLEVÉ et MOYEN
    - 3 - accepte uniquement les chiffrements définis sur ÉLEVÉ

    La valeur par défaut est de 3.

- **ECDSA 256 :** vous pouvez utiliser la valeur suivante pour limiter l'utilisation du chiffrement :
  - 4 - autorise un chiffrement de 128 ou 256 bits.
- **ECDSA 384 :** vous pouvez utiliser les valeurs suivantes pour restreindre l'utilisation du chiffrement :
  - 5 - autorise un chiffrement de 128 ou 256 bits.
  - 6 - autorise un chiffrement de 256 bits.

Dans le cas des certificats ECDSA, eDirectory autorise uniquement les chiffrements SuiteB.

Pour configurer les interfaces LDAP et httpstk en mode SuiteB, connectez-vous à iManager avec des droits d'administrateur et activez l'un des modes SuiteB, puis associez un certificat de serveur ECDSA approprié à ces interfaces. Vous devez effectuer cette opération pour chaque serveur eDirectory à l'aide d'objets de configuration des serveurs LDAP et httpstk, tels que ldapServer et httpServer. Avant d'activer le mode SuiteB, assurez-vous que tous les clients LDAP, les navigateurs LDAP et Web de l'environnement eDirectory prennent en charge les certificats TLS 1.2 et EC.

Configuration des paramètres de la pile HTTP à l'aide de ndsconfig

Voici les paramètres de la pile HTTP, après utilisation de ndsconfig :

- **http.server.interfaces :** contient l'interface en texte clair sur laquelle écoute le serveur HTTP. Cette option est définie au cours d'une nouvelle configuration de l'instance par ndsconfig.
- **http.server.request-io-buffer-size :** indique la taille du tampon d'entrée et de sortie du serveur HTTP. La valeur par défaut est de 8192 octets.
- **http.server.request_timeout-seconds :** indique le timeout de chaque requête HTTP. La valeur par défaut est de 300 secondes.
- **http.server.keep-timeout-seconds :** indique le timeout de maintien en activité de chaque requête HTTP. La valeur par défaut est de 15 secondes.
- **http.server.threads-per-processor :** indique les threads HTTP qui doivent être générés par unité centrale. La valeur par défaut est de 2 threads.
- **http.server.session-exp-seconds :** indique le timeout des sessions HTTP. La valeur par défaut est de 900 secondes.
- **http.server.trace-level :** indique le niveau de débogage de la pile HTTP dans DSTrace. Le niveau par défaut est 2.
- **http.server.clear-port :** indique le port en texte clair sur lequel écoute le serveur HTTP.
- **http.server.tls-port :** indique le port sécurisé sur lequel écoute le serveur HTTP.
- **http.server.auth-req-tls :** indique si les requêtes acheminées via le port en texte clair doivent être redirigées vers un port sécurisé.
- **https.server.interfaces :** contient l'interface sécurisée sur laquelle écoute le serveur HTTP. Elle est définie au cours d'une nouvelle configuration de l'instance par ndsconfig.
- **https.server.cached-cert-dn :** indique le nom distinctif de l'objet Certificat que le serveur HTTP doit utiliser lors de la gestion de la connexion sécurisée.

Utilisation de cn=monitor pour la surveillance

eDirectory fournit une méthode de recherche LDAP pour la surveillance de l'état actuel d'un serveur eDirectory. eDirectory enregistre des mesures de performances utiles et des informations sur l'état du serveur pour les sous-systèmes et processus en arrière-plan d'eDirectory, tels que la réserve de threads, la table des connexions, Dclient, l'agent DS, les processus en arrière-plan et le serveur LDAP en tant qu'entrée avec le DN de base de `cn=monitor`. Vous pouvez obtenir les statistiques du serveur en lançant une requête de recherche avec `cn=monitor` comme base de recherche et utiliser ces informations pour la surveillance de votre environnement eDirectory.

IMPORTANT : `cn=monitor` est un objet virtuel et ne réside pas réellement dans l'arborescence eDirectory. Vous pouvez utiliser cette méthode pour la surveillance d'eDirectory au moyen d'interfaces LDAP.

Les sous-systèmes d'eDirectory sont enregistrés en tant que producteurs de données dans le cadre de surveillance. Le Tableau 8-1 dresse la liste des producteurs de données enregistrés dans eDirectory. L'infrastructure rassemble les données en temps réel de tous les producteurs de données enregistrés et les partage avec les demandeurs qui sont, en fin de compte, les consommateurs de ces données. L'infrastructure de surveillance génère et renvoie dynamiquement des objets en réponse aux requêtes de recherche dans la sous-arborescence `cn=monitor`. Chaque objet contient des informations sur un aspect spécifique du serveur. Certains objets servent de conteneurs à d'autres objets et permettent d'établir une hiérarchie des objets au somment de laquelle se trouve `cn=monitor`. Vous pouvez utiliser les clients LDAP pour accéder aux informations fournies par l'infrastructure de surveillance, conformément aux contrôles d'accès et autres contrôles, tels que les informations relatives au serveur LDAP ou les informations spécifiques de la connexion. eDirectory permet de restreindre cette requête de recherche aux seuls utilisateurs disposant de droits d'écriture sur l'attribut NDSRightsToMonitor de l'objet Serveur NCP.

Vous pouvez accéder aux données de tous les producteurs de données enregistrés à l'aide de ldapsearch ou de tout navigateur LDAP à usage général.

Pour afficher les données de surveillance à partir de tous les producteurs de données enregistrés, utilisez la commande ldapsearch :

```
ldapsearch -h <SrvIP> -p <port> -D <user dn> -w <password> -s sub -b cn=monitor
```

REMARQUE : eDirectory ne prend pas en charge le filtrage des données lors d'une recherche `cn=monitor`. Pour certains processus en arrière-plan dont la planification d'exécution est récursive, eDirectory affiche ces processus plusieurs fois, comme prévu dans la réponse de recherche `cn=monitor`. Par exemple, SkulkerWorkerProc.

Affichage des statistiques de surveillance

`ldapsearch` renvoie des données provenant de tous les producteurs de données enregistrés au format LDAP en utilisant comme base `cn=monitor`. Le serveur LDAP fait également office de consommateur de données dans le format d'objet LDAP.

Le Tableau 8-1 dresse la liste des producteurs de données et des paramètres correspondants contenant les statistiques de surveillance. Des producteurs de données supplémentaires peuvent exister lorsque d'autres produits sont configurés avec eDirectory.

Tableau 8-1 Producteurs de données et paramètres des statistiques de surveillance

Producteurs de données	Paramètres des statistiques de surveillance
Agent	◆ Processus en arrière-plan ◆ Partition ◆ État du système

DHOST	Les informations de connexion et les processus DHOST suivants sont surveillés :
	◆ Connexions entrantes
	◆ Informations sur la réserve de threads
	  ◆ ThreadsSpawned
	  ◆ ThreadsDied
	  ◆ ThreadsIdle
	  ◆ ThreadsWorkers
	  ◆ ThreadPeakWorkers
	  ◆ ThreadPoolReadyQueueItems
	  ◆ ThreadPoolReadyQueueMaxWaitTime
	  ◆ ThreadMinWaitTime
	  ◆ ThreadMaxWaitTime

DClient	◆ Contexte sortant ◆ Connexion sortante
LDAP	◆ Reliure ◆ Opérations entrantes ◆ Opérations sortantes ◆ Volume de trafic
Gestionnaire d'enregistrements	◆ Recherches des défauts de cache ◆ Défauts de cache ◆ Taille actuelle, correspondances ◆ Recherches des correspondances ◆ Élément en cache ◆ Taille maximale ◆ OldVersionCachedCount ◆ OldVersionCachedSize ◆ Taille de la DIB ◆ Thread de point de contrôle

Lorsque vous émettez une requête de recherche avec une base de recherche `cn=monitor`, la structure de surveillance génère et renvoie dynamiquement des objets en réponse à la requête de recherche dans la sous-arborescence cn=monitor, comme indiqué dans le Tableau 8-2.

Tableau 8-2 *Objets surveillés par la recherche cn=monitor*

Nom d'objet	Description
cn=Monitor	Objet de niveau racine pour la surveillance des données.
cn=Agent,cn=Monitor	Fournit des informations sur l'agent du service Annuaire.
cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations à propos des processus en arrière-plan (qu'il s'agisse d'un processus spécifique ou des processus en arrière-plan en général).
cn=ARC resolve timer thread,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de coût avancé des renvois.
cn=BacklinkProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan des liaisons en amont.
cn=CPU Usage monitor,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de l'utilisation de l'UC.
cn=CheckBacklinks,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de vérification des liaisons en amont.
cn=CheckExtRefProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de vérification des références externes.
cn=ExtRefRefreshProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de rafraîchissement des références externes.
cn=Janitor,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan du nettoyeur (janitor).
cn=RunLimberUp,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de planification du contrôleur de connectivité.
cn=Limber,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan du contrôleur de connectivité
cn=HiConvergenceHeartBeat,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de planification du contrôleur de synchronisation (skulker).
cn=ObitProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de notices nécrologiques.
cn=PartitionPurgeProcess,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de l'outil de purge des partition.
cn=Predicate Statistics Update,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de mise à jour des statistiques d'estimation.
cn=RNRAdvertise,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan d'annonce d'adresse de service.
cn=RefreshBinderyContext,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de rafraîchissement de Bindery.

Nom d'objet	Description
cn=Repair Inactive Replicas,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de réparation des répliques inactives.
cn=SchemaProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de synchronisation des schémas.
cn=SkulkerProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de synchronisation.
cn=SkulkerWorkerProc,cn=BackGroundProcInterval,cn=Agent,cn=Monitor	Fournit des informations sur le processus en arrière-plan de synchronisation.
cn=Partition,cn=Agent,cn=Monitor	Fournit des informations sur toutes les partitions utilisateur sur le serveur. Plusieurs valeurs pour le même attribut indiquent la présence de plusieurs partitions.
cn=Status,cn=Agent,cn=Monitor	Fournit des informations à propos de l'état du serveur.
cn=DHOST,cn=Monitor	Fournit des informations sur les sous-systèmes DHOST.
cn=InBoundConnection,cn=DHOST,cn=Monitor	Fournit des informations sur la table des connexions entrantes.
cn=ThreadPool,cn=DHOST,cn=Monitor	Fournit des informations sur les statistiques de réserve de threads DHOST.
cn=Dclient,cn=Monitor	Fournit des informations sur DClient côté serveur.
cn=OutBoundConnection,cn=Dclient,cn=Monitor	Fournit des informations sur la table des connexions sortantes.
cn=OutBoundContext,cn=Dclient,cn=Monitor	Fournit des informations sur la table des contextes sortants.
cn=LDAP,cn=Monitor	Fournit des informations sur le serveur LDAP.
cn=LDAPStatistics,cn=LDAP,cn=Monitor	Fournit des informations sur les statistiques du serveur LDAP.
cn=Bindings,cn=LDAPStatistics,cn=LDAP,cn=Monitor	Fournit des informations sur les statistiques de liaison sur le serveur LDAP.
cn=IncomingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor	Fournit des informations sur les statistiques d'opérations entrantes sur le serveur LDAP.
cn=OutgoingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor	Fournit des informations sur les statistiques d'opérations sortantes sur le serveur LDAP.
cn=TrafficVolume,cn=LDAPStatistics,cn=LDAP,cn=Monitor	Fournit des informations sur les statistiques de volume du trafic du serveur LDAP.
cn=RecordManager,cn=Monitor	Fournit des informations sur la base de données FLAIM.
cn=Size,cn=RecordManager,cn=Monitor	Fournit des informations sur la taille de la base de données FLAIM.
cn=CheckPointThreadData,cn=RecordManager,cn=Monitor	Fournit des informations sur le thread de point de contrôle.

Nom d'objet	Description
cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur les statistiques du Cache de la base de données FLAIM.
cn=CacheFaultLooks,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur la recherche d'anomalies dans le cache.
cn=CacheFaults,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur les anomalies dans les cache.
cn=HitLooks,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur la recherche d'occurrences dans le cache.
cn=Hits,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur les correspondances dans le cache.
cn=ItemsCached,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur le nombre d'éléments en cache.
cn=OldVersionCachedCount,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur le nombre d'éléments en cache dans l'ancienne version.
cn=MaximumSize,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur la taille maximale du cache.
cn=CurrentSize,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur la taille actuelle du cache.
cn=OldVersionCachedSize,cn=CacheStatistics,cn=RecordManager,cn=Monitor	Fournit des informations sur la taille du cache de l'ancienne version.

Chaque objet contient des informations sur un aspect particulier du serveur, tel qu'une connexion ou un thread. Le Tableau 8-3 dresse la liste des attributs qui contiennent les statistiques de surveillance.

Tableau 8-3 *Statistiques de surveillance des attributs*

Attribut	Description
BackgroundProcScheduled	Heure de la prochaine planification du processus en arrière-plan. Plusieurs valeurs signifient que le processus en arrière-plan est planifié à plusieurs reprises.
BackgroundProcStartTime	Heure de début du prochain processus en arrière-plan. Plusieurs valeurs signifient que le processus en arrière-plan est exécuté à plusieurs reprises.
PerishableData	Quantité de données dont la synchronisation sur un autre serveur a échoué (exprimée en secondes).
OBIT_NEWRDN_PURGEABLE	Nombre de notices nécrologiques NEWRDN dont l'état est PURGEABLE.
OBIT_NEWRDN_OK_TO_PURGE	Nombre de notices nécrologiques NEWRDN dont l'état est OK_TO_PURGE.
OBIT_NEWRDN_NOTIFIED	Nombre de notices nécrologiques NEWRDN dont l'état est NOTIFIÉ.
OBIT_NEWRDN_ISSUED	Nombre de notices nécrologiques NEWRDN dont l'état est ÉMIS.
OBIT_MOVED_PURGEABLE	Nombre de notices nécrologiques déplacées dont l'état est PURGEABLE.

Attribut	Description
OBIT_MOVED_OK_TO_PURGE	Nombre de notices nécrologiques déplacées dont l'état est OK_TO_PURGE.
OBIT_MOVED_NOTIFIED	Nombre de notices nécrologiques déplacées dont l'état NOTIFIÉ.
OBIT_MOVED_ISSUED	Nombre de notices nécrologiques déplacées dont l'état est ÉMIS.
OBIT_DEAD_PURGEABLE	Nombre de notices nécrologiques ayant expiré dont l'état est PURGEABLE.
OBIT_DEAD_OK_TO_PURGE	Nombre de notices nécrologiques ayant expiré dont l'état est OK_TO_PURGE.
OBIT_DEAD_NOTIFIED	Nombre de notices nécrologiques ayant expiré dont l'état est NOTIFIÉ.
OBIT_DEAD_ISSUED	Nombre de notices nécrologiques ayant expiré dont l'état est ÉMIS.
OBIT_COUNT_FROM_DATABASE_INDEX	Nombre total de notices nécrologiques.
MaxRingDelta	Quantité maximale de données non synchronisées entre deux serveurs de l'anneau de répliques (indiquée en secondes).
ChangeCacheCount	Nombre actuel de changements de cache sur la partition.
eDirectoryUpTime	Nombre de secondes écoulées depuis la dernière exécution du serveur.
eDirectorySystemCurrTime	Heure actuelle du système du serveur.
eDirectoryAgentVersion	Version actuelle de l'agent de serveur Annuaire.
MaxInBoundConnection	Nombre maximal de connexions entrantes.
InBoundConnectionCount	Nombre actuel de connexions entrantes.
ThreadsWorkers	Nombre de threads d'employés dans la réserve de threads.
ThreadsSpawned	Nombre de threads générés.
ThreadsIdle	Nombre de threads inactifs.
ThreadsDied	Nombre de threads ayant expiré.
ThreadWaitingQueuePeakItems	Nombre maximal de threads dans la file d'attente.
ThreadWaitingQueueItems	Nombre actuel de threads dans la file d'attente.
ThreadPoolReadyQueueMaxWaitTime	Temps d'attente maximal d'un thread dans la file d'attente des éléments prêts.
ThreadPoolReadyQueueItems	Nombre actuel de threads dans la file d'attente des éléments prêts.
ThreadPeakWorkers	Nombre maximal de threads d'employés dans la réserve.
ThreadMinWaitTime	Temps d'attente minimale d'un thread avant sa planification.
ThreadMaxWaitTime	Temps d'attente maximale d'un thread avant sa planification.
TotalOpenOutBoundConnection	Nombre de connexions sortantes actuellement ouvertes.
RefusedOutBoundConnection	Nombre de connexions sortantes refusées.
MaxOutBoundConnection	Nombre maximal de connexions sortantes.
TotalOutBoundContextCount	Nombre maximal de contextes sortants.

Attribut	Description
ActiveOutBoundContextCount	Nombre de contextes sortants en cours.
unAuthBinds	Nombre de requêtes de liaison non authentifiées/anonymes reçues.
strongAuthBinds	ndsProtoIfStrongAuthBinds Nombre de requêtes de liaison authentifiées à l'aide des procédures d'authentification supérieures SASL et X.500. Ceci englobe les liaisons qui ont été authentifiées à l'aide de procédures d'authentification externes.
simpleAuthBinds	Nombre de requêtes de liaison authentifiées à l'aide de procédures d'authentification simples dans lesquelles le mot de passe est envoyé sur le réseau, au format chiffré ou en texte clair.
bindSecurityErrors	Nombre de requêtes de liaison rejetées en raison d'une authentification erronée ou de références non valides.
wholeSubtreeSearchOps	Nombre de requêtes de recherche reçues portant sur l'ensemble de la sous-arborescence.
searchOps	Nombre de requêtes de recherche reçues (portant sur un objet de base, sur un niveau ou sur l'ensemble de la sous-arborescence).
removeEntryOps	Nombre de requêtes removeEntry reçues.
readOps	Nombre de requêtes de lecture reçues.
oneLevelSearchOps	Nombre de requêtes de recherche portant sur un niveau reçues.
modifyRDNOps	Nombre de requêtes modifyRDN reçues.
modifyEntryOps	Nombre de requêtes modifyEntry reçues.
listOps	Nombre de requêtes de liste reçues.
inOps	Nombre de requêtes reçues de la part du client.
extendedOps	Nombre d'opérations avancées.
compareOps	Nombre de requêtes de comparaison reçues.
addEntryOps	Nombre de requêtes addEntry reçues.
abandonOps	Nombre de requêtes LDAP abandonnées.
referrals	Nombre de renvois renvoyés en réponse aux requêtes pour des opérations.
chainings	Nombre d'opérations transmises par ce serveur eDirectory aux autres serveurs eDirectory.
outBytes	Trafic sortant, en octets, sur l'interface. Comprend les réponses au client et aux serveurs eDirectory ainsi que des requêtes adressées à d'autres serveurs eDirectory.
inBytes	Trafic entrant, en octets, sur l'interface. Il inclut les requêtes envoyées par le client ainsi que les réponses d'autres serveurs eDirectory.
Capacité	Nombre total d'éléments dans le cache FLAIM.
EntryCache	Nombre total d'éléments dans le cache d'entrées.
BlockCache	Nombre total d'éléments dans le cache de blocs.
TotalSize	Taille totale des éléments dans le cache FLAIM.

Attribut	Description
EntryCacheSize	Taille totale des éléments dans le cache d'entrées.
BlockCacheSize	Taille totale des éléments dans le cache de blocs.
CheckPointThreadWritingDataBlocks	0 indique que le point de contrôle n'écrit pas de Dirty Blocks. 1 indique que le point de contrôle écrit des Dirty Blocks.
CheckPointThreadStartTime	Heure de début du thread de point de contrôle. Ne tenez compte de cette valeur que si le thread de point de contrôle est en cours d'exécution.
CheckPointThreadLogBlocksWritten	Nombre de blocs de journal écrits.
CheckPointThreadIsRunning	0 indique que le point de contrôle n'est pas en cours d'exécution. 1 indique que le thread de point de contrôle est en cours d'exécution.
CheckPointThreadIsForced	Indique si le point de contrôle a été forcé.
CheckPointThreadForceStartTime	Heure de début du point de contrôle forcé. Ne tenez compte de cette valeur que si le démarrage du point de contrôle a été forcé.
CheckPointThreadDirtyCacheBlocks	Nombre de blocs Dirty Cache.
CheckPointThreadDataBlocksWritten	Nombre de Dirty blocks écrits.
CheckPointThreadBlockSize	Taille actuelle du bloc.
TotalDIBSize	Taille totale de la base de données FLAIM.
DIBStreamFileSize	Taille totale des fichiers de flux.
DIBRollBackFileSize	Taille totale des fichiers de retour à l'état initial
DIBRflmFileSize	Taille totale des fichiers journaux de transaction individuelle.
DIBFileSize	Taille totale des fichiers DIB.

Ci-dessous, un exemple de résultat de la recherche LDAP.

```
# LDAPv3
# base <cn=monitor> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
# BackGroundProcInterval, Agent, Monitor
dn: cn=BackGroundProcInterval,cn=Agent,cn=Monitor
slowSyncInterval: 1800
fastSyncInterval: 5
ServerStateUpThreshold: 1800
JanitorInterval: 120
HeartBeatSkulkInterval: 3600
FlatCleaningInterval: 43200
DRLInterval: 60
BacklinkInterval: 46800
objectclass: Top
objectclass: extensibleObject
# .GOOD-ONE., Partition, Agent, Monitor
dn: cn=.GOOD-ONE.,cn=Partition,cn=Agent,cn=Monitor
ChangeCacheCount: 0
objectclass: Top
objectclass: extensibleObject
# InBoundConnection, DHOST, Monitor
```

```
dn: cn=InBoundConnection,cn=DHOST,cn=Monitor
MaxInBoundConnection: 256
InBoundConnectionCount: 20
objectclass: Top
objectclass: extensibleObject
# ThreadPool, DHOST, Monitor
dn: cn=ThreadPool,cn=DHOST,cn=Monitor
ThreadsWorkers: 37
Monitoring
ThreadsSpawned: 3572
ThreadsIdle: 7
ThreadsDied: 3535
ThreadWaitingQueuePeakItems: 24
ThreadWaitingQueueItems: 20
ThreadPoolReadyQueueMaxWaitTime: 574529
ThreadPoolReadyQueueItems: 0
ThreadPeakWorkers: 90
ThreadMinWaitTime: 2
ThreadMaxWaitTime: 16394616
objectclass: Top
objectclass: extensibleObject
# OutBoundConnection, Dclient, Monitor
dn: cn=OutBoundConnection,cn=Dclient,cn=Monitor
TotalOpenOutBoundConnection: 17
RefusedOutBoundConnection: 0
MaxOutBoundConnection: 4294967295
objectclass: Top
objectclass: extensibleObject
# OutBoundContext, Dclient, Monitor
dn: cn=OutBoundContext,cn=Dclient,cn=Monitor
TotalOutBoundContextCount: 256
objectclass: Top
objectclass: extensibleObject
# Bindings, LDAPStatistics, LDAP, Monitor
dn: cn=Bindings,cn=LDAPStatistics,cn=LDAP,cn=Monitor
unAuthBinds: 6908
strongAuthBinds: 0
simpleAuthBinds: 4433475
bindSecurityErrors: 0
objectclass: Top
objectclass: extensibleObject
# IncomingOperations, LDAPStatistics, LDAP, Monitor
dn: cn=IncomingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor
wholeSubtreeSearchOps: 4426462
searchOps: 4426462
removeEntryOps: 0
readOps: 0
oneLevelSearchOps: 0
modifyRDNOps: 0
modifyEntryOps: 4
listOps: 0
inOps: 8901739
extendedOps: 0
compareOps: 0
addEntryOps: 5
abandonOps: 0
objectclass: Top
objectclass: extensibleObject
# OutgoingOperations, LDAPStatistics, LDAP, Monitor
dn: cn=OutgoingOperations,cn=LDAPStatistics,cn=LDAP,cn=Monitor
```

```
referrals: 0
chainings: 0
objectclass: Top
objectclass: extensibleObject
# TrafficVolume, LDAPStatistics, LDAP, Monitor
dn: cn=TrafficVolume,cn=LDAPStatistics,cn=LDAP,cn=Monitor
outBytes: 326809576
inBytes: 380249498
objectclass: Top
objectclass: extensibleObject
Monitoring
# CacheFaultLooks, RecordManager, Monitor
dn: cn=CacheFaultLooks,cn=RecordManager,cn=Monitor
TotalSize: 2699
EntryCacheSize: 2539
BlockCacheSize: 160
objectclass: Top
objectclass: extensibleObject
# CacheFaults, RecordManager, Monitor
dn: cn=CacheFaults,cn=RecordManager,cn=Monitor
TotalSize: 1948
EntryCacheSize: 1788
BlockCacheSize: 160
objectclass: Top
objectclass: extensibleObject
# CurrentSize, RecordManager, Monitor
dn: cn=CurrentSize,cn=RecordManager,cn=Monitor
TotalSize: 4849664
EntryCacheSize: 3866624
BlockCacheSize: 983040
objectclass: Top
objectclass: extensibleObject
# HitLooks, RecordManager, Monitor
dn: cn=HitLooks,cn=RecordManager,cn=Monitor
TotalSize: 656418775
EntryCacheSize: 489811630
BlockCacheSize: 166607145
objectclass: Top
objectclass: extensibleObject
# Hits, RecordManager, Monitor
dn: cn=Hits,cn=RecordManager,cn=Monitor
TotalSize: 449815580
EntryCacheSize: 283226835
BlockCacheSize: 166588745
objectclass: Top
objectclass: extensibleObject
# ItemsCached, RecordManager, Monitor
dn: cn=ItemsCached,cn=RecordManager,cn=Monitor
TotalSize: 1865
EntryCacheSize: 1691
BlockCacheSize: 174
objectclass: Top
objectclass: extensibleObject
# MaximumSize, RecordManager, Monitor
dn: cn=MaximumSize,cn=RecordManager,cn=Monitor
TotalSize: 200015872
EntryCacheSize: 100007972
BlockCacheSize: 100007900
objectclass: Top
objectclass: extensibleObject
```

```
# OldVersionCachedCount, RecordManager, Monitor
dn: cn=OldVersionCachedCount,cn=RecordManager,cn=Monitor
TotalSize: 7
EntryCacheSize: 3
BlockCacheSize: 4
objectclass: Top
objectclass: extensibleObject
# OldVersionCachedSize, RecordManager, Monitor
dn: cn=OldVersionCachedSize,cn=RecordManager,cn=Monitor
Monitoring
TotalSize: 21376
EntryCacheSize: 4448
BlockCacheSize: 16928
objectclass: Top
objectclass: extensibleObject
# search result
search: 2
result: 0 Success
# numResponses: 20
# numEntries: 19
```

Utilisation de DSTrace

Pour utiliser l'utilitaire DSTrace dans un environnement Linux, exécutez la commande suivante à l'invite du serveur :

```
/opt/novell/eDirectory/bin/ndstrace
```

La syntaxe complète de la commande ndstrace est la suivante :

```
ndstrace [-l|-u|-c "command1;......"|--version] [-h <local_interface:port>] [--
config-file <configuration_file_path>] [thrd <thread ID>] [svty <severity_level>]
[conn <connection_ID>]
```

L'utilitaire DSTrace comporte trois parties principales :

- « Fonctions de base » page 281
- « Messages de débogage » page 282
- « Processus à l'arrière plan » page 285

Fonctions de base

Les fonctions de base de DSTrace sont les suivantes :

- Affichage de l'activité interne d'eDirectory et des messages de débogage sous Linux.
- Lancement des processus de synchronisation limités.

Vous pouvez utiliser l'utilitaire DSTrace en mode interface utilisateur ou en mode ligne de commande. Par défaut, DSTrace s'exécute en mode interface utilisateur. Pour lancer DSTrace en mode interface utilisateur, entrez la commande suivante à l'invite du serveur :

```
/opt/novell/eDirectory/bin/ndstrace
```

Pour démarrer DSTrace en mode ligne de commande, entrez la commande suivante à l'invite de commande :

```
/opt/novell/eDirectory/bin/ndstrace -l
```

Pour lancer les fonctions de base de DSTrace, entrez les commandes correspondantes à l'invite du serveur en respectant la syntaxe suivante :

`ndstrace command_option`

La table ci-dessous liste les options de commande que vous pouvez entrer.

Option	Description
ON	Affiche l'écran de trace eDirectory et présente les messages de trace élémentaires.
OFF	Désactive l'écran de suivi.
ALL	Affiche l'écran de trace eDirectory et présente tous les messages de trace.
AGENT	Affiche l'écran de trace eDirectory et présente les messages de trace qui correspondent aux drapeaux ON, BACKLINK, DSAGENT, JANITOR, RESNAME et VCLIENT.
DEBUG	Active un ensemble prédéfini de messages de suivi, qui sont en général utilisés pour le débogage. Les indicateurs suivants sont activés : ON, BACKLINK, ERRORS, EMU, FRAGGER, INIT, INSPECTOR, JANITOR, LIMBER, MISC, PART, RECMAN, REPAIR, SCHEMA, SKULKER, STREAMS et VCLIENT.
NODEBUG	Ne désactive pas l'écran de suivi, mais désactive tous les messages de débogage qui ont été activés précédemment. Cette option laisse également les messages définis sur l'option de commande ON.

Messages de débogage

Lorsque l'écran DSTrace est activé, les informations affichées se fondent sur un ensemble de filtres par défaut. Pour obtenir un affichage plus ou moins détaillé que celui par défaut, vous pouvez modifier les filtres à l'aide des indicateurs des messages de débogage. Les messages de débogage aident à déterminer l'état d'eDirectory ainsi qu'à vérifier si tout fonctionne normalement.

Chaque processus eDirectory comporte un ensemble de messages de débogage. Pour afficher les messages de débogage d'un processus particulier, précisez le signe plus (+) ainsi que le nom ou l'option du processus. Pour désactiver l'affichage d'un processus, entrez un signe moins (-) ainsi que le nom ou l'option du processus. Voici quelques exemples :

Message	Description
`set ndstrace = +SYNC`	Active les messages de synchronisation.
`set ndstrace = -SYNC`	Désactive les messages de synchronisation.
`set ndstrace = +SCHEMA`	Active les messages de schéma.

Vous pouvez également combiner les indicateurs des messages de débogage à l'aide des opérateurs booléens « & » (qui signifie ET) et | » (qui signifie OU). La syntaxe de commande des messages de débogage sur la console du serveur est la suivante :

`set ndstrace = <trace_flag> [parameter]`

Le tableau ci-dessous décrit les drapeaux de trace pour les messages de débogage. Vous pouvez entrer une abréviation pour chacun des indicateurs de suivi.

Indicateur de suivi	Description
ABUF	Messages et informations liés aux tampons de paquets entrants et sortants qui contiennent des données reçues avec une requête eDirectory, ou en réponse à celle-ci.
ALOC	Messages qui affichent les détails de l'allocation de mémoire.
AREQ	Messages liés aux requêtes entrantes d'autres serveurs ou clients.
AUTH	Messages et rapports d'erreur liés à l'authentification.
BASE	Messages d'erreur de débogage au niveau de débogage minimal.
BLNK	Rapports d'erreur et messages de lien en amont et de notice nécrologique entrante.
CBUF	Messages liés aux requêtes sortantes du client DS.
CHNG	Messages du cache de changement.
COLL	Rapports d'état et d'erreur concernant les informations de mise à jour d'un objet lorsque la mise à jour a été reçue précédemment.
CONN	Messages qui affichent des informations sur les serveurs auxquels votre serveur essaie de se connecter, et sur les erreurs et les timeouts qui empêchent éventuellement ces connexions.
DNS	Messages sur les processus de serveur DNS intégrés dans eDirectory.
DRLK	Messages sur les liens de référence distribués.
DVRS	Messages qui affichent les zones propres au pilote DirXML® sur lesquelles eDirectory est susceptible de fonctionner.
DXML	Messages qui affichent les détails des événements DirXML.
FRAG	Messages du fragmenteur NCP qui fractionne les messages eDirectory en messages au format NCP.
IN	Messages liés aux requêtes et processus entrants.
INIT	Messages liés à l'initialisation d'eDirectory.
INSP	Messages liés à l'intégrité des objets dans la base de données locale du serveur source. L'emploi de ce drapeau entraîne une sollicitation accrue du système de stockage sur disque, de la mémoire et du processeur du serveur source. Ne laissez ce drapeau activé que si des objets sont altérés.
JNTR	Messages liés aux processus d'arrière-plan suivants : nettoyeur (janitor), synchronisation des répliques et gestionnaire d'attributs (flat cleaner).
LDAP	Messages liés au serveur LDAP.
LMBR	Messages liés au contrôle de la connectivité (processus limber).
LOCK	Messages liés à l'utilisation et à la manipulation des verrous de la base de données locale du serveur source.
LOST	Messages liés aux entrées perdues.
MISC	Messages provenant de différentes sources dans eDirectory.
MOVE	Messages provenant des opérations de déplacement de partition ou de sous-arborescence.

Indicateur de suivi	Description
NCPE	Messages montrant le serveur qui reçoit les requêtes de niveau NCP.
NMON	Messages liés à iMonitor.
OBIT	Messages du processus de notice nécrologique.
PART	Messages liés aux opérations de partition lancées par les processus d'arrière-plan et par le traitement des requêtes.
PURG	Messages liés au processus de purge.
RECM	Messages liés à la manipulation de la base de données du serveur source.
RSLV	Rapports liés au traitement des requêtes de résolution de noms.
SADV	Messages liés à l'enregistrement des noms d'arborescence et des partitions auprès du protocole SLP (Service Location Protocol).
SCMA	Messages liés au processus de synchronisation du schéma.
SCMD	Messages qui affichent les détails des opérations liées au schéma. Ils fournissent des détails sur la synchronisation entrante et sortante.
SKLK	Messages liés au processus de synchronisation des répliques.
SPKT	Messages liés aux informations eDirectory au niveau du serveur NCP.
STRM	Messages liés au traitement des attributs à l'aide d'une syntaxe de flux.
SYDL	Messages qui affichent des informations complémentaires pendant le processus de réplication.
SYNC	Messages sur le trafic de synchronisation entrant (informations reçues par le serveur).
TAGS	Affiche la chaîne d'étiquettes qui identifie l'option de trace ayant généré l'événement spécifié sur chaque ligne affichée par le processus de trace.
THRD	Messages qui affichent le début et la fin des processus d'arrière-plan (threads).
TIME	Messages liés aux vecteurs de transition utilisés pendant le processus de synchronisation.
TVEC	Messages associés aux attributs suivants : Synchronisé jusqu'à, Réplique jusqu'à et Vecteur de transition.
VCLN	Messages liés à l'établissement ou à la suppression de connexions avec d'autres serveurs.

Lorsque vous utiliserez ces messages de débogage sous DSTrace, vous constaterez que les drapeaux de trace sont plus ou moins utiles. L'un des paramètres DSTrace favoris de prise en charge NetIQ est en fait un raccourci :

```
set ndstrace = A81164B91
```

Ce paramètre active un groupe de messages de débogage.

Processus à l'arrière plan

En plus des messages de débogage, qui aident à vérifier l'état d'eDirectory, vous disposez d'un ensemble de commandes qui imposent l'exécution des processus en arrière-plan d'eDirectory. Pour forcer le lancement d'un processus d'arrière-plan, entrez un astérisque (*) avant la commande. Par exemple :

```
set ndstrace = *H
```

Vous pouvez également changer l'état, la séquence et le contrôle de certains processus d'arrière-plan. Pour modifier ces valeurs, entrez un point d'exclamation (!) avant la commande et entrez un nouveau paramètre ou une nouvelle valeur. Par exemple :

```
set ndstrace = !H 15 (parameter_value_in_minutes)
```

La syntaxe de chaque instruction qui régit les processus en arrière-plan d'eDirectory est la suivante :

```
set ndstrace = <trace_flag> [parameter]
```

Le tableau ci-dessous répertorie les drapeaux de trace des processus d'arrière-plan, les paramètres éventuellement requis et le processus que les drapeaux de trace affichent.

Indicateur de suivi	Paramètres	Description
*Un fichier	Aucun(e)	Réinitialise le cache des adresses sur le serveur source.
*AD	Aucun(e)	Désactive le cache des adresses sur le serveur source.
*AE	Aucun(e)	Active le cache des adresses sur le serveur source.
*B	Aucun(e)	Planifie le processus de liaison en amont pour que son exécution commence dans une seconde sur le serveur source.
!B	Heure	Définit la fréquence (en minutes) du processus de liaison en amont. Valeur par défaut = 1 500 minutes (25 heures) ; Plage = 2 à 10 080 minutes (168 heures)
*CT	Aucun(e)	Affiche la table des connexions sortantes du serveur source et les statistiques actuelles pour cette table. Ces statistiques ne fournissent pas d'informations sur les connexions entrantes d'autres serveurs ou clients au serveur source.
*CTD	Aucun(e)	Affiche, en utilisant le format séparé par une virgule, la table des connexions sortantes du serveur source et les statistiques actuelles pour cette table. Ces statistiques ne fournissent pas d'informations sur les connexions entrantes d'autres serveurs ou clients au serveur source.
*D	Replica rootEntry ID	Supprime l'ID d'entrée locale spécifié de la liste Envoyer tous les objets du serveur source. Cet ID doit indiquer un objet Racine de partition propre à la base de données locale du serveur. Cette commande n'est généralement employée que lorsqu'un processus Envoyer toutes les mises à jour tente indéfiniment d'afficher les mises à jour et échoue parce qu'un serveur est inaccessible.

Indicateur de suivi	Paramètres	Description
!D	Heure	Attribue à l'intervalle de synchronisation entrante et sortante le nombre de minutes spécifié. Valeur par défaut = 24 minutes. Plage = 2 à 10 080 minutes (168 heures)
!DI	Heure	Attribue à l'intervalle de synchronisation entrante le nombre de minutes spécifié. Valeur par défaut = 24 minutes ; Plage = 2 à 10 080 minutes (168 heures)
!DO	Heure	Attribue à l'intervalle de synchronisation sortante le nombre de minutes spécifié. Valeur par défaut = 24 minutes ; Plage = 2 à 10 080 minutes (168 heures)
*E	Aucun(e)	Réinitialise le cache d'entrées du serveur source.
!E	Aucun(e)	Planifie l'exécution des processus de synchronisation entrante et sortante.
!EI	Aucun(e)	Planifie l'exécution du processus de synchronisation entrante.
!EO	Aucun(e)	Planifie l'exécution du processus de synchronisation sortante.
*F	Aucun(e)	Planifie l'exécution du processus Gestionnaire d'attributs (flat cleaner), qui fait partie du processus Nettoyeur (janitor), sur le serveur source afin qu'elle commence dans les cinq secondes.
!F	Heure	Définit la fréquence (en minutes) du processus Gestionnaire d'attributs (flat cleaner). Valeur par défaut = 240 minutes (4 heures) ; Plage = 2 à 10 080 minutes (168 heures)

Indicateur de suivi	Paramètres	Description
*FL	1-10	Définit le nombre de fichiers journaux de déploiement utilisés par DSTrace. Si vous définissez ce paramètre sur une valeur supérieure à 1, lorsque le fichier `ndstrace.log` du serveur source atteint la taille de fichier maximale configurée, DSTrace renomme le fichier et lui attribue le nom `ndstrace1.log`, puis crée un nouveau fichier `ndstrace.log`. Lorsque ce fichier atteint sa taille maximale, le fichier `ndstrace1.log` précédent est renommé `ndstrace2.log` et le dernier fichier `ndstrace.log` est renommé `ndstrace1.log`. Ce processus se poursuit jusqu'à ce que DSTrace atteigne le nombre maximal de fichiers journaux générés par cette option. Une fois que la limite spécifiée est atteinte, les anciens fichiers journaux sont supprimés et seul le nombre maximal spécifié de fichiers est conservé. Vous pouvez configurer un maximum de 10 fichiers journaux progressifs. Par défaut, DSTrace doit utiliser au moins un fichier journal progressif. Si vous définissez ce paramètre sur 0, DSTrace utilise la valeur de paramètre 1.
*G	Replica rootEntry ID	Recrée le cache de changement de l'ID de partition racine indiqué.
*H	Aucun(e)	Planifie l'exécution immédiate du processus de synchronisation des répliques sur le serveur source.
!H	Heure	Définit la fréquence (en minutes) du processus de synchronisation des pulsations. Valeur par défaut = 30 minutes ; Plage = 2 à 1 440 minutes (24 heures)
*HR	Aucun(e)	Efface le dernier vecteur envoyé de la mémoire.
*I	Replica rootEntry ID	Ajoute l'ID d'entrée locale spécifié dans la liste Envoyer tous les objets du serveur source. Cet ID doit indiquer un objet Racine de partition propre à la base de données locale du serveur. Le processus de synchronisation des répliques vérifie la liste Envoyer tous les objets. Si l'ID d'entrée d'un objet Racine de partition figure dans la liste, eDirectory synchronise tous les objets et attributs de la partition, quelle que soit la valeur de l'attribut Synchronisé jusqu'à.
!I	Heure	Définit la fréquence (en minutes) du processus de synchronisation des pulsations. Valeur par défaut = 30 minutes ; Plage = 2 à 1 440 minutes (24 heures)
*J	Aucun(e)	Planifie l'exécution sur le serveur source du processus de purge, qui fait partie du processus de synchronisation des répliques.
!J	Heure	Définit la fréquence (en minutes) du processus Nettoyeur (janitor). Valeur par défaut = 2 minutes ; Plage = 1 à 10 080 minutes (168 heures)

Indicateur de suivi	Paramètres	Description
*L	Aucun(e)	Planifie l'exécution du contrôle de la connectivité (processus limber) sur le serveur source pour qu'elle commence dans cinq secondes.
*M	Octets	Modifie la taille maximale allouée au fichier `ndstrace.log` du serveur source. Cette commande peut être employée quel que soit l'état du fichier de débogage. Le nombre d'octets indiqué doit être une valeur décimale comprise entre 10 000 octets et 100 Mo. Si la valeur indiquée n'est pas comprise dans cette plage, aucune modification n'a lieu.
!M	Aucun(e)	Indique la quantité maximale de mémoire utilisée par eDirectory.
!N	0|1	Définit le format du nom. 0 = format hexadécimal uniquement ; 1 = notation à points
*P	Aucun(e)	Affiche les paramètres modifiables et leurs valeurs par défaut.
*R	Aucun(e)	Rétablit la taille du fichier `ndstrace.log` sur 0 octet. Cette commande est la même que le paramètre NDS SET de réglage à zéro de la taille du fichier de suivi.
*S	Aucun(e)	Programme le processus Contrôleur de sync, qui vérifie si une des répliques figurant sur le serveur doit être synchronisée.
!SI	Heure	Définit la fréquence (en minutes) du processus de synchronisation entrante du schéma. Valeur par défaut = 24 minutes ; Plage = 2 à 10 080 minutes (168 heures)
!SO	Heure	Définit la fréquence (en minutes) du processus de synchronisation sortante du schéma. Valeur par défaut = 24 minutes ; Plage = 2 à 10 080 minutes (168 heures)
!SIO	Heure	Désactive le processus de synchronisation entrante du schéma pendant le nombre de minutes spécifié. Valeur par défaut = 24 minutes ; Plage = 2 à 10 080 minutes (168 heures)
!SO0	Heure	Désactive le processus de synchronisation entrante du schéma pendant le nombre de minutes spécifié. Valeur par défaut = 24 minutes ; Plage = 2 à 10 080 minutes (168 heures)
*SS	Aucun(e)	Force la synchronisation immédiate du schéma.
*SSA	Aucun(e)	Lance l'exécution immédiate du processus de synchronisation du schéma et impose la synchronisation du schéma sur tous les serveurs cibles, même s'ils ont déjà été synchronisés au cours des dernières 24 heures.

Indicateur de suivi	Paramètres	Description
*SSD	Aucun(e)	Réinitialise la liste Synchronisation du schéma cible sur le serveur source. Cette liste identifie les serveurs avec lesquels le serveur source doit se synchroniser pendant le processus de synchronisation du schéma. Un serveur qui ne contient aucune réplique envoie une requête pour être inclus dans la liste cible d'un serveur qui contient une réplique avec son objet Serveur.
*SSL	Aucun(e)	Imprime la liste de synchronisation du schéma des serveurs cibles.
*ST	Aucun(e)	Affiche les informations sur l'état des processus en arrière-plan exécutés sur le serveur source.
*STX	Aucun(e)	Affiche les informations sur l'état du processus de liaison en amont (références externes) exécuté sur le serveur source.
*STS	Aucun(e)	Affiche les informations sur l'état du processus de synchronisation du schéma exécuté sur le serveur source.
*STO	Aucun(e)	Affiche les informations sur l'état du processus de liaison en amont (notices nécrologiques) exécuté sur le serveur source.
*STL	Aucun(e)	Affiche les informations sur l'état du contrôle de la connectivité (processus limber) exécuté sur le serveur source.
!T	Heure	Définit la fréquence (en minutes) de vérification de l'état actif du serveur. Valeur par défaut = 30 minutes ; Plage = 1 à 720 minutes (12 heures)
*U	ID facultatif du serveur	Si la commande ne comporte pas d'ID d'entrée, l'état de chaque serveur préalablement défini comme**Inactif** a été changé en **Actif**. Si la commande comprend un ID d'entrée locale, le serveur spécifié voit son état passer de **Inactif** à **Actif**. Les ID d'entrée sont propres à la base de données du serveur source et doivent faire référence à un objet qui représente un serveur.
!V	Liste	Liste les versions limitées d'eDirectory. Si aucune version n'est listée, cela indique qu'il n'existe aucune restriction. Les versions sont séparées par une virgule.
*Z	Aucun(e)	Affiche les tâches actuellement planifiées.

Messages DSTrace

Vous pouvez filtrer les messages de trace en fonction de leur ID de thread, de leur ID de connexion et de leur gravité.

Après avoir spécifié un filtre pour les messages, seuls les messages qui lui correspondent sont affichés à l'écran. Tous les autres messages pour les balises activées sont consignés dans le fichier `ndstrace.log` s'il est défini sur ON.

Vous ne pouvez appliquer qu'un seul filtre à la fois. Il doit être spécifié pour chaque session de DSTrace.

Par défaut, le niveau de gravité est défini sur INFO, ce qui signifie que tous les messages de niveau supérieur à INFO sont affichés. Pour afficher le niveau de gravité, activez la balise `svty`.

Pour filtrer les messages de trace, vous pouvez également utiliser iMonitor. Pour plus d'informations, reportez-vous à la « Filtrage des messages d'iMonitor » page 293.

Linux

Pour filtrer les messages de trace, procédez comme suit :

1. Activez le filtrage à l'aide de la commande suivante :

   `ndstrace` *`tag filter_value`*

   Pour désactiver le filtrage, entrez la commande suivante :

   `ndstrace` *`tag`*

   Exemples d'activation du filtrage :

   - Pour activer le filtre pour l'ID de thread 35, entrez la commande suivante :

     ```
     ndstrace thrd 35
     ```

   - Pour activer le filtre pour le niveau de gravité FATAL, entrez la commande suivante :

     ```
     ndstrace svty fatal
     ```

     Les niveaux de gravité sont `FATAL`, `WARN`, `ERR`, `INFO` et `DEBUG`.

   - Pour activer le filtre pour l'ID de connexion 21, entrez la commande suivante :

     ```
     ndstrace conn 21
     ```

   Exemples de désactivation du filtrage :

   - Pour désactiver le filtre basé sur l'ID de thread, entrez la commande suivante :

     ```
     ndstrace thrd
     ```

   - Pour désactiver le filtre basé sur l'ID de connexion, entrez la commande suivante :

     ```
     ndstrace conn
     ```

   - Pour désactiver le filtre basé sur la gravité, entrez la commande suivante :

     ```
     ndstrace svty
     ```

Figure 8-5 *Exemple d'écran des messages de trace avec filtres*

```
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 241, size 121, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 120, size 32, err 0.
NCPEng  : INFO    : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 120, size 54, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 22, task 0, seq 121, size 248, err 0.
NCPEng  : INFO    : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent   : DEBUG   : Calling DSAResolveName conn:22 for client .[Public].
Reslv   : DEBUG   : ConvertDNToID: dn=\T=WIN-0510\O=novell\CN=OSG-NTS-2-NDS, cts=4281a5dc:01:001
NCPCli  : DEBUG   : DCCreateContext context 3464002c moduleHandle 60000000 C:\Novell\NDS\ds.dlm, idHandle
00000000
Reslv   : DEBUG   : Connect to tcp:164.99.148.219:524 succeeded
DRL     : INFO    : Primary object is ID_INVALID
NCPCli  : DEBUG   : DCFreeContext context 3464002c idHandle 00000000, connHandle 00001b00, C:\Novell\NDS
\ds.dlm
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 22, task 0, seq 121, size 74, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 242, size 32, err 0.
NCPEng  : INFO    : NCP: 104 (1) - Novell eDirectory Services (Novell eDirectory Ping).
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 242, size 46, flags 0, ncperr
0.
NCPEng  : INFO    : NCP Request from tcp:164.99.148.243, conn 14, task 0, seq 243, size 196, err 0.
NCPEng  : INFO    : NCP: 104 (2) - Novell eDirectory Services (Fragged Request).
Agent   : DEBUG   : Calling DSAStartUpdateReplica conn:14 for client .OSG-NTS-2-NDS.novell.WIN-0510.
Reslv   : DEBUG   : ConvertDNToID: dn=\T=WIN-0510, cts=4281a5dc:01:001
SyncI   : INFO    :  ** SYNCHRONIZATION DISABLED! .WIN-0510., .OSG-NTS-2-NDS.novell.WIN-0510.
Agent   : DEBUG   : DSAStartUpdateReplica failed, synchronization disabled (-701).
NCPEng  : INFO    : NCP Reply to tcp:164.99.148.243, conn 14, task 0, seq 243, size 32, flags 0, ncperr
0.
```

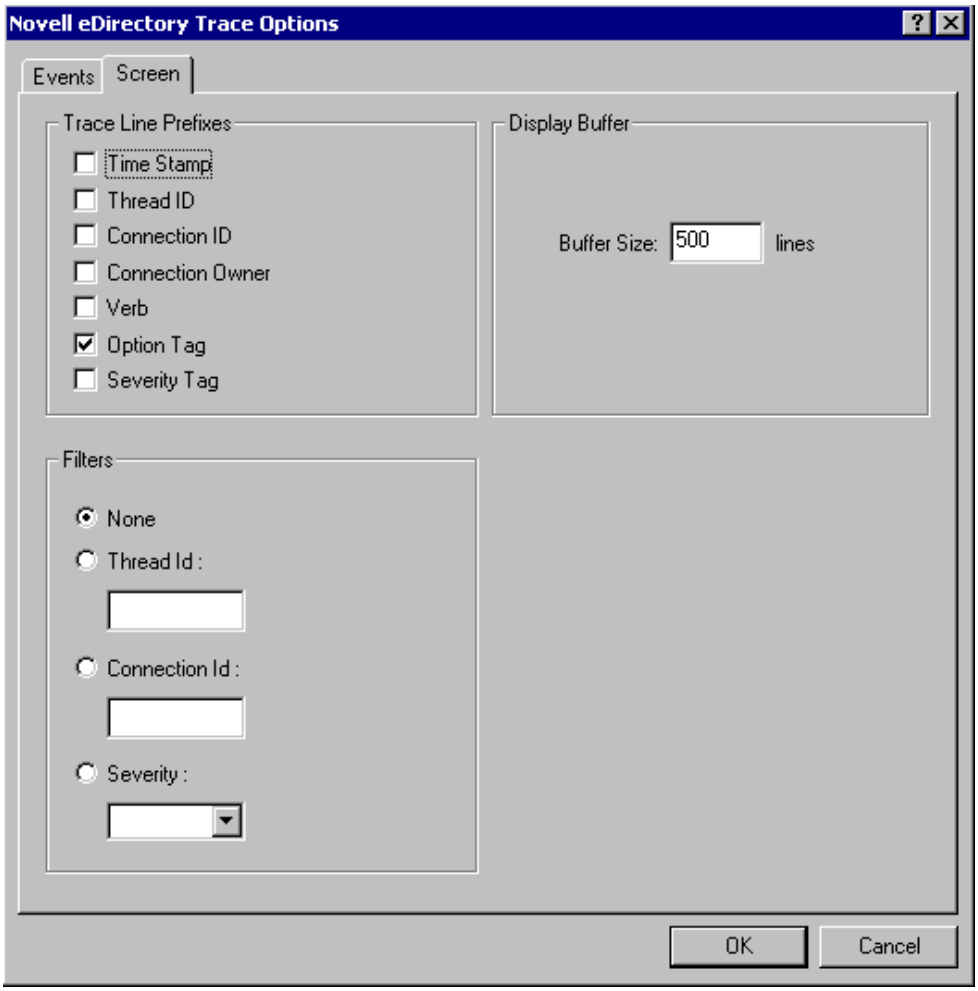
Windows

Pour filtrer les messages de trace, procédez comme suit :

1. Sélectionnez **Démarrer**-> **Panneau de configuration** -> **Services eDirectory**.
2. Dans l'onglet **Services**, sélectionnez **dstrace.dlm**.
3. Cliquez sur **Éditer** > **Options** dans la fenêtre de Trace.

   La boîte de dialogue Options de DS Trace de NetIQ eDirectory apparaît.

Figure 8-6 Écran des options de trace sous Windows



4 Cliquez sur l'onglet **Écran**.

5 Sélectionnez l'option de filtrage dans le groupe **Filtres** et saisissez la valeur du filtre.

Vous pouvez filtrer les messages en fonction des éléments suivants :

- ID du thread
- ID de connexion
- Gravité

Avant de sélectionner l'un des filtres, assurez-vous qu'il est activé sous **Préfixes des lignes de Trace**.

Vous pouvez également désactiver le filtrage en sélectionnant **Aucun** ou en désélectionnant l'option de filtre.

REMARQUE

- si vous avez sélectionné l'option de filtre **ID de thread** ou **ID de connexion** et saisissez une valeur qui n'existe pas, les messages ne s'affichent pas à l'écran. Toutefois, tous les autres messages continuent à être consignés dans le fichier `ndstrace.log`.
- La gravité du niveau de trace ne fonctionne pas sous Windows.

Filtrage des messages d'iMonitor

Vous pouvez filtrer les messages de trace d'iMonitor en fonction de leur ID de connexion, de leur ID de thread ou de leur numéro d'erreur.

Pour filtrer selon les deux premiers éléments, veillez à ce qu'ils soient activés dans l'onglet Configuration de Trace.

Pour plus d'informations, consultez l'aide en ligne d'iMonitor.

Filtrage des messages de SAL

SAL a fait l'objet d'améliorations pour permettre la consignation d'informations détaillées sur les erreurs à la demande. Les appels de fonction peuvent être suivis avec des arguments dans les versions de débogage.

Configuration des niveaux de gravité

Pour configurer les niveaux de gravité des messages de SAL, vous pouvez utiliser le paramètre `SAL_LogLevels`. Cette liste `SAL_LogLevels` répertorie les niveaux de consignation souhaités, séparés par une virgule.

Les niveaux de consignation sont expliqués dans le tableau ci-dessous :

Tableau 8-4 *Paramètres de filtrage des messages de SAL*

Nom du paramètre	Description
`LogCrit`	Messages critiques. Ce niveau est activé par défaut. Après la consignation d'une erreur critique, le système s'arrête.
`LogErr`	Tous les messages d'erreur. Le système continue à fonctionner, mais les résultats sont imprévisibles.
`LogWarn`	Messages d'avertissement. Il s'agit simplement d'un avertissement qui vous informe d'une erreur imminente.
`LogInfo`	Messages d'information.
`LogDbg`	Messages utilisés à des fins de débogage au moment du développement. Ils sont compilés à partir d'une version diffusée pour réduire la taille du binaire.
`LogCall`	Suit les appels de fonction. Il s'agit d'un sous-ensemble des messages de débogage.
`LogAll`	Active tous les messages sauf `LogCall`.

Un signe « - » au début d'un niveau de consignation spécifique désactive ce niveau.

Exemples

Pour effectuer le filtrage en fonction de tous les niveaux du journal, à l'exception de `LogInfo` et de `LogDbg`, procédez comme suit :

Linux

1. Arrêtez `ndsd`.
2. Saisissez la commande suivante :

   ```
   export SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

3. Démarrez `ndsd`.

Windows

1. Arrêtez `DHost`.
2. À l'invite de commande, saisissez la commande suivante :

   ```
   set SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

   ```
   c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
   ```

3. Redémarrez `DHost`.

Définition du chemin de fichier journal

La variable d'environnement `SAL_LogFile` permet de définir l'emplacement du fichier journal. Il peut s'agir d'un nom de fichier valide avec un chemin valide ou de l'une des options suivantes.

- Console : tous les messages sont consignés sur la console.
- Syslog : sous Linux, les messages sont placés dans le journal système. Sous Windows, les messages sont consignés dans un fichier nommé syslog. C'est le comportement par défaut de la consignation.

  Toutes les erreurs critiques sont toujours consignées dans syslog sauf en cas de désactivation spécifique.

9 Configuration de SecretStore pour un serveur eDirectory

Les bibliothèques et les fichiers exécutables SecretStore sont installés par défaut dans le cadre de l'installation d'eDirectory. Toutefois, la configuration de SecretStore est facultative lors d'une nouvelle installation d'eDirectory. Pour la mise à niveau du serveur eDirectory, aucune modification n'est apportée à la configuration existante. Vérifiez que vous étendez le schéma eDirectory pour la fonctionnalité SecretStore sur les plates-formes Linux et Windows à l'aide de la commande suivante :

```
ice -S SCH -f /var/opt/novell/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -s
<serverIP> -d <adminDN>
```

Par exemple, `ice -S SCH -f /var/opt/novell/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -s 1.2.3.4 -d cn=admin,o=administrators`

Pour configurer SecretStore ou annuler sa configuration, utilisez les procédures décrites dans les sections suivantes :

- « Linux » page 295
- « Windows » page 295

Linux

Configuration de SecretStore

Utilisez la procédure suivante pour configurer SecretStore :

1. Pour configurer, exécutez `ssscfg -c`.
2. Ajoutez une entrée `ssncp` au fichier situé à l'emplacement `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` pour charger le module SecretStore par défaut au démarrage d'eDirectory. Vous pouvez également utiliser l'utilitaire `nss` pour charger ou décharger le module SecretStore ultérieurement.

Annulation de la configuration de SecretStore

Pour annuler la configuration, exécutez la commande `ssscfg -d`. Supprimez l'entrée `ssncp` si elle existe à l'emplacement `/etc/opt/novell/eDirectory/conf/ndsmodules.conf`.

Windows

Exécutez les étapes suivantes pour configurer SecretStore ou annuler sa configuration :

1. Pour configurer, exécutez `ssscfg.exe -c.`
2. Pour annuler la configuration, exécutez `ssscfg.exe -d.`

L'utilitaire `ssscfg.exe` existe dans le répertoire `eDirectoryInstallDrive:>\Novell\NDS\` . Pour charger automatiquement le module SecretStore au démarrage du serveur eDirectory, définissez le module `ssncp.dlm` sur `automatique` à partir de l'interface graphique du fichier exécutable `NDSCons.exe`.

10 Fusion d'arborescences NetIQ eDirectory

L'utilitaire de fusion NetIQ eDirectory permet de fusionner deux arborescences NetIQ eDirectory distinctes pour n'en former plus qu'une seule. Seuls les objets Arborescence sont fusionnés ; les objets Conteneur et leurs objets Feuille gardent leur propre identité au sein de la nouvelle arborescence.

SUGGESTION : pour déplacer des objets Feuille ou fusionner des partitions, utilisez NetIQ iManager.

Les deux arborescences que vous fusionnez sont appelées arborescence source locale et arborescence cible. Avant la fusion de deux arborescences, il ne doit rester qu'une seule réplique de la partition racine dans l'arborescence cible, les autres doivent avoir été supprimées. Une fois cette opération effectuée, vous pouvez lancer la fusion. Après la fusion, deux répliques de la partition racine coexistent : celle de l'arborescence cible et celle qui se trouvait sur le serveur de l'arborescence source à l'origine de la fusion. Si vous avez besoin d'autres répliques de la partition racine dans votre arborescence, vous pouvez les intégrer après la fusion.

Si le serveur de l'arborescence cible contient plusieurs répliques de la partition racine au moment de la fusion, les serveurs ne disposant pas de la réplique maîtresse risquent d'avoir des difficultés à placer les objets de référence externe. Ces objets se trouvent dans des racines de partition de référence subordonnée qui doivent être placées sur les autres serveurs disposant d'une réplique de la partition racine afin de représenter les limites de la partition. Pour chaque partition subordonnée à la partition racine de l'arborescence source, une racine de partition de référence subordonnée doit être placée dans l'arborescence cible. En cas d'échec, le code d'erreur eDirectory -605, révélant un problème d'état de synchronisation, sera renvoyé. Dans ce cas, utilisez DSRepair pour réparer la base de données locale sur le serveur qui a généré l'erreur. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale » page 340.

DSMerge ne modifie pas les noms ou contextes eDirectory au sein des conteneurs. Les droits d'objet et de propriété des objets fusionnés sont conservés.

Ce chapitre comprend les rubriques suivantes :

- « fusion des arborescences eDirectory » page 298
- « Greffe d'une arborescence à serveur unique » page 304
- « Changement du nom d'une arborescence » page 310
- « Utilisation du client pour fusionner des arborescences » page 311

fusion des arborescences eDirectory

Pour fusionner des arborescences eDirectory, utilisez l'Assistant de fusion d'arborescence d'iManager. Celui-ci permet de fusionner les racines de deux arborescences eDirectory distinctes. Seuls les objets Arborescence sont fusionnés ; les objets Conteneur et leurs objets Feuille gardent leur propre identité au sein de la nouvelle arborescence.

Les deux arborescences que vous fusionnez sont appelées arborescence source et arborescence cible. L'arborescence cible constitue la destination de l'arborescence source.

DSMerge ne modifie pas le nom des objets au sein des conteneurs. Les droits d'objet et de propriété de l'arborescence fusionnée sont conservés.

- « Conditions préalables » page 298
- « Exigences relatives à l'arborescence cible » page 298
- « Exigences relatives au schéma » page 299
- « Fusion de l'arborescence source avec l'arborescence cible » page 299
- « Modification des partitions » page 299
- « Préparation des arborescences source et cible » page 300
- « Synchronisation des heures avant la fusion » page 301
- « Fusion de deux arborescences » page 302
- « Tâches postérieures à la fusion » page 303

Conditions préalables

- ❒ eDirectory doit être installé sur le serveur contenant la réplique maîtresse de la partition [Root] de l'arborescence source.
- ❒ Les autres serveurs de l'arborescence source doivent faire l'objet d'une mise à niveau vers eDirectory 8.8 ou version ultérieure pour offrir les fonctionnalités appropriées.

REMARQUE : pour supprimer des méthodes de connexion autorisées, utilisez l'outil ldapdelete ou iManager.

Exigences relatives à l'arborescence cible

- ❒ NetIQ eDirectory doit être installé sur le serveur contenant la réplique maîtresse de la partition [Root] de l'arborescence cible. Si ce serveur exécute une autre version des services NDS® ou d'eDirectory, la fusion échoue.
- ❒ Les autres serveurs de l'arborescence cible doivent faire l'objet d'une mise à niveau vers eDirectory 8.8 ou version ultérieure pour offrir les fonctionnalités appropriées.
- ❒ Vous ne pouvez pas mettre à jour des conteneurs qui portent le même nom et sont subordonnés à l'objet Arborescence dans les arborescences source et cible. Avant de fusionner les deux arborescences, vous devez renommer l'un de ces conteneurs.
- ❒ Si les arborescences source et cible contiennent un objet Sécurité, vous devez supprimer l'un de ces objets avant de fusionner les arborescences.

Exigences relatives au schéma

Avant de tenter d'effectuer une opération de fusion, vérifiez que les schémas de chacune des deux arborescences sont strictement identiques. Vous devez exécuter DSRepair sur le serveur contenant la réplique maîtresse de la partition [Racine] de chaque arborescence. Utilisez l'option Importer le schéma à distance afin de vous assurer que chaque arborescence prend en compte l'ensemble des schémas de l'autre arborescence.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Maintenance du schéma**.
3. Indiquez quel serveur effectuera l'opération de maintenance du schéma, puis cliquez sur **Suivant**.
4. Authentifiez-vous auprès du serveur indiqué, puis cliquez sur **Suivant**.
5. Cliquez sur **Importer le schéma à distance** > **Suivant**.
6. Spécifiez le nom de l'arborescence à partir de laquelle le schéma doit être importé.
7. Cliquez sur **Démarrer**.

   Il se peut que vous deviez exécuter cette option sur les arborescences source et cible jusqu'à ce qu'il n'y ait plus de différence entre les schémas. Sinon, la fusion échouera.
8. Lorsque le message « Effectué » s'affiche avec les informations renvoyées par l'opération de maintenance du schéma, cliquez sur **Fermer** pour quitter le processus.

Fusion de l'arborescence source avec l'arborescence cible

Lorsque vous fusionnez les arborescences, les serveurs de l'arborescence source sont intégrés à l'arborescence cible.

L'objet cible Arborescence devient le nouvel objet Arborescence des objets de l'arborescence source et l'arborescence de tous les serveurs de l'arborescence source prend le nom de l'arborescence cible.

Une fois la fusion terminée, le nom d'arborescence des serveurs de l'arborescence cible est conservé.

Les objets qui étaient subordonnés à l'objet Arborescence source deviennent subordonnés à l'objet Arborescence cible.

Modification des partitions

Au cours de la fusion, DSMerge sépare les objets situés sous l'objet Arborescence source en partitions distinctes.

Toutes les répliques de la partition Arborescence sont ensuite retirées des serveurs dans l'arborescence source, à l'exception de la réplique maîtresse. Le serveur qui contenait la réplique maîtresse de l'arborescence source reçoit une réplique de la partition Arborescence de l'arborescence cible.

La Figure 10-1 et la Figure 10-2 illustrent les effets de la fusion de deux arborescences sur les partitions.

Figure 10-1 *Arborescences eDirectory avant la fusion*

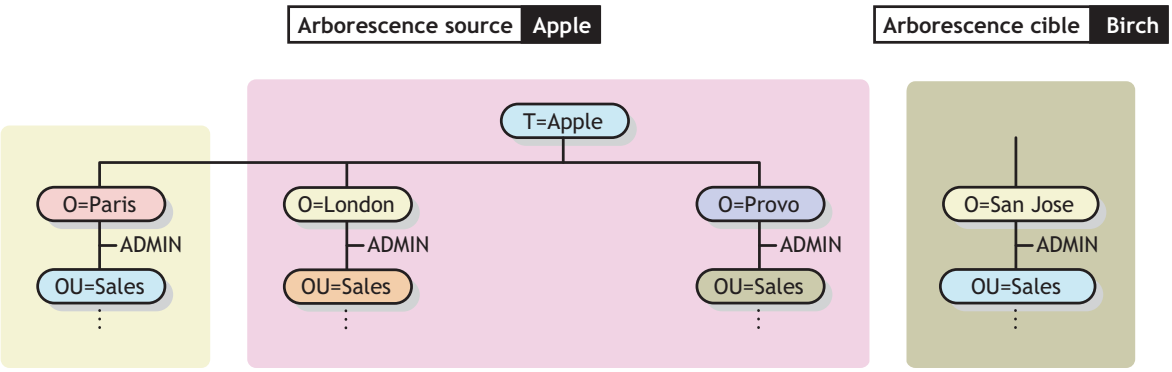
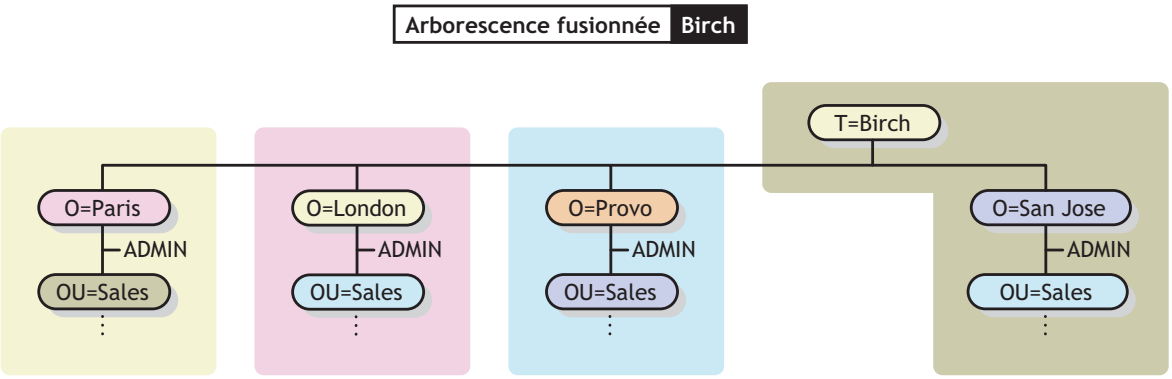


Figure 10-2 *Arborescence eDirectory fusionnée*



Préparation des arborescences source et cible

Avant d'effectuer une fusion, vérifiez que l'état de la synchronisation de l'ensemble des serveurs concernés par cette opération est stable. Le tableau suivant indique les conditions préalables pour préparer les arborescences source et cible à la fusion.

Conditions préalables	Action requise
Vous devez désactiver WANMAN sur tout serveur qui contient une réplique de la partition Arborescence de l'arborescence source ou cible.	Passez en revue la règle WANMAN afin que les restrictions de communication WAN n'interfèrent pas avec la fusion. Si besoin est, désactivez WANMAN avant de commencer la fusion.
Aucun alias ou objet Feuille ne peut exister sur l'objet Arborescence de l'arborescence source.	Supprimez tout alias ou objet Feuille sur l'objet Arborescence de l'arborescence source.

Conditions préalables	Action requise
Les arborescences source et cible ne doivent pas comporter de noms semblables.	Renommez les objets dont le nom est identique sur les arborescences source et cible. Si vous ne souhaitez pas renommer les objets Conteneur, déplacez-les vers un autre conteneur de l'arborescence et supprimez ensuite le conteneur vide avant d'exécuter DSMerge. Pour plus d'informations, reportez-vous au Chapitre 3, « Gestion des objets », page 101. Des objets Conteneur identiques peuvent être présents dans les deux arborescences s'ils ne sont pas immédiatement subordonnés à l'objet Arborescence.
Il ne devrait y avoir aucune connexion via un compte de connexion dans l'arborescence source.	Fermez toutes les connexions dans l'arborescence source.
Les arborescences source et cible doivent utiliser la même version d'eDirectory.	Mettez à niveau tous les serveurs qui contiennent une réplique de la partition racine sur lesquels eDirectory n'est pas encore installé.
L'arborescence cible doit contenir une seule copie de la réplique racine.	Supprimez toutes les répliques de l'arborescence cible, à l'exception de la réplique maîtresse.
Le schéma des arborescences source et cible doit être le même.	Exécutez DSMerge. Si des rapports font état de problèmes au niveau du schéma, utilisez DSRepair pour les faire correspondre. Pour plus d'informations, reportez-vous à la section « Importation du schéma distant » page 351. Exécutez à nouveau DSMerge.
Seule une des deux arborescences peut posséder un conteneur de sécurité subalterne sur la racine de l'arborescence.	Si les arborescences source et cible sont dotées d'un conteneur de sécurité, supprimez-en un en suivant les indications de l'Annexe A, « Considérations relatives à NMAS », page 851.

Étant donné que l'opération de fusion est une transaction unique, elle ne peut pas subir de défaillance catastrophique due à une coupure de courant ou à une panne matérielle. Toutefois, avant d'utiliser DSMerge, effectuez une sauvegarde en bonne et due forme de la base de données eDirectory. Pour plus d'informations, reportez-vous au Chapitre 15, « Sauvegarde et restauration de NetIQ eDirectory », page 443.

Synchronisation des heures avant la fusion

IMPORTANT : Le processus permettant d'obtenir une synchronisation horaire correcte est complexe. Prévoyez suffisamment de temps pour synchroniser les deux arborescences avant de les fusionner.

eDirectory ne fonctionnera pas correctement si les heures des différentes sources horaires utilisées ne concordent pas ou si les serveurs d'une arborescence ne sont pas tous synchronisés.

Avant de procéder à la fusion, vérifiez que l'heure des serveurs des deux arborescences est synchronisée et qu'un seul serveur horaire fait office de source horaire. Toutefois, l'heure de l'arborescence cible peut avancer (de cinq minutes maximum) par rapport à celle de l'arborescence source.

En règle générale, une arborescence ne doit comporter qu'un serveur de référence ou qu'un serveur horaire unique. De même, une arborescence qui vient d'être fusionnée ne doit contenir qu'un serveur de référence ou qu'un serveur horaire unique.

Si chacune des arborescences que vous fusionnez comporte un serveur de référence ou un serveur horaire unique, réassignez l'un d'eux de manière qu'il fasse référence au serveur de référence ou au serveur horaire unique de l'autre arborescence afin d'obtenir un seul serveur de référence ou serveur horaire unique dans l'arborescence finale.

Pour plus d'informations sur les types de serveur horaire, reportez-vous à la section Time Services (Services horaire) du *OES Planning and Implementation Guide* (http://www.novell.com/documentation/oes11/oes_implement_lx/data/time.html) (Guide d'implémentation et de planification d'OES).

Fusion de deux arborescences

Pour obtenir l'ensemble des fonctions des options de menu, exécutez DSMerge sur un serveur qui contient la réplique maîtresse de la partition Arborescence.

Si vous ne savez pas où est stockée la réplique maîtresse, un message vous indique le nom de serveur correct lorsque vous tentez une opération qui requiert cette réplique maîtresse.

Pour effectuer une fusion, utilisez l'une des méthodes suivantes :

- iManager
- Le client à ligne de commande

  Pour plus d'informations, reportez-vous à la « Utilisation du client pour fusionner des arborescences » page 311.

Lors de la fusion d'arborescences volumineuses, vous gagnerez du temps à désigner comme arborescence source celle qui comporte le moins d'objets immédiatement subordonnés à l'objet Arborescence. Cela permet de minimiser le nombre de divisions en partitions lors de la fusion, puisque tous les objets subordonnés à l'objet Arborescence entraînent la création de nouvelles partitions au cours de cette opération.

Le nom de l'arborescence source n'existant plus après la fusion, vous devrez probablement modifier la configuration des postes de travail client. Pour le client Novell pour DOS/Windows, vérifiez les instructions Preferred Tree (Arborescence préférée) et Preferred Server (Serveur préféré) dans les fichiers `net.cfg`. Concernant le client Novell pour Windows, vérifiez les instructions Preferred Tree (Arborescence préférée) et Preferred Server (Serveur préféré) sur la page de propriétés du client.

Si l'instruction Preferred Server est utilisée, le client n'est pas concerné par la fusion ou le changement de nom des arborescences car il continue d'utiliser le nom pour se connecter au serveur. Si l'instruction Arborescence préférée est utilisée, et que l'arborescence est fusionnée ou renommée, alors le nom de l'arborescence disparaît. Seul le nom de l'arborescence cible est conservé après la fusion. Remplacez le nom de l'arborescence préférée par le nom de la nouvelle arborescence.

SUGGESTION : Pour réduire au maximum le nombre de postes de travail client à mettre à jour, désignez comme arborescence cible celle qui comporte le plus grand nombre de postes de travail client, car l'arborescence finale conserve le nom de l'arborescence cible. Vous pouvez également changer le nom de l'arborescence après la fusion pour que le nom de l'arborescence finale corresponde à l'arborescence avec le plus grand nombre de postes de travail client. Pour plus d'informations, reportez-vous à la « Changement du nom d'une arborescence » page 310.

Grâce à la liste suivante de conditions requises, déterminez l'état d'avancement préalable à la fusion :

❒ Vous avez accès au serveur de l'arborescence source via iManager.

- ❒ Vous connaissez le nom et le mot de passe des objets Administrateur disposant de droits d'objet Superviseur sur l'objet Arborescence des deux arborescences à fusionner.
- ❒ La base de données eDirectory des deux arborescences a été sauvegardée.
- ❒ Les serveurs des deux arborescences doivent être synchronisés et utiliser la même source horaire.
- ❒ (Facultatif) Tous les serveurs de l'arborescence sont opérationnels (les serveurs hors service sont automatiquement mis à jour lorsqu'ils sont opérationnels.)
- ❒ Reportez-vous aux conditions préalables à la fusion énumérées dans la section « Préparation des arborescences source et cible » page 300

Le processus de fusion en lui-même ne prend que quelques minutes, mais d'autres variables rallongent la durée d'exécution de cette opération :

- L'objet Arborescence contient de nombreux objets subordonnés qui doivent être divisés en partitions.
- L'arborescence source contient de nombreux serveurs qui requièrent la modification du nom de l'arborescence.

Pour fusionner deux arborescences :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Fusionner l'arborescence**.
3. Indiquez le serveur qui exécutera la fusion (il s'agit de l'arborescence source), puis cliquez sur **Suivant**.
4. Authentifiez-vous auprès du serveur, puis cliquez sur **Suivant**.
5. Spécifiez le nom et le mot de passe d'un administrateur pour l'arborescence source.
6. Spécifiez le nom de l'arborescence cible, le nom et le mot de passe d'un administrateur, puis cliquez sur **Démarrer**.

   La fenêtre d'état de l'Assistant de fusion d'arborescence s'affiche et présente la progression de la fusion.
7. Lorsque le message « Effectué » s'affiche avec les informations renvoyées par l'opération de fusion, cliquez sur **Fermer** pour quitter le processus.

REMARQUE : Ne fusionnez pas deux partitions si l'authentification n'est pas activée pour la partition parente et est activée pour la partition enfant. Cette opération est susceptible de nuire au fonctionnement de l'authentification EBA.

Tâches postérieures à la fusion

Après avoir fusionné deux arborescences, il peut s'avérer nécessaire d'exécuter également les tâches suivantes :

1. Vérifiez que tous les noms d'arborescence ont été correctement modifiés.
2. Vérifiez les partitions nouvellement créées au cours de l'opération de fusion.

   Si la nouvelle arborescence comporte de nombreuses partitions peu volumineuses ou des partitions qui contiennent des informations connexes, vous pouvez les fusionner. Pour plus d'informations, reportez-vous à la « Fusion d'une partition » page 153.

3 Recréez dans l'arborescence tout objet Feuille ou tout alias supprimé avant l'exécution de DSMerge.

4 Évaluez le partitionnement de l'arborescence eDirectory.

   La fusion des arborescences peut changer les exigences de placement des répliques sur la nouvelle arborescence. Évaluez soigneusement le partitionnement et modifiez-le selon les besoins.

5 Mettez à niveau la configuration des postes de travail client.

   Pour le client Novell pour Windows, vérifiez les instructions Preferred Tree (Arborescence préférée) et Preferred Server (Serveur préféré) sur la page de propriétés du client, ou renommez l'arborescence cible.

   Si l'instruction Preferred Server est utilisée, le client n'est pas concerné par la fusion ou le changement de nom des arborescences car il continue d'utiliser le nom pour se connecter au serveur. Si l'instruction Arborescence préférée est utilisée, et que l'arborescence est fusionnée ou renommée, alors le nom de l'arborescence disparaît. Seul le nom de l'arborescence cible est conservé après la fusion. Remplacez le nom de l'arborescence préférée par le nom de la nouvelle arborescence.

La liste ACL (Access Control List - liste de contrôle d'accès) de l'objet Arborescence de l'arborescence source est conservée. Par conséquent, les droits de l'utilisateur Admin de l'arborescence source sur l'objet Arborescence restent valides.

Une fois la fusion terminée, les deux utilisateurs Admin existent toujours et sont identifiés de manière unique par des objets Conteneur différents.

Pour des raisons de sécurité, vous pouvez supprimer l'un des deux objets Utilisateur Admin ou restreindre leurs droits.

Greffe d'une arborescence à serveur unique

L'option **Greffer l'arborescence** permet de greffer l'objet Arborescence d'une arborescence source à serveur unique sous un conteneur spécifié dans l'arborescence cible. Une fois la greffe terminée, l'arborescence source reçoit le nom de l'arborescence cible.

Lors de la greffe, DSMerge transforme la classe d'objet Arborescence de l'arborescence source en Domaine et crée une nouvelle partition. Le nouvel objet Domaine correspond à la racine de partition de la nouvelle partition. Tous les objets situés sous l'objet Arborescence de l'arborescence source se retrouvent désormais sous l'objet Domaine.

L'administrateur de l'arborescence cible dispose de droits sur le conteneur racine de l'arborescence obtenue et, par conséquent, dispose de droits sur la racine greffée de l'arborescence source.

REMARQUE : Plusieurs heures sont parfois requises pour que les droits hérités soient recalculés et qu'ils deviennent effectifs. Cette durée dépend de la complexité, de la taille et du nombre de partitions de l'arborescence.

L'administrateur de l'arborescence source dispose uniquement de droits sur le nouvel objet Domaine créé.

La Figure 10-3 et la Figure 10-4 illustrent les effets de la greffe d'une arborescence sur un conteneur spécifique.

Figure 10-3 *Arborescences eDirectory avant une greffe*

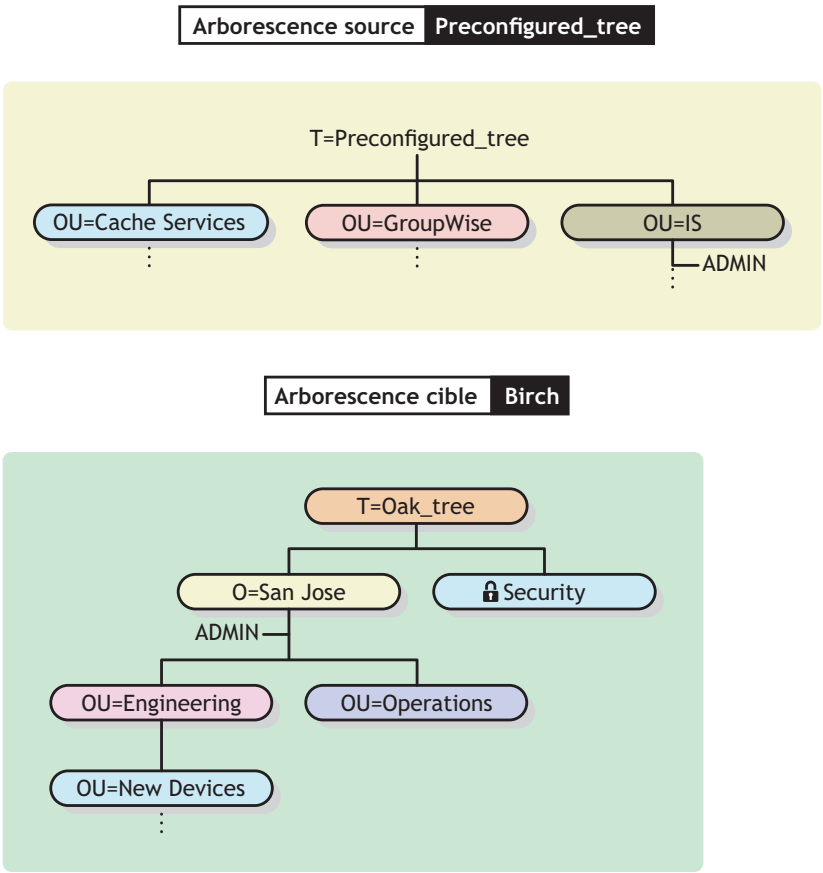
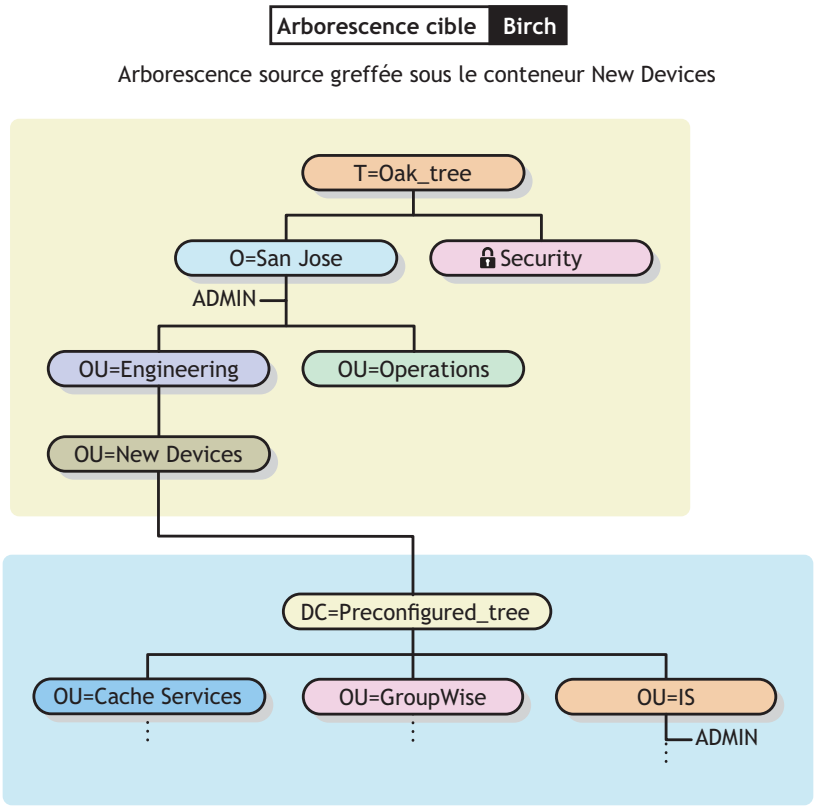


Figure 10-4 *Arborescence eDirectory greffée*



Cette section comprend les informations suivantes :

- « Changement des noms de contexte - Présentation » page 306
- « Préparation des arborescences source et cible » page 307
- « Exigences liées à l'endiguement pour le greffage » page 308
- « Greffe des arborescences source et cible » page 309

Changement des noms de contexte - Présentation

Après la greffe de l'arborescence source dans le conteneur de l'arborescence cible, les noms distinctifs des objets de l'arborescence source sont suivis du nom de l'arborescence source, puis du nom distinctif du nom du conteneur de l'arborescence cible dans lequel l'arborescence source a été fusionnée. Le nom distinctif relatif n'est pas modifié.

Par exemple, si vous utilisez des points comme séparateurs, le nom avec type pour Admin dans l'arborescence source Arbo_préconfigurée est

```
CN=Admin.OU=IS.T=Preconfigured_tree
```

Une fois l'arborescence Arbo_préconfigurée fusionnée dans le conteneur Nouveaux périphériques de l'arborescence Arbo_chêne, le nom avec type de l'Admin est

```
CN=Admin.OU=IS.DC=Preconfigured_tree.OU=Newdevices.
OU=Engineering.O=Sanjose.T=Oak_tree.
```

REMARQUE : le nombre maximal de caractères autorisés dans un nom distinctif quel que soit sont type, en compris un nom distinctif de conteneur DN, est de 255 caractères. Cette limitation est particulièrement importante lorsque vous greffez la racine d'une arborescence sur un conteneur proche du bas de l'arborescence cible.

Le dernier point qui suit Oak_tree (`Oak_tree.`) indique que le dernier élément du nom distinctif est le nom de l'arborescence. Si vous ne mettez pas le point final, ne mettez pas non plus le nom de l'arborescence.

Préparation des arborescences source et cible

Avant de lancer une greffe, vérifiez que l'état de l'ensemble des serveurs affectés par cette opération est stable. Le tableau suivant indique les conditions préalables pour préparer les arborescences source et cible à la greffe.

Conditions préalables	Action requise
L'arborescence source ne doit comporter qu'un serveur.	Ne conservez qu'un serveur dans l'arborescence source.
Aucun alias ou objet Feuille ne peut exister sur l'objet Arborescence de l'arborescence source.	Supprimez tout alias ou objet Feuille sur l'objet Arborescence de l'arborescence source.
Le conteneur de greffage ne peut pas contenir de noms identiques.	Renommez les objets dans le conteneur de greffage de l'arborescence cible ou renommez l'arborescence source. Si vous ne souhaitez pas renommer les objets, déplacez-les d'un conteneur à l'autre de l'arborescence, puis supprimez le conteneur vide avant de lancer DSMerge. Pour plus d'informations, reportez-vous au Chapitre 3, « Gestion des objets », page 101. Des objets Conteneur identiques peuvent être présents dans les deux arborescences s'ils ne sont pas immédiatement subordonnés au même objet parent. Les objets sont identifiés de manière unique par leur objet Conteneur immédiat.
Le conteneur des arborescences source et cible doit exécuter eDirectory version 8.5.1 ou ultérieure.	DSMerge recherche la version appropriée d'eDirectory. Si aucune version compatible ne peut être trouvée, DSMerge renverra une erreur. Pour obtenir la dernière version d'eDirectory, rendez-vous sur la page de téléchargement NetIQ (https://www.netiq.com/products).
Le conteneur pour la jonction de l'arborescence cible se trouve dans une partition qui ne comporte aucune réplique (partition à serveur unique).	Si le conteneur cible contient plusieurs répliques, effectuez l'une des opérations suivantes : ◆ Faites de la partition associée au conteneur la réplique maîtresse, puis supprimez les autres répliques. ◆ Divisez le conteneur de greffe de l'arborescence cible pour en faire une partition distincte, puis supprimez les répliques. Après la greffe, l'association de la partition peut être rétablie.

Conditions préalables	Action requise
Le serveur possédant le conteneur cible doit également comporter une réplique de la partition RACINE.	Si le serveur ne contient aucune réplique de ROOT, la greffe échoue et un message d'erreur `-672 No Access` (-672 Accès refusé) s'affiche, l'annuaire ne pouvant vérifier les droits Administrateur pour l'arborescence cible. Ajoutez une réplique de la partition racine à l'aide d'iManager. Pour plus d'informations, reportez-vous à la section « Ajout d'une réplique » page 156.
Le schéma des arborescences source et cible doit être le même.	Exécutez l'option Greffer l'arborescence dans DSMerge. Si les rapports font état de problèmes avec le schéma, exécutez DSRepair sur l'arborescence cible afin d'importer le schéma depuis l'arborescence source. L'opération de greffe importe automatiquement le schéma depuis l'arborescence source vers l'arborescence cible. Exécutez à nouveau DSMerge.
Seule une des deux arborescences peut posséder un conteneur de sécurité subordonné à la racine de l'arborescence.	Si les arborescences source et cible possèdent un conteneur de sécurité, supprimez-en un en suivant les indications de l'Annexe A, « Considérations relatives à NMAS », page 851.
La référence temporelle de l'arborescence source doit être reconfigurée.	L'arborescence source doit généralement être définie comme serveur secondaire configuré pour obtenir sa source horaire d'un serveur de l'arborescence cible. Pour reconfigurer Timesync, reportez-vous à la section Configuring and Administering Time Synchronization (http://www.novell.com/documentation/oes11/oes_implement_lx/data/time.html#time-cfgnadmin) (Configuration et administration de la synchronisation horaire) du *OES Planning and Implementation Guide* (Guide d'implémentation et de planification d'OES).

Exigences liées à l'endiguement pour le greffage

Pour que vous puissiez greffer une arborescence source sur un conteneur de l'arborescence cible, ce dernier doit être préparé à accepter l'arborescence source. Le conteneur de l'arborescence cible doit être capable de contenir un objet de la classe Domaine. En cas de problème d'endiguement, le message d'erreur `–611 Endiguement interdit` s'affiche pendant l'opération de greffe.

Utilisez les informations contenues dans le tableau suivant afin de déterminer si vous devez exécuter DSRepair pour modifier les listes d'endiguement.

Exigences liées au conteneur de l'arborescence cible	L'objet Domaine doit figurer dans la liste d'endiguement de l'objet Conteneur de l'arborescence cible. Vous pouvez le vérifier en cliquant sur **iMonitor** > **Schéma**. Si l'objet Domaine ne figure pas dans la liste d'endiguement, exécutez DSRepair pour améliorer le schéma.
Exigences liées à l'arborescence source	Avec la greffe, la classe de la racine de l'arborescence source passe de Racine de l'arborescence à Domaine. Toutes les classes d'objets qui sont subordonnées à l'arborescence doivent pouvoir appartenir à la classe Domaine conformément aux règles du schéma. Vous pouvez le vérifier en cliquant sur **iMonitor** > **Schéma**. Si l'objet Domaine ne figure pas dans la liste d'endiguement, exécutez DSRepair pour améliorer le schéma.

Si les conditions liées à l'endiguement ne sont pas respectées, exécutez DSRepair pour corriger le schéma.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Maintenance du schéma**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Améliorations de schéma facultatives**, puis sur **Démarrer**.
6. Suivez les instructions en ligne pour terminer l'opération.

Greffe des arborescences source et cible

Après avoir vérifié que les conditions préalables sont remplies, exécutez la greffe à l'aide de DSMerge.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Greffer l'arborescence**.
3. Indiquez le serveur qui exécutera la greffe (il s'agit de l'arborescence source), puis cliquez sur **Suivant**.
4. Authentifiez-vous auprès du serveur, puis cliquez sur **Suivant**.
5. Spécifiez le nom et le mot de passe de l'administrateur de l'arborescence source. Indiquez le nom de l'arborescence cible, le nom et le mot de passe de son administrateur.
6. Cliquez sur **Démarrer**.

   Une fenêtre d'état de l'Assistant de greffe d'arborescence s'ouvre et affiche la progression de la greffe. Enfin, le message « Terminé » contenant les informations renvoyées par le processus de greffe s'affiche.
7. Cliquez sur **Fermer** pour quitter.

Changement du nom d'une arborescence

Si les deux arborescences à fusionner portent le même nom, vous devez en renommer une.

Vous ne pouvez renommer que l'arborescence source. Pour renommer l'arborescence cible, exécutez l'Assistant Renommer l'arborescence dans NetIQ iManager sur un serveur de l'arborescence cible.

Si vous renommez une arborescence, le contexte de Bindery ne change pas automatiquement. Étant donné que le contexte de Bindery défini dans le fichier `autoexec.ncf` contient également le nom de l'arborescence (par exemple, `SET Bindery Context=O=n.`*`nom_arborescence_test`*), un serveur contenant un nom d'arborescence récemment modifié ne se sert pas du contexte qu'il utilisait avant le changement de nom.

Dès lors, après avoir modifié le nom d'une arborescence, vous devrez probablement modifier la configuration des postes de travail client. Pour le client Novell pour DOS/Windows, vérifiez les instructions Preferred Tree (Arborescence préférée) et Preferred Server (Serveur préféré) dans les fichiers `net.cfg`. Concernant le client Novell pour Windows, vérifiez les instructions Preferred Tree (Arborescence préférée) et Preferred Server (Serveur préféré) sur la page de propriétés du client.

Si l'instruction Preferred Server est utilisée, le client n'est pas concerné par la fusion ou le changement de nom des arborescences car il continue d'utiliser le nom pour se connecter au serveur. Si l'instruction Arborescence préférée est utilisée, et que l'arborescence est fusionnée ou renommée, alors le nom de l'arborescence disparaît. Seul le nom de l'arborescence cible est conservé après la fusion. Remplacez le nom de l'arborescence préférée par le nom de la nouvelle arborescence.

Lorsque vous fusionnez deux arborescences, pour réduire au maximum le nombre de postes de travail client à mettre à jour, désignez comme arborescence cible celle qui contient le plus grand nombre de postes de travail client, car l'arborescence finale conserve le nom de l'arborescence cible.

Vous pouvez également renommer l'arborescence après la fusion pour que le nom de l'arborescence finale corresponde à celui de l'arborescence qui comporte la majorité des postes de travail client.

Une autre option encore consiste à remplacer le nom de l'arborescence fusionnée par le nom de l'arborescence source d'origine. Si vous sélectionnez cette option, vous devez mettre à jour les fichiers `net.cfg` sur les postes de travail client de l'arborescence cible.

Grâce à la liste suivante de conditions requises, déterminez l'état d'avancement préalable à l'attribution du nouveau nom :

- ❒ Accès à une console de serveur dans l'arborescence source ou à une session RCONSOLE définie avec le serveur
- ❒ Le droit d'objet Superviseur sur l'objet Arborescence de l'arborescence source
- ❒ (Facultatif) Tous les serveurs de l'arborescence sont opérationnels (les serveurs hors service sont automatiquement mis à jour lorsqu'ils sont opérationnels.)

Pour renommer l'arborescence :

1. Dans NetIQ iManager, cliquez sur l'option **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Renommer l'arborescence**.
3. Indiquez quel serveur (de l'arborescence cible) doit exécuter l'Assistant Renommer l'arborescence, puis cliquez sur **Suivant**.
4. Authentifiez-vous auprès du serveur, puis cliquez sur **Suivant**.

5 Indiquez un nouveau nom pour l'arborescence ainsi que le nom et le mot de passe d'un administrateur.

6 Cliquez sur **Démarrer**.

Une fenêtre d'état de l'Assistant Renommer l'arborescence s'ouvre et affiche la progression du processus de changement de nom.

7 Lorsque le message « Effectué » contenant les informations renvoyées par le processus de changement de nom s'affiche, cliquez sur **Fermer** pour quitter le processus.

REMARQUE : après avoir renommé une arborescence eDirectory pour laquelle l'authentification EBA est activée, téléchargez le fichier `.eba.p12` à l'aide de l'utilitaire `ebaclientinit`. Pour plus d'informations, reportez-vous à la section « Exécution de l'utilitaire ebaclientinit » page 516.

Utilisation du client pour fusionner des arborescences

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à DSMerge. Le fichier `emboxclient.jar` est installé sur votre serveur dans le cadre de l'installation d'eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client, reportez-vous à la « Utilisation du client à ligne de commande » page 594.

Utilisation de l'outil eMTool DSMerge

1 Exécutez le client en mode interactif en entrant les éléments suivants dans la ligne de commande :

```
java -cp path_to_the_file/emboxclient.jar  -i
```

(Si votre chemin d'accès à la classe contient déjà le fichier `emboxclient.jar`, il vous suffit d'entrer `java -i`.)

L'invite du client apparaît :

```
Client>
```

2 Pour vous connecter au serveur qui exécutera DSMerge (il s'agit de l'arborescence source), entrez la commande suivante :

```
login -sserver_name_or_IP_address -pport_number
-uusername.context -wpassword -n
```

Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option `-n` ouvre une connexion non sécurisée.

Le client indique si la connexion a abouti.

3 Entrez une commande de fusion à l'aide de la syntaxe suivante :

```
dsmerge.options  tâche
```

Par exemple, `dsmerge.m -uadmin -ptest -TApple -Uadmin -Ptest` fusionne l'arborescence cible `Apple` (avec `Admin` comme nom d'utilisateur de l'arborescence cible et `test` comme mot de passe) avec l'arborescence source à laquelle vous êtes actuellement connecté (avec `Admin` comme nom d'utilisateur de l'arborescence source et `test` comme mot de passe).

`dsmerge.g -uadmin -ptest -TOrange -Uadmin -Ptest -CFruit` greffe l'arborescence source à laquelle vous êtes actuellement connecté (avec `Admin` comme nom d'utilisateur de l'arborescence source et `test` comme mot de passe) sur le conteneur `Fruit` de l'arborescence cible `Orange` (avec `Admin` comme nom d'utilisateur de l'arborescence cible et `test` comme mot de passe).

Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

Le client indique la réussite ou l'échec de la fusion.

Pour plus d'informations sur les options de l'outil eMTool DSMerge, reportez-vous à la section « Options de l'outil eMTool DSMerge » page 312.

4 Déconnectez-vous du client en entrant la commande suivante :

```
logout
```

5 Quittez le client en entrant la commande suivante :

```
exit
```

Options de l'outil eMTool DSMerge

Les tableaux suivants répertorient les options de l'outil eMTool DSMerge. Vous pouvez également utiliser la commande `list -t dsmerge` du client pour afficher une liste détaillée des options DSMerge. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services » page 597.

Opération de fusion	Commande du client
Vérifier si l'arborescence peut être renommée	`dsmerge.pr -uUtilisateur -pMot_de_passe_utilisateur -nNouveau_nom_arborescence`
Renommer l'arborescence	`dsmerge.r -uUtilisateur -pMot_de_passe_utilisateur -nNouveau_nom_arborescence`
Vérifier si deux arborescences peuvent être fusionnées	`dsmerge.pm -uUtilisateur_arborescence_source-pMot_de_passe_utilisateur_arborescence_source -TNom_arborescence_cible -UUtilisateur_arborescence_cible -PMot_de_passe_arborescence_cible`
Fusion de deux arborescences	`dsmerge.m -uUtilisateur_arborescence_source-pMot_de_passe_utilisateur_arborescence_source -TNom_arborescence_cible-UUtilisateur_arborescence_cible -PMot_de_passe_arborescence_cible`
Vérifier si l'arborescence source peut être greffée sur le conteneur de l'arborescence cible	`dsmerge.pg -uUtilisateur_arborescence_source -pMot_de_passe_utilisateur_arborescence_source -TNom_arborescence_cible -UUtilisateur_arborescence_cible -PMot_de_passe_arborescence_cible -CConteneur_arborescence_cible`

Opération de fusion	Commande du client
Greffer l'arborescence source sur le conteneur de l'arborescence cible	`dsmerge.g -u`*`Utilisateur_arborescence_source`* `-p`*`Mot_de_passe_utilisateur_arborescence_source`* `-T`*`Nom_arborescence_cible`* `-U`*`Utilisateur_arborescence_cible`* `-P`*`Mot_de_passe_arborescence_cible`* `-C`*`Conteneur_arborescence_cible`*
Annuler l'opération DSMerge en cours	`cancel`

11 Chiffrement des données dans eDirectory

NetIQ eDirectory permet de chiffrer certaines données lorsque les données sont :

- stockées sur le disque ;
- transmises entre plusieurs serveurs eDirectory. Vous bénéficiez ainsi d'une plus grande sécurité pour les données confidentielles.

Pour protéger les données, vous pouvez coder les éléments suivants :

- Attributs : pour protéger les données confidentielles stockées sur le disque.

  Reportez-vous à la « Attributs codés » page 315.
- Réplication : pour protéger les données confidentielles pendant la réplication entre des serveurs eDirectory.

  Reportez-vous à la « Réplication codée » page 325.

IMPORTANT : depuis l'introduction de l'authentification EBA (Enhanced Background Authentication), les données sont chiffrées automatiquement lors de leur réplication entre les serveurs eDirectory activés pour l'authentification EBA. Si l'un des serveurs n'est pas activé pour l'authentification EBA, vous pouvez configurer des stratégies de réplication chiffrée pour chiffrer les données.

Attributs codés

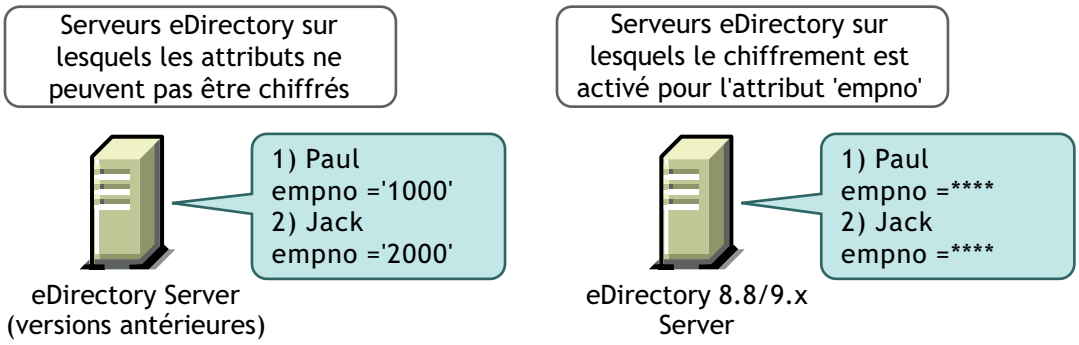
Vous pouvez chiffrer les attributs pour protéger les données lorsqu'elles sont stockées sur le disque. Le chiffrement d'attributs est une fonctionnalité propre au serveur. Vous pouvez utiliser cette fonction lorsque vous souhaitez protéger des données confidentielles, par exemple les numéros de carte de crédit des clients d'une banque.

Si vous codez un attribut, sa valeur est cryptée. Par exemple, vous pouvez chiffrer un attribut `empno` stocké dans la DIB. Si Numéro_employé=1000, la valeur de l'attribut (1000) n'est pas stockée comme du texte clair sur le disque. Vous ne pouvez lire cette valeur codée que lorsque vous accédez à l'annuaire par le biais d'un canal sécurisé.

Tous les attributs d'un schéma peuvent être activés pour le chiffrement. Nous vous recommandons toutefois de ne pas activer l'attribut CN (nom commun) pour le chiffrement et de n'activer pour le chiffrement que les données sensibles. Reportez-vous à la « Règles de sécurité lors du chiffrement de données » page 332 avant de décider de marquer des attributs pour le chiffrement.

Il n'existe pas de limite d'accès aux attributs chiffrés lisibles Public et Serveur. Autrement dit, un client peut accéder à ces attributs en texte clair, mais vous pouvez les marquer pour le chiffrement au niveau de la DIB. L'activation du chiffrement sur un attribut qui est marqué `[Public Read]` (Lecture publique) dans le schéma n'empêche pas qu'il soit ouvert par le biais de méthodes non sécurisées.

Figure 11-1 *Attributs codés*



Les données dans eDirectory peuvent être stockées selon l'une des méthodes suivantes :

- dans la DIB (Data Information Base) ou base de données ;
- sous la forme de données de sauvegarde ;
- sous la forme d'un fichier LDIF.

Pour coder des attributs, vous pouvez créer et appliquer des règles d'attributs codés aux serveurs.

Pour coder les attributs, effectuez les opérations suivantes dans iManager :

1. Créez et définissez une règle d'attributs codés.
   - **1a** Sélectionnez les attributs à coder.
   - **1b** Sélectionnez le modèle de chiffrement pour les attributs.

     Reportez-vous à la section « Création et définition des règles des attributs codés » page 319 pour plus d'informations.
2. Appliquez la règle des attributs codés à un serveur.

   Reportez-vous à la section « Application des règles des attributs codés » page 319 pour plus d'informations.

Vous pouvez également coder des attributs par le biais de LDAP.

Reportez-vous à la section « Gestion des règles des attributs codés via LDAP » page 319 pour plus d'informations.

REMARQUE : l'assignation d'une stratégie d'attributs codés s'applique lors de l'exécution du contrôleur de connectivité (limber).

En guise de meilleure pratique, NetIQ vous recommande d'effectuer les opérations suivantes :

- Ne marquez pour le chiffrement que les attributs sensibles et non l'ensemble des attributs (dont les attributs lisibles Public ou Serveur) .
- Lors du marquage d'un attribut pour chiffrement, utilisez AES puisqu'il s'agit d'un algorithme de chiffrement fort.

La suite de cette section fournit les informations ci-après :

- « Utilisation de modèles de chiffrement » page 317
- « Gestion des règles des attributs codés » page 317
- « Accès aux attributs codés » page 322

- « Affichage des attributs codés » page 323
- « Chiffrement et déchiffrement des données de sauvegarde » page 324
- « Clonage de l'ensemble de fichiers DIB contenant des attributs codés » page 324
- « Ajout de serveurs eDirectory à des anneaux de répliques » page 324
- « Compatibilité avec les versions précédentes » page 324
- « Migration vers des attributs codés » page 325
- « Réplication des attributs codés » page 325

Utilisation de modèles de chiffrement

eDirectory offre les meilleurs niveaux de sécurité pour un attribut grâce à la prise en charge des modèles de codage suivants :

- Standard de chiffrement avancé (AES)
- Triple DES
- Standard de chiffrement des données (DES)

Vous pouvez sélectionner des modèles de codage distincts pour différents attributs d'une même règle d'attributs codés. Par exemple, dans une règle d'attributs codés RC1, vous pouvez sélectionner AES comme modèle de codage pour un attribut Numéro_unité et 3DES pour un attribut Numéro_employé. Reportez-vous à la section « Création et définition des règles des attributs codés » page 319 pour plus d'informations.

Vous pouvez changer le modèle de codage d'un attribut codé en éditant la règle des attributs codés. Vous pouvez également supprimer le chiffrement d'un attribut précédemment codé. Reportez-vous à la section « Édition des règles des attributs codés » page 319 pour plus d'informations.

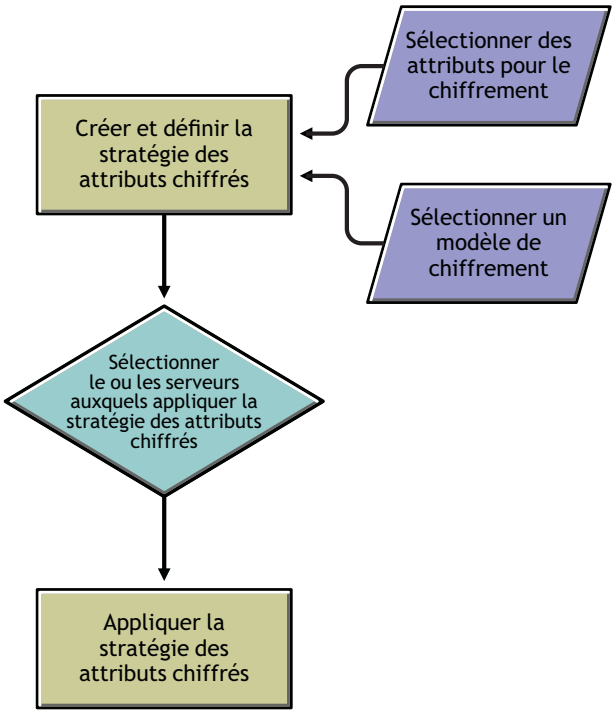
Vous pouvez décider d'affecter des modèles de codage distincts à différents serveurs de l'anneau de répliques. Par exemple, un attribut peut être activé pour le chiffrement AES sur le serveur 1, pour le chiffrement 3DES sur le serveur 2 et sans aucun modèle de chiffrement sur le serveur 3.

Gestion des règles des attributs codés

Pour gérer le chiffrement des attributs, vous pouvez créer des stratégies, puis les définir et les appliquer à des serveurs.

Vous définissez une stratégie d'attributs codés en sélectionnant les attributs à chiffrer ainsi qu'un modèle de chiffrement.

Figure 11-2 *Chiffrement d'attributs*



Vous pouvez gérer les règles des attributs codés à l'aide d'iManager. Cette section contient les informations suivantes :

- « Gestion des règles des attributs codés via iManager » page 318
- « Gestion des règles des attributs codés via LDAP » page 319
- « Copie des règles des attributs codés » page 321
- « Opérations de partition » page 321

Gestion des règles des attributs codés via iManager

Il se compose des sections suivantes :

- « Création et définition des règles des attributs codés » page 319
- « Édition des règles des attributs codés » page 319
- « Application des règles des attributs codés » page 319
- « Suppression des règles des attributs codés » page 319

Si le serveur eDirectory contient des attributs codés, iManager présente le comportement suivant :

1. La lecture, l'affichage ou la modification des attributs codés ne sont pas autorisés par le biais de canaux en texte clair ou sécurisés.
2. Une entrée qui possède des attributs non codés n'est pas autorisée à lire, afficher ou modifier des attributs via iManager par le biais de canaux en texte clair ou sécurisés, ce qui implique le blocage de l'entrée complète.

Création et définition des règles des attributs codés

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Codage eDirectory** > **Attributs de chiffrement**.
3. Dans l'assistant de gestion des stratégies d'attributs codés, sélectionnez **Créer, éditer et assigner la stratégie**.
4. Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour créer et définir la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

Édition des règles des attributs codés

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Codage eDirectory** > **Attributs de chiffrement**.
3. Dans l'assistant de gestion des stratégies d'attributs codés, sélectionnez **Éditer la stratégie**.
4. Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour éditer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

Application des règles des attributs codés

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Codage eDirectory** > **Attributs de chiffrement**.
3. Dans l'assistant de gestion des stratégies d'attributs codés, sélectionnez **Créer, éditer et assigner la stratégie**.
4. Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour appliquer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

Suppression des règles des attributs codés

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Codage eDirectory** > **Attributs de chiffrement**.
3. Dans l'assistant de gestion des stratégies d'attributs codés, sélectionnez **Supprimer les stratégies**.
4. Suivez les instructions de l'Assistant Gestion des règles d'attributs codés pour supprimer la règle.

   L'Assistant fournit l'aide nécessaire tout au long de la procédure.

Gestion des règles des attributs codés via LDAP

IMPORTANT : NetIQ recommande vivement d'utiliser iManager pour la gestion des attributs codés, et non LDAP.

Il se compose des sections suivantes :

- « Création et définition des règles des attributs codés » page 320
- « Édition des règles des attributs codés » page 320

- « Application d'une règle d'attributs codés » page 321
- « Suppression d'une règle d'attributs codés » page 321

REMARQUE : lorsque vous marquez un attribut quelconque pour le cryptage via LDIF, vous devez spécifier la paire attribut/modèle, et non la liste des attributs et le modèle. Il s'agit là de l'actuelle contrainte pour les attributs codés.

Création et définition des règles des attributs codés

1. Créez une stratégie de chiffrement des attributs.

   Par exemple, si la règle des attributs codés est AE Policy- test-server, alors

   ```
   dn: cn=AE Policy - test-server, o=novell
   changetype: add
   objectClass: encryptionPolicy
   ```

2. Ajoutez l'attribut attrEncryptionDefinition à l'objet stratégie que vous avez créé et marquez les attributs pour le chiffrement.

   Par exemple, si le nom de l'attribut à coder est CRID, spécifiez le modèle de codage et le nom de l'attribut comme indiqué ci-dessous :

   ```
   dn: cn=AE Policy - test-server, o=novell
   changetype: modify
   add: attrEncryptionDefinition
   attrEncryptionDefinition: aes$CRID
   ```

   REMARQUE : le nom de l'attribut implique ici son nom NDS. Dans eDirectory, de nombreux attributs ont à la fois un nom LDAP et un nom NDS. Dans ce cas, vous devez spécifier le nom NDS de l'attribut.

   ---

3. Ajoutez l'attribut attrEncryptionRequiresSecure à la règle.

   La valeur de cet attribut indique si un canal sécurisé est toujours requis pour accéder aux attributs codés. La valeur 0 signifie que ce type de canal n'est pas toujours nécessaire. La valeur 1 signifie qu'il est toujours indispensable.

   Par exemple :

   ```
   dn: cn=AE Policy - test-server, o=novell
   changetype: modify
   add: attrEncryptionRequiresSecure
   attrEncryptionRequiresSecure: 0
   ```

4. Associez la règle à un serveur NCP.

   Par exemple, si le serveur NCP est test-server :

   ```
   dn: cn=test-server, o=novell
   changetype: modify
   add: encryptionPolicyDN
   encryptionPolicyDN: cn=AE Policy - test-server, o=novell
   ```

Édition des règles des attributs codés

Le fichier LDIF suivant illustre l'édition d'une règle d'attributs codés par le changement de la valeur de l'attribut attrEncryptionRequireSecure :

```
dn: cn=AE Policy - test-server, o=novell
changetype: modify
replace: attrEncryptionRequiresSecure
attrEncrytionRequiresSecure: 1
```

Application d'une règle d'attributs codés

Le fichier LDIF suivant illustre l'application d'une règle d'attributs codés AE Policy-test-server à un serveur test-server :

```
dn: cn=test-server, o=novell
changetype: modify
add: encryptionPolicyDN
encryptionPolicyDN: cn=AE Policy - test-server, o=novell
```

Suppression d'une règle d'attributs codés

Le fichier LDIF suivant illustre la suppression d'une règle d'attributs codés :

```
dn: cn=AE Policy - test-server, o=novell
changetype: delete
```

REMARQUE : pour plus d'informations sur la gestion des attributs chiffrés via LDAP, reportez-vous à la « Utilisation des outils LDAP sous Linux » page 377 et à la « Utilitaire Importation/Conversion/Exportation NetIQ » page 165.

Copie des règles des attributs codés

Vous pouvez copier les stratégies d'attributs codés pour disposer de configurations identiques sur plusieurs serveurs. Les règles sont stockées sous la forme d'objets dans eDirectory.

Pour une explication détaillée de la procédure de copie d'un objet Règle à l'aide d'iManager, reportez-vous à la section « Copie d'objets » page 105.

Opérations de partition

Lorsque vous fusionnez deux partitions, les règles du parent sont conservées pour la partition résultante. Lorsque vous divisez une partition, la partition enfant hérite la règle de la partition parent.

Recommandation: eDirectory stocke plusieurs attributs pour ses propres opérations, qui ne doivent pas être marqués pour le chiffrement. Si ces attributs sont marqués pour le chiffrement, certaines fonctionnalités d'eDirectory seront probablement interrompues ou ne s'effectueront pas comme prévu.

Les attributs qui ne doivent pas être marqués pour le chiffrement sont :

- federationBoundaryType
- Volume
- ACL
- federationBoundary
- member
- federationControl
- federationSearchPath

- encryptionPolicyDN
- Définition_index
- dgIdentity
- dgAllowUnknown
- agTimeout
- Serveur hôte
- hostResourcePath
- ndsPredicateState
- ndsStatusExternalReference
- ndsStausLimber
- ndsStatusSchema

Bien que la liste ne soit pas exhaustive, les attributs de ce type ne doivent pas être marqués pour le chiffrement.

Accès aux attributs codés

Lorsque vous chiffrez les attributs, vous protégez également l'accès aux attributs codés. eDirectory peut en effet restreindre l'accès aux attributs codés par le biais d'un canal sécurisé, tel qu'un canal sécurisé LDAP ou NCP. Toutefois, seuls les clients NetIQ internes peuvent configurer et utiliser une connexion NCP sécurisée, car l'application DClient, avec laquelle une connexion NCP sécurisée est créée, n'est pas disponible pour un usage public.

Vous pouvez également sauvegarder les attributs codés à l'aide de l'utilitaire de sauvegarde (ndsbackup).

Par défaut, l'accès aux attributs codés est uniquement possible par canal sécurisé.

Toutefois, si vous souhaitez que les clients puissent accéder au format texte clair des attributs chiffrés, désactivez l'option Toujours exiger un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair » page 322.

Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair

Vous pouvez activer ou désactiver l'accès aux attributs chiffrés sur des canaux en texte clair en activant ou désactivant l'option Toujours exiger un canal sécurisé (autrement dit, l'attribut attrEncryptionRequireSecure) à l'aide d'iManager ou de LDAP.

Ce chapitre comprend les informations suivantes :

- « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide d'iManager » page 323
- « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide de LDAP » page 323

Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide d'iManager

Pour activer ou désactiver, à l'aide d'iManager, l'accès aux attributs chiffrés sur des canaux en texte clair, vous devez activer/désactiver l'option Toujours exiger un canal sécurisé dans l'Assistant Gestion des stratégies d'attributs chiffrés lors de :

- Création et définition des stratégies d'attributs codés.
- Édition des stratégies d'attributs codés.

Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair à l'aide de LDAP

Pour activer ou désactiver, à l'aide de LDAP, l'accès aux attributs codés par le biais de canaux en texte clair, vous devez ajouter l'attribut suivant à la règle des attributs codés :

```
attrEncryptionRequiresSecure
```

Si vous définissez cet attribut sur 0, un canal sécurisé n'est pas toujours requis ; autrement dit, vous pouvez accéder aux attributs codés au moyen d'un canal en texte clair. Si vous le définissez sur 1, un canal sécurisé est toujours indispensable ; autrement dit, vous ne pouvez accéder aux attributs codés qu'à l'aide d'un canal sécurisé.

Reportez-vous à l'Étape 3 page 320 pour plus d'informations.

Affichage des attributs codés

L'affichage des attributs chiffrés dépend de l'activation ou de la désactivation de l'option Toujours exiger un canal sécurisé, autrement dit de l'éventuelle nécessité d'utiliser un canal sécurisé pour y accéder.

- « Affichage des attributs codés avec iManager » page 323
- « Affichage des attributs codés avec DSBrowse » page 323
- « Trappes SNMP » page 324

Affichage des attributs codés avec iManager

Si l'option Toujours exiger un canal sécurisé est activée, vous ne pouvez pas afficher les attributs codés. Vous obtenez l'erreur -6089, ce qui signifie que vous avez besoin d'un canal sécurisé pour y accéder.

Dans le cas contraire, vous pouvez afficher les valeurs des attributs chiffrés dans iManager.

Pour plus d'informations, reportez-vous à la section « Exploration d'objets dans l'arborescence » page 257.

Affichage des attributs codés avec DSBrowse

Si vous avez activé l'option Toujours exiger un canal sécurisé, autrement dit, si un canal sécurisé est indispensable pour accéder aux attributs chiffrés, vous ne pouvez pas afficher les attributs de l'entrée qui sont marqués pour le chiffrement. Vous pouvez toutefois voir ceux qui ne sont pas codés.

Trappes SNMP

Les événements Valeur NDS® sont bloqués si vous avez demandé de toujours exiger un canal sécurisé pour accéder aux attributs codés. Les trappes liées à des événements Valeur ont la donnée de valeur NULL et le résultat sera défini sur -6089, ce qui signifie que vous avez besoin d'un canal sécurisé pour obtenir la valeur d'attribut codé. Les trappes ayant la donnée de valeur NULL sont les suivantes :

- ndsAddValue
- ndsDeleteValue
- ndsDeleteAttribute

Chiffrement et déchiffrement des données de sauvegarde

Lors de la sauvegarde de données sur un serveur qui comporte des attributs marqués pour le chiffrement, vous êtes invité à fournir un mot de passe pour le chiffrement/déchiffrement des données de sauvegarde. Ce mot de passe est défini par l'option `-E` dans l'utilitaire de sauvegarde. Pour plus d'informations, reportez-vous à la page `ndsbackup` du manuel.

Pour plus d'informations sur la sauvegarde de vos données, reportez-vous au Chapitre 15, « Sauvegarde et restauration de NetIQ eDirectory », page 443.

Clonage de l'ensemble de fichiers DIB contenant des attributs codés

Lors du clonage, si la base de données eDirectory contient des attributs codés, les valeurs de ces attributs seront également codées dans l'ensemble de fichiers DIB cloné. Afin de sécuriser la clé utilisée par eDirectory pour le chiffrement des valeurs dans cet ensemble, vous devez définir un mot de passe que vous devrez spécifier lorsque vous placerez l'ensemble cloné sur un autre serveur.

Pour plus d'informations, reportez-vous à la section « Cas d'emploi de l'option Cloner l'ensemble DIB » page 263.

Ajout de serveurs eDirectory à des anneaux de répliques

Vous pouvez ajouter des serveurs eDirectory à des anneaux de répliques, que les attributs soient ou non marqués pour le chiffrement sur tout ou partie des serveurs qui hébergent la réplique, ou que l'option Toujours exiger un canal sécurisé soit ou non activée.

Pour plus d'informations sur l'ajout du serveur eDirectory à l'anneau de répliques, reportez-vous à la section « Ajout d'une réplique » page 156.

Compatibilité avec les versions précédentes

Pour accéder aux attributs codés, vous devez changer tous les utilitaires eDirectory, tels que iManager, SNMP, DirXML® et NSureAudit pour les rendre conformes à NCP™ sécurisé. Dans le cas contraire, vous devez indiquer qu'un canal sécurisé n'est pas toujours requis pour y accéder. Reportez-vous à la section « Activation/désactivation de l'accès aux attributs codés par le biais de canaux en texte clair » page 322 pour plus d'informations.

Migration vers des attributs codés

Lors d'une mise à niveau d'eDirectory, vous pouvez chiffrer les attributs existants en créant et en définissant des stratégies d'attributs codés. Pour plus d'informations, reportez-vous à la « Gestion des règles des attributs codés » page 317.

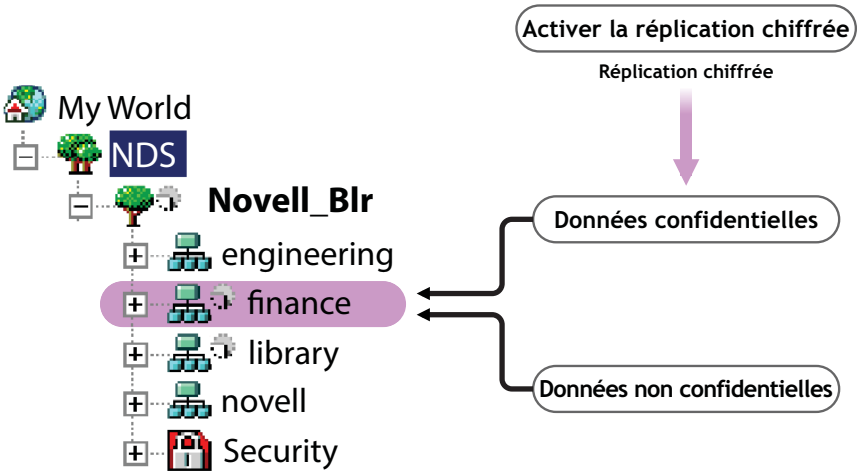
Réplication des attributs codés

Par défaut, la réplication codée n'est pas activée même si le serveur comporte des attributs codés. Vous devez l'activer pour répliquer les attributs codés en toute sécurité. Pour la configuration de la réplication codée, reportez-vous à la « Réplication codée » page 325.

Réplication codée

eDirectory vous permet de chiffrer les données transmises entre des serveurs eDirectory. Cette option offre ainsi un niveau de sécurité élevé pendant la réplication puisque les données ne circulent pas en texte clair.

Figure 11-3 *Réplication codée*



Sur la Figure 11-3, « finance » et « library » sont les partitions de l'arborescence. Il se peut que « finance » contienne des données sensibles à chiffrer lors de la réplication. Vous pouvez dès lors activer la partition « finance » pour la réplication codée. Il est, par contre, inutile d'activer la réplication codée de partitions telles que « library », car elles ne contiennent pas nécessairement de données sensibles.

IMPORTANT : activer la réplication codée pour une partition peut ralentir le processus de réplication. Vous pouvez activer ou désactiver la réplication codée à l'aide d'iManager.

Cette section contient les informations suivantes :

- « Avantage de la réplication codée » page 326
- « Activation de la réplication codée » page 326
- « Ajout d'une nouvelle réplique à un anneau de répliques » page 330
- « Synchronisation et réplication codée » page 331
- « Affichage de l'état de la réplication codée » page 331

Avantage de la réplication codée

Avant eDirectory 8.8, les données étaient transmises sur le réseau pendant la réplication en texte clair. Il convenait alors de protéger les données confidentielles sur le réseau en les codant, surtout si les répliques étaient séparées géographiquement et connectées via Internet.

Cette fonction peut être utilisée dans les scénarios suivants :

- Si les serveurs d'annuaire sont répartis sur différents sites géographiques via WAN et Internet et qu'il est nécessaire de coder les données sensibles sur le réseau.
- Si vous ne souhaitez protéger que certaines partitions de votre arborescence, vous pouvez sélectionner les partitions contenant les données sensibles à coder pour la réplication.
- Si vous avez besoin d'une réplication codée entre certaines répliques d'une partition qui contiennent des données sensibles.
- Si vous pensez que le réseau de votre installation est hostile, vous pouvez protéger les données sensibles pendant la réplication.

Activation de la réplication codée

Pour activer la réplication codée, vous devez lui configurer une partition. Les paramètres de configuration sont stockés dans l'objet Racine de la partition.

Vous pouvez choisir d'activer la réplication codée au niveau de la partition ou de la réplique.

Les configurations au niveau de la réplique priment sur celles au niveau de la partition. Cela signifie que si la réplication codée est :

- activée au niveau de la partition et désactivée pour des répliques spécifiques, la réplication entre les répliques spécifiques s'effectue en texte clair ;
- désactivée au niveau de la partition et activée pour des répliques spécifiques, la réplication entre les répliques spécifiques s'effectue sous forme codée ;

Tableau 11-1 *Remplacement de la configuration de la réplication codée au niveau de la partition*

Niveau de la partition	Niveau de la réplique	Réplication
Activé	Désactivé	Non codés
Désactivé	Activé	Codée

Il se compose des sections suivantes :

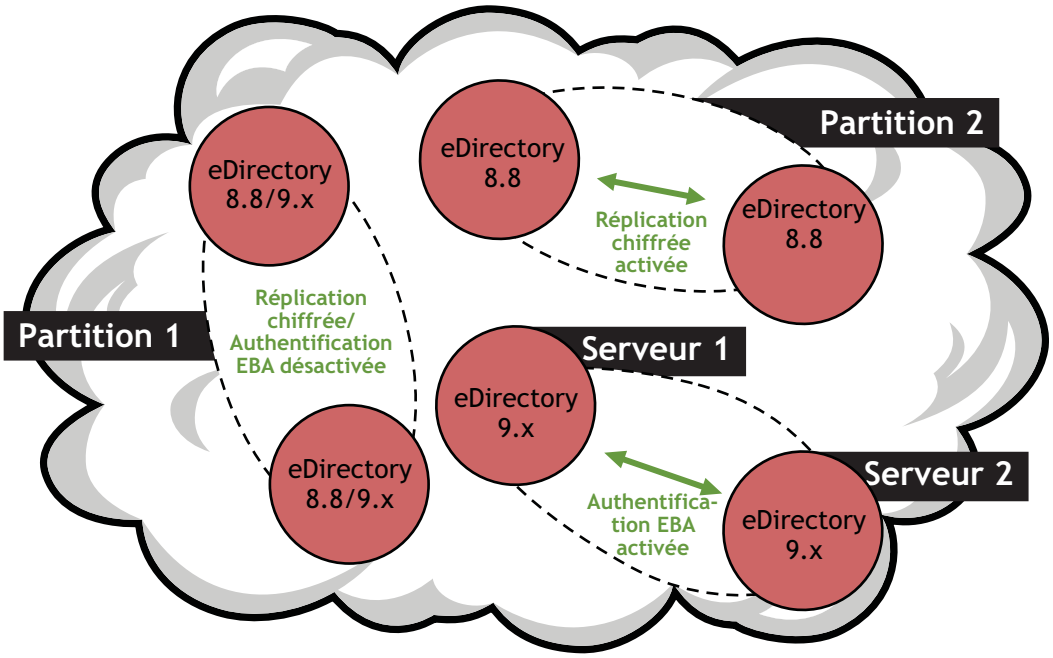
- « Activation de la réplication codée au niveau de la partition » page 326
- « Activation de la réplication codée au niveau de la réplique » page 328

Activation de la réplication codée au niveau de la partition

Lorsque vous activez la réplication codée au niveau d'une partition, la réplication entre toutes les répliques hébergeant la partition est codée. Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Vous pouvez coder la réplication entre toutes les répliques ; toutes les réplications, entrantes et sortantes, seront codées pour ces répliques.

Pour activer une partition pour la réplication codée, tous les serveurs hébergeant cette partition doivent exécuter eDirectory 8.8 ou une version ultérieure.

Figure 11-4 *Réplication codée*



Les configurations pour la réplication codée au niveau de la partition sont ignorées si vous disposez de configurations de ce type au niveau de la réplique. Reportez-vous au Tableau 11-1 page 326.

La compatibilité avec les versions précédentes dépend de l'activation/la désactivation de la réplication codée au niveau de la partition. Reportez-vous à la « Ajout d'une nouvelle réplique à un anneau de répliques » page 330 pour plus d'informations.

Vous pouvez activer la réplication codée au niveau de la partition à l'aide d'iManager ou de LDAP, comme expliqué aux sections suivantes :

- « Activation de la réplication codée au niveau de la partition avec iManager » page 327
- « Activation de la réplication codée au niveau de la partition avec LDAP » page 328
- « Opérations de partition » page 330

Activation de la réplication codée au niveau de la partition avec iManager

1. Cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Codage eDirectory** > **Réplication codée**.
3. Accédez à la partition pour laquelle vous voulez activer la réplication codée ou recherchez-la.
4. Cliquez sur **Suivant**.
5. Dans l'assistant de réplication codée, sélectionnez **Coder toutes les synchronisations de répliques**.

   Vous pouvez obtenir de l'aide via l'Assistant.

   REMARQUE : pour désactiver la réplication codée au niveau de la partition, désélectionnez **Coder toutes les synchronisations de répliques**.

6. Cliquez sur **Terminer**.

Dans l'Assistant de réplication codée, si vous activez la réplication codée pour toute la partition, vous pouvez la désactiver pour des répliques spécifiques. Ces répliques ne recevront et n'enverront pas de données sous forme codée. Vous pouvez également désactiver le chiffrement pour l'ensemble de la partition en désélectionnant **Coder toutes les synchronisations de répliques**.

Activation de la réplication codée au niveau de la partition avec LDAP

IMPORTANT : il est vivement recommandé d'utiliser iManager pour activer la réplication codée.

Pour coder la réplication, vous devez utiliser l'attribut dsEncryptedReplicationConfig. La syntaxe est :

```
enable/disable flag#destination replica number#source replica number
```

Remplacez par l'un de ces drapeaux :

- 0 : désactive la réplication codée
- 1 : active la réplication codée

Les numéros de réplique source et cible représentent les numéros de réplique source et cible d'une partition. Ces numéros peuvent être spécifiés dans n'importe quel ordre, car si la réplication de A vers B est codée, celle de B vers A l'est également.

REMARQUE : si les numéros de réplique source et cible au niveau de la partition sont 0 et si le drapeau est 1, toutes les répliques sont considérées comme activées pour la réplication codée.

Pour activer la réplication codée au niveau de la partition, la valeur de l'attribut dsEncryptedReplicationConfig doit être 1#0#0.

Voici un exemple de fichier LDIF pour l'activation de la réplication codée au niveau de la partition :

```
dn: o=ou
changetype:modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig:1#0#0
```

Ces configurations au niveau de la réplique priment sur celles au niveau de la partition. Reportez-vous à la section « Activation de la réplication codée au niveau de la réplique avec LDAP » page 329 pour plus d'informations.

Activation de la réplication codée au niveau de la réplique

Lorsque vous activez la réplication codée au niveau de la réplique, la réplication, tant entrante que sortante, entre des répliques spécifiques est codée.

Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Vous pouvez coder la réplication entre les répliques R1 et R2 ou entre R2 et R4.

Pour activer la réplication codée entre des répliques d'une partition, vous devez définir entre elles un lien de codage. Reportez-vous à la section « Activation de la réplication codée au niveau de la réplique avec iManager » page 329 pour plus d'informations.

Si vous avez activé la réplication codée pour une réplique, cela signifie que :

- la synchronisation entrante d'un serveur vers cette réplique et
- la synchronisation sortante de cette réplique vers un autre serveur sont codées.

Les répliques activées pour la réplication codée doivent être situées sur des serveurs eDirectory 8.8 ou version ultérieure. Les autres répliques de l'anneau, qui ne sont pas activées pour cette réplication, peuvent se trouver sur des serveurs exécutant des versions antérieures d'eDirectory.

Pour désactiver la réplication codée au niveau de la réplique, vous devez désactiver **Coder le lien** pour les répliques spécifiques à l'aide de l'assistant de configuration de la réplication codée dans iManager.

Vous pouvez activer la réplication codée au niveau de la réplique à l'aide d'iManager ou de LDAP, comme expliqué aux sections suivantes :

- « Activation de la réplication codée au niveau de la réplique avec iManager » page 329
- « Activation de la réplication codée au niveau de la réplique avec LDAP » page 329

Activation de la réplication codée au niveau de la réplique avec iManager

Vous pouvez activer la réplication codée au niveau de la réplique par le biais d'iManager en créant des liens de codage. Ces derniers relient les répliques entre lesquelles la réplication doit être codée. Vous les créez lors de la configuration d'une réplique pour la réplication codée, en sélectionnant une réplique source et une ou plusieurs répliques cibles.

Imaginons, par exemple, que la partition P1 comporte les répliques R1, R2, R3 et R4. Pour coder la réplication entre les répliques R1 et R2, vous devez créer un lien de codage en identifiant l'une d'elles comme la source et l'autre comme la cible.

Une fois les liens de codage créés, vous pouvez choisir de chiffrer ou pas ces liens pour des répliques spécifiques en sélectionnant ou non **Coder le lien** dans l'assistant de configuration de la réplication codée dans iManager. Reportez-vous à la section « Activation de la réplication codée au niveau de la réplique avec iManager » page 329 pour plus d'informations.

Pour activer la réplication codée au niveau de la réplique :

1. Cliquez sur le bouton **Rôles et tâches**  .
2. Cliquez sur **Codage eDirectory** > **Réplication codée**.
3. Accédez à la partition pour laquelle vous voulez activer la réplication codée ou recherchez-la.
4. Cliquez sur **Suivant**.
5. Dans l'assistant de réplication codée, dans le tableau **Synchronisations codées**, cliquez sur **Nouveau** pour définir un lien de codage.
   - **5a** Dans le champ **Sélectionner la réplique source**, spécifiez ou accédez à la réplique que vous souhaitez utiliser comme source.
   - **5b** Dans le champ **Répliques cibles**, spécifiez une ou plusieurs répliques ou accédez à une ou plusieurs répliques que vous souhaitez utiliser comme cible pour la réplication.
   - **5c** Sélectionnez **Coder le lien**.
   - **5d** Cliquez sur **OK**.
6. Cliquez sur **Terminer**.

Activation de la réplication codée au niveau de la réplique avec LDAP

IMPORTANT : il est vivement recommandé d'utiliser iManager pour activer la réplication codée.

Pour chiffrer la réplication, vous devez utiliser l'attribut `dsEncryptedReplicationConfig`. La syntaxe est :

```
enable/disable flag#destination replica number#source replica number
```

Pour plus d'informations sur la syntaxe, reportez-vous à la section « Activation de la réplication codée au niveau de la partition avec LDAP » page 328.

Lorsque vous spécifiez les numéros des répliques dans la syntaxe ci-dessus, vous activez la réplication codée entre celles-ci. Exemples de syntaxe :

- 1#0#1 : la réplication codée est activée à partir de et vers la réplique 1, ainsi que vers et à partir de toutes les autres répliques de la partition.
- 0#3#1 : la réplication codée est désactivée entre les répliques 1 et 3.
- 0#1#1 : la réplication codée est désactivée pour la réplique 1.

Voici un exemple de fichier LDIF qui désactive la réplication codée entre les répliques 1 et 3 :

```
dn: o=ou
changetype: modify
replace: dsEncryptedReplicationConfig
dsEncryptedReplicationConfig: 0#3#1
```

Opérations de partition

Lorsque vous divisez une partition, la configuration de la réplication codée pour la partition parent est héritée par la partition enfant. Lorsque vous fusionnez une partition, cette configuration est conservée pour la partition résultante.

Ajout d'une nouvelle réplique à un anneau de répliques

L'ajout d'une nouvelle réplique à un anneau dépend de l'activation/la désactivation de la réplication codée pour la partition au niveau de cette dernière et de la réplique.

Pour plus d'informations sur l'ajout d'une réplique à un anneau de répliques, reportez-vous à la « Gestion des répliques » page 155.

À chacun de ces niveaux, vous disposez de scénarios différents selon la version du serveur eDirectory à ajouter à l'anneau de répliques, comme expliqué aux sections suivantes :

- « Activation de la réplication codée au niveau de la partition » page 330
- « Activation de la réplication codée au niveau de la réplique » page 331
- « Activation de la réplication codée pour le serveur à ajouter » page 331

Activation de la réplication codée au niveau de la partition

Les scénarios varient en fonction de la version du serveur eDirectory à ajouter.

Scénario	Chiffrement de données
Ajout d'un serveur eDirectory 9.1 ou version ultérieure sans EBA et avec la réplication chiffrée désactivée	Les données sont transférées en texte clair.
Ajout d'un serveur eDirectory 9.1 ou version ultérieure avec la réplication chiffrée et sans EBA	eDirectory chiffre les données en fonction des stratégies de réplication chiffrée.
Ajout d'un serveur eDirectory 9.1 ou version ultérieure avec EBA	Le chiffrement EBA a la priorité sur la réplication codée.

Activation de la réplication codée au niveau de la réplique

Si la réplication codée est activée entre une réplique source et des répliques cibles spécifiques, vous pouvez ajouter un serveur eDirectory 8.8 ou version ultérieure à l'anneau de répliques.

Les scénarios varient si la réplication codée est activée entre une réplique source et toutes les autres répliques de l'anneau. C'est alors une situation similaire à l'ajout de répliques à un anneau pour lequel la réplication codée est activée ou désactivée au niveau de la partition. Reportez-vous à la section « Activation de la réplication codée au niveau de la partition » page 330 pour plus d'informations.

Activation de la réplication codée pour le serveur à ajouter

Si le serveur à ajouter fonctionne sous Linux, vous pouvez utiliser l'option `ndsconfig -E` pour activer la réplication codée sur ce serveur. Pour plus d'informations, reportez-vous aux pages du manuel ndsconfig.

Si le serveur à ajouter fonctionne sous Windows, vous pouvez sélectionner l'option Activer la réplication codée dans l'Assistant d'installation.

Si le serveur à ajouter se trouve sur des plates-formes autres que Linux, vous pouvez activer la réplication codée à l'aide d'iManager ou de LDAP. Reportez-vous à la « Activation de la réplication codée » page 326 pour plus d'informations.

Synchronisation et réplication codée

Si une réplique est activée pour la réplication codée et que les changements de configuration ne sont pas synchronisés avec les autres serveurs, la réplication entre les répliques s'effectue sous forme codée. Celles qui ne sont pas synchronisées avec les changements de configuration pour la réplication codée continuent la synchronisation en texte clair.

Même si la configuration de la réplication codée n'a pas été synchronisée entre les répliques, la réplication entre ces dernières aura lieu sous forme codée.

Affichage de l'état de la réplication codée

Vous pouvez afficher l'état de la réplication codée via iMonitor de la manière suivante :

1. Dans iMonitor, cliquez sur **Synchronisation de l'agent** dans le cadre de l'assistant.
2. Cliquez sur **Synchronisation de réplique** pour la partition à afficher.

Les informations relatives à l'état des répliques s'affichent. Le champ **État de codage** indique si le lien de la réplique à laquelle vous êtes actuellement connecté est chiffré ou non.

En fait, la réplication codée (RC) comporte trois scénarios :

- **RC activée au niveau de la partition :** La réplique à laquelle vous êtes connecté indique que l'**État de codage** est activé.

  Pour déterminer la réplique à laquelle vous êtes connecté, vous devez rechercher dans le cadre de la réplique celle qui n'a pas de lien hypertexte. Si vous parcourez les autres répliques, vous constatez que l'**État de codage** est également marqué comme activé.

- **RC activée au niveau de la réplique :** vous avez activé la RC pour toutes les répliques à partir d'une réplique spécifique (autrement dit, une vers toutes). Dans ce cas, lorsque vous êtes connecté à cette réplique, son **État de codage** est marqué comme activé.

- **RC activée/désactivée pour une combinaison de répliques :** RC activée/désactivée pour une combinaison de répliques - vous avez activé la RC pour l'ensemble de la partition, mais pas pour un groupe sélectionné de serveurs, ou inversement.

  Par exemple, vous avez activé la RC pour la partition A qui compte trois répliques (1, 2 et 3) et l'avez désactivée pour 1 <--> 3. Dans ce cas, si vous êtes connecté à la réplique 1, l'**État de codage** apparaît comme suit :

  Serveur 1 Activé

  Serveur 2

  Serveur 3 Désactivé

  Ce qui signifie que le serveur 1 est activé pour la réplication codée vers tous les serveurs de l'anneau de répliques, mais que 1<-->3 est désactivé par l'administrateur.

Règles de sécurité lors du chiffrement de données

La première règle de base à respecter avant de coder les données est la suivante :

Les informations qui seront codées ne doivent jamais apparaître en texte clair sur le disque dur (ou tout autre support).

Lorsque vous marquez des données en texte clair pour le chiffrement, celles-ci seront certes chiffrées, mais il se peut qu'elles restent présentes en texte clair sur une partie du disque dur qui héberge la DIB.

Des données resteront en texte clair dans certains blocs de la base de données si vous tentez d'effectuer les opérations suivantes :

- Marquage de données en texte clair existantes pour le chiffrement
- Modification du modèle de chiffrement d'un attribut chiffré

Les sections suivantes présentent des scénarios de déploiement pour des données codées ainsi que des procédures permettant de garantir la sécurité de ce type de données :

- « Chiffrement de données dans une toute nouvelle configuration » page 333
- « Chiffrement de données dans une configuration existante » page 333
- « Conclusion » page 335

Chiffrement de données dans une toute nouvelle configuration

Dans le cas d'une nouvelle configuration, vous venez d'installer le système d'exploitation puis eDirectory. Vous êtes certain que le disque dur hébergeant la DIB ne contient pas de données en texte clair.

Respectez la procédure suivante pour garantir la sécurité des données codées dans eDirectory :

1. Déterminez à l'avance les attributs que vous souhaitez coder et le modèle à utiliser.

   En d'autres termes, vous devez décider à l'avance quels attributs vous allez coder avant de charger les données en texte clair dans eDirectory.

   AVERTISSEMENT : une fois que des données en texte clair sont chargées dans eDirectory, vous ne devriez plus marquer d'attribut pour le chiffrement. Vous pouvez certes le faire, mais au risque d'entraîner des problèmes de sécurité.

   ---

2. Configurez eDirectory et définissez les modèles de chiffrement souhaités pour les attributs.
3. Chargez les données existantes sur le nouveau serveur.

   Les deux scénarios les plus probables sont le chargement par lots à partir d'un fichier LDIF ou la réplication avec un autre serveur. Si vous choisissez le chargement par lots, veillez à ne pas copier le fichier LDIF en texte clair sur le disque dur hébergeant la DIB.

   REMARQUE : N'oubliez pas la règle susmentionnée : aucune donnée en texte clair ne peut être écrite sur le disque.

   ---

4. Détruisez toutes les données en texte clair existantes

   Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

Chiffrement de données dans une configuration existante

Ce scénario inclut les opérations suivantes :

- « Conversion de données en texte clair existantes en données codées » page 333
- « Modification du modèle des données codées » page 335

Conversion de données en texte clair existantes en données codées

Vous pouvez marquer pour le chiffrement des données en texte clair et vous assurer de la sécurité des données en utilisant les méthodes suivantes :

- « La réplication : » page 333
- « La sauvegarde et la restauration : » page 334

La réplication :

1. Configurez le chiffrement sur un nouveau serveur en respectant la procédure suivante :

   1a Déterminez à l'avance les attributs que vous souhaitez coder et le modèle à utiliser.

En d'autres termes, vous devez décider à l'avance quels attributs vous allez coder avant de charger les données en texte clair dans eDirectory.

AVERTISSEMENT : une fois que des données en texte clair sont chargées dans eDirectory, vous ne devriez plus marquer d'attribut pour le chiffrement. Vous pouvez certes le faire, mais au risque d'entraîner des problèmes de sécurité.

1b Commencez par une installation nette (incluant probablement le système d'exploitation) sur un disque récemment formaté et partitionné.

Vous êtes ainsi certain qu'il ne contient pas de données en texte clair. En d'autres termes, vous ne pouvez pas vous contenter de réinstaller eDirectory sur un ordinateur ayant contenu des données en texte clair. Vous devez avoir effacé soigneusement toute trace de données sur le disque. Utilisez un logiciel d'effacement sécurisé, un démagnétiseur sur le disque ou tout autre programme de suppression de données avant d'installer eDirectory.

1c Configurez eDirectory et définissez les modèles de chiffrement souhaités pour les attributs.

2 Déplacez ce serveur dans un anneau de répliques contenant les données existantes à coder, effectuez la réplication, puis mettez l'ancien serveur hors ligne.

3 Détruisez toutes les données en texte clair existantes

Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

La sauvegarde et la restauration :

1 Configurez le chiffrement sur un nouveau serveur en respectant la procédure suivante :

1a Déterminez à l'avance les attributs que vous souhaitez coder et le modèle à utiliser.

En d'autres termes, vous devez décider à l'avance quels attributs vous allez coder avant de charger les données en texte clair dans eDirectory.

AVERTISSEMENT : une fois que des données en texte clair sont chargées dans eDirectory, vous ne devriez plus marquer d'attribut pour le chiffrement. Vous pouvez certes le faire, mais au risque d'entraîner les problèmes de sécurité mentionnés à la remarque A.

1b Commencez par une installation à partir de rien (incluant probablement le système d'exploitation) sur un disque récemment formaté et partitionné.

Vous êtes ainsi certain qu'il ne contient pas de données en texte clair. En d'autres termes, vous ne pouvez pas vous contenter de réinstaller eDirectory sur un ordinateur ayant contenu des données en texte clair. Vous devez avoir effacé soigneusement toute trace de données sur le disque. Utilisez un logiciel d'effacement sécurisé, un démagnétiseur sur le disque ou tout autre programme de suppression de données avant d'installer eDirectory.

1c Configurez eDirectory et définissez les modèles de chiffrement souhaités pour les attributs.

2 Restaurez la DIB sauvegardée (qui contient les données en texte clair existantes) sur le nouveau serveur. Vous pouvez sauvegarder la DIB à l'aide de l'option Cloner l'ensemble DIB ou de la sauvegarde à chaud.

3 Détruisez toutes les données en texte clair existantes

Tous les disques (ou autres supports) contenant les données en texte clair doivent être effacés de manière sûre. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement par lots sur le serveur, de tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

Modification du modèle des données codées

Pour réaliser cette modification à l'aide de la sauvegarde et de la restauration, les opérations suivantes sont nécessaires :

1. Modifiez les algorithmes de chiffrement d'un attribut.
2. Effectuez une sauvegarde de la DIB. Vous pouvez sauvegarder la DIB à l'aide de l'option Cloner l'ensemble DIB ou de la sauvegarde à chaud.
3. Restaurez la DIB sauvegardée sur un nouveau serveur et supprimez l'ancien.
4. Détruisez toutes les données en texte clair existantes sur l'ancien serveur pour éviter que des données basées sur l'ancien modèle restent sur le disque dur.

   Tous les disques (ou autre média) avec des données en texte clair doivent être effacés en toute sécurité. Il s'agit notamment du fichier LDIF en texte clair utilisé pour le chargement en bloc du serveur, ou tout autre serveur utilisé pour la réplication ou encore des bandes contenant d'anciennes sauvegardes.

Conclusion

Les scénarios mentionnés ici ne sont pas exhaustifs et le problème peut se poser dans d'autres scénarios. Tant que vous respectez la règle, *Les informations qui seront codées ne doivent jamais apparaître en texte clair sur le disque dur (ou tout autre support)*, les données codées seront parfaitement sécurisées.

12 Réparation de la base de données NetIQ eDirectory

L'utilitaire DSRepair permet de maintenir à jour et de réparer la base de données d'une arborescence eDirectory. Cet utilitaire permet d'effectuer les opérations suivantes :

- corriger les problèmes d'eDirectory tels que les enregistrements erronés, les discordances de schémas, les adresses de serveur incorrectes et les références externes ;
- apporter des changements complexes au schéma eDirectory ;
- vérifier automatiquement la structure de la base de données, sans fermer celle-ci et sans intervention de l'utilisateur ;
- vérifier les index opérationnels de la base de données ;
- Récupération de l'espace libre par suppression des enregistrements vides.
- Répare la base de données locale.
- réparer les répliques, les anneaux de répliques et les objets Serveur ;
- Analyser chaque serveur dans chaque partition locale afin de détecter d'éventuelles erreurs de synchronisation.
- repérer et synchroniser les objets de la base de données locale.

Un certain nombre de problèmes rencontrés par la base de données eDirectory ne sont pas fatals et n'empêchent pas le fonctionnement d'eDirectory. Cependant, si la base de données est endommagée, un message apparaît sur la console ; il indique que le serveur n'a pas pu ouvrir la base de données locale. Dans ce cas, exécutez l'utilitaire de réparation ou contactez le support technique de NetIQ.

NetIQ ne conseille pas d'exécuter les opérations de réparation, excepté en cas de problème avec eDirectory ou sur instruction du service de support de NetIQ. Néanmoins, vous êtes invité à faire appel aux fonctions de diagnostic de l'utilitaire de réparation et d'autres utilitaires NetIQ, tels qu'iMonitor. Pour plus d'informations, reportez-vous au Chapitre 8, « Surveillance d'eDirectory », page 239.

iManager propose les assistants de réparation suivants :

Assistant	Description
Assistant de réparation de base	Permet d'effectuer une réparation complète sans surveillance et de réparer la base de données locale ou un seul objet. Vous pouvez également rechercher d'éventuelles références externes et supprimer les objets Feuille inconnus.
Assistant Fichier journal	Permet d'ouvrir le fichier journal des réparations et d'en définir les options.
Réparer via iMonitor	Permet d'ouvrir iMonitor et d'utiliser les options de réparation proposées par ce programme.

Assistant	Description
Assistant de réparation des répliques	Permet de réparer toutes les répliques ou celles sélectionnées, de réparer les tampons horaires et de déclarer une nouvelle période, de désigner le serveur en cours comme nouvelle réplique maîtresse et de détruire la réplique sélectionnée, si nécessaire.
Assistant de réparation des anneaux de répliques	Permet de réparer tous les anneaux de répliques ou ceux que vous avez sélectionnés, d'envoyer tous les objets vers chaque serveur de l'anneau, de recevoir tous les objets transmis de la réplique maîtresse vers la réplique sélectionnée et, si nécessaire, de supprimer le serveur actuel de l'anneau de répliques.
Assistant de maintenance du schéma	Permet de demander un schéma de l'arborescence, de réinitialiser le schéma local, de déclarer une nouvelle période de schéma, d'apporter des améliorations facultatives au schéma, d'importer un schéma distant et de réaliser une mise à jour du schéma.
Assistant de réparation du serveur	Permet de réparer toutes les adresses réseau ou uniquement celles d'un serveur.
Assistant de réparation de la synchronisation	Permet de synchroniser la réplique sélectionnée sur le serveur actuel, d'indiquer l'état de synchronisation de ce serveur ou de tous les serveurs, d'effectuer une synchronisation horaire et de planifier une synchronisation immédiate.

Grâce aux assistants, vous pouvez réaliser les opérations suivantes :

- « Opérations de réparation de base » page 338
- « Affichage et configuration du fichier journal des réparations » page 342
- « Exécution d'une réparation dans NetIQ iMonitor » page 343
- « Réparation des répliques » page 344
- « Réparation des anneaux de répliques » page 347
- « Maintenance du schéma » page 350
- « Réparation des adresses réseau du serveur » page 352
- « Opérations de synchronisation » page 354
- « Options DSRepair » page 356
- « Utilisation du client pour réparer une base de données » page 361
- « Utilitaire graphique DS Repair » page 363

Opérations de réparation de base

L'Assistant de réparation de base permet d'effectuer une réparation complète sans surveillance, ainsi qu'une réparation de la base de données locale ou d'un seul objet. Vous pouvez également rechercher d'éventuelles références externes et supprimer les objets Feuille inconnus.

- « Réalisation d'une réparation complète sans surveillance » page 339
- « Réparation de la base de données locale » page 340
- « Vérification des références externes » page 341
- « Réparation d'un seul objet » page 341
- « Suppression des objets Feuille inconnus » page 342

Réalisation d'une réparation complète sans surveillance

Cette opération recherche et corrige les erreurs eDirectory les plus graves qui figurent dans les fichiers de base de données eDirectory d'un serveur donné. Cette réparation réalise huit opérations principales, dont aucune ne requiert l'intervention de l'administrateur. Pendant certaines de ces opérations, la base de données locale est verrouillée. La réparation complète sans surveillance génère un ensemble temporaire de fichiers de la base de données locale et effectue les corrections nécessaires par rapport à ces fichiers. De cette manière, en cas de problème grave, les fichiers d'origine demeurent intacts.

Résoudre des problèmes spécifiques est bien plus efficace que d'effectuer une réparation sans surveillance. L'exécution de la réparation complète sans surveillance peut occuper le double de l'espace disque actuellement utilisé par les fichiers de la base de données. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale » page 340.

La reconstitution des index opérationnels utilisés par eDirectory n'est possible que lorsque la base de données locale est verrouillée.

Le tableau ci-dessous liste les opérations réalisées au cours d'une réparation complète sans surveillance :

Opération	Base de données verrouillée ?	Description
Vérifier la structure et l'index de la BdD	Oui	Analyse la structure et le format des enregistrements et des index de la base de données. Cette opération permet de s'assurer qu'aucune altération structurelle n'a été introduite dans l'environnement eDirectory au niveau de la base de données.
Reconstruire toute la base de données	Oui	Élimine les erreurs détectées lors de la vérification de la structure et de l'index. Les structures de données correctes sont rétablies et les fichiers de la base de données et de l'index eDirectory sont recréés.
Vérifier la structure de l'arborescence	Oui	Examine les liens entre les enregistrements de la base de données pour s'assurer qu'à chaque enregistrement enfant correspond un parent valide. Cette opération contribue à garantir la cohérence de la base de données. Les enregistrements non valides sont marqués pour pouvoir être rétablis à partir d'une autre réplique de partition lors de la synchronisation des répliques eDirectory.

Opération	Base de données verrouillée ?	Description
Réparer toutes les répliques locales	Oui	Élimine les incohérences de la base de données eDirectory en comparant chaque objet et attribut aux définitions du schéma. Vérifie également le format de toutes les structures de données internes. Cette opération peut également éliminer les incohérences détectées pendant la vérification de la structure de l'arborescence, via la suppression des enregistrements non valides de la base de données. Ainsi, tous les enregistrements enfants reliés par l'intermédiaire des enregistrements non valides sont marqués comme orphelins. Ces enregistrements orphelins ne sont pas perdus, mais cette opération peut générer de nombreuses erreurs pendant la reconstitution de la base de données. Tout cela est parfaitement normal. Les objets orphelins seront automatiquement réorganisés pendant la synchronisation des répliques.
Réparation des adresses réseau	Non	Compare les adresses réseau du serveur stockées dans eDirectory aux valeurs gérées dans les tables locales SAP, SLP ou DNS pour s'assurer que eDirectory dispose de données correctes. En cas d'incohérence, eDirectory est mis à jour avec les informations correctes.
Valider les fichiers de syntaxe de flux	Oui	Les fichiers de syntaxe de flux, tels que les scripts de connexion, sont stockés dans une zone spéciale de la base de données eDirectory. Cette opération vérifie que chaque fichier de syntaxe de flux est associé à un objet eDirectory valide. Si tel n'est pas le cas, le fichier de syntaxe de flux est supprimé et son attribut de référence purgé.

Pour effectuer une réparation complète sans surveillance :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance d'eDirectory** > **Réparer eDirectory**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Réparation complète sans surveillance**, puis sur **Démarrer**.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation de la base de données locale

Cette option de réparation permet d'éliminer les incohérences dans la base de données locale afin que eDirectory puisse ouvrir cette dernière et y accéder.

Si vous le souhaitez, la réparation de la base de données locale peut s'effectuer sur un ensemble temporaire de fichiers. Sinon, la réparation est effectuée sur la base de données existante.

Pour que la réparation s'effectue sur un ensemble temporaire de fichiers de la base de données, vous devez fermer celle-ci pendant cette partie de l'opération. Si vous décidez de travailler sur un ensemble temporaire de fichiers, vous êtes invité à valider les modifications apportées lors de la réparation pour les rendre permanentes. Dans le cas contraire, les modifications sont appliquées immédiatement.

Après une réparation, vous pouvez afficher le journal des opérations de réparation pour déterminer si d'autres réparations sont nécessaires. Pour plus d'informations, reportez-vous à la « Affichage et configuration du fichier journal des réparations » page 342.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance d'eDirectory** > **Réparer eDirectory**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Réparation de base de données locale**, puis sur **Suivant**.
6. Spécifiez les options de l'opération de réparation locale, puis cliquez sur **Démarrer**.
7. Suivez les instructions en ligne pour terminer l'opération.

Vérification des références externes

Cette option vérifie chaque objet de référence externe afin de déterminer si une réplique contenant l'objet peut être localisée. Si tous les serveurs qui contiennent une réplique de la partition sur laquelle se trouve l'objet sont inaccessibles, l'objet est introuvable. Si l'objet est introuvable, un avertissement est envoyé.

Cette opération fournit également les informations de notice nécrologique.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance d'eDirectory** > **Réparer eDirectory**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Vérifier les références externes**, puis sur **Démarrer**.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation d'un seul objet

Cette opération tente d'éliminer toutes les incohérences dans un objet eDirectory qui pourraient empêcher eDirectory d'accéder à ces données. Elle n'est possible que pour les partitions créées par l'utilisateur et pour la partition de référence externe.

Elle est exécutée sur les fichiers de base de données actifs. Si l'altération se situe au niveau physique, vous pouvez être amené à exécuter une vérification physique et une vérification de structure avant de tenter de réparer l'objet.

Veillez à toujours disposer d'une copie de sauvegarde actualisée de la base de données eDirectory.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance d'eDirectory** > **Réparer eDirectory**.

3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.

5 Cliquez sur **Réparation d'objet unique**, puis sur **Démarrer**.

6 Spécifiez l'objet à réparer, puis cliquez sur **Suivant**.

7 Suivez les instructions en ligne pour terminer l'opération.

Suppression des objets Feuille inconnus

La réparation transforme les objets incohérents en objets inconnus lorsque des propriétés obligatoires font défaut ou lorsqu'ils ne sont pas valides pour d'autres raisons (leurs propriétés ne satisfont pas aux exigences minimales pour un type d'objet). Les objets inconnus sont des objets réels identifiés par eDirectory. Ils sont considérés comme « inconnus » car leur classe n'a pas pu être complètement validée. Vous pouvez supprimer des objets inconnus, représentés par des icônes en forme de point d'interrogation, mais il est difficile de leur rendre leur type d'origine.

Cette réparation supprime tous les objets de la base de données eDirectory locale qui appartiennent à la classe d'objet Inconnu et ne possèdent aucun objet subordonné. La suppression sera ensuite synchronisée avec d'autres répliques de l'arborescence eDirectory.

IMPORTANT : N'effectuez cette opération qu'en parfaite connaissance de cause ou sur instruction du support technique de NetIQ.

---

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Maintenance d'eDirectory** > **Réparer eDirectory**.

3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.

5 Cliquez sur **Supprimer les objets Feuille inconnus**, puis sur **Démarrer**.

6 Suivez les instructions en ligne pour terminer l'opération.

Affichage et configuration du fichier journal des réparations

Le fichier journal des réparations contient des informations détaillées sur les partitions et serveurs locaux. Ces informations vous aident à diagnostiquer l'étendue des dommages causés à la base de données. L'assistant Fichier journal permet d'ouvrir le fichier journal des réparations et d'en définir les options.

Cette section contient des informations sur les opérations suivantes :

- « Ouverture du fichier journal » page 343
- « Définition des options du fichier journal » page 343

Ouverture du fichier journal

Cette opération permet d'afficher le fichier journal des réparations. Le nom par défaut de ce fichier est `dsrepair.log`. Il contient les résultats des opérations réalisées par les réparations.

Vous pouvez activer ou désactiver le fichier journal, le supprimer, le réinitialiser ou le renommer. Pour plus d'informations, reportez-vous à la section « Définition des options du fichier journal » page 343.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Fichier journal**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Ouvrir le fichier journal**, puis sur **Démarrer**.
6. Suivez les instructions en ligne pour terminer l'opération.

Définition des options du fichier journal

Ces options permettent de gérer le fichier journal des réparations. Vous pouvez activer ou désactiver le fichier journal, le supprimer, l'annexer au fichier journal existant ou le renommer.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Fichier journal**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Options du fichier journal**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Exécution d'une réparation dans NetIQ iMonitor

Vous pouvez accéder aux fonctions de réparation à l'aide de l'option **Réparer via iMonitor** de NetIQ iManager. La page Réparer d'iMonitor permet d'afficher les problèmes et de sauvegarder ou de nettoyer la base de données eDirectory.

Dans iMonitor, DSRepair est une fonction centrée sur le serveur. Autrement dit, cette fonction n'est disponible que sur le serveur local qui exécute iMonitor. Si vous tentez d'accéder à cette fonction sur un autre serveur, vous devez basculer sur l'application iMonitor exécutée sur ce serveur.

Vous devez être assimilé à l'administrateur du serveur ou à un opérateur de la console sur le serveur à partir duquel vous essayez d'accéder à la page DS Repair. Par conséquent, vous devez d'abord vous connecter afin que vos références puissent être vérifiées ; ce n'est qu'alors que vous pourrez accéder aux informations de cette page.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparer via iMonitor**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **OK**.

Pour ouvrir iMonitor et exécuter manuellement les options de réparation, cliquez sur **Exécuter iMonitor** et **accédez à l'utilitaire de réparation**, avant de cliquer sur **OK**.

4 Entrez un nom d'utilisateur, un contexte et un mot de passe pour le serveur auquel vous essayez d'accéder, puis cliquez sur **OK** pour ouvrir la page Réparer d'iMonitor.

5 Sélectionnez les options de réparation, puis cliquez sur **Lancer la réparation**.

Pour plus d'informations sur l'utilisation des fonctions de réparation proposées par iMonitor, reportez-vous à la section « Affichage des informations DSRepair » page 256.

Réparation des répliques

La réparation d'une réplique consiste à vérifier la cohérence de chacun des objets qu'elle contient par rapport au schéma et la cohérence de chaque attribut de ces objets par rapport au schéma et aux données en fonction de la syntaxe de l'attribut. D'autres structures de données internes associées à la réplique sont également vérifiées.

Utilisez l'Assistant de réparation des répliques pour effectuer les opérations suivantes :

- « Réparation de toutes les répliques » page 344
- « Réparation de répliques sélectionnées » page 345
- « Réparation des tampons horaires » page 345
- « Désignation d'un serveur comme la nouvelle réplique maîtresse » page 346
- « Destruction de la réplique sélectionnée » page 347

Réparation de toutes les répliques

Cette opération permet de réparer toutes les répliques figurant dans la table des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale » page 340.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Maintenance** > **Réparation des répliques**.

3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.

5 Cliquez sur **Réparer toutes les répliques**, puis sur **Démarrer**.

6 Suivez les instructions en ligne pour terminer l'opération.

Réparation de répliques sélectionnées

Cette opération permet de ne réparer que la réplique sélectionnée dans l'affichage des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale » page 340.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Réparer la réplique sélectionnée**, puis sur **Suivant**.
6. Spécifiez la réplique à réparer, puis cliquez sur **Démarrer**.
7. Suivez les instructions en ligne pour terminer l'opération.

Réparation des tampons horaires

REMARQUE : avant d'effectuer cette opération, exécutez l'Assistant de réparation de la synchronisation pour vérifier que tous les serveurs de l'anneau de répliques communiquent convenablement. Pour plus d'informations, reportez-vous à la « Opérations de synchronisation » page 354.

Cette opération fournit un nouveau point de référence à la réplique maîtresse afin que toutes les mises à jour appliquées aux répliques de la partition sélectionnée soient actualisées.

Cette opération est toujours effectuée sur la réplique maîtresse d'une partition. La réplique maîtresse n'est pas obligatoirement la réplique locale sur ce serveur.

Les tampons horaires, placés sur les objets lors de leur création ou modification, doivent être uniques. Tous les tampons horaires d'une réplique maîtresse sont analysés. Si un tampon horaire est postérieur à l'heure réseau actuelle, il est remplacé par un nouveau. Si le tampon horaire est correct, aucun nouveau tampon n'est émis. Une fois tous les tampons horaires synchronisés, une nouvelle période est définie.

Effectuez cette opération si vous remarquez un écart entre les objets d'une réplique ou entre les propriétés d'un objet. Par exemple, si vous mettez à jour votre script de connexion mais que l'ancien apparaît toujours lorsque vous vous connectez, vérifiez que les répliques sont correctement synchronisées. Si l'écart entre les tampons horaires de l'heure future et de l'heure actuelle se compte en minutes, eDirectory le corrigera de lui-même. La déclaration d'une nouvelle période étant une opération extrêmement coûteuse, il est préférable de ne pas l'utiliser régulièrement.

eDirectory constitue une base de données souple en matière de cohérence ; prévoyez donc cinq à dix minutes avant de vérifier la synchronisation des répliques. Les conséquences de cette opération sont les suivantes :

- Une nouvelle période est définie au niveau de la réplique maîtresse ; elle peut influer sur tous les objets de la réplique.
- Tous les tampons horaires sont examinés et réparés si nécessaire.

- Les mises à jour ne sont pas acceptées de la part de répliques contenant des tampons horaires (périodes) postdatés tant que les répliques ne sont pas synchronisées.|
- Une réplique reçoit une copie de tous les objets d'une réplique maîtresse ou de toute autre réplique pour laquelle une nouvelle période a été définie.
- La période de la réplique devient identique à celle de la réplique maîtresse.
- Les modifications apportées à une période précédente sont perdues.
- Il n'est pas nécessaire que la réplique maîtresse réside sur le serveur actuel, mais vous devez disposer du droit Superviseur sur cette réplique pour pouvoir effectuer la réparation.
- Les autres répliques sont placées dans un nouvel état.

Pour réparer les tampons horaires et déclarer une nouvelle période :

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Réparer les tampons horaires et déclarer une nouvelle période**, puis cliquez sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Désignation d'un serveur comme la nouvelle réplique maîtresse

Cette opération désigne la réplique locale de la partition sélectionnée comme étant la réplique maîtresse. Vous pouvez ainsi désigner une nouvelle réplique maîtresse si l'original est perdu. Une réplique maîtresse peut être perdue si le serveur qui la contient subit une défaillance au niveau du disque dur et doit de ce fait être remplacé.

N'utilisez pas cette option pour réaliser les opérations classiques sur les partitions disponibles dans NetIQ iManager. Pour plus d'informations, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des répliques**.
3. Spécifiez le serveur à désigner comme nouvelle réplique maîtresse, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour vous authentifier auprès du serveur, puis cliquez sur **Suivant**.
5. Cliquez sur **Désigner ce serveur comme nouvelle réplique maîtresse**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Destruction de la réplique sélectionnée

Cette opération permet de supprimer la réplique sélectionnée du serveur actuel. La réplique est supprimée ou transformée en référence subordonnée.

N'utilisez pas cette option pour réaliser les opérations classiques sur les partitions disponibles dans NetIQ iManager. Pour plus d'informations, reportez-vous au Chapitre 6, « Gestion des partitions et des répliques », page 151.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des répliques**.
3. Spécifiez le serveur contenant la réplique à détruire, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour vous authentifier auprès du serveur, puis cliquez sur **Suivant**.
5. Cliquez sur **Détruire la réplique sélectionnée**, puis sur **Suivant**.
6. Spécifiez la réplique à détruire, puis cliquez sur **Suivant**.
7. Suivez les instructions en ligne pour terminer l'opération.

Réparation des anneaux de répliques

La réparation d'un anneau de répliques consiste à vérifier les informations qui correspondent à l'anneau de répliques sur chacun des serveurs contenant une réplique et à valider les informations d'ID à distance.

Utilisez l'Assistant de réparation des anneaux de répliques pour effectuer les opérations suivantes :

- « Réparation de tous les anneaux de répliques » page 347
- « Réparation de l'anneau de répliques sélectionné » page 348
- « Envoi de tous les objets à chaque serveur de l'anneau » page 348
- « Réception de tous les objets de la réplique maîtresse sur la réplique sélectionnée » page 349
- « Suppression d'un serveur de l'anneau de répliques » page 349

Réparation de tous les anneaux de répliques

Cette opération permet de réparer l'anneau de toutes les répliques qui figurent dans la vue Réplique.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale » page 340.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des anneaux de répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Repair All Replica Rings** (Réparer tous les anneaux de répliques), puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation de l'anneau de répliques sélectionné

Cette opération permet de réparer l'anneau de répliques de la réplique sélectionnée affichée dans la table des répliques.

Si vous n'avez pas lancé d'opération Réparation de base de données locale sur la base de données eDirectory locale au cours des 30 dernières minutes, il est conseillé de le faire avant d'effectuer cette nouvelle opération. Pour plus d'informations, reportez-vous à la section « Réparation de la base de données locale » page 340.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des anneaux de répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Repair the Selected Replica Ring** (Réparer l'anneau de répliques sélectionné), puis sur **Suivant**.
6. Spécifiez la réplique à réparer, puis cliquez sur **Suivant**.
7. Suivez les instructions en ligne pour terminer l'opération.

Envoi de tous les objets à chaque serveur de l'anneau

Cette opération permet d'envoyer tous les objets du serveur sélectionné dans l'anneau de répliques vers tous les autres serveurs contenant une réplique de cette partition.

Grâce à cette opération, vous pouvez vérifier si la réplique de partition désignée sur le serveur sélectionné est synchronisée avec les autres serveurs de l'anneau de répliques. Vous ne pouvez pas exécuter cette opération sur un serveur ne contenant qu'une réplique de référence subordonnée de la partition.

Les modifications apportées aux répliques n'ayant pas encore été synchronisées avec la réplique du serveur sélectionné sont perdues. Vérifiez l'état de la synchronisation avant de lancer cette opération.

IMPORTANT : cette opération peut générer un trafic réseau très important lié à la nouvelle création des objets de la réplique. Il ne s'agit pas d'une opération de diagnostic.

---

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des anneaux de répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Entrez un nom d'utilisateur, un mot de passe et un contexte pour le serveur, puis cliquez sur **Suivant**.
5. Cliquez sur **Envoyer tous les objets à chaque serveur de l'anneau**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Réception de tous les objets de la réplique maîtresse sur la réplique sélectionnée

Cette opération permet de recevoir tous les objets de la réplique maîtresse sur la réplique des serveurs sélectionnés.

Grâce à cette opération, vous pouvez vérifier que la réplique de la partition désignée sur le serveur sélectionné dans l'anneau de répliques est synchronisée avec la réplique maîtresse. Vous ne pouvez pas exécuter cette opération sur le serveur contenant la réplique maîtresse.

IMPORTANT : cette opération risque de générer un trafic réseau particulièrement dense. Lorsque vous effectuez cette opération, la réplique actuelle se comporte comme si une nouvelle réplique était placée sur le serveur. Cette opération fait également passer la réplique dans un nouvel état.

---

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des anneaux de répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Entrez un nom d'utilisateur, un mot de passe et un contexte pour le serveur, puis cliquez sur **Suivant**.
5. Cliquez sur **Recevoir tous les objets de la réplique maîtresse sur la réplique sélectionnée**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Suppression d'un serveur de l'anneau de répliques

Cette option enlève un serveur spécifique de la réplique sélectionnée stockée sur le serveur actuel.

AVERTISSEMENT : si vous n'effectuez pas cette opération correctement, vous risquez d'endommager définitivement la base de données eDirectory. N'ayez recours à cette opération qu'à la demande du support technique de NetIQ.

---

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparation des anneaux de répliques**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Entrez un nom d'utilisateur, un mot de passe et un contexte pour le serveur, puis cliquez sur **Suivant**.
5. Cliquez sur **Supprimer ce serveur de l'anneau de répliques**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Maintenance du schéma

Le schéma est un système de règles et de définitions pour les attributs d'objet. Il détermine le contenu et le format de chaque objet, ainsi que les relations entre les objets dans la base de données.

L'Assistant de maintenance du schéma comprend plusieurs opérations de schéma dont vous pouvez avoir besoin pour rendre un schéma de serveur eDirectory conforme à la réplique maîtresse de la racine. Cependant, vous ne devez utiliser ces opérations que lorsque cela s'avère nécessaire. Les opérations de réparation locales et sans surveillance effectuent déjà une vérification du schéma.

Pour plus d'informations sur les objets eDirectory, reportez-vous au Chapitre 5, « Gestion du schéma », page 139.

Utilisez l'Assistant de maintenance du schéma pour effectuer les opérations suivantes :

- « Demande du schéma de l'arborescence » page 350
- « Reconfiguration du schéma local » page 350
- « Améliorations de schéma facultatives » page 351
- « Importation du schéma distant » page 351
- « Déclaration d'une nouvelle période de schéma » page 351

Demande du schéma de l'arborescence

Effectuez cette opération pour que la réplique maîtresse de la racine de l'arborescence synchronise son schéma avec ce serveur. Toutes les modifications apportées au schéma sont répercutées sur ce serveur depuis la réplique maîtresse de la racine pendant 24 heures.

IMPORTANT : Si tous les serveurs demandent ce schéma à la réplique maîtresse, le trafic réseau peut augmenter. Il est par conséquent recommandé d'utiliser cette option avec prudence.

---

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Maintenance du schéma**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Demander le schéma de l'arborescence**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Reconfiguration du schéma local

Cette opération provoque la réinitialisation du schéma qui efface les tampons horaires du schéma local et implique une synchronisation de schéma entrante.

Elle n'est pas disponible si elle est exécutée à partir de la réplique maîtresse de la partition [Root]. Cette restriction évite que tous les serveurs de l'arborescence soient réinitialisés en même temps.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Maintenance du schéma**.

3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Réinitialiser le schéma local**, puis sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Améliorations de schéma facultatives

Cette opération étend et modifie le schéma pour des raisons d'endiguement et pour y apporter d'autres améliorations.

Cette opération implique que ce serveur contient une réplique de la partition [Racine] et que l'état de la réplique est Actif.

Les versions précédentes d'eDirectory ne sont pas en mesure de synchroniser ces modifications.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Maintenance** > **Maintenance du schéma**.
3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Améliorations de schéma facultatives**, puis sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Importation du schéma distant

Cette opération permet de choisir une arborescence eDirectory qui contient le schéma à ajouter à celui de l'arborescence actuelle.

Une fois l'arborescence sélectionnée, le serveur contenant la réplique maîtresse de la partition [Root] est contacté. Le schéma de ce serveur est utilisé pour étendre le schéma sur l'arborescence actuelle.

Pour fusionner deux arborescences, vous devrez peut-être importer plusieurs fois le schéma d'une arborescence vers l'autre. Pour plus d'informations, reportez-vous au Chapitre 10, « Fusion d'arborescences NetIQ eDirectory », page 297.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Maintenance** > **Maintenance du schéma**.
3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Importer le schéma à distance**, puis sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Déclaration d'une nouvelle période de schéma

Une période est un moment sélectionné de façon arbitraire comme point de référence. Elle équivaut à une ère ou à une nouvelle version. Une période contrôle la synchronisation des répliques. Lorsqu'une nouvelle période est définie, elle débute au niveau de la réplique maîtresse. Les autres

répliques ne peuvent pas envoyer de mise à jour à une réplique d'une période plus récente, mais elles reçoivent des mises à jour de sa part jusqu'à ce qu'elles soient parfaitement synchronisées avec elle.

Lorsque d'autres répliques d'une partition donnée sont synchronisées avec la réplique mise à jour, c'est-à-dire lorsque les périodes de chaque réplique sont identiques, la synchronisation bidirectionnelle est à nouveau autorisée.

Lorsque vous définissez une nouvelle période de schéma, la réplique maîtresse de la partition [Root] est contactée et les tampons horaires non autorisés sont réparés dans les enregistrements du schéma. Une nouvelle période de schéma est déclarée sur ce serveur, mais elle s'applique à l'ensemble de l'arborescence.

Tous les autres serveurs reçoivent une nouvelle copie du schéma, ainsi que les tampons horaires réparés.

Si le serveur récepteur contient un schéma non compris dans la nouvelle période, les objets et les attributs qui utilisent l'ancien schéma passent dans la catégorie ou l'attribut d'objet Inconnu.

IMPORTANT : n'effectuez cette opération que sur instruction du support technique de NetIQ.

---

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Maintenance du schéma**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Déclarer une nouvelle période**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Réparation des adresses réseau du serveur

L'Assistant de réparation du serveur permet de réparer toutes les adresses réseau de serveur figurant dans les anneaux de répliques ainsi que les objets Serveur de la base de données locale. Vous pouvez également réparer l'adresse réseau d'un serveur sélectionné dans les anneaux de répliques et les objets Serveur de la base de données locale.

Utilisez l'Assistant de réparation du serveur pour effectuer les opérations suivantes :

- « Réparation de toutes les adresses réseau » page 352
- « Réparation des adresses réseau du serveur » page 353

Réparation de toutes les adresses réseau

Cette opération permet de vérifier l'adresse réseau de tous les serveurs dans la base de données eDirectory locale. Le système recherche le nom de chaque serveur dans les tables SAP, auprès de l'agent Annuaire SLP et dans les informations DNS locales ou distantes, suivant le protocole de transport disponible.

Chaque adresse est ensuite comparée à l'attribut d'adresse réseau de l'objet Serveur eDirectory et à l'enregistrement d'adresse des attributs de réplique des objets [Root] de la partition. Si les adresses sont différentes, elles sont mises à jour de façon à être identiques.

Si l'adresse du serveur est introuvable dans les tables SAP, auprès de l'agent Annuaire SLP et dans les informations DNS locales ou distantes, aucune réparation n'est effectuée.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Maintenance** > **Réparer le serveur**.
3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Réparer toutes les adresses réseau**, puis sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Réparation des adresses réseau du serveur

Cette opération permet de vérifier l'adresse réseau d'un serveur sélectionné dans les fichiers de la base de données eDirectory locale. Le système recherche le nom du serveur dans les tables SAP locales, auprès de l'agent Annuaire SLP ou dans les informations DNS locales ou distantes, suivant les protocoles de transport actuellement liés. L'adresse du serveur est ensuite comparée à l'attribut d'adresse réseau de l'objet Serveur eDirectory et à l'enregistrement d'adresse de chaque attribut de réplique des objets [Root] de la partition. Si les adresses sont différentes, elles sont mises à jour de façon à être identiques.

Si l'adresse du serveur est introuvable dans les tables SAP, auprès de l'agent Annuaire SLP et dans les informations DNS locales ou distantes, aucune autre réparation n'est effectuée.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Maintenance** > **Réparer le serveur**.
3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Réparer les adresses réseau de ce serveur**, puis cliquez sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Problèmes connus

NetIQ SLP est un paquetage facultatif. La fonction d'authentification n'y est pas implémentée.

eDirectory est désormais compatible avec OpenSLP et prend donc en charge ses fonctions d'authentification.

REMARQUE : sous Linux, eDirectory n'écoute pas sur toutes les interfaces, à l'exception de l'adresse IP spécifique mentionnée dans le fichier `nds.conf`. Lorsque vous ajoutez une nouvelle adresse IPV6, veillez à ce que le fichier `nds.conf` contienne bien la nouvelle adresse pour permettre à l'écouteur de démarrer et aux renvois correspondants d'être ajoutés.

Opérations de synchronisation

L'Assistant de réparation de la synchronisation permet de synchroniser la réplique sélectionnée sur le serveur actuel, d'indiquer l'état de synchronisation de ce serveur ou de tous les serveurs, d'effectuer une synchronisation horaire et de planifier une synchronisation immédiate.

Utilisez l'Assistant de réparation de la synchronisation pour effectuer les opérations suivantes :

- « Synchronisation de la réplique sélectionnée sur ce serveur » page 354
- « Indication de l'état de synchronisation sur un serveur » page 354
- « Indication de l'état de la synchronisation sur tous les serveurs » page 355
- « Synchronisation horaire » page 355
- « Planification d'une synchronisation immédiate » page 356

Synchronisation de la réplique sélectionnée sur ce serveur

Cette opération indique l'état de synchronisation complète sur chaque serveur possédant une réplique de la partition sélectionnée.

Vous pouvez ainsi déterminer plus facilement l'état de santé d'une partition. Si tous les serveurs comportant une réplique de la partition se synchronisent correctement, la partition est considérée comme saine. Chaque serveur de l'anneau de répliques est contacté, puis chacun procède à une synchronisation immédiate avec les autres serveurs de l'anneau.

Les serveurs ne se synchronisent pas avec eux-mêmes. Par conséquent, l'état de la réplique du serveur actuel est Hôte.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparer la synchronisation**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5. Cliquez sur **Synchroniser la réplique sélectionnée sur ce serveur**, puis sur **Suivant**.
6. Suivez les instructions en ligne pour terminer l'opération.

Indication de l'état de synchronisation sur un serveur

Cette opération indique l'état de synchronisation des répliques de chaque partition possédant une réplique sur le serveur actuel.

Cette option obtient l'attribut Etat de la synchronisation de l'objet [Root] de la réplique sur chacun des serveurs contenant des répliques des partitions. L'heure de la dernière synchronisation réussie avec tous les serveurs et les erreurs survenues depuis cette synchronisation sont affichées.

Un message d'avertissement apparaît également si la synchronisation n'est pas terminée dans un délai de 12 heures.

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Réparer la synchronisation**.
3. Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.

5 Cliquez sur **Rapporter l'état de la synchronisation** sur ce serveur, puis sur **Suivant**.

6 Suivez les instructions en ligne pour terminer l'opération.

Indication de l'état de la synchronisation sur tous les serveurs

Cette opération indique l'état de synchronisation des répliques de chacune des partitions possédant une réplique sur le serveur actuel.

Cette option obtient l'attribut Etat de la synchronisation de l'objet [Root] de la réplique sur chacun des serveurs contenant des répliques des partitions. L'heure de la dernière synchronisation réussie avec tous les serveurs et les erreurs survenues depuis cette synchronisation sont affichées.

Un message d'avertissement apparaît également si la synchronisation n'est pas terminée dans un délai de 12 heures.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Maintenance** > **Réparer la synchronisation**.

3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.

4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.

5 Cliquez sur **Rapporter l'état de la synchronisation sur tous les serveurs**, puis sur **Suivant**.

6 Suivez les instructions en ligne pour terminer l'opération.

Synchronisation horaire

Cette opération contacte chaque serveur répertorié dans la base de données eDirectory locale et demande des informations sur eDirectory et sur l'état de synchronisation horaire de chaque serveur.

La version d'eDirectory exécutée sur chaque serveur est indiquée dans le champ **Version DS**.

La valeur du champ **Profondeur de la réplique** est -1 si aucune réplique n'est stockée sur un serveur donné. La valeur 0 indique que le serveur contient une réplique de la partition [Root]. Un nombre entier positif signale qu'une réplique existe sur un serveur donné. Il correspond au nombre d'objets qui séparent la racine ([Root]) de la réplique la plus proche.

Tous les serveurs d'une arborescence eDirectory doivent être synchronisés d'après la même source horaire. Si tous les serveurs ne sont pas synchronisés avec la même heure, la synchronisation d'objets entre répliques n'est pas gérée correctement lors de conflits.

L'Assistant de réparation de la synchronisation ne peut pas indiquer la source horaire de chaque serveur ; il signale en revanche le type de serveur horaire. Ces informations peuvent ensuite être utilisées pour déterminer si la synchronisation horaire est lement configurée.

IMPORTANT : plutôt que d'utiliser DSRepair, utilisez NetIQ iMonitor pour surveiller l'état de synchronisation horaire « Nearly-In-Sync » (Presque en synchronisation). Pour plus d'informations, reportez-vous au Chapitre 8, « Surveillance d'eDirectory », page 239.

Pour plus d'informations, reportez-vous à la « Synchronisation des heures réseau » page 100.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Maintenance** > **Réparer la synchronisation**.
3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Synchronisation horaire**, puis sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Planification d'une synchronisation immédiate

Cette opération permet de lancer immédiatement la synchronisation de toutes les répliques. Utilisez-la pour obtenir des informations sur la synchronisation sans attendre que le processus soit exécuté au moment prévu.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2 Cliquez sur **Maintenance** > **Réparer la synchronisation**.
3 Spécifiez le serveur qui effectuera l'opération, puis cliquez sur **Suivant**.
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel l'opération doit être exécutée, puis cliquez sur **Suivant**.
5 Cliquez sur **Planifier une synchronisation immédiate**, puis sur **Suivant**.
6 Suivez les instructions en ligne pour terminer l'opération.

Options DSRepair

Outre les fonctions de réparation disponibles dans NetIQ iManager, les utilitaires DSRepair de chaque plate-forme eDirectory offrent des fonctions avancées insoupçonnables dans le cadre d'une utilisation normale du programme. Ces dernières sont activées par des paramètres spécifiques lors du chargement de l'utilitaire DSRepair sur ces différentes plates-formes.

- « Exécution de DSRepair sur le serveur eDirectory » page 356
- « Options de ligne de commande DSRepair » page 358
- « Utilisation des paramètres DSRepair avancés » page 360

Exécution de DSRepair sur le serveur eDirectory

- « Windows » page 356
- « Linux » page 357

Windows

1 Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**.
2 Cliquez sur **dsrepair.dlm**, puis sur `Démarrer`.

   Pour accéder à DSRepair avec des options avancées, entrez `-a` dans le champ **Paramètres de démarrage** de la console NetIQ eDirectory Services avant de lancer le fichier `dsrepair.dlm`.

Linux

Pour exécuter DSRepair, entrez `ndsrepair` sur la console du serveur en utilisant la syntaxe suivante :

```
ndsrepair {-U |-E |-C |-P [-Ad] |-S [-Ad]|-N |-T |-J <entry_id> [-Ad -AM <attribute name>]} [-A <yes/no>] [-O <yes/no>][-F filename] [-h <local_interface:port>] [--config-file <configuration_file_path>]
```

ou

```
ndsrepair -R [-l yes|no] [-u yes|no] [-m yes|no] [-i yes|no] [-f yes|no][-d yes|no] [-t yes|no] [-o yes|no][-r yes|no] [-v yes|no] [-c yes|no] [-F filename] [-A yes|no] [-O yes|no]
```

IMPORTANT : le paramètre avancé [-Ad] doit être spécifié comme dernier argument. Il est recommandé de n'activer le paramètre avancé -Ad qu'à la demande du support technique de NetIQ. Si le fichier de configuration est fourni comme argument, il doit être spécifié avant le paramètre avancé [-Ad].

Exemples

Pour effectuer une réparation sans surveillance et consigner des événements dans le fichier `/root/ndsrepair.log` ou pour annexer des événements au fichier journal existant, entrez la commande suivante :

```
ndsrepair -U -A no -F /root/ndsrepair.log
```

Pour afficher la liste de toutes les opérations globales de schéma ainsi que des options avancées, entrez la commande suivante :

```
ndsrepair -S -Ad
```

Pour réparer la base de données locale en provoquant son verrouillage, entrez la commande suivante :

```
ndsrepair -R -l yes
```

Pour réparer un objet unique si l'ID d'entrée de l'objet est connu, entrez la commande suivante :

```
ndsrepair -J <entry ID in hex>
```

Pour réparer une réplique ou une partition spécifique, entrez la commande suivante :

```
ndsrepair -P
```

Cette commande renvoie une liste de toutes les partitions présentes sur le serveur. Vous pouvez choisir une partition quelconque pour obtenir la liste des opérations pouvant être effectuées.

Pour afficher des informations sur l'espace disponible dans la base de données qu'il est possible de libérer pour votre usage, entrez la commande suivante :

```
ndsrepair -I
```

Pour réparer des adresses réseau, entrez la commande suivante :

```
ndsrepair -N
```

REMARQUE : l'entrée de la commande `ndsrepair` peut être réacheminée à partir d'un fichier d'options. Il s'agit d'un fichier texte qui contient des options et sous-options liées aux répliques et au fonctionnement des partitions qui n'exigent pas une authentification auprès du serveur. Les options ou sous-options sont séparées par un retour à la ligne. Vérifiez que le contenu du fichier se présente dans le bon ordre. Si ce contenu n'est pas dans le bon ordre, le résultat est imprévisible.

Options de ligne de commande DSRepair

Option	Description
`-U`	Option Réparation complète sans surveillance. Indique à DSRepair de s'exécuter et de quitter sans autre intervention de l'utilisateur. Vous pouvez consulter le fichier journal une fois la réparation effectuée pour connaître les opérations effectuées par DSRepair. Cette option n'est pas une réparation normalement recommandée par défaut. Résoudre des problèmes spécifiques est bien plus efficace que d'effectuer une réparation sans surveillance.
`-P`	Option Opérations de partition et de réplique. Liste les partitions dont des répliques sont stockées dans les fichiers de la base de données eDirectory du serveur actuel. Le menu des options de réplique permet de réparer les répliques, d'annuler une opération de partition, de planifier une synchronisation et de désigner la réplique locale comme réplique maîtresse.
`-S`	Option Opérations globales du schéma. Contient plusieurs opérations de schéma qui pourraient s'avérer nécessaires pour mettre le schéma du serveur en conformité avec la réplique maîtresse de l'objet Arborescence. Cependant, vous ne devez utiliser ces opérations que lorsque cela s'avère nécessaire. Les opérations de réparation locales et sans surveillance effectuent déjà une vérification du schéma.
`-C`	Option de vérification des objets de référence externe. Cette option vérifie chaque objet de référence externe afin de déterminer si une réplique contenant l'objet peut être localisée. Si tous les serveurs qui contiennent une réplique de la partition sur laquelle se trouve l'objet sont inaccessibles, l'objet ne peut pas être trouvé. Si l'objet est introuvable, un avertissement est envoyé.
`-E`	Option Rapporter la synchronisation de la réplique. Cette option indique l'état de synchronisation des répliques de chacune des partitions possédant une réplique sur le serveur actuel. Cette opération lit l'attribut État de la synchronisation de l'objet Arborescence de la réplique sur chacun des serveurs contenant des répliques des partitions. L'heure de la dernière synchronisation réussie avec tous les serveurs et les erreurs survenues depuis cette synchronisation sont affichées. Un message d'avertissement s'affiche si la synchronisation n'est pas terminée dans les douze heures.
`-N`	Option Serveurs connus de cette base de données. Liste tous les serveurs connus de la base de données eDirectory locale. Si le serveur actuel contient une réplique de la partition Arborescence, il affiche la liste de tous les serveurs de l'arborescence eDirectory. Sélectionnez un serveur pour l'exécution des options.

Option	Description
`-J`	Répare un seul objet du serveur local. Vous devez fournir l'ID d'entrée (au format hexadécimal) de l'objet à réparer. Vous pouvez utiliser cette option à la place de Réparation sans surveillance (`-U`) pour réparer un objet endommagé spécifique. L'exécution de l'option Réparation sans surveillance peut prendre plusieurs heures, selon la taille de la base de données. Cette option permet de gagner du temps.
`-T`	Option Synchronisation horaire. Contacte chaque serveur listé dans la base de données eDirectory locale pour lui demander des informations sur son état de synchronisation horaire. Si ce serveur contient une réplique de la partition Arborescence, chaque serveur de l'arborescence eDirectory est interrogé. Indique également la version d'eDirectory exécutée sur chaque serveur.
`-Un fichier`	Option d'ajout au fichier journal existant. Les informations sont ajoutées au fichier journal existant. cette option est activée par défaut.
`-O`	Option de consignation de la sortie dans un fichier. cette option est activée par défaut.
`-F` *`nom_fichier`*	Consigne la sortie dans le fichier spécifié.
`-R`	Option Réparer la base de données locale. Répare la base de données eDirectory locale. Cette option de réparation résout les incohérences existant dans la base de données locale afin d'en permettre l'ouverture et l'accès par eDirectory. Elle est associée à des sous-options qui facilitent les opérations de réparation réalisées sur la base de données. Cette option comporte des modificateurs de fonction qui sont décrits dans le tableau ci-dessous.
`-I`	Affiche des informations sur l'espace disponible dans la base de données qu'il est possible de libérer pour votre usage. eDirectory vous permet de récupérer les enregistrements vides et de réutiliser l'espace disponible à l'aide de l'option Récupérer de la commande ndsrepair.

Les modificateurs de fonction utilisés avec l'option `-R` sont décrits ci-après :

Option	Description
`-l`	Verrouille la base de données eDirectory durant la réparation.
`-u`	Utilise une base de données eDirectory temporaire lors de la réparation. Invite l'utilisateur à enregistrer ou rejeter les modifications et à afficher le fichier journal.
`-m`	Option de maintien de la base de données initiale non réparée.
`-i`	Vérifie la structure et l'index de la base de données eDirectory.
`-f`	Option de récupération de l'espace libre dans la base de données.
`-d`	Option de reconstitution de l'ensemble de la base de données.
`-t`	Vérifie la structure de l'arborescence. Précisez Oui pour vérifier que tous les liens de l'arborescence à la base de données sont corrects. Indiquez Non pour ignorer cette vérification. Valeur par défaut = Yes.
`-o`	Option de reconstitution du schéma opérationnel.
`-r`	Option de réparation de toutes les répliques locales.
`-v`	Option de validation des fichiers de flux.
`-c`	Option de vérification des références locales.

Utilisation des paramètres DSRepair avancés

AVERTISSEMENT : Les fonctions décrites dans cette section peuvent causer des dommages irréparables à votre arborescence eDirectory si elles ne sont pas correctement utilisées. N'exécutez ces fonctions que sur instruction du support technique de NetIQ.

Effectuez une sauvegarde complète d'eDirectory sur le serveur avant d'utiliser ces fonctions dans un environnement de production. Pour plus d'informations, reportez-vous au Chapitre 15, « Sauvegarde et restauration de NetIQ eDirectory », page 443.

Sous Linux, entrez `ndsrepair -R -Ad -XK2`.

Sous Windows, entrez ces options dans le champ **Paramètres de démarrage** de NDSConsole avant de lancer `dsrepair.dlm`. Reportez-vous à la section « Exécution de DSRepair sur le serveur eDirectory » page 356 pour plus d'informations.

Basculement	Description
`-P`	Marque tous les objets eDirectory de type Inconnu comme étant référencés. Les objets référencés ne participent pas à la synchronisation des répliques dans eDirectory.
`-WM`	Dans de nombreux cas, l'attribut WM: Registered Workstations prend une valeur très élevée en cas d'utilisation de ZENworks® 2.0. L'exécution de DSRepair avec -WM supprime ces valeurs élevées.
`-XK2`	Supprime tous les objets eDirectory dans la base de données eDirectory de ce serveur. Cette opération permet de détruire une réplique altérée qui ne peut être supprimée autrement.

Basculement	Description
-XK3	Supprime toutes les références externes dans la base de données eDirectory de ce serveur. Cette opération permet de détruire toutes les références externes d'une réplique défectueuse. Si les références sont à l'origine du problème, eDirectory peut les recréer afin de rétablir le bon fonctionnement de la réplique.
-RC	Sauvegarde la DIB. Cette option n'est disponible que sous Windows.
-OT	Applique des tampons horaires aux notices nécrologiques pendant une réparation locale de la base de données. Toutes les notices nécrologiques reçoivent un tampon horaire sauf INHIBIT MOVE.
-NLD	Supprime IRF des objets NLS:Certificat de licence et NLS:Conteneur du produit.
-AM	Déplace les attributs qui répondent aux critères spécifiques vers un autre conteneur dans la base de données FLAIM. Pour plus d'informations sur les attributs eDirectory qui répondent aux critères pour être déplacés vers un autre conteneur, reportez-vous à la section Mise en conteneur des attributs FLAIM du Guide d'optimisation de NetIQ eDirectory.
-AH	Ne crée pas les fichiers NDO lorsque la taille DIB est inférieure à 1 Go et que les anciens fichiers NDO ont plus de 72 heures.

Utilisation du client pour réparer une base de données

Le client eDirectory Management Toolbox (eMBox) est un client Java à ligne de commande qui permet d'accéder à DSRepair à distance. Le client peut être lancé en mode de traitement par lots (batch). Vous pouvez donc l'utiliser pour effectuer des réparations sans surveillance à l'aide de l'outil eMTool DSRepair d'eDirectory.

Le fichier `emboxclient.jar` est installé sur votre serveur dans le cadre de l'installation d'eDirectory. Vous pouvez l'exécuter sur toute machine dotée d'une JVM. Pour plus d'informations sur le client, reportez-vous à la « Utilisation du client à ligne de commande » page 594.

Utilisation de l'outil eMTool DSRepair

1. Exécutez le client en mode interactif en entrant les éléments suivants dans la ligne de commande :

   ```
   java -cp path_to_the_file/emboxclient.jar -i
   ```

   (Si le fichier `emboxclient.jar` figure déjà dans votre chemin d'accès à la classe, il vous suffit d'entrer la commande `java -i`.)

   L'invite du client apparaît :

   ```
   Client>
   ```

2. Connectez-vous au serveur à réparer en entrant la commande suivante :

   ```
   login -s server_name_or_IP_address -p port_number
   -u username.context -w password -n
   ```

   Le numéro de port est généralement 80 ou 8028, à moins qu'il ne soit déjà utilisé par un serveur Web. L'option `-n` ouvre une connexion non sécurisée.

   Le client indique si la connexion a abouti.

3 Entrez une commande de réparation à l'aide de la syntaxe suivante :

```
dsrepair.options  tâche
```

Par exemple, `dsrepair.ufr` effectue une réparation complète sans surveillance.

```
dsrepair.rld -a -v répare la base de données locale à l'aide des options
Réparer toutes les répliques locales et Vérifier les références locales.
```

Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

Le client indique la réussite ou l'échec de la réparation.

Pour plus d'informations sur les options de l'outil eMTool DSRepair, reportez-vous à la section « Options de l'outil eMTool DSRepair » page 362.

4 Déconnectez-vous du client en entrant la commande suivante :

```
logout
```

5 Quittez le client en entrant la commande suivante :

```
exit
```

Options de l'outil eMTool DSRepair

Les tableaux suivants listent les options de l'outil eMTool DSRepair. Vous pouvez également utiliser la commande `list -t dsrepair` du client pour afficher les options DSRepair de manière détaillée. Pour plus d'informations, reportez-vous à la section « Liste des outils eMTools et de leurs services » page 597.

Option	Description
`rso -o -d`	Réparation d'objet unique, ID d'objet au format hexadécimal, DN d'objet
`rts`	Synchronisation horaire
`rss`	Signaler l'état de la synchronisation de toutes les partitions
`rld -l -t -d -p -i -f -c -o -a -m -v`	◆ Réparer la base de données locale ◆ Verrouiller la base de données eDirectory pendant toute la durée de la réparation ◆ Utiliser la base de données temporaire d'eDirectory pendant la réparation ◆ Maintenir la base de données initiale non réparée ◆ Vérifier la structure de la base de données ◆ Vérifier la structure et l'index de la base de données ◆ Récupérer l'espace disponible de la base de données ◆ Vérifier la structure de l'arborescence ◆ Reconstruire le schéma opérationnel ◆ Réparer toutes les répliques locales ◆ Valider les répertoires de messagerie et les fichiers de flux ◆ Vérifier les références locales
`ufr`	Réparation complète sans surveillance

Option	Description
`rsn -o -d`	Réparer l'adresse réseau du serveur sélectionné, ID d'objet au format hexadécimal, DN d'objet
`ran`	Réparer toutes les adresses réseau
`rsr -p -d`	Réparer la réplique sélectionnée, ID de partition, DN de partition
`rer`	Réparation de toutes les répliques
`ror -p -d`	Réparer l'anneau de répliques sélectionné, ID de partition, DN de partition
`rar`	Réparer l'anneau, toutes les répliques
`ssa -p -d`	Signaler l'état de synchronisation des répliques de tous les serveurs, ID de partition, DN de partition
`cer`	Vérifier les références externes
`rao -p -d -s -d`	Recevoir tous les objets pour cette réplique, ID de partition, DN de partition, ID de serveur, DN de serveur
`sao -p -d -s -d`	Envoyer tous les objets à chaque réplique de l'anneau, ID de partition, DN de partition, ID de serveur, DN de serveur
`dne -p -d`	Réparer les tampons horaires et déclarer une nouvelle période, ID de partition, DN de partition
`sri -p -d`	Planifier une synchronisation immédiate, ID de partition, DN de partition, ID de serveur, DN de serveur
`sks -p -d -s -d`	Synchroniser les répliques sur le serveur sélectionné, ID de partition, DN de partition, ID de serveur, DN de serveur
`ske -p -d`	Synchroniser les répliques sur tous les serveurs, ID de partition, DN de partition
`dsr -p -d`	Détruire la réplique sélectionnée sur ce serveur, ID de partition, DN de partition
`xsr -p -d -s -d`	Supprimer ce serveur de l'anneau de répliques, ID de partition, DN de partition, ID de serveur, DN de serveur
`dnm -p -d`	Désigner ce serveur comme la nouvelle réplique maîtresse, ID de partition, DN de partition
`dul`	Supprimer les objets Feuille inconnus

Utilitaire graphique DS Repair

L'utilitaire graphique DS Repair a été ajouté à OES 11 SP1. Cet outil est automatiquement installé lors d'une nouvelle installation d'OES 11 SP1.

Pour appeler l'interface utilisateur, exécutez la commande `ndsgrepair` sur la console du serveur. La plupart des opérations de réparation pouvant être exécutées à l'aide de la console peuvent l'être également à l'aide de l'interface graphique. Pour accéder à toutes les rubriques d'aide telles que les options de menu, appuyez sur F1 ou cliquez sur **Aide** > **Sommaire de l'aide** dans le menu principal de l'interface utilisateur.

Si vous effectuez la mise à niveau vers OES 11 SP1, effectuez la procédure suivante pour sélectionner manuellement novell-ndsgrepair sous le modèle eDirectory :

1. Ouvrez YaST, puis sélectionnez **OES Install and Configuration** (Installation et configuration d'OES).
2. Cliquez sur Détails, puis sélectionnez **Novell eDirectory Pattern** (Modèle Novell eDirectory) sur la gauche, puis faites défiler jusqu'au bas des paquetages sur la droite.
3. Sélectionnez **novell-ndsgrepair**, cliquez sur **Accepter**, puis sur Suivant et enfin sur **Terminer**.

13 Présentation des services LDAP pour NetIQ eDirectory

LDAP (Lightweight Directory Access Protocol) est un protocole de communications Internet qui permet aux applications client d'accéder aux informations sur l'Annuaire. Basé sur le protocole DAP (Directory Access Protocol) X.500, il est moins complexe qu'un client traditionnel et peut être utilisé avec tout autre service Annuaire répondant à la norme X.500.

LDAP est souvent utilisé en tant que protocole d'accès simplifié aux annuaires.

Les services LDAP pour NetIQ eDirectory correspondent à une application serveur qui permet aux clients LDAP d'accéder aux informations stockées dans eDirectory.

Ils comportent les fonctions d'eDirectory disponibles via LDAP :

- Provisioning
- Gestion de compte
- Authentification
- Autorisation
- Gestion des identités
- Notification
- Création de rapports
- Qualification
- Segmentation

Vous pouvez accorder à vos clients différents niveaux d'accès à l'Annuaire, ou y accéder par le biais d'une connexion sécurisée. Ces mécanismes de sécurité vous permettent de mettre certains types d'informations sur l'annuaire à disposition du public, tandis que d'autres sont uniquement réservés à votre organisation, ou à des groupes ou personnes en particulier.

Les fonctions d'annuaire accessibles aux clients LDAP dépendent des fonctions intégrées au client et au serveur LDAP. Les services LDAP pour eDirectory permettent, par exemple, aux clients LDAP de lire et d'écrire des données dans la base de données eDirectory s'ils disposent des autorisations nécessaires. Certains clients ont un accès en lecture et en écriture sur les données de l'annuaire, d'autres n'ont qu'un accès en lecture.

Les fonctions client type permettent aux clients d'effectuer une ou plusieurs des opérations suivantes :

- Rechercher des informations sur une personne spécifique, telles qu'une adresse électronique ou un numéro de téléphone.
- Rechercher des informations sur toutes les personnes répondant à un nom donné ou dont le nom commence par une certaine lettre.
- Rechercher des informations sur un objet ou une entrée eDirectory quelconque.
- Récupérer un nom, une adresse électronique, un numéro de téléphone professionnel ou un numéro de téléphone personnel.
- Récupérer un nom de société et un nom de ville.

Les sections suivantes fournissent des informations sur les services LDAP pour eDirectory :

- « Termes clés des services LDAP » page 366
- « Comprendre le fonctionnement de LDAP avec eDirectory » page 368
- « Utilisation des outils LDAP sous Linux » page 377
- « Filtre de recherche de concordance extensible » page 388
- « Transactions LDAP » page 390

Pour plus d'informations sur LDAP, visitez les sites Web suivants :

- OpenLDAP (http://www.openldap.org/)
- An LDAP Roadmap & FAQ (guide LDAP et FAQ) (http://www.kingsmountain.com/ldapRoadmap.shtml)

Termes clés des services LDAP

- « Clients et serveurs » page 366
- « Objets » page 366
- « Références » page 367

Clients et serveurs

Client LDAP— Application (par exemple, Internet Explorer ou l'utilitaire d'importation/conversion/exportation NetIQ).

Serveur LDAP— Serveur sur lequel `nldap.dlm` (pour Windows) ou `libnldap.so` (pour Linux) est en cours d'exécution.

Objets

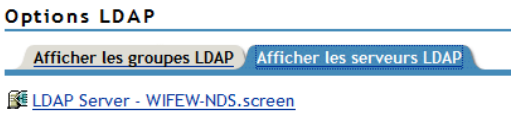
Objet Groupe LDAP— Définit et gère les propriétés LDAP NetIQ sur un serveur LDAP.

Cet objet est créé lors de l'installation d'eDirectory. L'objet Groupe LDAP contient des informations de configuration pouvant être partagées par plusieurs serveurs LDAP.

Objet Serveur LDAP— Définit et gère l'accès des clients LDAP aux informations figurant sur un serveur LDAP NetIQ et l'utilisation qu'ils en font.

Cet objet est créé lors de l'installation d'eDirectory. L'objet Serveur LDAP représente des données de configuration propres au serveur.

La figure ci-après montre un objet Serveur LDAP dans NetIQ iManager.



Références

Référence— Message que le serveur LDAP envoie au client LDAP pour lui indiquer qu'il ne peut pas fournir de résultats complets et que d'autres données se trouvent peut-être sur un autre serveur LDAP.

Le renvoi contient toutes les informations nécessaires à la poursuite de l'opération.

Scénario : un client LDAP envoie une requête à un serveur LDAP, mais celui-ci ne trouve pas l'entrée cible localement. Grâce aux références de connaissances qu'il possède sur les partitions et les autres serveurs, le serveur LDAP identifie un autre serveur possédant plus d'informations sur l'entrée. Le serveur LDAP envoie ces informations au client.

Le client établit alors une nouvelle connexion LDAP avec le serveur identifié et tente à nouveau l'opération.

Les renvois présentent les avantages suivants :

- Le client LDAP conserve le contrôle de l'opération.

  Le client ayant toujours connaissance des opérations, il prend de meilleures décisions et transmet des commentaires à l'utilisateur. Le client peut également décider de ne pas suivre le renvoi ou de signaler à l'utilisateur qu'il s'apprête à le suivre.
- En général, les renvois permettent d'utiliser les ressources réseau plus efficacement que le chaînage.

  Le chaînage permet de transmettre deux fois une recherche à plusieurs entrées via le réseau. La première transmission passe du serveur qui détient les données à celui qui effectue le chaînage. La seconde passe du serveur qui effectue le chaînage au client.

  Le renvoi permet au client d'obtenir les données directement en provenance du serveur qui les détient, en une seule transmission.
- Lorsqu'un client connaît l'emplacement de stockage d'une entrée, il peut aller directement sur le serveur qui détient les données.

  Le chaînage masque les détails au client. S'il ignore la provenance des données, le client n'ira probablement pas sur le serveur qui les détient.

Les renvois présentent les inconvénients suivants :

- Le client doit savoir reconnaître et suivre les renvois.
- Les clients LDAPv2 ne savent pas reconnaître les renvois ou utilisent une méthode obsolète et non standard pour les détecter.
- Chaque partition eDirectory doit être gérée par un serveur LDAP.

  Sinon, aucun renvoi n'est transmis pour les données de cette partition.

Renvoi supérieur— Renvoi vers un serveur qui détient des données à un niveau de l'arborescence supérieur à celui du serveur avec lequel il communique. Reportez-vous à la « Configuration des renvois supérieurs » page 428.

Les renvois supérieurs traitent les requêtes concernant des objets situés dans une partition non-eDirectory de niveau supérieur ou contiguë dans une arborescence multifournisseur.

Pour qu'un serveur eDirectory puisse participer à ce type d'arborescence, eDirectory classe les données hiérarchiques au-dessus de lui dans une partition marquée comme « non experte ». Les objets de la zone non experte sont uniquement les entrées nécessaires à la construction de la hiérarchie DN appropriée. Ces entrées sont analogues aux entrées d'association X.500.

eDirectory permet de placer dans la zone non experte des informations de connaissance sous la forme de données de renvoi LDAP. Ces informations servent à envoyer des renvois au client LDAP.

Lorsqu'une opération LDAP est effectuée dans une zone non experte de l'arborescence eDirectory, le serveur LDAP recherche les données de référence correspondantes et transmet un renvoi au client.

chaînage— Protocole de résolution de nom basé sur un serveur.

Un client LDAP envoie une requête à un serveur LDAP, mais celui-ci ne trouve pas l'entrée cible localement. Grâce aux références de connaissances qu'il possède sur les partitions et sur d'autres serveurs de l'arborescence eDirectory, le serveur LDAP identifie un autre serveur LDAP possédant plus d'informations sur le DN. Le premier serveur LDAP contacte le serveur LDAP identifié (second).

Au besoin, ce processus se poursuit jusqu'à ce que le premier serveur en contacte un autre qui dispose d'une réplique de l'entrée. eDirectory gère alors tous les détails pour terminer l'opération. Ne connaissant pas les opérations serveur à serveur, le client suppose que le premier serveur a terminé la requête.

Sur un serveur LDAP, le chaînage présente les avantages suivants :

- Il masque tous les détails de résolution de nom au client.
- Il effectue automatiquement une nouvelle authentification.
- Il joue le rôle de proxy pour le client.
- Il fonctionne de manière transparente, même lorsque des serveurs de l'arborescence eDirectory ne prennent pas en charge les services LDAP.

Le chaînage présente les inconvénients suivants :

- Il est possible que la transmission des commentaires du serveur au client prenne du temps, pendant que le serveur effectue un chaînage pour résoudre le nom.
- Si l'opération requiert que le serveur LDAP envoie de nombreuses entrées via une liaison WAN, elle peut même s'avérer très longue.
- Si plusieurs serveurs sont capables d'effectuer l'opération, des serveurs distincts peuvent traiter deux requêtes pour gérer la même entrée.

  eDirectory essaie de classer les serveurs en fonction du coût encouru pour les contacter. Pour l'équilibrage des charges, eDirectory sélectionne de façon aléatoire un serveur à faible coût.

Comprendre le fonctionnement de LDAP avec eDirectory

Cette section fournit les informations suivantes :

- « Connexion à eDirectory à partir de LDAP » page 369
- « Assignations de classes et d'attributs » page 372
- « Autorisation d'une sortie de schéma non standard » page 375
- « Différences de syntaxe » page 376
- « Contrôles et extensions LDAP NetIQ pris en charge » page 377

Connexion à eDirectory à partir de LDAP

Tous les clients LDAP se relient (se connectent) à NetIQ eDirectory en tant qu'un des types d'utilisateur suivants :

- Utilisateur [Public] (liaison anonyme)
- Utilisateur proxy (liaison anonyme d'utilisateur proxy)
- Utilisateur NDS ou eDirectory (liaison d'utilisateur NDS)

Le type de liaison avec lequel l'utilisateur s'authentifie détermine le contenu auquel le client LDAP peut accéder. Les clients LDAP accèdent à un annuaire en créant une requête puis en l'envoyant à l'annuaire. Lorsqu'un client LDAP envoie une requête via les services LDAP pour eDirectory, eDirectory traite la requête des seuls attributs pour lesquels le client LDAP dispose de droits appropriés.

Si le client LDAP fait par exemple porter sa requête sur une valeur d'attribut (nécessitant le droit Lire) mais que l'utilisateur dispose uniquement du droit Comparer sur cet attribut, la requête est rejetée.

Les restrictions standard de connexion et de mot de passe s'appliquent toujours. Elles sont cependant fonction de l'emplacement à partir duquel s'exécute LDAP. Les restrictions de temps et d'adresse sont respectées, mais les restrictions d'adresse dépendent de l'endroit d'où la connexion à eDirectory a été effectuée ; dans le cas présent, il s'agit du serveur LDAP.

Connexion en tant qu'utilisateur [Public]

Une liaison anonyme est une connexion qui ne contient ni de nom d'utilisateur ni de mot de passe. Si un client LDAP sans nom ni mot de passe se connecte aux services LDAP pour eDirectory et que le service n'est pas configuré pour utiliser un utilisateur proxy, l'utilisateur est authentifié auprès d'eDirectory en tant qu'utilisateur [Public].

L'utilisateur [Public] est un utilisateur eDirectory non authentifié. Par défaut, l'utilisateur [Public] dispose du droit Parcourir sur les objets de l'arborescence eDirectory. Le droit Parcourir accordé par défaut à l'utilisateur [Public] permet de naviguer dans les objets eDirectory, mais verrouille l'accès à la majorité des attributs d'objets.

En règle générale, les droits par défaut [Public] sont trop limités pour la plupart des clients LDAP. Bien que vous puissiez modifier les droits [Public], leur modification confère ces droits à tous les utilisateurs. C'est la raison pour laquelle il est recommandé d'utiliser plutôt une liaison anonyme d'utilisateur proxy. Pour plus d'informations, reportez-vous à la section « Connexion en tant qu'utilisateur proxy » page 369.

Pour conférer à un utilisateur [Public] un accès aux attributs des objets, vous devez transformer l'utilisateur [Public] en ayant droit du ou des conteneurs concernés, puis lui assigner les droits appropriés sur les objets et les attributs.

Connexion en tant qu'utilisateur proxy

Une liaison anonyme d'utilisateur proxy est une connexion anonyme liée à un nom d'utilisateur eDirectory. Si un client LDAP se lie anonymement aux services LDAP pour eDirectory et que le protocole est configuré pour utiliser un utilisateur proxy, l'utilisateur est authentifié auprès d'eDirectory en tant qu'utilisateur proxy. Le nom est alors configuré à la fois dans les services LDAP pour et dans eDirectory.

En règle générale, la liaison anonyme se fait sur le port 389 dans les services LDAP. Cependant,vous pouvez configurer manuellement d'autres ports lors de l'installation.

Les concepts-clés des liaisons anonymes d'utilisateur proxy sont les suivants :

- Tout accès d'un client LDAP par des liaisons anonymes est assigné par l'objet Utilisateur proxy.
- Les clients LDAP ne fournissant pas de mot de passe lors des liaisons anonymes, l'utilisateur proxy doit avoir un mot de passe nul et ne doit avoir aucune restriction de mot de passe (intervalle de changement de mot de passe, par exemple). N'indiquez pas de date d'expiration du mot de passe ou n'autorisez pas l'utilisateur proxy à changer de mot de passe.
- Vous pouvez limiter les emplacements depuis lesquels l'utilisateur peut se connecter en définissant des restrictions d'adresse pour l'objet Utilisateur proxy.
- L'objet Utilisateur proxy doit être créé dans eDirectory et des droits sur les objets eDirectory que vous souhaitez publier doivent lui être assignés. Les droits d'utilisateur par défaut confèrent un accès en lecture à un ensemble limité d'objets et d'attributs. Assignez à l'utilisateur proxy des droits Lire et Rechercher sur tous les objets et attributs de chaque sous-arborescence à laquelle l'accès est nécessaire.
- L'objet Utilisateur proxy doit être activé dans la page Général de l'objet Groupe LDAP qui configure les services LDAP pour eDirectory. C'est pourquoi il n'existe qu'un objet Utilisateur proxy pour tous les serveurs d'un groupe LDAP. Pour plus d'informations, reportez-vous à la « Configuration des objets LDAP » page 397.
- Vous pouvez accorder à un utilisateur proxy des droits d'objet sur toutes les propriétés (par défaut) ou sur des propriétés spécifiques.

Pour accorder à l'utilisateur proxy des droits sur les propriétés sélectionnées :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Droits** > **Modifier les ayants droit**.
3. Entrez le nom et le contexte du conteneur de niveau supérieur sur lequel l'utilisateur proxy a des droits ou cliquez sur pour accéder au conteneur concerné, puis sur **OK**.
4. Dans l'écran Modifier les ayants droit, cliquez sur **Ajouter un ayant droit**.
5. Accédez et cliquez sur l'objet Utilisateur proxy, puis cliquez sur **OK**.
6. Cliquez sur **Droits assignés** à gauche de l'utilisateur proxy que vous venez d'ajouter.
7. Cochez les cases **Tous les droits d'attribut** et **Droits d'entrée**, puis cliquez sur **Supprimer la propriété**.
8. Cliquez sur **Ajouter une propriété**, puis cochez la case **Afficher toutes les propriétés dans le schéma**.
9. Sélectionnez un droit héritable pour l'utilisateur proxy, tel que `mailstop` (boîte postale) (dans la section de la liste en minuscules) ou Titre, puis cliquez sur **OK**.

   Pour ajouter d'autres droits héritables, répétez l'Étape 8 et l'Étape 9.
10. Cliquez sur **Terminé**, puis sur **OK**.

Pour mettre en oeuvre les liaisons anonymes d'utilisateur proxy, vous devez créer l'objet Utilisateur proxy dans eDirectory et lui assigner les droits appropriés. Assignez à l'utilisateur proxy des droits Lire et Rechercher sur tous les objets et attributs de chaque sous-arborescence à laquelle l'accès est nécessaire. Vous devez également activer l'utilisateur proxy dans les services LDAP pour eDirectory en spécifiant le même nom d'utilisateur proxy.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP**.
3. Cliquez sur **Afficher les groupes LDAP**.

4 Cliquez sur le nom d'un objet Groupe LDAP à configurer.

5 Entrez le nom et le contexte d'un objet Utilisateur eDirectory dans le champ **Utilisateur Proxy**.

6 Cliquez sur **Appliquer**, puis sur **OK**.

Utilisation de l'utilitaire ldapconfig sous Linux

Par exemple, vous trouverez des informations sur la manière dont le serveur LDAP traite les renvois LDAP dans Utilisation de renvois lors d'une recherche pour LDAP.

1 À l'invite du système, entrez la commande suivante :

```
ldapconfig -s "LDAP:otherReferralUsage=1"
```

2 Entrez le nom distinctif complet de l'utilisateur pour eDirectory (FDN utilisateur) et son mot de passe.

Connexion en tant qu'utilisateur NDS ou eDirectory

Une liaison d'utilisateur eDirectory est une connexion établie par un client LDAP à l'aide d'un nom d'utilisateur eDirectory complet et d'un mot de passe. La liaison d'utilisateur eDirectory est authentifiée dans eDirectory et le client LDAP a accès à toutes les informations que l'utilisateur eDirectory est autorisé à consulter.

Les concepts clés des liaisons d'utilisateur eDirectory sont les suivants :

- Les liaisons d'utilisateur eDirectory sont authentifiées auprès d'eDirectory à l'aide du nom d'utilisateur et du mot de passe entrés au niveau du client LDAP.
- Le nom d'utilisateur et le mot de passe eDirectory utilisés pour l'accès du client LDAP peuvent également être utilisés pour l'accès du client Novell à eDirectory.
- Lors de connexions non-TLS, le mot de passe eDirectory est transmis en texte clair entre le client LDAP et les services LDAP pour eDirectory.
- Si les mots de passe en texte clair ne sont pas autorisés, toutes les requêtes de liaison eDirectory comportant un nom d'utilisateur ou un mot de passe sur des connexions non-TLS sont rejetées.
- En cas d'expiration du mot de passe d'un utilisateur eDirectory, les requêtes de liaison eDirectory de cet utilisateur sont rejetées.

Assignation de droits eDirectory aux clients LDAP

1 Déterminez le type de nom d'utilisateur que les clients LDAP vont utiliser pour accéder à eDirectory :

   - Utilisateur [Public] (liaison anonyme)
   - Utilisateur proxy (liaison anonyme d'utilisateur proxy)
   - Utilisateur NDS (liaison d'utilisateur NDS)

   Pour plus d'informations, reportez-vous à la section « Connexion à eDirectory à partir de LDAP » page 369.

2 Si les utilisateurs utilisent un nom d'utilisateur proxy ou plusieurs noms d'utilisateur eDirectory pour accéder aux services LDAP, utilisez iManager pour créer ces noms d'utilisateur dans eDirectory ou via les services LDAP.

3 Assignez les droits eDirectory correspondants aux noms d'utilisateur que les clients LDAP vont utiliser.

Les droits par défaut qui sont accordés à la plupart des utilisateurs constituent des droits limités pour l'objet appartenant à l'utilisateur. Pour accorder l'accès à d'autres objets et à leurs attributs, vous devez changer les droits assignés dans eDirectory.

Lorsqu'un client LDAP demande l'accès à un objet et à un attribut eDirectory, eDirectory accepte ou refuse cette requête en fonction de l'identité eDirectory du client LDAP. Cette identité est définie à l'établissement de la liaison.

Assignations de classes et d'attributs

Une *classe* est un type d'objet dans un annuaire, par exemple un utilisateur, un serveur ou un groupe. Un attribut correspond à un élément d'annuaire qui définit des informations supplémentaires portant sur un objet spécifique. Par exemple, un objet Utilisateur peut avoir pour attribut un nom de famille ou un numéro de téléphone.

Un *schéma* est un ensemble de règles qui définit les classes et attributs permis dans un répertoire, ainsi que la structure du répertoire (des relations peuvent prévaloir entre les classes). Étant donné que les schémas des annuaires LDAP et eDirectory sont parfois différents, l'assignation de classes et d'attributs LDAP aux objets et aux attributs eDirectory correspondants peut s'avérer nécessaire. Ces assignations définissent la conversion des noms du schéma LDAP au schéma eDirectory.

Les services LDAP pour eDirectory proposent des assignations par défaut. Dans de nombreux cas, la correspondance entre les classes et attributs LDAP et les types et propriétés d'objets eDirectory est logique et intuitive. Toutefois, en fonction de vos besoins de mise en oeuvre, vous désirerez peut-être reconfigurer l'assignation des classes et attributs.

Dans la plupart des cas, l'assignation d'une classe LDAP à un type d'objet eDirectory correspond à une relation de type un à un. Cependant, le schéma LDAP prend en charge les noms d'alias, tels que CN, et les noms communs faisant référence à un même attribut.

Assignation des attributs du groupe LDAP

La configuration par défaut des services LDAP pour eDirectory comprend un ensemble prédéfini d'assignations de classes et d'attributs. Celles-ci assignent un sous-ensemble d'attributs LDAP à un sous-ensemble d'attributs eDirectory. Si un attribut n'est pas encore assigné dans la configuration par défaut, une assignation auto-générée est assignée à l'attribut. De même, si le nom de schéma est un nom LDAP valide ne comportant ni espace ni deux points, aucune assignation n'est nécessaire. Passez en revue l'assignation de classe et d'attribut et reconfigurez-la au besoin.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP** > **Afficher les groupes LDAP**.
3. Cliquez sur un objet Groupe LDAP, puis sur **Assignation d'attribut**.
4. Ajoutez, supprimez ou modifiez les attributs de votre choix.

   Étant donné que certains attributs LDAP peuvent disposer de noms de remplacement (comme NC pour nom commun), vous devrez peut-être assigner plusieurs attributs LDAP à un nom d'attribut eDirectory correspondant. Lorsque les services LDAP pour eDirectory renvoient les informations sur les attributs LDAP, ils renvoient la valeur du premier attribut correspondant repéré dans la liste.

   Si vous assignez plusieurs attributs LDAP à un seul attribut eDirectory, vous devez réorganiser la liste afin de préciser l'attribut prioritaire, car l'ordre est important.
5. Cliquez sur **Appliquer**, puis sur **OK**.

Assignation de classes dans les groupes LDAP

Lorsqu'un client LDAP demande au serveur LDAP des informations sur les classes LDAP, le serveur renvoie les informations sur les classes eDirectory correspondantes. La configuration par défaut des services LDAP pour eDirectory comprend un ensemble prédéfini d'assignations de classes et d'attributs.

REMARQUE : eDirectory ne propage pas les assignations de classes dans les objets Groupe LDAP sur plusieurs serveurs LDAP. Pour utiliser la même assignation de classes sur plusieurs serveurs, ajoutez manuellement l'assignation à tous les objets Groupe LDAP dans votre environnement.

---

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP**.
3. Cliquez sur un objet Groupe LDAP, puis sur **Assignation de classe**.
4. Ajoutez, supprimez ou modifiez les classes de votre choix.

   La configuration par défaut des services LDAP pour eDirectory comprend un ensemble prédéfini d'assignations de classes et d'attributs. Ces assignations assignent un sous-ensemble de classes et d'attributs LDAP à un sous-ensemble de classes et d'attributs eDirectory. Si un attribut ou une classe n'est pas encore assigné dans la configuration par défaut, une assignation auto-générée est assignée à l'attribut ou à la classe.

   De même, si le nom de schéma est un nom LDAP valide ne comportant ni espace ni deux points, aucune assignation n'est nécessaire. Passez en revue l'assignation de classe et d'attribut et reconfigurez-la au besoin.
5. Cliquez sur **Appliquer**, puis sur **OK**.

Assignation de classes et d'attributs LDAP

Étant donné que les schémas des annuaires LDAP et eDirectory sont différents, l'assignation de classes et d'attributs LDAP aux objets et aux attributs eDirectory correspondants s'avère nécessaire. Ces assignations définissent la conversion des noms du schéma LDAP au schéma eDirectory.

Aucune assignation de schéma LDAP n'est requise pour une entrée de schéma si le nom est un nom de schéma LDAP valide. Dans LDAP, les seuls caractères autorisés dans un nom de schéma sont les caractères alphanumériques et les tirets (-). Le nom de schéma LDAP ne doit pas comporter d'espace.

Pour garantir le résultat d'une recherche par ID d'objet après une extension de schéma autre que LDAP, comme pour les fichiers `.sch`, vous devez rafraîchir la configuration du serveur LDAP si le schéma s'étend en dehors de LDAP.

Assignations de plusieurs éléments à un seul

Pour prendre en charge LDAP depuis eDirectory, les services LDAP utilisent des assignations au niveau du protocole (plutôt qu'au niveau des services Annuaire) pour effectuer la conversion entre les attributs et les classes LDAP et eDirectory. C'est pourquoi deux classes ou attributs LDAP peuvent être assignés à la même classe ou au même attribut eDirectory.

Par exemple, si vous créez un Cn via LDAP, puis recherchez CommonName=Value, vous pouvez obtenir un nom commun susceptible d'avoir la même valeur d'attribut que Cn.

Si vous demandez tous les attributs, vous obtenez le premier attribut de la liste des assignations correspondant à cette classe. Si vous demandez un attribut d'après son nom, vous obtenez le nom correct.

Assignations de plusieurs classes à une seule

Nom de classe LDAP	Nom de classe eDirectory
alias aliasObject	Alias
groupOfNames groupOfUniqueNames group	Groupe
mailGroup rfc822mailgroup	NSCP:mailGroup1

Assignations de plusieurs attributs à un seul

Nom d'attribut LDAP	Nom d'attribut eDirectory
c countryName	C
cn commonName	CN
uid userId	uniqueID
description multiLineDescription	Description
l localityname	L
member uniqueMember	Member
o organizationname	O
ou organizationalUnitName	OU
sn surname	Nom
st stateOrProvinceName	S
certificateRevocationList;binary certificateRevocationList	ndspkiCertificateRevocationList
authorityRevocationList;binary authorityRevocationList	authorityRevocationList
deltaRevocationList;binary deltaRevocationList	deltaRevocationList
cACertificate;binary cACertificate	cACertificate
crossCertificatePair;binary crossCertificatePair	crossCertificatePair
userCertificate;binary userCertificate	userCertificate

REMARQUE : les attributs contenant la valeur `;binary` concernent la sécurité. Ils figurent dans la table d'assignation, si votre application a besoin du nom récupéré avec la valeur `;binary`. Si vous avez besoin qu'il soit récupéré sans `;binary`, vous pouvez modifier l'ordre des assignations.

Autorisation d'une sortie de schéma non standard

eDirectory comporte un commutateur de mode de compatibilité autorisant une sortie de schéma non standard que les clients ADSI actuels et les anciens clients Netscape peuvent lire. Pour le mettre en oeuvre, il convient de définir un attribut dans l'objet Serveur LDAP. Le nom de l'attribut concerné est nonStdClientSchemaCompatMode. L'objet Serveur LDAP est généralement créé dans le même conteneur que l'objet Serveur.

La sortie non standard n'est pas conforme aux conventions IETF actuelles de LDAP, mais elle fonctionne avec la version actuelle des clients ADSI et plus anciens.

Dans le format de sortie non standard :

- SYNTAX OID apparaît entre guillemets simples.
- Aucune limite supérieure n'apparaît en sortie.
- Aucune option X n'apparaît en sortie.
- S'il existe plusieurs noms, seul le premier détecté apparaît en sortie.
- Les attributs ou classes sans OID défini sortent sous la forme « attributename-oid » ou « classname-oid » en minuscules.
- Les attributs ou classes dont le nom comporte un tiret et ne possédant pas d'OID défini ne sont pas obtenus en sortie.

L'OID, ou identificateur d'objet, est une chaîne numérique d'octets nécessaire pour ajouter votre propre attribut ou classe d'objets à un serveur LDAP.

Pour autoriser la sortie de schéma non standard, procédez comme suit :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP**.
3. Cliquez sur **Afficher les serveurs LDAP**, puis sur un objet Serveur LDAP.
4. Cliquez sur **Recherches**, puis sur **Autoriser la sortie de schéma pour les anciens clients ADSI et Netscape**.

   La sortie non standard n'est pas conforme aux conventions IETF actuelles définies pour LDAP, mais elle fonctionne avec les clients ADSI actuels et les anciens clients Netscape.
5. Cliquez sur **Appliquer**, sur **Informations**, puis sur **Rafraîchir**.

Différences de syntaxe

Les services LDAP et eDirectory n'utilisent pas la même syntaxe. Certaines différences importantes sont indiquées ci-dessous :

- « Virgules » page 376
- « Noms avec type » page 376
- « Caractère d'échappement » page 376
- « Attributs de dénomination multiples » page 376

Virgules

LDAP utilise des virgules comme séparateur et non des points. Exemple de nom distinctif (ou complet) dans eDirectory :

CN=JANEB.OU=MKTG.O=EMA

Le même nom distinctif avec la syntaxe LDAP :

CN=JANEB,OU=MKTG,O=EMA

Autres exemples de noms distinctifs LDAP :

CN=Bill Williams,OU=PR,O=Bella Notte Corp
CN=Susan Jones,OU=Humanities,O=University College London,C=GB

Noms avec type

eDirectory utilise aussi bien les noms sans type (.JOHN.MARKETING.ABCCORP) que les noms avec type (CN=JOHN.OU=MARKETING.O=ABCCORP). LDAP utilise uniquement les noms avec type, le séparateur étant une virgule (CN=JEAN,OU=MARKETING,O=ABCSA).

Caractère d'échappement

La barre oblique inverse (\) est utilisée comme caractère d'échappement dans les noms distinctifs LDAP. Si vous utilisez le signe plus (+) ou la virgule (,), vous pouvez utiliser une barre oblique inverse pour changer de code.

Par exemple :

CN=Pralines\+Crème,OU=Saveurs,O=MFG (CN est Pralines+Crème)

CN=DCardinal,O=Lionel\,Thomas et Catherine,C=US (O correspond à Lionel, Thomas et Catherine)

Pour plus d'informations, reportez-vous au fichier RFC 2253 (http://www.ietf.org/rfc/rfc2253.txt?number=2253) d'IETF (Internet Engineering Task Force).

Attributs de dénomination multiples

Vous pouvez définir des objets en utilisant dans le schéma plusieurs attributs de dénomination. Dans les services LDAP comme dans eDirectory, l'objet Utilisateur en possède deux : CN et UID. Le signe plus (+) sépare les attributs de dénomination dans le nom distinctif. Si les attributs ne sont pas explicitement libellés, le schéma détermine la chaîne associée à chaque attribut (la première serait CN et la seconde UID pour eDirectory et LDAP). Vous pouvez les réorganiser en un nom distinctif en libellant manuellement chaque portion.

Par exemple, voici deux noms distinctifs relatifs :

Smith (CN correspond à Smith CN=Smith)

Smith+Lisa (CN correspond à Smith et UID correspond à Lisa, CN=Smith UID=Lisa)

Les deux noms distinctifs relatifs (Smith et Smith+Lisa) peuvent exister dans le même contexte étant donné qu'ils doivent être référencés par deux noms distinctifs relatifs très différents.

Contrôles et extensions LDAP NetIQ pris en charge

Le protocole LDAP 3 permet aux clients et aux serveurs LDAP d'utiliser des contrôles et des extensions pour étendre une opération LDAP. Les contrôles et les extensions vous permettent d'indiquer des informations supplémentaires comme partie d'une requête ou d'une réponse. Chaque opération étendue est identifiée par un OID, ou identificateur d'objet, une chaîne numérique d'octets nécessaire pour ajouter votre propre attribut ou classe d'objet à un serveur LDAP. Les clients LDAP

peuvent envoyer des requêtes d'opération étendue en indiquant l'OID de l'opération étendue qui doit être effectuée, ainsi que les données qui lui sont propres. Lorsque le serveur LDAP reçoit la requête, il effectue l'opération étendue et envoie une réponse contenant un OID et des données supplémentaires au client.

Par exemple, un client peut inclure un contrôle qui indique un tri avec la requête de recherche qu'il envoie à ce serveur. Lorsque le serveur reçoit la requête de recherche, il trie les résultats de la recherche avant de les renvoyer au client. Les serveurs peuvent également envoyer des contrôles aux clients. Par exemple, un serveur peut envoyer un contrôle avec la requête d'authentification qui informe le client de l'expiration du mot de passe.

Par défaut, le serveur LDAP eDirectory charge toutes les extensions système, ainsi que les extensions et les contrôles facultatifs sélectionnés au démarrage du serveur LDAP. L'attribut extensionInfo des extensions facultatives de l'objet Serveur LDAP permet à l'administrateur du système de sélectionner ou de désélectionner les extensions et les contrôles facultatifs.

Pour que le protocole LDAP 3 puisse activer les opérations étendues, les serveurs doivent fournir la liste des contrôles et des extensions pris en charge dans les attributs supportedControl et supportedExtension de l'entrée rootDSE. L'entrée rootDSE (entrée propre au DSA [Directory System Agent - Agent du système d'annuaire]) est située à la racine de l'arborescence qui contient les informations de l'annuaire (DIT - Directory Information Tree). Pour plus d'informations, reportez-vous à la « Obtention d'informations sur le serveur LDAP » page 435.

Pour obtenir la liste des contrôles et extensions LDAP pris en charge, reportez-vous aux sections LDAP Controls (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/cchbehhc.html) (Contrôles LDAP) et LDAP Extensions (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html) (Extensions LDAP) de la documentation relative au NDK d'intégration de LDAP et d'eDirectory.

Utilisation des outils LDAP sous Linux

eDirectory inclut les outils LDAP suivants, stockés dans `/opt/novell/eDirectory/bin`, afin de vous aider à gérer le serveur d'annuaire LDAP.

REMARQUE : à partir de la version 9.0 d'eDirectory, les certificats `.PEM` sont transmis par le biais de variables TLS spécifiques. Ces variables peuvent être définies dans le fichier `/etc/opt/novell/eDirectory/conf/openldap/ldap.conf` ou peuvent être exportées individuellement. Pour plus d'informations, reportez-vous au site Web de documentation OpenLDAP et aux pages du manuel.

Outil	Description
ice	Importe les entrées d'un fichier vers un annuaire LDAP, modifie les entrées d'un fichier dans un annuaire, exporte les entrées vers un fichier et ajoute des définitions de classes et d'attributs à partir d'un fichier.
ldapadd	Ajoute de nouvelles entrées à un annuaire LDAP.
ldapdelete	Supprime les entrées d'un serveur d'annuaire LDAP. L'outil ldapdelete ouvre une connexion vers un serveur LDAP, crée une liaison et supprime une ou plusieurs entrées.
ldapmodify	Ouvre une connexion à un serveur LDAP, crée une liaison et modifie ou ajoute des entrées.

Outil	Description
ldapmodrdn	Modifie le nom distinctif relatif (RDN) d'entrées d'un serveur d'annuaire LDAP. Ouvre une connexion à un serveur LDAP, crée une liaison et modifie le nom distinctif relatif des entrées.
ldapsearch	Recherche des entrées dans un serveur d'annuaire LDAP. Ouvre une connexion à un serveur LDAP, crée une liaison et effectue une recherche à l'aide du filtre spécifié. Ce filtre doit correspondre à la représentation de type chaîne définie pour les filtres LDAP dans le fichier RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt).
ndsindex	Crée, liste, suspend, reprend ou supprime des index.

Pour plus d'informations, reportez-vous à la section LDAP Tools (http://developer.novell.com/ndk/doc/cldap/ltoolenu/data/hevgtl7k.html) (Outils LDAP) dans le document *LDAP Libraries for C Doc* (Documentation des bibliothèques LDAP pour C).

Pour effectuer des opérations sécurisées avec les outils LDAP, reportez-vous à la section Opérations eDirectory sécurisées sur des ordinateurs Linux et insérez le fichier PEM dans toutes les opérations LDAP à ligne de commande qui établissent des connexions LDAP sécurisées à eDirectory.

Outils LDAP

Les utilitaires LDAP permettent de supprimer, modifier et ajouter des entrées, d'étendre le schéma, de modifier les noms distinctifs relatifs, de déplacer des entrées dans de nouveaux conteneurs, de créer des index de recherche et d'effectuer des recherches.

REMARQUE : conformément à la demande de commentaires RFC 2256, l'interface LDAP d'eDirectory n'autorise les liaisons qu'avec des mots de passe de 128 caractères au maximum. En outre, lorsqu'ils sont configurés via le protocole LDAP, les mots de passe ne peuvent comporter qu'un maximum de 128 caractères.

ldapadd

L'utilitaire ldapadd ajoute de nouvelles entrées. Sa syntaxe est la suivante :

```
ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l limit] [-M[M]] [-d
debuglevel] [-D  binddn] [[-W]| [-w passwd]] [-h  ldaphost] [-p ldapport] [-P
version] [-Z[Z]] [-f file]
```

Si l'option `-f` est spécifiée, ldapadd lit les modifications dans un fichier. Si l'option `-f` n'est pas spécifiée, ldapadd lit les modifications dans stdin.

SUGGESTION : le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier. Par exemple, `ldapadd [options] > out.txt`.

Option	Description
`-a`	Ajoute de nouvelles entrées. L'action par défaut de ldapmodify est de modifier des entrées existantes. S'il est appelé sous la forme ldapadd, cet indicateur est toujours paramétré.
`-r`	Remplace les valeurs existantes par défaut.
`-c`	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapmodify continue les modifications. L'action par défaut est de quitter une fois chaque erreur signalée.
`-f` *`file`*	Lit les informations de modification de l'entrée à partir d'un fichier LDIF et non de l'entrée standard. La longueur maximale des enregistrements est de 4 096 lignes.
`-F`	Impose l'application de toutes les modifications, quel que soit le contenu des lignes d'entrée qui commencent par `replica:`. Par défaut, les lignes `replica:` sont comparées à l'hôte et au port du serveur LDAP utilisés pour décider si un enregistrement replog doit être appliqué.

Options communes à tous les outils LDAP

Certaines options sont communes à tous les outils LDAP. Elles sont présentées dans le tableau suivant :

Option	Description
`-C`	Active le suivi de renvoi (liaison anonyme).
`-d` *`niveau_débogage`*	Définit le niveau de débogage LDAP sur niveau_débogage. Pour que cette fonction ait un effet quelconque, l'outil ldapmodify doit être compilé avec une valeur définie pour LDAP_DEBUG.
`-D` *`binddn`*	Utilise DN_liaison pour établir une liaison avec l'annuaire LDAP. *`DN_liaison`* doit être un nom distinctif représenté par une chaîne conformément à la convention RFC 1779.
`-f` *`file`*	Lit une série de lignes du fichier, en effectuant une recherche LDAP par ligne. Dans ce cas, le filtre spécifié sur la ligne de commande sert de modèle, la première occurrence de `%s` étant remplacée par une ligne du fichier. Si le fichier se résume à un tiret (-), les lignes sont lues depuis l'entrée standard.
`-h` *`ldaphost`*	Définit un autre hôte sur lequel le serveur LDAP est exécuté.
`-l` *`limite`*	Définit le timeout de la connexion (en secondes).
`-M`	Active la commande Gérer DSA IT (non critique).
`-MM`	Active la commande Gérer DSA IT (critique).
`-n`	Indique les conséquences de cette opération sans modifier réellement les entrées. Utile pour le débogage conjointement avec l'option -v.
`-p` *`port_LDAP`*	Spécifie un autre port TCP™ sur lequel le serveur LDAP écoute.
`-P` *`version`*	Spécifie la version de LDAP (2 ou 3).
`-v`	Utilise le mode verbeux avec un grand nombre de diagnostics écrits dans la sortie standard.

Option	Description
`-w` *`passwd`*	Utilise *`mot_de_passe`* comme mot de passe pour l'authentification simple.
`-M`	Invite à une authentification simple. Cette option est utilisée au lieu d'indiquer le mot de passe sur la ligne de commande.
`-Z`	Démarre TLS avant la liaison pour effectuer l'opération. Toute erreur survenant au cours du démarrage de TLS est ignorée et l'opération se poursuit. Il est recommandé d'utiliser plutôt l'option `-ZZ` qui permet d'annuler l'opération en cas d'erreur. Si vous indiquez un port avec cette option, il doit accepter les connexions en texte clair. Pour vérifier l'identité du serveur, utilisez cette option en association avec l'option `-e` afin de spécifier un fichier de certificat de serveur. Ainsi, le certificat de racine approuvée du serveur est validé au démarrage de TLS. Si l'option `-e` n'est pas spécifiée, tous les certificats du serveur sont acceptés.
`-ZZ`	Démarre TLS avant la liaison pour effectuer l'opération. Toute erreur survenant au cours du démarrage de TLS entraîne l'interruption de l'opération. Si vous indiquez un port avec cette option, il doit accepter les connexions en texte clair. Pour vérifier l'identité du serveur, utilisez cette option en association avec l'option `-e` afin de spécifier un fichier de certificat de serveur. Ainsi, le certificat de racine approuvée du serveur est validé au démarrage de TLS. Si l'option `-e` n'est pas spécifiée, tous les certificats du serveur sont acceptés.

Exemples

Supposons que le fichier `/tmp/entrymods` existe et contienne les éléments suivants :

```
dn: cn=Modify Me, o=University of Michigan, c=US

changetype: modify

replace: mail

mail: modme@terminator.rs.itd.umich.edu

-

add: title

title: Manager

-

add: jpegPhoto

jpegPhoto: /tmp/modme.jpeg

-

delete: description

-
```

Dans ce cas, la commande `ldapmodify -b -r -f /tmp/entrymods` remplace le contenu de l'attribut de messagerie de l'entrée Modify Me par la valeur `modme@terminator.rs.itd.umich.edu`, ajoute le titre Manager, ainsi que le contenu du fichier `/tmp/modme.jpeg` (jpegPhoto) et supprime complètement l'attribut de description.

Vous pouvez apporter les mêmes modifications que ci-dessus en utilisant l'ancien format d'entrée ldapmodify :

```
cn=Modify Me, o=University of Michigan, c=US

mail=modme@terminator.rs.itd.umich.edu

+title=Manager

+jpegPhoto=/tmp/modme.jpeg

-description
```

et la commande :

```
ldapmodify -b -r -f /tmp/entrymods
```

Supposons que le fichier `/tmp/newentry` existe et contienne les éléments suivants :

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US

objectClass: person

cn: Barbara Jensen

cn: B Jensen

sn: Jensen

title: Manager

mail: bjensen@terminator.rs.itd.umich.edu

uid: bjensen
```

Dans ce cas, la commande `ldapadd -f /tmp/entrymods` ajoute une nouvelle entrée pour B Jensen, en utilisant les valeurs du fichier `/tmp/newentry`.

Supposons que le fichier `/tmp/newentry` existe et contienne les éléments suivants :

```
dn: cn=Barbara Jensen, o=University of Michigan, c=US

changetype: delete
```

Dans ce cas, la commande `ldapmodify -f /tmp/entrymods` supprime l'entrée B Jensen.

ldapdelete

L'utilitaire ldapdelete supprime l'entrée spécifiée. Il ouvre une connexion à un serveur LDAP, crée une liaison et supprime l'entrée. Sa syntaxe est la suivante :

```
ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d debuglevel] [-f file] [-D binddn]
[[-W]| [-w passwd]] [-h ldaphost] [-p ldapport] [-Z[Z]] [dn]...
```

Le paramètre `dn` est la liste des noms distinctifs des entrées à supprimer.

Il interagit avec l'option `-f` de l'une des façons suivantes :

- Si l'option `-f` n'apparaît pas dans la ligne de commande mais que les DN sont spécifiés, l'utilitaire supprime les entrées spécifiées.
- Si les `DN` et l'option `-f` sont tous deux spécifiés dans la ligne de commande, l'utilitaire cherche dans le fichier les DN à supprimer et ignore ceux de la ligne de commande.
- Si les `DN`et l'option `-f` sont tous deux manquants dans la ligne de commande, l'utilitaire lit le DN dans stdin.

SUGGESTION : le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier, par exemple, `ldapdelete [options] > out.txt`.

Option	Description
`-c`	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapdelete continue les suppressions. L'action par défaut est de quitter une fois chaque erreur signalée.
`-f` *`file`*	(fichier) Lit une série de lignes du fichier, en réalisant une recherche LDAP pour chaque ligne. Dans ce cas, le filtre spécifié sur la ligne de commande sert de modèle, la première occurrence de `%s` étant remplacée par une ligne du fichier.
`-r`	Suppression récursive.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP » page 379.

Exemple

La commande `ldapdelete "cn=Delete Me, o=University of Michigan, c=US"` tente de supprimer l'entrée dont le nom commun est Delete Me directement sous l'entrée organisationnelle University of Michigan. Dans ce cas, il sera probablement nécessaire de fournir un DN de liaison (`binddn`) et un mot de passe (`passwd`) pour autoriser la suppression (reportez-vous aux options `-D` et `-w`).

ldapmodify

L'utilitaire ldapmodify modifie les attributs d'une entrée existante ou ajoute de nouvelles entrées. Sa syntaxe est la suivante :

```
ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l limit] [-M[M]] [-d
debuglevel] [-D binddn] [[-W]|[-w passwd]] [-h ldaphost] [-p ldap-port] [-P
version] [-Z[Z]] [-f file]
```

Si l'option `-f` est spécifiée, ldapmodify lit les modifications dans un fichier. Si l'option `-f` n'est pas spécifiée, ldapmodify lit les modifications dans stdin.

SUGGESTION : le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier. Par exemple, `ldapmodify [options] > out.txt`.

Option	Description
`-a`	Ajoute de nouvelles entrées. L'action par défaut de ldapmodify est de modifier des entrées existantes. S'il est appelé sous la forme ldapadd, cet indicateur est toujours paramétré.
`-r`	Remplace les valeurs existantes par défaut.
`-c`	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapmodify continue les modifications. L'action par défaut est de quitter une fois chaque erreur signalée.
`-f` *`file`*	Lit les informations de modification de l'entrée à partir d'un fichier LDIF et non de l'entrée standard. La longueur maximale des enregistrements est de 4 096 lignes.
`-F`	Impose l'application de toutes les modifications, quel que soit le contenu des lignes d'entrée qui commencent par `replica:`. Par défaut, les lignes `replica:` sont comparées à l'hôte et au port du serveur LDAP utilisés pour décider si un enregistrement replog doit être appliqué.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP » page 379.

ldapmodrdn

L'utilitaire ldapmodrdn modifie le nom distinctif relatif d'une entrée. L'entrée peut également être déplacée vers un nouveau conteneur. Sa syntaxe est la suivante :

```
ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s newsuperior] [-d debuglevel] [-D
binddn] [[-W]|[-w  passwd]]  [-h ldaphost] [-p ldapport] [-Z[Z]] [-f file] [dn
newrdn]
```

REMARQUE : le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier. Par exemple, `ldapmodrdn [options] > out.txt`.

Option	Description
`-c`	Mode de fonctionnement continu. Des erreurs sont signalées, mais ldapmodify continue les modifications. L'action par défaut est de quitter une fois chaque erreur signalée.
`-f` *`file`*	(fichier) Lit les informations de modification d'entrée depuis le fichier et non à partir de l'entrée standard ou de la ligne de commande. Veillez à ce qu'il n'y ait pas de ligne vide entre l'ancien et le nouveau RDN, sinon l'option `-f` n'est pas prise en compte.
`-r`	Retire les anciennes valeurs RDN de l'entrée. Par défaut, les anciennes valeurs sont conservées.
`-s` *`nouveau_supérieur`*	Nom distinctif du conteneur vers lequel l'entrée est déplacée.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section Options communes à tous les outils LDAP.

Exemple

Supposons que le fichier `/tmp/entrymods` existe et contienne les éléments suivants :

```
cn=Modify Me, o=University of Michigan, c=US

cn=The New Me
```

ldapsearch

L'utilitaire ldapsearch recherche des attributs et classes d'objet spécifiés dans le répertoire. Sa syntaxe est la suivante :

```
ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d debuglevel]
[-f file] [-D binddn] [[-W]| [-w bindpasswd]] [-h ldaphost] [-p ldapport] [-b
searchbase] [-s scope] [-a deref] [-l time limit] [-z size limit] [-Z[Z]] filter
[attrs....]
```

L'outil ldapsearch établit une connexion à un serveur LDAP, effectue la liaison et lance une recherche à l'aide du filtre. Ce filtre doit correspondre à la représentation de type chaîne définie pour les filtres LDAP dans la demande de commentaires RFC 2254 (http://www.ietf.org/rfc/rfc2254.txt).

Si ldapsearch trouve une ou plusieurs entrées, les attributs définis par `attrs` sont récupérés et les entrées et leurs valeurs sont affichées dans la sortie standard. Si aucun attribut n'est répertorié, tous les attributs sont renvoyés.

SUGGESTION : le résultat des utilitaires LDAP est envoyé à stdout. Si vous quittez l'utilitaire avant de pouvoir consulter les résultats, redirigez ces derniers vers un fichier. Par exemple, `ldapsearch [options] filter [attribute list] > out.txt`.

Option	Description
`-a` *`suppr_réf`*	Indique comment gérer la suppression des références aux alias. Elle utilise les valeurs suivantes : ◆ Jamais : les références aux alias ne sont jamais supprimées lors de la localisation de l'objet de base ou de la recherche. ◆ Toujours : les références aux alias sont toujours supprimées lors de la localisation de l'objet de base et de la recherche. ◆ Rechercher : les références aux alias sont supprimées lors de la recherche de subordonnés de l'objet de base, mais pas lors de la localisation de l'objet de base. ◆ Trouver : les références aux alias sont supprimées lors de la localisation de l'objet de base, mais pas lors de la recherche de ses subordonnés.
`-Un fichier`	Récupère uniquement des attributs (aucune valeur). Cette fonction est utile lorsque vous voulez savoir si un attribut figure dans une entrée et que les valeurs elles-mêmes ne vous intéressent pas.
`-CC`	Active le suivi de renvoi (liaison authentifiée avec DN de liaison et mot de passe identiques).
`-b` *`base_recherche`*	Utilisez *`base_recherche`* comme point de départ de la recherche.
`-L`	Affiche les entrées au format LDIF.

Option	Description
`-LL`	Affiche les entrées au format LDIF sans commentaires.
`-LLL`	Affiche les entrées au format LDIF sans commentaires ni version.
`-s` *`étendue`*	Définit l'étendue de la recherche. L'étendue peut être `base`, one ousub pour spécifier une recherche portant respectivement sur un objet de base, sur un seul niveau ou sur une sous-arborescence. La valeur par défaut est `sub`.
`-S` *`attribut`*	Trie les entrées renvoyées selon l'attribut. Par défaut, les entrées renvoyées ne sont pas triées. Si l'attribut est une chaîne vide (« »), les entrées sont triées sur la base des composants de leur nom distinctif. Pour plus d'informations, reportez-vous à ldap_sort. ldapsearch affiche normalement les entrées au fur et à mesure qu'il les reçoit. L'option `–S`, lorsqu'elle est activée, annule ce comportement. Toutes les entrées sont alors récupérées, triées, puis affichées.
`-t`	Écrit les valeurs binaires récupérées dans un ensemble de fichiers temporaires. Cette fonction est utile pour traiter des valeurs non-ASCII comme jpegPhoto ou audio.
`-tt`	Écrit toutes les valeurs dans des fichiers temporaires.
`-T` *`chemin`*	Écrit les fichiers dans le répertoire indiqué par path (le répertoire par défaut est `/tmp`).
`-u`	Insère la forme conviviale du nom distinctif (DN) dans la sortie.
`-V`	Préfixe d'URL pour les fichiers.
`-V` *`préfixe`*	Spécifie le préfixe d'URL pour les fichiers (par défaut : `file://tmp/`).
`-z` *`limite_taille`*	Essaie d'atteindre la valeur *`limite_taille`* avant d'arrêter la recherche.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP » page 379.

Exemples

La commande suivante :

```
ldapsearch "cn=mark smith" cn telephoneNumber
```

permet de rechercher dans une sous-arborescence (à l'aide de la base de recherche par défaut) des entrées dont la valeur commonName est `mark smith`. Les valeurs commonName et telephoneNumber sont récupérées et affichées dans une sortie standard. Si deux entrées sont détectées, cette sortie peut se présenter comme suit :

```
cn=Mark D Smith, ou="College of Literature, Science, and the Arts", ou=Students,
ou=People, o=University of Michigan, c=US

cn=Mark Smith

cn=Mark David Smith

cn=Mark D Smith 1

cn=Mark D Smith

telephoneNumber=+1 313 930-9489
```

```
cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People,o=University of Michigan, c=US

cn=Mark Smith

cn=Mark C Smith 1

cn=Mark C Smith

telephoneNumber=+1 313 764-2277
```

La commande :

```
ldapsearch -u -t "uid=mcs" jpegPhoto audio
```

recherche dans une sous-arborescence (à l'aide de la base de recherche par défaut) les entrées dont l'ID utilisateur est mcs. La forme conviviale du nom distinctif de l'entrée s'affiche dans la sortie après la ligne comportant le nom distinctif proprement dit et les valeurs jpegPhoto et audio sont récupérées et écrites dans des fichiers temporaires. Si la recherche permet d'obtenir une entrée avec une valeur pour chacun des attributs demandés, la sortie peut se présenter comme suit :

```
cn=Mark C Smith, ou=Information Technology Division, ou=Faculty and Staff,
ou=People, o=University of Michigan, c=US

Mark C Smith, Information Technology Division, Faculty and Staff, People,
University of Michigan, US

audio=/tmp/ldapsearch-audio-a19924

jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

La commande suivante effectue une recherche à un niveau sur le niveau `c=US` pour toutes les organisations dont le nom commence par `university.` :

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

Les résultats de cette recherche sont affichés au format LDIF. Les valeurs des attributs organizationName et description sont récupérées et affichées dans la sortie standard, ce qui donne une sortie semblable à la suivante :

```
dn: o=University of Alaska Fairbanks, c=US

o: University of Alaska Fairbanks

description: Preparing Alaska for a brave new yesterday.

description: leaf node only

dn: o=University of Colorado at Boulder, c=US

o: University of Colorado at Boulder

description: No personnel information

description: Institution of education and research

dn: o=University of Colorado at Denver, c=US

o: University of Colorado at D
```

ndsindex

L'utilitaire `ndsindex` crée, répertorie, suspend, reprend ou supprime les index et index composés. Vous pouvez spécifier plusieurs attributs séparés par le signe $ dans l'utilitaire de création d'index composé `ndsindex`. Sa syntaxe est la suivante :

REMARQUE

- Vous pouvez spécifier plusieurs attributs pour l'index composé. Pour de meilleures performances, NetIQ vous recommande d'entrer jusqu'à 3 attributs. Dans le cas d'un index composé de type valeur, vous pouvez ajouter 5 attributs maximum.
- Nous vous recommandons de connecter l'utilitaire `ndsindex` au même serveur que celui sur lequel l'index a été ajouté.

```
ndsindex list [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] [<indexName1>, <indexName2>.....]
```

```
ndsindex add -a [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexDefinintion1>
[<indexDefinintion2>.....]
```

REMARQUE

- Un index comportant un ID d'ancêtre ne peut être créé qu'avec le type d'index `valeur`. Les types d'index `Présence` et `Sous-chaîne` ne sont pas pris en charge avec l'ID d'ancêtre.
- La taille de la base de données augmente après la création d'un index avec l'ID d'ancêtre.

```
ndsindex delete [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexName1> [<indexName2>.....]
```

```
ndsindex resume [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexName1> [<indexName2>.....]
```

```
ndsindex suspend [-h <hostname>] [-p <port>] -D <bind DN> -W|[-w <password>] [-l
limit] -s <eDirectory Server DN> [-Z[Z]] <indexName1> [<indexName2>.....]
```

Option	Description
`list`	Liste les index spécifiés. Si aucun index n'est spécifié, ndsindex liste tous les index présents sur le serveur.
`ajouter`	Crée de nouveaux index.
`suppression`	Supprime les index spécifiés.
`resume`	Reprend les index hors ligne spécifiés.
`suspendre`	Suspend les index spécifiés en les mettant hors ligne.
`-s` *`DN_serveur_eDirectory`*	DN du serveur eDirectory.

REMARQUE : pour plus d'informations sur les options communes, reportez-vous à la section « Options communes à tous les outils LDAP » page 379.

Exemples

Pour lister les index du serveur Mon_Hôte, entrez la commande suivante :

```
ndsindex list -h MyHost -D cn=admin,o=mycompany -w password -s cn=MyHost,o=novell
```

Pour créer un index de sous-chaîne appelé Mon_Index sur l'attribut d'adresse électronique, entrez la commande suivante :

```
ndsindex add -h myhost -D cn=admin, o=mycompany -w password -s cn=myhost, o=novell
"MyIndex;email address;substring"
```

Pour créer un index de valeur appelé Mon_Index sur l'attribut de ville, entrez la commande suivante :

```
ndsindex add -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
"MyIndex;city;value"
```

Pour créer un index de sous-chaîne appelé Mon_Index sur l'attribut de numéro de téléphone personnel, entrez la commande suivante :

```
ndsindex add -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
"MyIndex;homephone;presence"
```

Pour supprimer l'index Mon_Index, entrez la commande suivante :

```
ndsindex delete -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
MyIndex
```

Pour suspendre l'index Mon_Index, entrez la commande suivante :

```
ndsindex suspend -h myhost -D cn=admin,o=mycompany -w password -s
cn=myhost,o=novell MyIndex
```

Pour reprendre l'index Mon_Index, entrez la commande suivante :

```
ndsindex resume -h myhost -D cn=admin,o=mycompany -w password -s cn=myhost,o=novell
MyIndex
```

Exemples d'index composés

Pour créer une valeur d'index portant le nom `MyIndex` sur les attributs `email address` et `surname`, entrez la commande suivante :

```
ndsindex add –h myhost –D cn=admin, o=mycompany –w password –s cn=myhost, o=netiq
'MyIndex;email address$surname;value'
```

REMARQUE : vous ne pouvez pas créer un index composé pour les types `Presence` et `Substring`.

Filtre de recherche de concordance extensible

Les spécifications du noyau du protocole LDAP 3 définies dans le document RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt) imposent aux serveurs LDAP de reconnaître un élément de recherche appelé « filtre de correspondance extensible ». La concordance extensible permet à un client LDAP de définir les éléments suivants dans un filtre de recherche :

- Un nom d'attribut facultatif
- une règle de concordance facultative ;

- un drapeau servant à préciser si les attributs DN doivent être considérés comme faisant partie de l'entrée ;
- La valeur à utiliser pour la concordance

Vous trouverez ci-dessous la représentation sous forme de chaîne du filtre de recherche de concordance extensible :

```
extensible = attr [":dn"] [":" matchingrule] ":=" value /
             [:dn"] ":" matchingrule ":=" value
```

Le tableau ci-dessous liste les paramètres du filtre de recherche de concordance extensible :

Paramètre	Description
attr	Définit l'attribut sur lequel établir la concordance.
[":*dn*"]	Indique que la règle de concordance doit être incluse dans la comparaison.
[":" *règle_concordance*]	Désigne la règle de concordance à utiliser.
":="	En l'absence de règle de concordance, entraîne une égalité.
valeur	Valeur de comparaison

extensibleMatch est un nouveau filtre fourni par LDAP 3. En l'absence du champ matchingRule, le champ d'attribut DOIT être présent, et la recherche d'égalité est effectuée pour cet attribut. Si le champ d'attribut est absent et la règle matchingRule présente, la valeur matchValue est comparée à tous les attributs d'une entrée qui prennent en charge cette règle, et cette dernière détermine la syntaxe de la valeur d'assertion.

Le résultat de l'élément de filtre :

- est TRUE (vrai) s'il correspond à au moins un attribut de l'entrée.
- est FALSE (faux) s'il ne correspond à aucun attribut de l'entrée.
- n'est pas défini si matchingRule n'est pas reconnue ou si assertionValue ne peut être analysée.

Si le champ de type et la règle matchingRule sont présents, matchingRule DOIT être une règle autorisée pour ce type. Dans le cas contraire, l'élément de filtre est indéfini. Si le `:dn` est spécifié dans le filtre de recherche, la concordance est effectuée pour tous les attributs du nom distinctif d'une entrée, et renvoie également TRUE (vrai) s'il existe au moins un attribut de nom distinctif pour lequel l'élément de filtre donne la valeur TRUE (vrai). Le champ dnAttributes est présent afin d'éviter de faire appel à plusieurs versions des règles de concordance génériques, par exemple pour la correspondance de mots, l'une s'appliquant aux entrées et l'autre aux entrées et aux attributs DN.

Pour l'essentiel, un filtre de concordance extensible permet à un client LDAP d'atteindre deux objectifs :

- Prendre en charge plusieurs règles de concordance pour le même type de données
- Inclure des éléments DN dans les critères de recherche

  La spécification de DN permet la recherche de concordance sur certains éléments du DN.

Les versions eDirectory 8.7.3 et ultérieures prennent en charge le filtre de concordance extensible pour la mise en correspondance des attributs DN. Les autres éléments du filtre de recherche de concordance extensible, notamment la règle de concordance, sont traités comme indéfinis et

ignorés. La recherche de concordance sur le DN permet à un client LDAP de réduire considérablement les recherches nécessaires pour localiser un objet dans une arborescence eDirectory. Par exemple, un filtre de recherche LDAP complexe, tel que

```
(&(ou:dn:=sales)(objectclass=user))
```

permet d'obtenir la liste de tous les objets Utilisateur appartenant à la fonction Ventes (c'est-à-dire situés n'importe où sous les conteneurs Ventes).

Exemples d'utilisation

Voici plusieurs exemples de représentations sous forme de chaîne du filtre de recherche de concordance extensible prises en charge dans eDirectory 8.7.3 et versions ultérieures.

```
(o:dn:=Ace Industry)
```

Cet exemple illustre l'utilisation de la notation `:dn`. Les attributs du nom distinctif d'une entrée doivent être considérés comme faisant partie de l'entrée lors de l'évaluation de la concordance. Dans cet exemple, le type de concordance est l'égalité.

```
(:dn:2.4.8.10:=Dino)
```

Cet exemple présente un filtre qui doit être appliqué à n'importe quel attribut d'une entrée. Les attributs contenus dans le DN et auxquels la règle de concordance 2.4.8.10 s'applique doivent également être pris en compte.

Voici quelques exemples de représentations sous forme de chaîne du filtre de recherche de concordance extensible *non* prises en charge dans eDirectory 8.7.3 et versions ultérieures :

```
(cn:1.2.3.4.5:=John Smith)
```

Cet exemple présente un filtre qui indique le type d'attribut cn et la valeur John Smith. Il implique que le serveur d'annuaire établit la correspondance en fonction de la règle de concordance identifiée par l'oid 1.2.3.4.5.

```
(sn:dn:2.4.6.8.10:=Barbara Jones)
```

Cet exemple illustre l'utilisation de la notation `:dn` pour indiquer que la règle de concordance 2.4.6.8.10 doit être utilisée lors des comparaisons et que les attributs du nom distinctif d'une entrée doivent être considérés comme faisant partie de cette dernière lors de l'évaluation de la correspondance.

Transactions LDAP

Le serveur LDAP eDirectory prend en charge le regroupement de plusieurs opérations de mise à jour en une seule opération atomique, également appelée transaction. Dans eDirectory, la prise en charge de transactions via le protocole LDAP est basée sur deux spécifications Internet : LDAP Transactions (http://www.watersprings.org/pub/id/draft-zeilenga-ldap-txn-05.txt) (Transactions LDAP) et LDAP: Grouping of Related Operations (http://www.watersprings.org/pub/id/draft-zeilenga-ldap-grouping-05.txt) (LDAP : Regroupement d'opérations associées).

Les transactions LDAP permettent à une application LDAP d'envoyer plusieurs opérations de mise à jour LDAP (ajouter, modifier, supprimer, renommer) en tant que groupe, puis de valider ou d'abandonner ce groupe d'opérations.

Il existe quelques entités qui figurent dans le contexte des transactions LDAP :

- CreateGroupingRequest (2.16.840.1.113719.1.27.103.1) : opération étendue LDAP qui permet de regrouper des opérations associées. L'opération étendue comporte une valeur : createGroupType qui identifie le type de regroupement demandé. Pour les transactions LDAP, le type de regroupement est transactionGroupingType. (2.16.840.1.113719.1.27.103.8)
- CreateGroupingResponse (2.16.840.1.113719.1.27.103.1) : réponse du serveur LDAP à la requête createGroupingRequest qui contient 2 champs de réponse groupCookie et createGroupValue (ce dernier étant facultatif).
- GroupingControl (2.16.840.1.113719.1.27.103.7) : sert à indiquer l'association d'une opération à un groupe via groupCookie qui est la valeur associée à ce contrôle.
- EndGroupingRequest (2.16.840.1.113719.1.27.103.2) : autre opération étendue LDAP qui permet d'indiquer la fin d'une requête de regroupement. En cas de transactions LDAP, cette opération indique l'issue de la transaction : validation ou annulation.
- EndGroupingResponse (2.16.840.1.113719.1.27.103.2) : réponse du serveur LDAP à la réponse endGroupingResponse indiquant le succès ou l'échec au client LDAP.

Voici l'ordre des requêtes et des réponses échangées entre le serveur LDAP et le client LDAP dans le cadre d'une transaction LDAP :

- Si un client souhaite envoyer plusieurs opérations LDAP devant être traitées par un serveur dans le cadre d'une opération atomique, autrement dit une transaction, il doit d'abord envoyer une requête createGroupingRequest, avec un type createGroupType de type transactionGroupingType et sans valeur createGroupValue.
- Si le serveur eDirectory est en mesure de traiter les transactions, il renvoie un code de résultat de réussite, avec un cookie groupingCookie qui identifie de manière unique le regroupement demandé par le client. Dans le cas contraire, le serveur renvoie un code de résultat d'échec précisant la raison au client.
- Si le client reçoit un code de résultat de réussite du serveur, il joint ensuite un contrôle GroupingControl, qui inclut le cookie groupingCookie renvoyé par le serveur, aux opérations de mise à jour suivantes pour indiquer qu'elles doivent être traitées dans le cadre d'une même transaction. Si le serveur est prêt et en mesure de traiter l'opération de mise à jour dans le cadre de la transaction, il renvoie un code de réussite et place cette requête dans une file d'attente. Si le serveur n'est pas prêt ou en mesure de traiter l'opération de mise à jour dans le cadre de la transaction, il renvoie un code de résultat d'échec indiquant la raison au client.
- Une fois que le client a envoyé à toutes les opérations de mise à jour accompagnées du contrôle de regroupement au serveur, il envoie une requête endGroupingRequest avec le cookie groupingCookie au serveur pour indiquer qu'il souhaite finaliser la transaction. L'absence de valeur endGroupValue indique une requête de validation, la présence d'une valeur endGroupValue vide indique une requête d'annulation.
- Le serveur applique toutes les opérations en attente dans le cadre d'une seule transaction. En cas de réussite, il renvoie un code de réussite. Dans le cas contraire, il renvoie un code de résultat d'échec.
- Si, à un moment donné au cours de l'échange ci-dessus entre le client et le serveur, le serveur n'est pas prêt ou en mesure de continuer la spécification d'une transaction, il émet une notification endGroupingNotice (2.16.840.1.113719.1.27.103.4). L'utilisation ultérieure d'un cookie par le client entraîne une réponse contenant un code de résultat d'échec.

La prise en charge de transactions LDAP est indiquée par la présence du type transactionGroupingType dans l'attribut supportedGroupingTypes de l'entrée rootDSE.

La mise en oeuvre des transactions LDAP dans eDirectory est basée sur une version datée de la spécification de transaction LDAP. Au moment de la rédaction du présent guide, la dernière révision du projet de document relatif aux transactions LDAP est disponible sur la page « Lightweight Directory Access Protocol (LDAP) Transactions » (http://tools.ietf.org/html/rfc5805) (Transactions LDAP).

Limites

La fonctionnalité de transactions LDAP présente les limites suivantes :

- Tous les objets concernés par les opérations regroupées dans le cadre d'une transaction doivent être hébergés localement sur le serveur. Aucune de ces opérations ne doit exiger un chaînage du serveur LDAP sur un autre serveur.
- Les modifications de schéma et l'opération de modification de DN (déplacement de sous-arborescence ?) ne peuvent pas être regroupées en une transaction LDAP.
- Les mots de passe et les attributs avec syntaxe de flux ne peuvent pas être ajoutés dans le cadre d'une transaction LDAP.
- L'imbrication d'une transaction dans une autre n'est pas prise en charge.

14 Configuration des services LDAP pour NetIQ eDirectory

Le programme d'installation d'eDirectory installe automatiquement les services LDAP pour NetIQ eDirectory. Pour plus d'informations sur l'installation d'eDirectory, reportez-vous au *Guide d'installation de NetIQ eDirectory*.

Ce chapitre décrit les éléments suivants :

- « Chargement et déchargement des services LDAP pour eDirectory » page 393
- « Vérification du chargement du serveur LDAP » page 394
- « Vérification du fonctionnement du serveur LDAP » page 395
- « Prévention des attaques POODLE en désactivant SSLv3 » page 397
- « Configuration des objets LDAP » page 397
- « Rafraîchissement du serveur LDAP » page 410
- « Authentification et sécurité » page 411
- « Utilisation du serveur LDAP pour effectuer des recherches dans l'annuaire » page 419
- « Configuration des renvois supérieurs » page 429
- « Recherche persistante : configuration d'événements eDirectory » page 433
- « Obtention d'informations sur le serveur LDAP » page 436
- « Configuration de la prise en charge de l'heure au format généralisé » page 437
- « Configuration du contrôle permissif des modifications » page 438
- « Contrôle de l'autorisation par proxy » page 438
- « Contrôle du DN étendu LDAP » page 439
- « Audit d'événements LDAP » page 442

Pour plus d'informations sur les outils LDAP, reportez-vous à la documentation relative au NDK sur les outils LDAP (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html).

Chargement et déchargement des services LDAP pour eDirectory

Pour charger les services LDAP pour eDirectory, entrez les commandes suivantes :

Serveur	Commande
Windows	Dans l'écran DHost (NDSCONS), cliquez sur **nldap.dlm** > **Démarrer**.
Linux	À l'invite de Linux, entrez : `/opt/novell/eDirectory/sbin/nldap -l`

Entrez les commandes suivantes pour décharger les services LDAP pour eDirectory :

Serveur	Commande
Windows	Dans l'écran DHost (NDSCONS), cliquez sur **nldap.dlm** > **Arrêter**.
Linux	Sur la page de gestion à distance DHost, pour décharger LDAP, cliquez sur l'icône d'action *LDAP v3 pour NetIQ eDirectory* pour arrêter ce service. ou À l'invite de Linux, entrez : `/opt/novell/eDirectory/sbin/nldap -u`

Vérification du chargement du serveur LDAP

Avant de configurer les objets LDAP, vérifiez que le serveur LDAP est chargé et qu'il fonctionne. Cette section explique comment vérifier que le serveur LDAP est chargé. Pour vous assurer que le serveur est en fonctionnement, reportez-vous à la « Vérification du fonctionnement du serveur LDAP » page 395.

Sous Windows

1. Sur un serveur Windows, ouvrez `ndscons.exe`.

   Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**.
2. Sous l'onglet **Services**, faites défiler jusqu'à **nldap.dlm**, puis affichez la colonne **État**.

   La colonne affiche En cours d'exécution.

Vous pouvez également utiliser NetIQ iManager.

1. Cliquez sur l'option **Rôles et tâches**.
2. Cliquez sur **Maintenance** > **Gestionnaire de services**.
3. Sélectionnez une connexion, un serveur, un nom DNS ou une adresse IP, puis cliquez sur **OK**.
4. Spécifiez votre mot de passe, puis cliquez sur **OK**.
5. Cliquez sur **LDAP Agent for NetIQ eDirectory 9.2** (Agent LDAP pour NetIQ eDirectory 9.2).

   La section Informations sur le module affiche `nldap.nlm` dans le champ du nom de fichier.

Sous Linux

Pour vérifier si le serveur LDAP est en cours d'exécution, exécutez la commande suivante :

```
ndstrace -c modules | grep nldap
```

Si le serveur LDAP n'est pas chargé ou en cours d'exécution, un message d'erreur indique que le module nldap n'est pas chargé.

Vous pouvez également utiliser les options suivantes :

- Pour vérifier si le serveur LDAP est en cours d'exécution et écoute sur le port SSL, exécutez la commande `nldap -s`.
- Pour vérifier si le serveur LDAP est en cours d'exécution et écoute sur le port TCL, exécutez la commande `nldap - c`.

Ces commandes répertorient toutes les instances d'eDirectory qui s'exécutent sans erreur. Si le serveur LDAP n'est pas chargé et n'écoute pas sur l'un des ports, les commandes ci-dessus affichent l'erreur -255 (assurez-vous que le serveur LDAP est en cours d'exécution).

Vérification du fonctionnement du serveur LDAP

Une fois le serveur LDAP chargé, assurez-vous qu'il est exécuté. Vérifiez ensuite qu'un périphérique est à l'écoute.

- « Scénarios » page 395
- « Vérification du fonctionnement du serveur LDAP » page 396
- « Vérification de l'écoute d'un périphérique » page 396

Scénarios

En règle générale, le serveur LDAP s'exécute dès qu'il est chargé. Toutefois, deux scénarios peuvent empêcher le bon fonctionnement du serveur.

Scénario : le serveur est en état de veille. Le serveur LDAP se charge à condition que les chargeurs DHost puissent résoudre les dépendances externes. Toutefois, le serveur LDAP ne fonctionne correctement qu'après avoir été correctement configuré par les deux objets de configuration (les objets Serveur LDAP et Groupe LDAP).

Tant que le serveur LDAP est dans un état chargé mais non actif (état de veille), il tente régulièrement de trouver et de lire les objets de configuration. Si les objets sont mal configurés ou corrompus, le serveur LDAP reste en état de veille jusqu'à son déchargement ou sa désactivation (`nldap.nlm`, `nldap.dlm`, `libnldap.so` ou `libnldap.sl`).

Les chargeurs indiquent que le serveur LDAP est chargé. Toutefois, aucun port LDAP (389, 636) n'est ouvert par `nldap.nlm` (ou `nldap.dlm`, `libnldap.so`, ou encore `libnldap.sl`). En outre, aucune requête de client LDAP n'est satisfaite.

Des messages DSTrace signalent les tentatives régulières et la raison pour laquelle le serveur ne peut passer en mode d'exécution.

Scénario : déni de service . Chez Digital Airlines, le serveur traite une très longue recherche (d'au moins 20 minutes). L'opération revient, dans les faits, à rechercher une aiguille dans une botte de foin.

Pendant la recherche, Henri effectue l'une des opérations suivantes :

- Il change un paramètre de configuration et met à jour un objet de configuration.
- Il clique sur **Refresh Server Now** (Rafraîchir le serveur maintenant).
- Il décharge le serveur LDAP (`nldap.nlm`, `nldap.dlm`, `libnldap.so` ou `libnldap.sl`).
- Il tente d'arrêter l'ensemble du serveur.

Le serveur LDAP attend la fin des opérations en cours avant d'appliquer une mise à jour. Il diffère également l'exécution de nouvelles opérations tant que la mise à jour n'est pas terminée. Ce retard peut laisser croire à une absence de réponse du serveur aux nouvelles requêtes jusqu'à la fin de la recherche et le rafraîchissement du serveur. Le serveur peut également sembler bloqué pendant le déchargement.

Lorsque la requête de recherche est longue, mais génère de nombreuses occurrences et qu'Henri souhaite commencer décharger le serveur LDAP, la recherche est annulée pour procéder rapidement au déchargement lorsque l'occurrence suivante est renvoyée au client. Toutefois, si en 20 minutes, la recherche ne renvoie qu'un seul ou aucun résultat, le serveur LDAP ne peut pas renoncer à la requête NDS® ou eDirectory en cours.

La recherche ne sera pas abandonnée pour un rafraîchissement ou une mise à jour, même si elle renvoie de nombreuses occurrences au client.

Vérification du fonctionnement du serveur LDAP

Pour vérifier la bonne exécution du service LDAP, utilisez l'utilitaire d'importation/ de conversion/ d'exportation (ICE) de NetIQ. Sur un poste de travail, exécutez `ice.exe` ou utilisez NetIQ iManager.

Avec NetIQ iManager

Pour vérifier si le serveur LDAP est fonctionnel avec NetIQ iManager, suivez la procédure mentionnée à la section « Exportation de données vers un fichier » page 168.

Si, après avoir saisi une adresse IP et un numéro de port, vous obtenez une connexion, le serveur est fonctionnel. Dans le cas contraire, vous obtenez un message d'erreur. Téléchargez (affichez) le fichier journal ou le fichier d'exportation.

Vérification de l'écoute d'un périphérique

Vérifiez qu'un périphérique écoute le port 389.

1. Dans la ligne de commande, entrez

   ```
   netstat -a
   ```

2. Localisez une ligne dans laquelle l'adresse locale est *`nom_serveur`*`:389 et l'état LISTENING.`

Si l'une des situations suivantes se produit, lancez NetIQ iMonitor :

- Vous ne parvenez pas à obtenir d'informations de l'utilitaire ICE.
- Vous n'êtes pas certain que le serveur LDAP gère les requêtes LDAP

Pour plus d'informations sur NetIQ iMonitor, reportez-vous aux sections « Fichiers de configuration » page 245 et « Configuration des paramètres Trace » page 253.

Pour plus d'informations sur les requêtes LDAP, reportez-vous à la section « Communicating with eDirectory through LDAP » (Communication avec eDirectory via LDAP) du *Guide d'installation de NetIQ eDirectory*.

Prévention des attaques POODLE en désactivant SSLv3

Si votre instance d'eDirectory utilise le protocole LDAPS avec SSLv3 pour une communication sécurisée, sachez que SSLv3 est vulnérable aux attaques POODLE conformément à CVE-2014-3566.

Par défaut, eDirectory s'exécute en mode FIPS et n'autorise pas les communications via SSLv3. Reportez-vous à la section Configuration d'eDirectory en Mode FIPS pour plus d'informations. Si vous désactivez le mode FIPS pour TLS sur votre serveur eDirectory, vous souhaiterez peut-être désactiver SSLv3 pour LDAP à l'aide de la procédure suivante :

Solution :

1. Téléchargez et installez la dernière version du plug-in iManager pour eDirectory à partir du site Web de téléchargement NetIQ (https://dl.netiq.com/index.jsp).
2. Lancez iManager et cliquez sur **Rôles et tâches**.
3. Cliquez sur **LDAP > Options LDAP > Afficher les serveurs LDAP** et sélectionnez **Serveur LDAP**.
4. Cliquez sur l'onglet **Connexions**.
5. Sélectionnez **Désactiver SSLv3**, puis cliquez sur **Appliquer**.

   REMARQUE : dans un environnement non anglais, il n'est pas possible d'accéder à l'option **Désactiver SSLv3**. Pour accéder à cette option, changez la langue d'affichage par défaut et sélectionnez l'anglais.

6. Déchargez et chargez les services LDAP pour eDirectory.

   Pour plus d'informations, reportez-vous à la section Chargement et déchargement des services LDAP pour eDirectory.

Configuration des objets LDAP

Une installation eDirectory crée un objet Serveur LDAP et un objet Groupe LDAP. La configuration par défaut des services LDAP est consignée dans ces deux objets. Vous pouvez modifier la configuration par défaut à l'aide de la tâche de gestion LDAP dans NetIQ iManager.

L'objet Serveur LDAP représente des données de configuration propres au serveur.

L'objet Groupe LDAP contient des informations de configuration pouvant aisément être partagées par plusieurs serveurs LDAP. Cet objet fournit des données de configuration communes et représente un groupe de serveurs LDAP. Les serveurs ont des données communes.

Vous pouvez associer plusieurs objets Serveur LDAP à un objet Groupe LDAP. Tous les serveurs LDAP associés obtiennent alors leur configuration de serveur de l'objet Serveur LDAP mais reçoivent les informations communes ou partagées de l'objet Groupe LDAP.

Par défaut, le programme d'installation d'eDirectory installe un seul objet Groupe LDAP et un seul objet Serveur LDAP pour chaque fichier `nldap.nlm` ou `nldap.dlm`. Par la suite, vous pouvez associer plusieurs objets Serveur LDAP à un objet Groupe LDAP unique.

IMPORTANT : bien qu'il soit possible d'associer les dernières versions d'un objet Serveur LDAP à des versions moins récentes d'objets Groupe LDAP, nous vous recommandons de ne pas le faire. Évitez par exemple d'associer un objet Groupe LDAP d'eDirectory 8.7.3 SP9 à un objet Serveur LDAP d'eDirectory 9.0 ou version ultérieure.

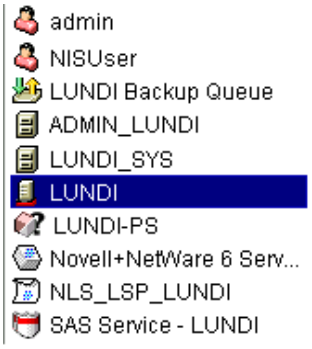
La quantité d'informations communes contenues dans un objet Groupe LDAP est limitée. LDAP n'a pas besoin de lire de nombreux attributs, étant donné que les données que contiennent ces derniers sont extrêmement courantes. De nombreux serveurs LDAP devront utiliser les mêmes données. En l'absence d'objet Groupe commun ou partagé, vous serez obligé de répliquer ces données sur chaque serveur LDAP.

En revanche, l'objet Serveur LDAP prend en charge davantage d'options et de données de configuration propres au serveur que l'objet Groupe LDAP.

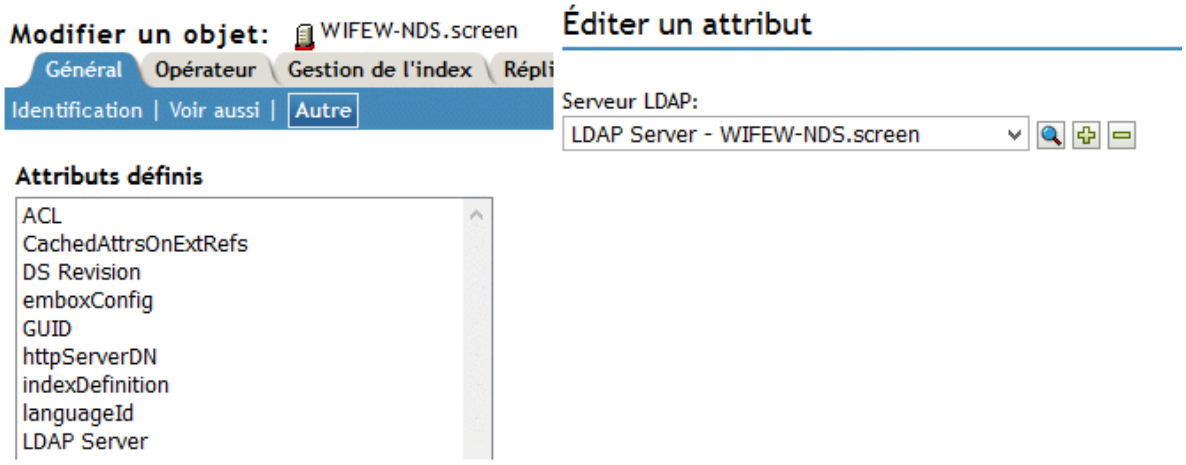
Les deux objets possèdent des attributs de syntaxe DN qui pointent les uns vers les autres.

Pour que le serveur LDAP puisse trouver ses données de configuration, une autre association est nécessaire. Elle est effectuée via le serveur NCP™, qui contient les données de configuration courantes d'eDirectory. Elle est effectuée automatiquement par le programme d'installation d'eDirectory.

Chaque serveur eDirectory possède un objet serveur NCP. Sur la figure suivante, le serveur Lundi illustre cet objet, tel qu'il s'affiche dans iManager :



Cet objet a un attribut Serveur LDAP qui pointe vers l'objet Serveur LDAP d'un serveur hôte eDirectory spécifique. La figure suivante illustre cet attribut :



En règle générale, les objets Serveur LDAP, Groupe LDAP et Serveur NCP sont situés dans le même conteneur. Vous nommez ce conteneur pendant l'installation d'eDirectory en même temps que le serveur et que le contexte Admin.

Si vous déplacez l'objet Serveur LDAP, vous devez le placer dans une réplique inscriptible.

Configuration des objets Serveur LDAP et Groupe LDAP sous Linux

L'utilitaire de configuration de LDAP est l'utilitaire ldapconfig. Vous pouvez utiliser ldapconfig sur des systèmes Linux pour modifier, afficher et rafraîchir les attributs des objets Serveur LDAP et Groupe LDAP.

Utilisez la syntaxe suivante pour afficher des valeurs d'attribut LDAP sur des systèmes Linux :

```
ldapconfig get [...] | set attribute-value-list  [-t treename | -p hostname[:port]]
[-w password] [-a user FDN] [-f]
```

```
ldapconfig [-t tree_name | -p host_name[:port]] [-w password] [-a user FDN] [-V] [-
R] [-H] [-f] -v attribute,attribute2...
```

Pour modifier des valeurs d'attributs LDAP sous Linux, utilisez la syntaxe suivante :

```
ldapconfig [-t tree_name | -p host_name[:port]] [-w password] [-a admin_FDN] -s
attribute=value,...
```

Paramètre	Description
`-t` *`nom_arborescence`*	Nom de l'arborescence eDirectory sur laquelle installer le composant.
`-p` *`nom_hôte`*	Nom de l'hôte. Vous pouvez également indiquer le nom DNS ou l'adresse IP.
`-w`	Mot de passe de l'utilisateur disposant des droits d'administrateur.
`-a`	Nom distinctif complet de l'utilisateur disposant des droits d'administrateur. Par exemple : cn=user.o=org1
`get | -V`	Permet d'afficher tous les attributs des objets Serveur/Groupe LDAP.
`get | -v` *`liste d'attributs`*	Affiche les valeurs actuelles des attributs dans la liste qui les contient.
`set | -s` *`paires attribut-valeur`*	Définit les attributs avec les valeurs spécifiées.
`-v`	Permet d'afficher la valeur de l'attribut LDAP.
`-s`	Définit une valeur pour un attribut des composants installés.
`-R`	Rafraîchit le serveur LDAP.
`-V`	Permet d'afficher les paramètres de configuration LDAP actuels.
`-H`	Permet d'afficher les chaînes de syntaxe et d'aide.
`-f`	Autorise les opérations sur une réplique filtrée.

Paramètre	Description
attribut	Nom configurable des attributs Serveur ou Groupe LDAP. Pour plus d'informations, reportez-vous aux sections « Attributs de l'objet Serveur LDAP » page 400 et « Attributs de l'objet Groupe LDAP » page 408.

Exemples

Pour afficher la valeur de l'attribut dans la liste qui le contient, saisissez la commande suivante :

```
ldapconfig [-t tree_name | -p host_name[:port]]
[-w password] [-a user_FDN] -v "Require TLS for simple binds with
password","searchTimeLimit"
```

Pour configurer le numéro de port TCP LDAP et la limite de taille de recherche à 1000, entrez la commande suivante :

```
ldapconfig [-t tree_name | -p host_name[:port]]
[-w password] [-a admin_FDN] -s "LDAP TCP Port=389","searchSizeLimit=1000”
```

Attributs de l'objet Serveur LDAP

Utilisez l'objet Serveur LDAP pour configurer et gérer les propriétés du serveur LDAP NetIQ.

Le tableau suivant décrit les attributs du serveur LDAP :

Attribut	Description
Serveur LDAP	Nom distinctif complet de l'objet Serveur LDAP dans eDirectory.
Hôte du serveur LDAP	Nom distinctif complet du serveur hôte eDirectory sur lequel le serveur LDAP est exécuté.
Groupe LDAP	Objet Groupe LDAP d'eDirectory auquel ce serveur LDAP appartient.
Limite de liaison du serveur LDAP	Nombre de clients qui peuvent établir simultanément une liaison avec le serveur LDAP. La valeur 0 (zéro) indique qu'il n'existe aucune limite.
Timeout d'inactivité du serveur LDAP	Période d'inactivité d'un client, à l'issue de laquelle le serveur LDAP interrompt la connexion avec ce client. La valeur 0 (zéro) indique qu'il n'existe aucune limite.
Activer le protocole TCP pour le serveur LDAP	Cette option a été abandonnée. Elle est accessible via ldapInterfaces. Pour plus d'informations, reportez-vous à la « ldapInterfaces » page 404.
LDAP Enable TLS	Cette option a été abandonnée. Elle est toutefois accessible via ldapInterfaces. Pour plus d'informations, reportez-vous à la « ldapInterfaces » page 404.
Port TCP LDAP	Cette option a été abandonnée. Elle est toutefois accessible via ldapInterfaces. Pour plus d'informations, reportez-vous à la « ldapInterfaces » page 404.
LDAP TLS Port	Cette option a été abandonnée. Elle est toutefois accessible via ldapInterfaces. Pour plus d'informations, reportez-vous à la « ldapInterfaces » page 404.
keyMaterialName	Nom de l'objet Certificat dans eDirectory associé à ce serveur LDAP et utilisé pour les connexions LDAP SSL.

Attribut	Description
searchSizeLimit	Nombre maximal d'entrées renvoyées par le serveur LDAP à un client LDAP en réponse à une recherche. La valeur 0 (zéro) indique qu'il n'existe aucune limite. Si l'utilisateur possède les droits d'administrateur sur l'objet Serveur LDAP, la valeur searchSizeLimit n'est pas prise en compte. Les modifications apportées aux droits d'administrateur d'un utilisateur ne sont pas prises en compte immédiatement, car les droits administratifs sont mis en cache. Les modifications des droits d'administrateur seront appliquées lors du prochain rafraîchissement du serveur LDAP. Par défaut, le serveur LDAP est rafraîchi toutes les 30 minutes.
searchTimeLimit	Nombre maximal de secondes après lesquelles le serveur LDAP abandonne la recherche LDAP pour cause de dépassement de délai. La valeur 0 (zéro) indique qu'il n'existe aucune limite. Si l'utilisateur possède les droits d'administrateur sur l'objet Serveur LDAP, la valeur searchTimeLimit n'est pas prise en compte. Les modifications apportées aux droits d'administrateur d'un utilisateur ne sont pas prises en compte immédiatement, car les droits administratifs sont mis en cache. Les modifications des droits d'administrateur seront appliquées lors du prochain rafraîchissement du serveur LDAP. Par défaut, le serveur LDAP est rafraîchi toutes les 30 minutes.
filteredReplicaUsage	Indique si le serveur LDAP doit utiliser une réplique filtrée pour une recherche LDAP. Valeurs = 1 (utiliser une réplique filtrée), 0 (ne pas utiliser de réplique filtrée)
sslEnableMutualAuthentication	Indique si l'authentification mutuelle SSL (authentification client basée sur un certificat) est activée sur le serveur LDAP..
ldapTLSVerifyClientCertificate	Active ou désactive la vérification du certificat du client pour une opération TLS qui passe par LDAP.
ldapNonStdAllUserAttrsMode	Active ou désactive les attributs de type tous les utilisateurs et opérationnels non standard.

Attribut	Description
ldapBindRestrictions	Active les restrictions de liaison LDAP et le niveau de chiffrement sur les connexions client LDAP. Cet attribut peut être utilisé pour contrôler les connexions client. Vous pouvez définir l'une des sept restrictions de liaison LDAP suivantes à l'aide d'iManager : ◆ **NONE :** cette option est activée par défaut. Cette option activera à la fois les liaisons simples anonymes et les liaisons simples non anonymes. La valeur de cette option est 0. ◆ **Refuser une liaison simple anonyme :** définissez la valeur sur 1 pour désactiver la liaison simple anonyme. La liaison simple non anonyme sera activée. ◆ **Disallow non-anonymous simple bind (Interdire l'utilisation d'une liaison simple non anonyme) :** définissez la valeur sur 2 pour désactiver une liaison simple non anonyme. ◆ **Disallow anonymous simple bind and non-anonymous simple bind (Interdire l'utilisation d'une liaison simple anonyme et d'une liaison simple non anonyme) :** définissez la valeur sur 3 pour désactiver une liaison simple anonyme et une liaison simple non anonyme. **REMARQUE :** la désactivation des liaisons simples non anonymes appliquera des limites de connexion gracieuse appropriées. ◆ **Interdire toute liaison non authentifiée :** définissez la valeur sur 4 pour désactiver une liaison simple sans mot de passe. ◆ **Interdire toute liaison anonyme et non authentifiée :** définissez la valeur sur 5 pour désactiver une liaison simple anonyme et une liaison non authentifiée. ◆ **Disallow non-anonymous simple bind and unauthenticated bind (Interdire l'utilisation d'une liaison simple non anonyme et d'une liaison non authentifiée) :** définissez la valeur sur 6 pour désactiver une liaison simple non anonyme et une liaison non authentifiée. Une liaison simple anonyme sera activée dans ce scénario. ◆ **Disallow anonymous simple bind, non-anonymous simple bind and unauthenticated bind (Interdire l'utilisation d'une liaison simple anonyme, d'une liaison simple non anonyme et d'une liaison non authentifiée) :** définissez la valeur sur 7 pour désactiver une liaison simple anonyme, une liaison simple non anonyme et une liaison non authentifiée. **REMARQUE :** les valeurs de 4 à 7 peuvent être définies à partir de l'utilitaire `ldapconfig`. iManager n'autorise pas la définition de cette valeur. Pour plus d'informations, reportez-vous au Tableau 14-1. Pour les algorithmes RSA et ECDSA (Elliptic Curve Digital Signature), eDirectory permet d'utiliser les valeurs suivantes pour restreindre l'utilisation du chiffrement : ◆ **RSA:** utilisez les valeurs suivantes : ◆ **Cipher élevé (supérieur à 128 bits) :** définissez la valeur sur 48 pour spécifier l'utilisation d'un niveau de chiffrement supérieur à 128 bits et certaines suites de chiffrement avec des clés de 128 bits. ◆ **Cipher moyennement élevé :** définissez la valeur sur 32 pour spécifier l'utilisation d'un niveau de chiffrement de 128 bits. ◆ **Cipher peu élevé :** définissez la valeur 16 pour spécifier l'utilisation d'un chiffrement de 56 ou 64 bits en excluant les suites de chiffrement d'exportation. ◆ **Exporter :** spécifie l'utilisation d'un niveau de chiffrement, y compris un chiffrement de 40 et 56 bits. Valeur 0. La valeur par défaut est **Cipher élevé** avec un niveau de chiffrement supérieur à 128 bits. Si cette valeur est définie sur **0**, une fois la mise à niveau vers eDirectory 9.1 SP4 terminée, elle sera automatiquement remplacée par **Cipher élevé**.

Attribut	Description
	Mode SuiteB : utilisez les valeurs suivantes : ◆ **Cipher SuiteB (128 bits) :** définissez la valeur sur 64 pour autoriser le fonctionnement en mode SuiteB à l'aide d'un niveau de sécurité de 128 bits. Lorsque vous sélectionnez cette option, eDirectory autorise l'utilisation d'un niveau de sécurité de 128 bits et 192 bits par des homologues (tout client LDAP). Cette option permet d'utiliser des certificats ECDSA 256 ou ECDSA 384. ◆ **Cipher SuiteB (128 bits uniquement) :** définissez la valeur sur 80 pour autoriser le fonctionnement en mode SuiteB à l'aide d'un niveau de sécurité de 128 bits. Lorsque vous sélectionnez cette option, eDirectory n'autorise pas l'utilisation du niveau de sécurité de 192 bits par des homologues (tout client LDAP). Vous ne pouvez utiliser que des certificats ECDSA 256 avec cette option. ◆ **Cipher SuiteB (192 bits) :** définissez la valeur sur 96 pour autoriser le fonctionnement en mode SuiteB à l'aide d'un niveau de sécurité de 192 bits. Lorsque vous sélectionnez cette option, eDirectory autorise uniquement l'utilisation du niveau de sécurité de 192 bits par des homologues (tout client LDAP). Vous ne pouvez utiliser que des certificats ECDSA 384 avec cette option. eDirectory vous permet d'utiliser une combinaison de valeurs `ldapbindrestrictions` et de niveaux de chiffrement. Pour plus d'informations, reportez-vous au Tableau 14-1.
ldapChainSecureRequired	Attribut booléen. S'il est activé, le chaînage à d'autres instances eDirectory s'effectuera via NCP sécurisé. Par défaut, ldapChainSecureRequired est désactivé.

Attribut	Description

ldapInterfaces	Attribut SYN_CI_STRING à plusieurs valeurs pour stocker les URL LDAP sur lesquelles le serveur LDAP écoute (tant sur les ports sécurisés qu'en texte clair). Cet attribut permet de configurer plusieurs instances lorsque chaque instance du serveur eDirectory écoute sur une interface spécifique. Il peut être configuré avec les adresses IP et les numéros de port au format d'URL LDAP. Le serveur LDAP écoute sur ces ports et adresses IP.
	
	Voici des exemples de récepteurs IPv4 et IPv6.
	
	`ldap://192.168.1.1:389 - To specify for IPv4 specific address on clear text port`
	
	`ldaps://192.168.2.1:636 - To specify for IPv4 specific address on secure port`
	
	`ldap://[2015::3]:389 - To specify for IPv6 specific address on clear text port`
	
	`ldaps://[2015::3]:636 - To specify for IPv6 specific address on secure port`
	
	`ldap://[::]:389 - To specify for IPv6 unspecified address on clear text port`
	
	`ldaps://[::]:636 - To specify for IPv6 unspecified address on secure port`
	
	Les attributs LDAP Enable TCP (Activer TCP pour LDAP), LDAP Enable TLS (Activer TLS pour LDAP), LDAP TCP Port (Port TCP LDAP) et LDAP TLS Port (Port TLS LDAP) ne sont pas remplis si un nouveau serveur est configuré dans eDirectory 9.1 ou version ultérieure. Les valeurs d'attribut `ldapInterface` correspondant aux ports sélectionnés pour ldap et ldaps pendant la configuration sont remplies. Par exemple, ldap://:389, ldaps://:636. Par défaut, seules les valeurs d'interface IPv4 sont ajoutées à l'attribut ldapInterfaces.
	
	Au cours de la mise à niveau, eDirectory est programmé pour supprimer les attributs LDAP Enable TCP, LDAP Enable TLS, LDAP TCP Port et LDAP TLS Port. Il renseigne les valeurs correspondantes de ces attributs dans `ldapInterface`. La commande `ldapconfig set` prend les valeurs séparées par des virgules et remplace toutes les valeurs existantes par les nouvelles valeurs.

ldapStdCompliance	Le serveur LDAP d'eDirectory par défaut ne retourne pas les renvois subordonnés pour les recherches à UN SEUL niveau. Pour activer cette fonctionnalité, vous devez renseigner la valeur 1 dans le champ `ldapStdCompliance`. Le serveur LDAP retournera alors les renvois subordonnés pour les recherches à UN SEUL niveau.
ldapChainSecureRequired	Attribut booléen. S'il est activé, le chaînage à d'autres instances eDirectory s'effectuera via NCP sécurisé. Par défaut, l'attribut est désactivé.
ldapEnablePSearch	Indique si la fonction de recherche persistante est activée ou non sur le serveur LDAP. Valeurs = yes, no
ldapMaximumPSearchOperations	Nombre entier qui limite le nombre d'opérations de recherche persistante simultanées. La valeur zéro autorise un nombre illimité d'opérations de recherche persistante.

Attribut	Description
ldapIgnorePSearchLimitsForEvents	Indique si les limites de taille et de durée doivent être ignorées après que la requête de recherche persistante a envoyé le jeu de résultats initial. Valeurs = yes, no Si la valeur False est sélectionnée pour cet attribut, l'ensemble des opérations de recherche persistante est soumis aux limites de recherche. Si l'une des limites est atteinte, la recherche échoue et le message d'erreur approprié apparaît.
ldapGeneralizedTime	Activez l'heure au format généralisé pour l'afficher au format *AAAAMMJJHHmmSS.0z*. Valeurs = yes, no
ldapPermissiveModify	Activez le contrôle permissif des modifications pour étendre l'opération de modification LDAP. Si vous tentez de supprimer un attribut qui n'existe pas ou d'ajouter une valeur à un attribut existant, l'opération s'effectue sans afficher de message d'erreur Valeurs = yes, no
ldapSSLConfig	Cet attribut vous permet de définir les protocoles TLS et les chiffrements dans l'objet Serveur LDAP. Par défaut, cet attribut est désactivé. Cet attribut de configuration respecte l'ordre de priorité suivant : ◆ Présence de la valeur d'attribut `ldapSSLConfig` sur l'objet Serveur LDAP ◆ Présence de la valeur d'attribut `ldapSSLConfig` sur l'objet Groupe LDAP Si aucun protocole et chiffrement n'est défini à l'aide de cet attribut, la configuration par défaut spécifiée dans les restrictions `ldapBindRestrictions` est utilisée. Pour plus d'informations, reportez-vous à la section « Configuration des protocoles et des chiffrements à l'aide de l'attribut ldapSSLConfig » page 408. **REMARQUE :** l'attribut `ldapSSLConfig` est disponible à partir de la version 9.0 SP2 d'eDirectory.
ldapGroupSSLConfig	Cet attribut vous permet de définir les protocoles TLS et les chiffrements dans l'objet Groupe LDAP. Par défaut, cet attribut est désactivé. Cet attribut de configuration respecte l'ordre de priorité suivant : ◆ Présence de la valeur d'attribut `ldapSSLConfig` sur l'objet Serveur LDAP ◆ Présence de la valeur d'attribut `ldapSSLConfig` sur l'objet Groupe LDAP Si aucun protocole et chiffrement n'est défini à l'aide de cet attribut, la configuration par défaut spécifiée dans les restrictions `ldapBindRestrictions` est utilisée. Pour plus d'informations, reportez-vous au « Configuration des protocoles et des chiffrements à l'aide de l'attribut ldapSSLConfig » page 408. **REMARQUE :** si cet attribut est défini par le biais de la commande `dapconfig get/set`, utilisez `ldapGroupSSLConfig` et, s'il est défini au moyen du fichier `ldif`, utilisez `ldapSSLConfig` à l'aide du `DN` de l'objet Groupe LDAP.

Tableau 14-1 Valeurs de combinaison de ldapbindrestrictions et des niveaux de chiffrement

ldapbindrestriction	Certificat	Niveau de chiffrement	Valeur de combinaison
Aucun	RSA	Export (Exporter)	0
	RSA	Élevé	48
	RSA	Moyen	32
	RSA	Faible	16
	ECDSA 256/384	SUITEB128	64
	ECDSA 56	SUITEB128ONLY	80
	ECDSA 384	SUITEB192	96
Refuser une liaison simple anonyme	RSA	Export (Exporter)	1
	RSA	Élevé	49
	RSA	Moyen	33
	RSA	Faible	17
	ECDSA 256/384	SUITEB128	65
	ECDSA 56	SUITEB128ONLY	81
	ECDSA 384	SUITEB192	97
Interdire la liaison locale	RSA	Export (Exporter)	2
	RSA	Élevé	50
	RSA	Moyen	34
	RSA	Faible	18
	ECDSA 256/384	SUITEB128	66
	ECDSA 56	SUITEB128ONLY	82
	ECDSA 384	SUITEB192	98
Refuser une liaison simple anonyme et annuler la liaison	RSA	Export (Exporter)	3
	RSA	Élevé	51
	RSA	Moyen	35
	RSA	Faible	19
	ECDSA 256/384	SUITEB128	67
	ECDSA 56	SUITEB128ONLY	83
	ECDSA 384	SUITEB192	99

ldapbindrestriction	Certificat	Niveau de chiffrement	Valeur de combinaison
Interdire toute liaison non authentifiée	RSA	Export (Exporter)	4
	RSA	Élevé	52
	RSA	Moyen	36
	RSA	Faible	20
	ECDSA 256/384	SUITEB128	68
	ECDSA 56	SUITEB128ONLY	84
	ECDSA 384	SUITEB192	100
Disallow anonymous and unauthenticated bind (Interdire toute liaison anonyme et non authentifiée)	RSA	Export (Exporter)	5
	RSA	Élevé	53
	RSA	Moyen	37
	RSA	Faible	21
	ECDSA 256/384	SUITEB128	69
	ECDSA 56	SUITEB128ONLY	85
	ECDSA 384	SUITEB192	101
Disallow non-anonymous simple bind and unauthenticated bind (Interdire l'utilisation d'une liaison simple non anonyme et d'une liaison non authentifiée)	RSA	Export (Exporter)	6
	RSA	Élevé	54
	RSA	Moyen	38
	RSA	Faible	22
	ECDSA 256/384	SUITEB128	70
	ECDSA 56	SUITEB128ONLY	86
	ECDSA 384	SUITEB192	102
Disallow anonymous simple bind, non-anonymous simple bind and unauthenticated bind (Interdire l'utilisation d'une liaison simple anonyme, d'une liaison simple non anonyme et d'une liaison non authentifiée)	RSA	Export (Exporter)	7
	RSA	Élevé	55
	RSA	Moyen	39
	RSA	Faible	23
	ECDSA 256/384	SUITEB128	71
	ECDSA 56	SUITEB128ONLY	87
	ECDSA 384	SUITEB192	103

Attributs de l'objet Groupe LDAP

L'objet Groupe LDAP permet de définir et de gérer le type d'accès autorisé pour les clients LDAP aux informations figurant sur le serveur LDAP NetIQ et l'utilisation qu'ils en font.

Pour exiger TLS en vue d'effectuer des liaisons simples, reportez-vous à la section « Utilisation de TLS en cas de liaison simple avec mot de passe » page 411. Cet attribut indique si le serveur LDAP autorise la transmission de mots de passe en texte clair de la part d'un client LDAP. Valeurs = 0 (non) ou 1 (oui).

Pour spécifier un renvoi par défaut, referralIncludeFilter, referralExludeFilter, ainsi que la méthode de traitement des renvois LDAP par les serveurs LDAP, reportez-vous à la section « Utilisation des renvois » page 420.

Pour spécifier les protocoles TLS et les chiffrements, vous pouvez utiliser l'attribut `ldapSSLConfig`. Pour plus d'informations, reportez-vous au « Configuration des protocoles et des chiffrements à l'aide de l'attribut ldapSSLConfig » page 408.

Configuration des protocoles et des chiffrements à l'aide de l'attribut ldapSSLConfig

eDirectory vous permet de définir divers chiffrements et paramètres TLS requis pour la communication TLS du serveur LDAP.

Vous pouvez spécifier le protocole et les chiffrements au format JSON dans l'attribut `ldapSSLConfig` pour le serveur LDAP et l'objet Groupe. Par exemple, vous pouvez définir les protocoles et les chiffrements comme indiqué dans le format JSON ci-dessous :

```
{
    "Version": 1,
    "Info": {
        "Protocol": "+ALL-SSLv3",
        "Ciphers": "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384"
    }
}
```

REMARQUE : si vous spécifiez des informations incorrectes dans l'attribut `ldapSSLConfig`, la configuration par défaut spécifiée dans les restrictions `ldapBindRestrictions` sera suivie.

Configuration des chiffrements

Vous pouvez configurer votre propre liste de chiffrements à l'aide du format de liste de chiffrement OpenSSL. Les exemples suivants illustrent l'utilisation de formats de liste de chiffrement employés dans le cadre d'une communication TLS du serveur LDAP :

- Pour les certificats RSA : `!CAMELLIA:!DH:!SRP:!MD5:HIGH+aRSA`
- Pour les certificats ECDSA : `HIGH+aECDSA`
- Pour la suite de chiffrement SuiteB 128 bits compatible avec les certificats ECDSA : `ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256`
- Pour la suite de chiffrement SuiteB 192 bits compatible avec les certificats ECDSA : `ECDHE-ECDSA-AES128-GCM-SHA256`

Pour plus d'informations sur le format de liste de chiffrement, reportez-vous à la documentation OpenSSL Ciphers (https://www.openssl.org/docs/man1.0.2/apps/ciphers.html) (chiffrements OpenSSL).

Configuration des protocoles

eDirectory offre la flexibilité de configurer la liste des protocoles requis pendant la communication TLS. Pour contrôler la liste des protocoles, définissez le protocole requis au format JSON dans l'attribut `ldapSSLConfig`. Vous pouvez configurer les chaînes de protocole suivantes :

- SSLv3
- TLSv1.0
- TLSv1.1
- TLSv1.2
- ALL

Chaque chaîne de protocole doit être précédée d'un symbole« + » ou d'un « - ». Le symbole « + » indique que les chaînes de protocole sont autorisées et le symbole « - » indique que les chaînes de protocole ne sont pas autorisées par eDirectory. Le tableau suivant répertorie certaines configurations de protocole TLS :

Configuration du protocole	Description
`+TLSv1.2`	Autorise uniquement TLSv1.2
`+ALL-TLSv1.0`	Autorise tout à l'exception de TLSv1.0
`+ALL-TLSv1.2-TLSv1.1`	Autorise SSLv3 et TLSv1.0
`+ALL`	Autorise SSLv3, TLSv1.0, TLSv1.1 et TLSv1.2

REMARQUE : un protocole peut uniquement être précédé du symbole « - » lorsque `+ALL` est spécifié.

Exemples :

Configuration des protocoles et des chiffrements dans un mode compatible avec SuiteB

```
{
    "Version": 1,
    "Info": {
        "Protocol": "+TLSv1.2",
        "Ciphers": "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384"
    }
}
```

Dans l'exemple ci-dessus, le protocole est défini en tant que `+ TLSv1.2` au format JSON. Le protocole `TLSv1.2` est le seul pris en charge pour un mode compatible avec SuiteB.

Configuration des protocoles et des chiffrements compatibles avec d'autres modes que SuiteB

```
{
    "Version": 1,
    "Info": {
        "Protocol": "+ALL-SSLv3",
        "Ciphers": "HIGH+aECDSA"
    }
}
```

Dans l'exemple ci-dessus, le protocole est défini en tant que `+ ALL-SSLv3` au format JSON, ce qui signifie que tous les protocoles pris en charge, à l'exception de `SSLv3`, sont autorisés lors d'une communication TLS.

Rafraîchissement du serveur LDAP

Après avoir modifié une option ou un paramètre de configuration sur un serveur LDAP, vous devez rafraîchir le serveur afin que les changements soit appliqués.

Vous ne pouvez cependant pas le rafraîchir lorsque des requêtes LDAP sont en cours de traitement. Par exemple, si une opération nécessite un parcours de l'arborescence eDirectory de quinze minutes, le rafraîchissement n'aura lieu qu'une fois cette opération terminée.

De même, vous ne pouvez pas arrêter le serveur LDAP lorsque ses threads sont en activité.

Lorsqu'un rafraîchissement est planifié, le serveur LDAP retarde le démarrage des nouvelles requêtes LDAP jusqu'à ce qu'il soit exécuté.

Par défaut, toutes les trente minutes, le serveur LDAP vérifie les tampons horaires sur les objets Serveur LDAP et Groupe LDAP afin de détecter les éventuels changements de paramètres. S'il en détecte, le serveur les applique.

S'il constate que les tampons horaires des paramètres n'ont pas changé, aucun rafraîchissement n'a lieu. Si vous imposez un rafraîchissement, le serveur ignore les tampons horaires et applique les modifications.

Pour rafraîchir le serveur LDAP, effectuez l'une des opérations ci-dessous :

- Utilisez iManager.

  1. Sur la page **Rôles et tâches**, cliquez sur **LDAP** > **Options LDAP** > **Afficher les serveurs LDAP**.
  2. Cliquez sur le serveur LDAP, puis sur **Rafraîchir**.
- Attendez que le serveur se reconfigure durant l'intervalle de rafraîchissement.
- Déchargez puis rechargez `nldap.nlm`.

  Il n'est pas nécessaire de décharger des programmes NLM préalablement requis avant de décharger le fichier `nldap.nlm`.

  `Nldap.nlm` décharge, puis recharge les programmes dépendants de NLM.
- Dans la ligne de commande, modifiez l'intervalle de rafraîchissement.

  Cette option peut s'avérer utile si vos liaisons WAN ne sont pas actives en permanence. Vous pouvez au besoin augmenter ou réduire temporairement la pulsation du serveur.

  Cette modification n'est pas permanente. Vous devez entrer à nouveau la commande lors de chaque chargement du fichier `nldap.nlm`.

À partir de la console du serveur, entrez

`ldap refresh [=] [date][heure][intervalle]`

- Le format de la variable de date est mm:jj:aaaa. Si vous entrez des zéros dans tous les champs de date, la date actuelle est utilisée.
- Le format de la variable d'heure est hh:mm:ss. Si vous entrez des zéros dans tous les champs d'heure, l'heure actuelle est utilisée.
- Le format de l'intervalle est égal à 0 ou compris entre 1 et 2 147 483 647 minutes. Si vous entrez zéro, la valeur par défaut utilisée est 30 minutes.

Vous pouvez afficher cette commande au fichier `autoexec.ncf` dans le répertoire `sys:\system`. Placez la commande après la ligne qui charge `nldap.nlm`.

Authentification et sécurité

Cette section contient des informations sur les éléments suivants :

- « Utilisation de TLS en cas de liaison simple avec mot de passe » page 411
- « Démarrage et arrêt de TLS » page 412
- « Configuration du serveur pour TLS » page 412
- « Configuration du client pour TLS » page 414
- « Exportation de la racine approuvée » page 414
- « Authentification auprès d'un certificat client » page 415
- « Utilisation d'autorités de certification de fournisseurs tiers » page 415
- « Création et emploi d'utilisateurs proxy LDAP » page 415
- « Utilisation de SASL » page 416
- « Utilisation de connexions NMAS pour l'authentification LDAP » page 419

Utilisation de TLS en cas de liaison simple avec mot de passe

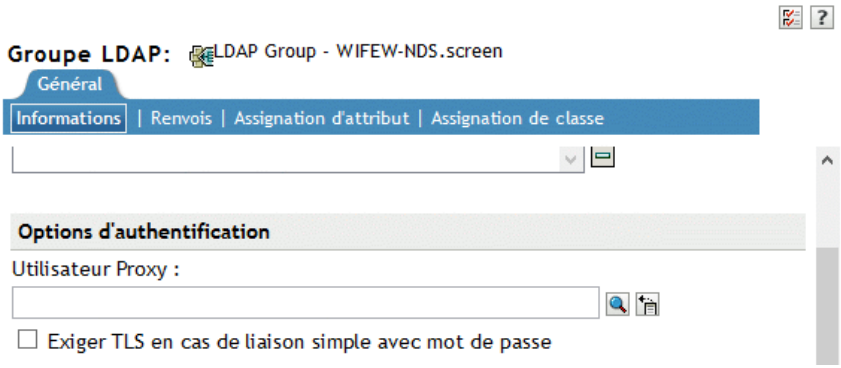
Le protocole SSL (Secure Socket Layer) 3.1 était à l'origine diffusé via Netscape. Le groupe de travail IETF prend possession de cette norme en mettant en oeuvre TLS (Transport Layer Security) 1.0. TLS 1.0 assure une compatibilité avec les versions précédentes de SSLv2 et v3.

TLS permet de coder les connexions dans la couche Session. Il n'est pas nécessaire d'utiliser un port codé pour obtenir une connexion TLS. Il existe une autre manière : le port 636 est le port TLS implicite et le serveur LDAP lance automatiquement une session TLS lorsqu'un client se connecte au port sécurisé.

Un client peut également se connecter au port en texte clair et utiliser ultérieurement TLS pour passer d'une connexion en clair à une connexion codée.

Pour exiger TLS en cas de liaison simple avec mot de passe :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP** > **Afficher les groupes LDAP**.
3. Cliquez sur l'objet Groupe LDAP, puis sur **Informations** sous l'onglet **Général**.
4. Cochez la case **Exiger TLS en cas de liaison simple avec mot de passe**.



5 Cliquez sur **Appliquer**, puis sur **OK**.

Démarrage et arrêt de TLS

La fonction LDAP étendue STARTTLS permet de passer d'une connexion en clair à une connexion codée. Cette mise à niveau constituait une nouveauté dans eDirectory 8.7.

Lorsque vous employez une connexion codée, c'est la totalité du paquet qui est codée. De ce fait, les analyseurs réseau (ou sniffers) sont dans l'impossibilité de diagnostiquer les données envoyées sur le réseau.

Scénario : à l'aide de STARTTLS— Vous créez une connexion en clair (sur le port 389) et effectuez quelques recherches anonymes. Toutefois, lorsque vous accédez à des données sécurisées, vous préférez lancer une session TLS. Vous exécutez donc une opération étendue STATTLS pour passer d'une connexion en clair à une connexion codée. Vos données sont alors sécurisées.

Vous arrêtez TLS pour passer d'une session codée à une session en clair. Avec les connexions en clair, la surcharge est moindre du fait qu'il n'est pas nécessaire de coder et décoder les données destinées au client et provenant de celui-ci. Les données sont donc acheminées plus rapidement. À ce stade, la connexion est rétrogradée au statut Anonymous (anonyme).

Pour vous authentifier, vous utilisez l'opération de liaison LDAP. La liaison établit votre ID en fonction des références que vous avez fournies. Lorsque vous arrêtez TLS, le service LDAP supprime les authentifications préalablement établies. Votre état d'authentification devient alors Anonyme. Par conséquent, pour passer à un autre état qu'Anonyme, vous devez de nouveau vous authentifier.

Scénario : réauthentification— Henri lance STOPTLS. Son état devient Anonyme. Pour accéder à ses fichiers sur Internet et les utiliser, Henri exécute la commande Bind, fournit ses références de connexion et, après avoir été authentifié, se remet à travailler sur ses données non codées sur Internet.

Configuration du serveur pour TLS

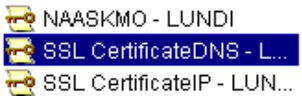
Lorsqu'une instance de session TLS est créée, un processus de reconnaissance mutuelle intervient. Le serveur et le client échangent des données. Le serveur détermine la façon dont cette reconnaissance se produit. Pour prouver qu'il est le serveur légitime, le serveur envoie toujours son certificat au client. Cette reconnaissance garantit au client que le serveur est bien celui prévu.

Pour exiger que le client établisse également sa légitimité, vous définissez une valeur sur le serveur. Il s'agit de l'attribut ldapTLSVerifyClientCertificate.

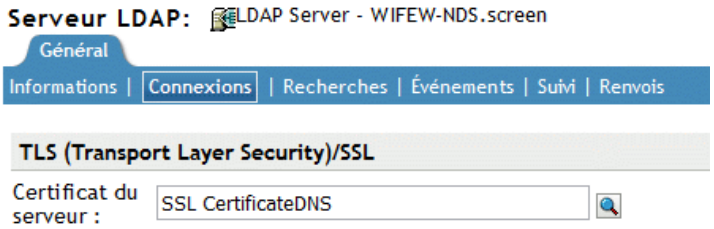
Valeur	Description
0	Inactif. Pendant un processus de reconnaissance mutuelle, le serveur fournit un certificat au client. Il n'impose jamais au client d'envoyer un certificat. Ce dernier peut utiliser le certificat ou l'ignorer. Une session sécurisée est établie.
1	Pendant le processus de reconnaissance mutuelle, le serveur fournit au client un certificat et demande à ce dernier de lui en faire parvenir un. Le client peut choisir de retourner son certificat. Le certificat du client est validé. Si le serveur ne peut pas le valider, il met fin à la connexion. Si le client n'envoie pas de certificat, le serveur maintient la connexion.
2	Pendant le processus de reconnaissance mutuelle, le serveur impose au client de lui faire parvenir un certificat. Si le client ne fournit pas de certificat ou que le certificat ne peut pas être validé, le serveur met fin à la connexion.

Pour que le serveur puisse prendre en charge TLS, vous devez lui fournir un certificat X.509 qu'il utilisera pour établir sa légitimité.

Ce certificat est fourni automatiquement pendant l'installation d'eDirectory. C'est au cours de cette installation que des objets matériels clés sont créés dans le cadre de l'infrastructure de clés publiques (PKI) et des services NMAS (NetIQ Modular Authentication Services). La figure suivante présente ces objets dans iManager :



L'installation associe automatiquement l'un de ces certificats au serveur LDAP. Dans NetIQ iManager, l'onglet Connexions de l'objet Serveur LDAP affiche un DN. Il représente le certificat X.509. Le champ Certificat du serveur de la figure suivante illustre ce DN.



Dans NetIQ iManager, vous pouvez parcourir le système jusqu'aux certificats d'objet Matériel clé (KMO). La liste déroulante vous permet de changer de certificat. Le certificat DNS ou IP fonctionne.

Dans le cadre de la validation, le serveur doit contrôler le nom (adresse IP matérielle ou DN) qui figure dans le certificat.

Pour établir une connexion TLS, vérifiez ce qui suit :

- Le serveur LDAP doit connaître l'objet Matériel clé du serveur
- Vous devez vous connecter au port sécurisé ou lancer TLS après vous être connecté au port en clair.

Une fois le serveur LDAP reconfiguré, rafraîchissez-le. Reportez-vous à la « Rafraîchissement du serveur LDAP » page 410. iManager rafraîchit automatiquement le serveur.

Configuration du client pour TLS

Un client LDAP est une application (par exemple, Internet Explorer ou ICE). Il doit être en mesure de comprendre l'autorité de certification qu'emploie le serveur LDAP.

IMPORTANT : à partir d'eDirectory 9.1, tous les utilitaires LDAP, y compris `ndsindex` et `ice` accepteront uniquement les certificats au format `.PEM`. Pour plus d'informations sur l'utilisation des certificats `PEM` dans les opérations LDAP, reportez-vous à la section « Utilisation des outils LDAP sous Linux » page 377.

Lorsqu'une arborescence eDirectory est configurée, la configuration crée par défaut :

- une autorité de certification pour l'arborescence (la CA de l'arborescence) ;
- un KMO à partir de la CA de l'arborescence.

Le serveur LDAP emploie ce fournisseur de certificat.

Le client doit importer un certificat dans lequel il a confiance, afin de valider la CA de l'arborescence que le serveur LDAP affirme utiliser. Cette importation est impérative pour que, lorsque le serveur envoie son certificat, le client puisse le valider et vérifier l'authenticité du serveur.

Pour pouvoir établir une connexion sécurisée, le client doit être configuré avant la connexion.

La méthode d'importation du certificat par le client diffère en fonction du type d'application utilisée. Chaque application doit avoir une méthode pour importer un certificat. Internet Explorer en a une et ICE, une autre. Ce sont des clients LDAP différents. Chaque client possède sa méthode pour localiser les certificats dans lesquels il a confiance.

Exportation de la racine approuvée

Vous pouvez exporter automatiquement la racine approuvée tout en acceptant le serveur de certificats.

Pour exporter manuellement la racine approuvée, reportez-vous à la section « Exportation d'un certificat de racine approuvée ou d'un certificat de clé publique » page 737.

La fonctionnalité d'exportation crée le fichier indiqué. Bien qu'il soit possible de modifier le nom du fichier, il peut s'avérer utile de laisser « DNS » ou « IP » dans le nom, de manière à pouvoir reconnaître le type d'objet Matériel. Laissez également le nom du serveur.

Installez l'autorité de certification auto-assignée dans tous les navigateurs établissant des connexions LDAP sécurisées avec eDirectory.

Si vous utilisez le certificat avec des produits Microsoft (par exemple, Internet Explorer), conservez l'extension `.der`.

Si des applications ou des SDK requièrent le certificat, importez-le dans une base de données de certificats.

Internet Explorer 5 exporte automatiquement les certificats de racine lors d'une mise à jour de la base de registres. L'extension classique .X509 utilisée par Microsoft est indispensable.

Authentification auprès d'un certificat client

L'authentification mutuelle exige une session TLS et un certificat client. Le serveur et le client doivent l'un et l'autre vérifier que leur correspondant est bien l'objet qu'il prétend être. Le certificat client a été validé au niveau de la couche Transport. Toutefois, au niveau de la couche du protocole LDAP, le client est anonyme jusqu'à ce qu'il effectue une requête de liaison LDAP.

À ce stade, le client a établi son authenticité vis-à-vis du serveur, mais pas de LDAP. Si un client souhaite s'authentifier à l'aide de l'identité mentionnée dans le certificat client, il exécute une opération de liaison en utilisant le mécanisme SASL EXTERNAL.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP**.
3. Cliquez sur **Afficher les serveurs LDAP**, puis cliquez sur le nom d'un objet Serveur LDAP.
4. Cliquez sur **Connexions**.
5. Dans la section TLS (Transport Layer Security), sélectionnez le menu déroulant **Certificat client**, puis **Requis**.

   L'authentification mutuelle est alors activée.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Utilisation d'autorités de certification de fournisseurs tiers

Pendant l'installation d'eDirectory, le serveur LDAP reçoit une autorité de certification (CA) de l'arborescence. L'objet Matériel clé LDAP repose sur cette CA. Tout certificat qu'un client envoie au serveur LDAP doit pouvoir être validé via cette CA de l'arborescence.

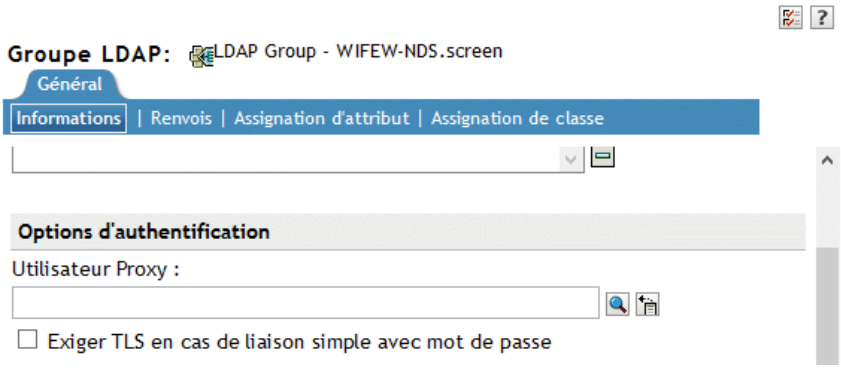
Les services LDAP pour eDirectory prennent en charge plusieurs autorités de certification. La CA de l'arborescence de NetIQ n'est qu'une autorité de certification parmi d'autres. Le serveur LDAP peut en avoir d'autres (par exemple VeriSign*, une société externe). Ce type d'autorité de certification supplémentaire est également une racine approuvée.

Pour configurer le serveur LDAP afin qu'il utilise plusieurs autorités de certification, définissez l'attribut ldapTLSTrustedRootContainer sur l'objet Serveur LDAP. En faisant référence à plusieurs autorités de certification, le serveur LDAP permet à un client d'employer un certificat d'une autorité externe.

Création et emploi d'utilisateurs proxy LDAP

NetIQ eDirectory affecte l'identité [Public] aux utilisateurs qui ne sont pas authentifiés. Dans le protocole LDAP, un utilisateur non authentifié est un utilisateur anonyme. Par défaut, le serveur LDAP accorde aux utilisateurs anonymes les droits d'une identité [Public]. Grâce à ces droits, les utilisateurs eDirectory non authentifiés et les utilisateurs anonymes de LDAP peuvent parcourir eDirectory en utilisant les droits [Public].

Le serveur LDAP permet également aux utilisateurs anonymes de se servir des droits d'un autre utilisateur proxy. La valeur correspondante est située dans l'objet Groupe LDAP. Dans NetIQ iManager, cette valeur est le champ Utilisateur proxy. La figure suivante illustre ce champ dans NetIQ iManager.



L'utilisateur proxy est un nom distinctif. Vous pouvez lui accorder d'autres droits que ceux dont bénéficie l'utilisateur Public. Avec l'utilisateur proxy, vous pouvez contrôler l'accès d'un client LDAP anonyme à des conteneurs spécifiques de l'arborescence eDirectory.

REMARQUE : n'imposez pas de restrictions de connexion à l'utilisateur proxy, sauf si vous souhaitez qu'elles soient appliquées à l'ensemble des utilisateurs LDAP anonymes.

Scénario : configuration d'un utilisateur proxy NLDAP— Digital Airlines a passé un contrat avec DataSure, un groupe de recherche. DataSure utilisera LDAP pour accéder aux résultats de recherche et les stocker sur DigitalAir43, un serveur Linux de Digital Airlines. Vous ne souhaitez pas que DataSure dispose de droits Public sur les répertoires de DigitalAir43.

Vous pouvez donc créer un utilisateur proxy LDAP et lui affecter des droits spécifiques sur le répertoire DataSure. Vous indiquez le Nom distinctif du proxy dans l'objet Groupe LDAP, et rafraîchissez le serveur. Le serveur emploie alors automatiquement les droits de l'utilisateur proxy pour tout utilisateur anonyme nouveau ou existant.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration de l'annuaire** > **Créer un objet**, puis créez un utilisateur proxy (par exemple, LDAPProxy).
3. Affectez un mot de passe nul à cet utilisateur.
4. (Facultatif) Assignez à l'utilisateur proxy des droits sur les répertoires spécifiés.
5. Cliquez sur **LDAP** > **Options LDAP** > **Afficher les groupes LDAP** > objet Groupe LDAP.
6. Dans le champ **Utilisateur Proxy**, cliquez sur le bouton **Parcourir**, accédez et sélectionnez l'utilisateur LDAPProxy, puis cliquez sur **OK**.

Utilisation de SASL

SASL (Simple Authentication and Security Layer) est un mécanisme permettant d'ajouter des services de sécurité des données et de prise en charge de l'authentification aux protocoles basés sur les connexions via différents mécanismes. Il présente une interface bien formée entre les protocoles et les mécanismes. En outre, il fournit un protocole pour la sécurisation des échanges de protocole suivants au sein d'une couche de sécurité des données, et garantit l'intégrité et la confidentialité des données ainsi que d'autres services.

SASL est conçu pour permettre à de nouveaux protocoles de réutiliser les mécanismes existants sans modifier ces derniers et aussi pour permettre aux protocoles existants, sans les modifier, d'utiliser de nouveaux mécanismes. Pour utiliser SASL, chaque protocole propose une méthode pour

identifier quel mécanisme utiliser, une méthode pour échanger des défis serveur et des réponses client spécifiques du mécanisme et une méthode pour communiquer le résultat de l'échange d'authentification.

Les mécanismes SASL sont nommés par des chaînes, composées de lettres majuscules, de chiffres, de traits d'union et de traits de soulignement. Les noms des mécanismes SASL doivent être enregistrés auprès de l'IANA (Internet Assigned Numbers Authority).

Si un serveur prend en charge le mécanisme demandé, il lance un échange de protocole d'authentification. Il s'agit d'une série de défis serveur et de réponses client qui sont propres au mécanisme demandé. Au cours de l'échange de protocole d'authentification, le mécanisme effectue une authentification, transmet une identité d'autorisation du client au serveur et négocie l'utilisation d'une couche de sécurité propre au mécanisme. Si l'utilisation d'une couche de sécurité est acceptée, le mécanisme doit également définir ou négocier la taille maximale du tampon de texte chiffré que chaque côté est capable de recevoir.

Le serveur LDAP gère les mécanismes suivants :

- DIGEST-MD5
- EXTERNAL
- NMAS_LOGIN
- GSSAPI

Ces mécanismes sont déployés sur le serveur pendant une installation ou une mise à niveau d'eDirectory. Cependant, sous Linux, l'utilitaire nmasinst doit être utilisé pour installer les méthodes NMAS.

Comme indiqué ci-dessus, le serveur LDAP interroge SASL pour connaître les mécanismes installés lorsqu'il reçoit sa configuration, et prend automatiquement en charge les éléments installés. Le serveur LDAP signale également les mécanismes SASL pris en charge dans son entrée rootDSE à l'aide de l'attribut supportedSASLMechanisms. Étant donné que ce sont les mécanismes enregistrés, les conventions de dénomination correctes doivent être utilisées pour les utiliser.

Le protocole de liaison LDAP autorise le client à utiliser différents mécanismes SASL pour l'authentification. Lorsque l'application utilise l'API de liaison LDAP, elle doit choisir soit la liaison simple et fournir un DN et un mot de passe, soit la liaison SASL et indiquer le nom du mécanisme SASL ainsi que les références SASL associées exigées par le mécanisme.

DIGEST-MD5

LDAP prend en charge le mécanisme DIGEST-MD5 via la requête de liaison. Au lieu de demander une liaison simple LDAP (DN et mot de passe en texte clair), vous demandez une liaison SASL LDAP et fournissez le DN et les références MD5. Le mécanisme DIGEST-MD5 n'a pas besoin de TLS. Le serveur LDAP prend en charge DIGEST-MD5 sur les connexions en clair et sécurisées.

MD5 fournit un hashage codé des mots de passe. Ces derniers sont codés même sur les connexions en clair. C'est la raison pour laquelle le serveur LDAP accepte les mots de passe utilisant MD5 sur le port en texte clair ou le port codé. Si un utilisateur tente de « renifler » cette connexion, le mot de passe ne peut pas être détecté. Toutefois, la connexion peut être simulée ou piratée.

Ce mécanisme est une liaison SASL LDAP (et non une liaison simple). Par conséquent, le serveur LDAP accepte ces requêtes, même si vous avez coché la case **Exiger TLS en cas de liaison simple avec mot de passe** pendant l'installation.

EXTERNAL

Le mécanisme EXTERNAL informe le serveur LDAP que le DN utilisateur et les références ont déjà été fournis au serveur. Par conséquent, il n'est pas nécessaire que le DN et les références soient communiqués dans la requête de liaison.

La requête de liaison LDAP utilise le mécanisme SASL EXTERNAL pour commander au server d'effectuer les opérations suivantes :

- demander les références à la couche EXTERNAL ;
- authentifier l'utilisateur avec ces références et cet utilisateur.

Une fois cette opération effectuée, elle est suivie d'une reconnaissance mutuelle sécurisée. Le serveur LDAP demande des références au client qui les lui communique, le serveur reçoit ensuite le certificat qui a été envoyé par le client et le transmet au module NMAS, puis il authentifie l'utilisateur comme le DN fourni dans le certificat

Pour disposer d'un certificat avec un DN utilisable, quelques opérations de configuration sont nécessaires sur le client. Pour plus d'informations sur la configuration du certificat, consultez la documentation en ligne NMAS (https://www.netiq.com/documentation/edir88/nmas88/data/bookinfo.html).

Même si le client envoie un mécanisme EXTERNAL, le serveur LDAP peut faire échouer la requête, pour les éventuelles raisons suivantes :

- La connexion n'est pas sécurisée.
- Bien que la connexion soit sécurisée, le client n'a pas fourni le certificat requis pendant la procédure de reconnaissance mutuelle.
- Le module SASL est indisponible.

NMAS_LOGIN

NMAS (NetIQ Modular Authentication Service) est une structure de développement qui permet d'écrire des applications qui s'authentifient auprès du réseau en utilisant différentes méthodes de connexion et d'authentification. La structure NMAS permet de concevoir un système de connexion et d'authentification flexible et évolutif utilisant des méthodes de plug-in modulaires qui tirent parti de l'infrastructure NICI (Novell International Cryptographic Infrastructure) et des services NetIQ Directory Services (eDirectory).

Le mécanisme NMAS_LOGIN permet au serveur LDAP d'accéder aux capacités biométriques de NMAS. Pour plus d'informations, reportez-vous à la documentation NetIQ Modular Authentication Services NDK (http://www.novell.com/documentation/developer/nmas/).

GSSAPI

Le mécanisme GSSAPI permet à un utilisateur Kerberos de s'authentifier auprès d'un serveur eDirectory à l'aide d'un ticket, sans devoir entrer un mot de passe utilisateur LDAP distinct. Cette fonctionnalité est destinée aux utilisateurs d'applications LDAP dans des environnements disposant d'une infrastructure Kerberos existante. Ces utilisateurs doivent pouvoir utiliser des tickets délivrés par le serveur Kerberos afin de s'authentifier auprès du serveur LDAP sans devoir fournir de mot de passe utilisateur LDAP distinct.

Pour plus d'informations sur la configuration de GSSAPI, reportez-vous à l'Annexe E, « Configuration de GSSAPI avec eDirectory », page 873.

Utilisation de connexions NMAS pour l'authentification LDAP

La connexion NMAS est activée par défaut dans eDirectory. Pour désactiver la connexion NMAS, définissez `NDSD_TRY_NMASLOGIN_FIRST` sur `false`.

REMARQUE : vous devez ajouter toutes les variables d'environnement requises pour l'exécution du service eDirectory dans le script pre_ndsd_start_custom sur les plates-formes RHEL 7.x et SLES 12.x.

Utilisation du serveur LDAP pour effectuer des recherches dans l'annuaire

Cette section contient des informations sur les éléments suivants :

- « Définition de limites de recherche » page 419
- « Utilisation des renvois » page 420
- « Recherche de répliques filtrées » page 428

Définition de limites de recherche

Les attributs suivants de l'objet Serveur LDAP contrôlent la façon dont le serveur LDAP effectue des recherches dans l'annuaire :

- Limite d'entrée de recherche

  Cette option limite la taille d'une recherche. La valeur par défaut est 0, indiquant qu'il n'y a pas de limite de taille. Afin d'éviter de surcharger le serveur LDAP, vous pouvez limiter le nombre d'entrées que le serveur LDAP renvoie lors d'une requête.

  Scénario : limitation de la taille d'une recherche— Henri lance une recherche qui peut renvoyer des milliers de réponses liées aux objets trouvés. Toutefois, vous avez défini une limite de dix résultats. Le serveur LDAP interrompt la recherche après avoir renvoyé dix résultats. Un message système informe Henri que la recherche a pris fin bien que d'autres données soient disponibles.

- Limite de temps de recherche

  Limite la durée de recherche du serveur. La valeur par défaut est 0, indiquant qu'il n'y a pas de limite de temps.

La figure suivante illustre ces attributs dans NetIQ iManager.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **LDAP** > **Options LDAP** > **Afficher les serveurs LDAP**.

3 Cliquez sur l'objet Serveur LDAP > **Recherches**.

4 Faites défiler jusqu'à la section Restrictions, entrez des valeurs, puis cliquez sur **OK**.

Le client peut également définir des limites de temps pour les requêtes (par exemple, limiter la recherche à deux secondes). En cas de conflit entre la limite définie par le client et celle du serveur LDAP, ce dernier emploie la valeur la plus faible.

La recherche repose sur des ACL (Access Control Lists). De ce fait, une recherche anonyme peut renvoyer simplement quelques entrées, celles que l'utilisateur Public est autorisé à voir, même si l'annuaire en contient des milliers.

Utilisation des renvois

Un renvoi est une méthode qui permet au client de résoudre des noms. Un client LDAP envoie une requête à un serveur LDAP, qui tente de trouver localement l'entrée cible. Si le serveur ne parvient pas à trouver l'entrée cible, il utilise les références de connaissance dont il dispose pour générer un renvoi à un deuxième serveur LDAP qui possède plus d'informations sur l'entrée. Le premier serveur envoie les informations de renvoi au client LDAP.

Le client LDAP établit alors une connexion avec le second serveur LDAP et tente de nouveau l'opération. Si le second serveur LDAP possède l'entrée cible de l'opération, il l'exécute. Sinon, il transmet également un renvoi dans la réponse au client. Ce processus se poursuit jusqu'à ce que l'un des événements suivants se produise :

- Le client contacte un serveur qui possède l'entrée et peut effectuer l'opération voulue.

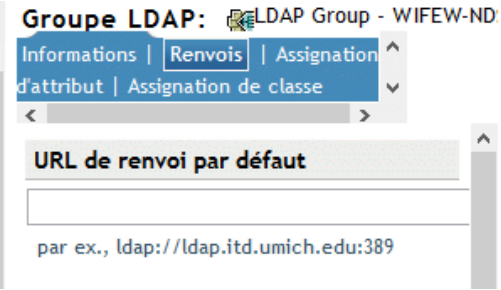
- Le serveur LDAP renvoie une erreur indiquant que l'entrée n'existe pas
- Le serveur LDAP indique que plus aucun renvoi ne peut être suivi.

Une fonctionnalité de LDAP pour eDirectory 8.7 occasionne un comportement légèrement différent des renvois par rapport aux anciennes versions d'eDirectory et NDS. Les différences influent sur la manière dont vous configurez les services LDAP.

Renvois par défaut

Généralement, une URL de renvoi par défaut contient une URL LDAP pointant vers un serveur qui contient la racine de l'arborescence. Une URL LDAP présente le format suivant : `ldap://hôte:port`.

Entrez un renvoi par défaut dans le champ URL de renvoi par défaut :



Au départ, le serveur LDAP eDirectory envoyait le renvoi par défaut dans un certain nombre de situations de reprise après échec. De nombreux utilisateurs estimaient ce comportement étrange et parfois imprévisible. Les services LDAP pour eDirectory vous permettent de contrôler quand le renvoi par défaut est envoyé pour tout type de renvoi subordonné.

La nouvelle option est une valeur (paramètre) qui réside dans l'attribut ldapDefaultReferralBehavior sur le serveur LDAP et les objets Groupe LDAP. Il s'agit d'un nombre entier qui est un masque binaire des bits ci-dessous.

bits	Valeur
0x00000001	Le DN de base est introuvable.
0x00000002	Le DN de base est sur un serveur eDirectory non disponible.
0x00000004	Une entrée dans l'étendue de la recherche se trouve sur un serveur eDirectory non disponible.

Si pour l'opération, le serveur LDAP est configuré pour Toujours référer et si l'une des conditions indiquées est respectée et que la valeur correspondante est définie, le renvoi par défaut est exécuté.

Définition de renvois pour les opérations de recherche

Une fonctionnalité de LDAP pour eDirectory 8.7 occasionne un comportement légèrement différent des renvois par rapport aux anciennes versions d'eDirectory et NDS. Les différences influent sur la manière dont vous configurez les services LDAP.

Vous pouvez configurer le serveur LDAP eDirectory pour qu'il transmette les renvois à d'autres serveurs eDirectory de l'arborescence. Par défaut, le serveur LDAP chaîne toutes les opérations vers d'autres serveurs eDirectory pour le compte de l'utilisateur et aucun renvoi n'est jamais retourné.

Avant eDirectory 8.7, les options de renvoi n'existaient que comme paramètres de l'objet Groupe LDAP. À partir de la version 9.0 d'eDirectory, vous pouvez également définir ces options sur l'objet Serveur LDAP. Tout paramètre de l'objet Serveur LDAP est prioritaire sur ceux de l'objet Groupe LDAP.

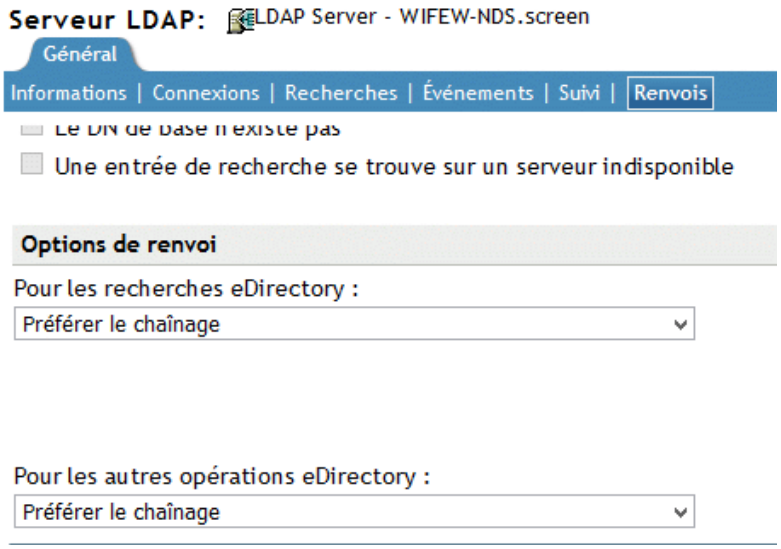
L'attribut ldapSearchReferralOption vous permet de définir l'option de renvoi. Dans les versions antérieures des services LDAP pour eDirectory 8.7, cet attribut pouvait être défini à l'aide des options suivantes :

- « Préférer le chaînage » page 423 (option par défaut)
- « Préférer les renvois » page 424
- « Toujours référer » page 424

Ces options de renvoi s'appliquent uniquement à la référence et au chaînage à d'autres serveurs eDirectory de l'arborescence eDirectory. Ces paramètres de configuration ne contrôlent pas les renvois provenant d'une partition non experte. Ainsi, même si vous sélectionnez une option (par exemple Toujours chaîner) dans la liste déroulante Options de renvois, les renvois parviendront toujours aux autres serveurs depuis des partitions non expertes.

Pour prendre en charge les renvois supérieurs vers des DSA non-eDirectory, les services LDAP pour eDirectory 8.7.a disposent d'une option Toujours chaîner. Reportez-vous à la section « Toujours chaîner » page 423.

La figure ci-dessous illustre les listes déroulantes de renvoi LDAP destinées aux recherches et aux autres opérations.



Les « autres » opérations eDirectory incluent des renvois pour les opérations d'ajout, de suppression, de modification et de liaison.

Toujours chaîner

L'option Toujours chaîner est une option indiquant qu'aucun renvoi ne sera jamais effectué. Si vous sélectionnez cette option, le serveur LDAP eDirectory ne retourne jamais les renvois à d'autres serveurs eDirectory de l'arborescence eDirectory. Le serveur LDAP effectue une vérification auprès des autres serveurs LDAP pour le compte du client demandeur et transmet le renvoi à celui-ci.

L'option Toujours chaîner s'avère très utile si eDirectory est déployé dans une arborescence fédérée globale sous la forme de serveurs subordonnés.

Ces options de renvoi s'appliquent uniquement à la méthode de gestion des renvois dans l'arborescence eDirectory. Elles n'ont aucun effet sur le comportement des renvois sur les serveurs non-eDirectory.

La raison du blocage des renvois sur d'autres serveurs eDirectory est subtile, mais peut s'avérer précieuse. Si les données non expertes d'un serveur eDirectory 8.7 ou ultérieur sont répliquées sur un autre serveur eDirectory, plus ancien, un renvoi au serveur plus ancien risque de fournir à une application client une vue déformée de l'arborescence globale.

Par exemple, imaginons qu'un client LDAP mette en cache les renvois vers les serveurs LDAP et envoie des requêtes au dernier serveur avec lequel il a communiqué. Si le client est configuré pour envoyer des requêtes à un serveur eDirectory prenant en charge des renvois supérieurs, la vue de l'arborescence globale doit être normale pour ce client.

Toutefois, les serveurs LDAP antérieurs à eDirectory 8.7 ne comprennent pas les zones non expertes et les renvois supérieurs. Par conséquent, si le client fait suivre un renvoi vers un serveur équipé d'une version plus ancienne d'eDirectory dans l'arborescence eDirectory et continue à envoyer des requêtes à ce serveur plus ancien, le serveur ayant la version plus ancienne de LDAP présentera les données non expertes comme s'il s'agissait des données réelles de l'arborescence Annuaire.

Un client intelligent doit, cependant, interroger l'attribut supportedFeatures de RootDSE pour vérifier si le serveur prend ou non en charge les renvois supérieurs.

Préférer le chaînage

L'option Préférer le chaînage indique que les résultats de recherche ne comprennent généralement pas de renvois. Au lieu de cela, le serveur LDAP fait progresser l'opération de recherche sur l'ensemble des DSA eDirectory pour la compléter.

L'exception à cela est une opération de recherche accompagnée du contrôle de recherche persistant. Dans ce cas, étant donné que la mise en oeuvre NetIQ de la recherche persistante ne prend pas en charge le chaînage, les renvois sont envoyés si l'étendue de la recherche ne reste pas totalement locale.

Le serveur LDAP reçoit une opération de recherche. Si l'entrée de l'arborescence n'est pas stockée localement, le serveur effectue automatiquement un chaînage vers les autres serveurs. Une fois l'entrée localisée, le serveur LDAP joue le rôle de proxy pour le client LDAP. En utilisant la même identité que celle à laquelle le client LDAP est lié, le serveur LDAP s'authentifie auprès du serveur distant et continue l'opération de recherche sur celui-ci.

Le serveur LDAP qui a reçu la demande de recherche initiale envoie au client LDAP l'ensemble des entrées de recherche et le résultat. Comme le serveur LDAP se charge intégralement de la demande, le client LDAP ne sait pas que d'autres serveurs étaient impliqués.

Grâce au chaînage d'eDirectory, un serveur LDAP qui contient peu d'informations peut sembler contenir les données de la totalité de l'arborescence.

L'option Préférer le chaînage est importante en ce qui concerne les partitions.

Scénario : recherche d'informations dans une autre partition— Dans la société Digital Airlines, Luc sélectionne l'option Préférer le chaînage pour le serveur LDAP DAir43. DAir43 se trouve dans la partition A. La partition B est une sous-partition de A et contient le serveur LDAP DAir44.

Un client LDAP lance une recherche. DAir43 recherche l'entrée localement mais ne trouve qu'une partie des données. DAir43 effectue automatiquement un chaînage vers DigitalAir44, qui contient l'entrée nécessaire. DAir44 envoie les données à DAir43, et ce dernier envoie l'entrée au client LDAP.

Avec l'option Préférer le chaînage, le serveur LDAP effectue un chaînage vers d'autres serveurs pour traiter les requêtes de recherche (le cas échéant), sauf si l'opération est une recherche persistante. Pour plus d'informations sur la recherche persistante, reportez-vous à la « Recherche persistante : configuration d'événements eDirectory » page 433.

Préférer les renvois

L'option Préférer les renvois indique que les opérations de recherche doivent retourner des renvois à d'autres serveurs eDirectory de l'arborescence le cas échéant. Des renvois sont émis seulement si le serveur local peut assurer que le serveur qui contient les données est opérationnel et que le service LDAP est exécuté. Dans le cas contraire, l'opération est chaînée à un autre serveur ou échoue si cet autre serveur est inutilisable.

Vous disposez de deux partitions et vous exécutez une recherche de sous-arborescence. Vous en arrivez à un stade où les entrées recherchées ne figurent plus sur le serveur local. La recherche doit donc porter sur un autre serveur. Si le serveur qui contient la réplique de ces données (de cette partition) exécute aussi le fichier `nldap.nlm`, le serveur LDAP crée un renvoi LDAP et le retourne au client LDAP.

Si le serveur contenant la réplique n'exécute pas `nldap.nlm`, le serveur LDAP chaîne la requête vers l'autre serveur, terminant ainsi la recherche.

Lorsque `nldap.nlm` démarre, le serveur LDAP indique à eDirectory que le serveur LDAP est un point de renvoi. Si un client a reçu des renvois mais que ceux-ci cessent, le serveur LDAP n'est pas en service.

Toujours référer

L'option Toujours référer suit la même logique que Préférer les renvois, sauf que le renvoi par défaut est envoyé dans différentes situations de reprise après échec (par exemple si l'objet est introuvable ou si le serveur est en panne).

Si un autre serveur contenant le reste des données n'exécute pas le service LDAP, le premier serveur LDAP ne chaîne alors pas la requête au deuxième.

Si vous activez l'option Toujours référer, vous êtes autorisé à saisir un renvoi par défaut. Le champ Renvoi par défaut est utile pour associer deux serveurs LDAP de fournisseurs différents et constituer votre propre arborescence Annuaire.

Scénario : utilisation d'un serveur par défaut— Vous disposez d'une arborescence LDAP. Une partie de cette arborescence est gérée par eDirectory. Une partition subordonnée est gérée par iPlanet. Dans le champ Renvoi par défaut, vous placez une URL renvoyant au serveur iPlanet. Un client LDAP lance une recherche.

Incapable de résoudre le DN de base, le serveur LDAP envoie au client la chaîne qui figure dans le champ Renvoi par défaut. Le renvoi indique au client LDAP de rechercher à l'endroit indiqué dans l'URL. Le client LDAP contacte le serveur iPlanet, qui exécute la recherche.

Si un renvoi par défaut est configuré et si le serveur ne trouve pas le DN de base recherché, le client reçoit ce renvoi par défaut.

Le renvoi présente le format d'une URL LDAP (par exemple, LDAP://123.23.45.6:389.

Lorsque le serveur LDAP transmet un renvoi par défaut à un client (parce que le DN de base est indisponible), il ajoute une barre oblique (/) et le DN recherché par le client. Le renvoi par défaut et les informations ajoutées sont transmis au client. Le client envoie la requête de recherche au serveur spécifié dans le renvoi par défaut.

L'objet Groupe LDAP comporte un champ de chaîne destiné au renvoi par défaut. Le serveur LDAP traite ces données comme une chaîne. Aucune validation n'a lieu. Tout ce qui est saisi est inséré au début du renvoi. Certaines données sont ajoutées à la fin de celui-ci. Le serveur LDAP s'attend à recevoir une chaîne semblable à une URL.

Lorsqu'ils reçoivent des renvois désignant d'autres serveurs eDirectory qui exécutent LDAP, les clients obtiennent deux renvois par serveur.

- un renvoi qui dirige le client vers le port en texte clair ;
- un renvoi qui dirige le client vers le port sécurisé.

Pour faire la différence entre les deux renvois, le renvoi en texte clair commence par `ldap://` et le port sécurisé par `ldaps://`.

En cas de renvoi provenant du serveur, le numéro de port est ajouté.

Définition de renvois pour d'autres opérations

Le paramétrage initial de l'option de renvoi ne s'appliquait qu'à l'opération de recherche. Pour fournir à d'autres opérations une option comparable, l'attribut ldapOtherReferralOption est utilisé. Cet attribut autorise les mêmes valeurs et contrôle le comportement des opérations qui ne comprennent pas de recherche (à l'exception de la liaison, qui n'émet jamais de renvois).

Filtrage de renvois

Si plusieurs serveurs de répliques sont en cours d'exécution dans une arborescence et que vous avez configuré les serveurs LDAP pour qu'ils retournent des renvois à l'aide de l'option Préférer les renvois/Toujours renvoyer, les serveurs LDAP retourneront des renvois si l'objet identifié par le DN dans l'opération demandée n'est pas présent localement. Dans ce cas, le client LDAP envoie une requête au serveur qui lui-même envoie une liste de renvoi de tous les serveurs LDAP contenant cet objet. À l'aide de cette liste de renvoi, les clients LDAP suivront l'un de ces renvois pour effectuer l'opération. Si le client choisit de suivre le renvoi vers un serveur en manque de ressources ou vers un serveur situé sur une liaison lente, il constatera une réponse lente de la part du serveur. Cette lenteur affecte les performances du client LDAP. Étant donné que les développeurs d'applications LDAP n'ont pas de connaissances complètes des serveurs et des configurations réseau, la solution à ce problème consiste à proposer un mécanisme de filtrage des renvois au niveau du serveur LDAP pour retourner les renvois de serveurs spécifiques. Les administrateurs disposeraient des connaissances nécessaires, par exemple, la nature des serveurs LDAP dans le réseau et les vitesses de liaison réseau pour effectuer la configuration appropriée du filtrage des renvois.

Définissez le filtre de renvoi sur l'objet Groupe LDAP à l'aide des attributs « referralIncludeFilter » et « referralExcludeFilter ». La configuration de ces filtres dans ces attributs sera applicable à tous les serveurs LDAP qui appartiennent à cet objet Groupe LDAP. Le serveur LDAP retournera tous les renvois LDAP correspondant au filtre referralIncludeList et omettra ceux qui correspondent au filtre referralExcludeFilter.

Si seul le filtre referralIncludeFilter est spécifié, les renvois LDAP correspondant aux valeurs referralIncludeFilter vont seront retournés aux clients LDAP, et tous les autres renvois seront exclus de la liste de renvoi. De même, si seul le filtre referralExcludeFilter est spécifié, les renvois LDAP qui ne correspondent pas aux valeurs referralExcludeFilter seront retournés aux clients LDAP. Si les deux filtres sont spécifiés et que le renvoi ne correspond pas à aucun d'eux, il sera exclu.

Si tous les renvois disponibles sont refusés par le filtre, le serveur se comporte comme si aucun renvoi n'est disponible et retourne LDAP_OTHER (80), que certains outils client rapportent comme une « Erreur inconnue ». Après avoir ajouté ou modifié ces attributs de filtre, si le serveur LDAP n'est pas rafraîchi, les modifications seront appliquées après le rafraîchissement automatique suivant.

Actuellement, l'ajout ou la modification de ces attributs de filtre n'est possible qu'avec l'onglet disponible dans iManager.

Format pour spécifier le filtrage des renvois LDAP — Le format de filtrage des renvois LDAP est un simple format d'adresse IP :

`[ldap://] | [ldaps://] Adresse_IP[:port]`

Dans ce cas, spécifier le port en texte clair ou le port TLS aura le même effet que d'ajouter `ldap://` ou `ldaps://` au début. Si vous ne spécifiez ni `ldap` ni `ldaps`, le filtre de correspondance est applicable aux renvois tant en texte clair que TLS.

Exemples :

Exemples	Description
`1.2.3.4`	# correspond aux renvois tant LDAP que LDAPS sur un port quelconque
`1.2.`	# correspond à toutes les adresses IP de 1.2.X.Y
`1.2.3.`	# correspond à toutes les adresses IP de 1.2.3.Y
`ldap://` ou `ldap://*`	# correspond à tous les renvois LDAP sur un port en texte clair
`ldaps://` ou `ldap://*`	# correspond à tous les renvois LDAP sur un port ssl
`*`	# correspond à tout
`ldaps://5.6.7.8:636`	# correspond au port SSL 636 sur les adresses IP 5.6.7.8

Les attributs de filtre (`referralIncludeFilter` et `referralExcludeFilter`) sont à plusieurs valeurs. Vous pouvez choisir autant de filtres de correspondance que nécessaire.

Exemples de scénarios

- Pour configurer un serveur LDAP pour qu'il retourne uniquement les renvois avec l'adresse IP 1.2.X.Y où X = {0 à 255} et Y = {0 à 255} et exclure tous les autres, entrez la commande suivante :

  referralIncludeFilter = { 1.2 }

- Pour configurer un serveur LDAP pour qu'il exclue tous les renvois qui correspondent à l'adresse IP 164.99.X.Y, où X n'est pas égal à 100, et inclue tous les renvois correspondant à l'adresse IP 164.99.100.Y, entrez les commandes suivantes :

  ```
  referralIncludeFilter = { 164.99.100., "*"}
  referralExcludeFilter = { 164.99. }
  ```

  Dans ce cas, même si l'adresse IP 164.99.100.Y correspond au filtre `referralExcludeFilter`, étant donné que ces adresses IP ont plusieurs champs correspondants, ces renvois seront retournés aux clients LDAP.

  REMARQUE : lorsque vous spécifiez une adresse IP partielle, le « . » final peut être omis.

- Pour configurer un serveur LDAP pour qu'il retourne uniquement les renvois de port en texte clair et omette les renvois de port SSL, entrez la commande suivante :

  ```
  referralIncludeFilter = { "ldap://" }
  ```

  OU

  ```
  referralExcludeFilter = { "ldaps://" }
  ```

- Pour configurer un serveur LDAP pour qu'il retourne les renvois de certaines adresses IP et omette tous les autres renvois d'adresse IP, entrez les commandes suivantes :

  ```
  referralIncludeFilter = { 1.2.3.4, 2.3.4.5:389, 3.4.5.6:636, ldaps://4.5.6.7 }
  referralExcludeFilter = { "*" }
  ```

  REMARQUE : dans ce cas, `referralExcludeFilter` n'est pas nécessaire. Un filtre `referralIncludeFilter` renseigne exclut tous les autres.

- Il existe deux types de filtres, comme suit :

  ```
  referralIncludeFilter = { 1.2.3.4 }
  referralExcludeFilter = { 2.3.4.5 }
  ```

  Un renvoi avec l'adresse IP 3.4.5.6 sera exclu, car il ne correspond pas au filtre referralInclude, même s'il ne correspond pas non plus au filtre `referralExcludeFilter`.

Filtres non valides — Les filtres suivants ne sont pas pris en charge.

« .2.3.4 » ou « *.2.3.4 » ne renvoie pas les adresses IP *X*.2.3.4.

« 2.3.4* » ne renvoie pas les adresses IP, telles que 2.3.41 ou 2.3.42.

Les noms DNS comme sever1.mydomain.com, ou *.mydomain.com ne sont pas pris en charge. L'ajout de la plage de ports aux filtres de type Autoriser l'adresse IP de renvoi sur le port start-to-end n'est pas pris en charge. Aucun contrôle de validation n'est effectué avant d'ajouter ces valeurs de filtre à ces attributs. Toutefois, dans le cas d'un filtre non valide, le serveur LDAP ignorera ces filtres et consignera les informations dans le fichier `ndsd.log`.

Problèmes connus — La recherche LDAP rootDSE renvoie altServers s'il existe des serveurs de réplique au format d'URL LDAP. Ces URL ne sont pas filtrées à l'aide de ce mécanisme.

Pas de prise en charge de la gestion de DSA IT

Dans les services LDAP pour eDirectory, les relations distribuées entre les serveurs eDirectory d'une arborescence eDirectory sont gérées par d'autres moyens que la commande Gérer DSA IT. La commande Gérer DSA IT n'autorise pas le client LDAP à interroger ou à mettre à jour les références eDirectory subordonnées ou croisées.

Fonctionnalité non prise en charge

Les services LDAP pour eDirectory ne prennent pas en charge les références subordonnées. Il n'est pas possible de créer de façon fiable une partition non experte qui soit subordonnée à une partition experte et de lui faire émettre des renvois. Si optez pour ce cas de figure, les renvois ne sont transmis que lors de la résolution du DN de base pour une opération. Les références SearchResultReferences ne sont pas envoyées.

Il n'existe aucune prise en charge des mises à jour distribuées de données dans la zone non experte. Si un changement de nom se produit sur le serveur racine, aucun mécanisme intégré n'est présent pour copier cette modification de nom dans le serveur eDirectory qui contient les mêmes données dans une zone non experte.

Recherche de répliques filtrées

Un filtre limite la quantité de données que contient la réplique. De ce fait, une réplique filtrée n'affiche pas l'ensemble des données réelles contenues dans l'annuaire. Voici quelques exemples de filtres appliqués à une réplique :

- La réplique contient uniquement des objets Utilisateur.
- La réplique contient tous les objets Utilisateur, mais ces derniers ne contiennent que des numéros de téléphone et des adresses d'expédition.

Comme les données d'une réplique filtrée sont incomplètes, une recherche LDAP peut donner lieu à des résultats tronqués. Par conséquent, une requête de recherche LDAP n'examine pas, par défaut, les répliques filtrées.

Lorsque vous effectuez une recherche dans les répliques filtrées, celle-ci peut ne pas retourner les résultats par filtre de réplique dans les cas suivants :

- Si les objets correspondant au filtre de recherche ne sont pas présents sur le serveur de répliques filtrées locales, les résultats peuvent ne pas correspondre au filtre de la réplique locale, dans la mesure où les résultats peuvent être trouvés par un serveur de répliques complètes.
- Lorsque la base de recherche n'est pas sur le serveur de répliques filtrées, les objets correspondant au filtre de recherche peuvent être obtenus à partir d'un serveur de répliques complètes et ne pas correspondre au filtre de la réplique locale.

Vous pouvez cependant configurer un serveur LDAP pour rechercher dans les répliques filtrées si vous êtes certain que ces dernières contiennent les données dont vous avez besoin.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **LDAP** > **Options LDAP**.
3. Cliquez sur **Afficher les serveurs LDAP**, puis cliquez sur le nom d'un serveur LDAP.
4. Cliquez sur **Recherches**.
5. Sélectionnez **Inclure les répliques filtrées dans la recherche**, puis cliquez sur **Appliquer**.

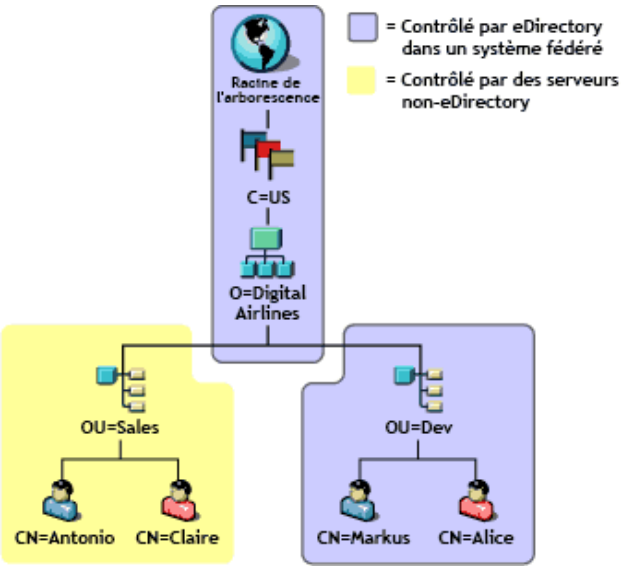
Configuration des renvois supérieurs

Il arrive souvent que les déploiements importants nécessitent une arborescence Annuaire utilisant des logiciels Serveur LDAP de différents fournisseurs. Elle est alors appelée arborescence fédérée globale. Les services LDAP pour eDirectory ont la capacité de retourner des renvois à un DSA supérieur de l'arborescence fédérée.

Scénario : renvois supérieurs dans une arborescence fédérée

Luc est responsable des réseaux de Digital Airlines. Un serveur OpenLDAP est utilisé pour gérer la racine d'une arborescence Annuaire de Digital Airlines (de la racine de l'arborescence à O=Digital Airlines). Une organisation (OU=Ventes) est gérée par un serveur eDirectory, et une autre (OU=Dev), réside sur un serveur iPlanet.

La figure suivante illustre cette arborescence :



eDirectory ne gère que les données de la partition pour OU=Ventes. Les données des autres zones sont gérées sur des DSA non-eDirectory. Luc configure les services LDAP de telle sorte qu'ils retournent des renvois supérieurs à chaque fois qu'une opération prend racine sur O=Digital Airlines ou au-dessus, ou à n'importe quel point sous O=Digital Airlines qui ne fait pas partie de la hiérarchie OU=Ventes.

Une opération est envoyée au serveur LDAP eDirectory, avec le DN de base OU=Dev,O=Digital Airlines,C=US. Le renvoi retourné pointe vers les serveurs qui contiennent cette entrée ou vers ceux qui savent quels serveurs la contiennent.

De même, lors d'une recherche dans la sous-arborescence ayant comme racine O=Digital Airlines, C=US débouche sur un renvoi au DSA racine. Ce dernier retourne à son tour des renvois vers les DSA qui gèrent OU=Ventes et OU=Dev.

Pour que le serveur eDirectory puisse intégrer cette arborescence, les services LDAP permettent à eDirectory de disposer des données hiérarchiques supérieures dans une partition marquée comme non experte. Les objets de la zone non experte sont seulement les entrées nécessaires à l'élaboration d'une hiérarchie DN correcte. Ces entrées sont analogues aux entrées d'association X.500.

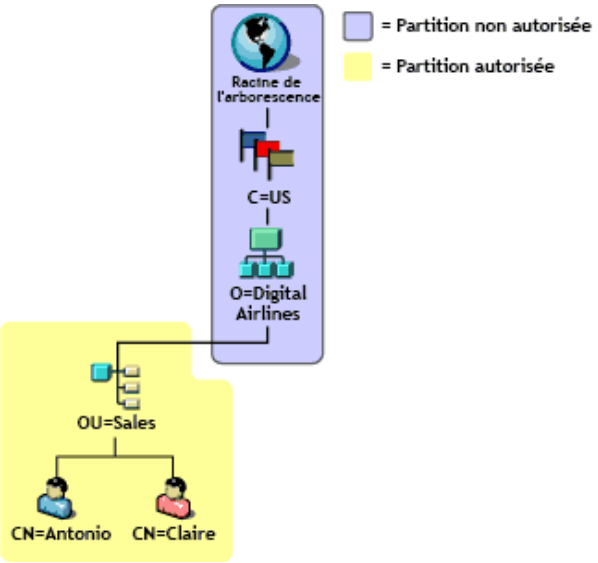
Dans ce scénario, les objets Racine, C=US et O=Digital Airlines résident sur le serveur eDirectory dans une zone non experte.

eDirectory permet de placer des informations de connaissance (données de renvoi) à l'intérieur de zones non expertes. Ces informations servent à retourner les renvois au client LDAP.

Lorsqu'une opération LDAP est effectuée dans une zone non experte de l'arborescence eDirectory, le serveur LDAP recherche les données de référence correspondantes et transmet un renvoi au client.

Création d'une zone non experte

La figure suivante illustre les données présentes sur le serveur eDirectory de l'arborescence fédérée présentée à la section « Scénario : renvois supérieurs dans une arborescence fédérée » page 429.



Notez que des entrées sont situées au-dessus de OU=Ventes, même si elles sont gérées par un autre DSA. Ce placement est nécessaire pour fournir les DN corrects aux entrées gérées par le serveur eDirectory.

Pour créer une zone non experte :

1. Séparez les données non expertes des données expertes.

   Créez une limite de partition au sommet de la zone experte. Un serveur eDirectory se considère expert pour toutes les données qu'il contient, sauf indication contraire.

2. Marquez la partition racine comme non experte.

   2a Ajoutez l'attribut expert à l'entrée la plus proche de la racine dans la partition.

   2b Attribuez la valeur zéro à l'attribut expert.

3. Tracez une limite au bas de la zone non experte.

   Créez des racines de partition dans les zones de la sous-arborescence pour lesquelles ce serveur doit être expert. Par exemple, sur la figure ci-dessus, l'entrée OU=Ventes est une racine de partition. Dans les nouvelles partitions, l'attribut expert n'est pas défini sur zéro. Par conséquent, le serveur sera expert pour les partitions.

4. Rafraîchissez le serveur LDAP.

   Le serveur LDAP met en cache les limites des zones experte et non experte à chaque rafraîchissement de sa configuration. Si vous ne rafraîchissez pas manuellement la configuration du serveur, celui-ci le fait automatiquement lors d'une tâche en arrière-plan de 30 minutes.

   Plusieurs partitions peuvent être empilées en une chaîne de zones non expertes. Toutefois, les services LDAP pour eDirectory nécessitent que toutes les partitions non expertes soient contiguës et présentes dans des répliques locales.

Spécification des données de référence

Quand le serveur LDAP détermine qu'une opération s'effectue dans une zone non experte, il recherche les informations qu'il peut utiliser pour retourner un renvoi au client. Ces informations de renvoi peuvent figurer aux emplacements suivants :

- sur n'importe quelle entrée de la zone non experte ou sur toutes ces entrées ;
- sur l'objet Serveur LDAP ou Groupe LDAP qui contient les données de configuration du serveur, sous forme de renvoi par défaut.

Les informations de renvoi présentes dans les entrées de la zone non experte constituent une référence supérieure immédiate. Ces informations de renvoi consistent en un attribut ref à valeurs multiples. Pour obtenir la description de cet attribut, reportez-vous au fichier RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt).

Les informations de renvoi présentes dans le paramètre de configuration Renvoi par défaut constituent une référence supérieure et ne contiennent qu'une seule valeur. Reportez-vous aux types de DSE immSupr et supr dans X.501.

Les données de référence sont consignées sous la forme d'une URL LDAP, mais n'indiquent que l'hôte et (de façon facultative) le port des DSA faisant l'objet de la référence. L'exemple suivant illustre ces données de référence :

```
ldap://ldap.digital_airlines.com:389
```

Le serveur LDAP observe le DN de base de l'opération (ou s'il est introuvable, le DN correspondant). Si le DN de base contient des informations de référence, le serveur LDAP renvoie celles-ci sous la forme d'un renvoi.

Si aucune information de référence n'est trouvée, le serveur LDAP parcourt l'arborescence vers le haut à la recherche d'informations de référence. S'il n'en trouve aucune après avoir essayé toutes les entrées, le serveur LDAP renvoie la référence supérieure. Cette référence figure dans le paramètre de renvoi par défaut de l'objet Groupe LDAP ou Serveur LDAP.

Ajout d'une référence supérieure immédiate

Vous pouvez ajouter une classe d'objet auxiliaire dénommée immeditateSuperiorReference (référence supérieure immédiate) à une entrée de la zone non experte. Cette classe auxiliaire ajoute un attribut ref indiqué avec une ou plusieurs URL LDAP. Chaque URL pointe sur le nom d'hôte et (facultatif) le port d'un DSA.

Ajout d'une référence supérieure

À l'origine, l'objet Groupe LDAP comportait un attribut ldapReferral. Cet attribut contenait une référence par défaut qui était utilisée pour diverses situations de reprise après erreur lors du retour de renvois à d'autres serveurs eDirectory d'une arborescence eDirectory. Dans les services LDAP pour eDirectory, cet attribut est utilisé pour contenir un seul renvoi par défaut vers un DSA supérieur au sein d'une arborescence fédérée.

Par ailleurs, l'attribut ldapReferral a été ajouté à l'objet Serveur LDAP. Si l'attribut ldapReferral contient une valeur pour l'objet Serveur LDAP, ce paramètre est prioritaire sur la valeur contenue dans le même attribut pour l'objet Groupe LDAP. Ce comportement vous permet de configurer tous les serveurs LDAP d'un groupe pour qu'ils aient un renvoi donné par défaut, en ne laissant qu'un ou deux serveurs remplacer cette valeur par un autre renvoi par défaut.

La valeur de l'attribut ldapReferral est une URL LDAP. Cette URL contient l'hôte et le port facultatif du DSA auquel il est fait référence.

Mise à jour des informations de références par l'intermédiaire de LDAP

Si vous avez suivi les procédures ci-dessus dans l'ordre et utilisé LDAP pour exécuter les tâches, vous n'avez probablement pas pu ajouter une référence supérieure immédiate. En effet, comme la partition racine a déjà été marquée comme non experte, LDAP émet des renvois pour toute opération agissant sur les données de cette partition.

Pour permettre la mise à jour ou l'interrogation des informations d'une zone non experte, la commande Gérer DSA IT doit accompagner la requête LDAP. Pour plus d'informations sur ce contrôle, reportez-vous au fichier RFC 3296 (http://www.ietf.org/rfc/rfc3296.txt). Ce contrôle pousse effectivement le serveur LDAP à considérer l'ensemble de la zone non experte comme si elle l'était.

REMARQUE : la fonction de référence supérieure est seulement accessible via LDAP. Les autres protocoles (par exemple, NDAP) ne sont pas influencés par la présence de l'attribut expert. Par conséquent, rien ne vient entraver l'utilisation de NetIQ iManager lors de l'interrogation et de la mise à jour de données dans la zone non experte.

Opérations touchées

Les zones non expertes et les renvois supérieurs agissent sur les opérations LDAP suivantes :

- Rechercher et comparer
- Modifier et ajouter

  Les valeurs des attributs de syntaxe du DN ne sont pas vérifiées. Par conséquent, un attribut membre du groupe peut contenir des DN qui pointent vers des entrées d'une zone non experte.
- Supprimer
- Renommer (moddn)
- Déplacer (moddn)

  Si le DN parent se situe dans une zone non experte, une erreur affectsMultipleDSAs doit être renvoyée.
- Opérations étendues

Prise en charge des références supérieures

Seuls les services LDAP pour eDirectory 8.7 et versions ultérieures prennent en charge les renvois supérieurs. Pour savoir si un serveur eDirectory prend en charge cette fonctionnalité, consultez l'attribut supportedFeatures sur le DSE racine. Si l'attribut supportedFeatures liste l'OID 2.16.840.1.113719.1.27.99.1, ces fonctions sont disponibles. Les autres modifications de l'objet DSE racine liées à la découverte sont notamment les suivantes :

- namingContexts

  Cet attribut ne liste que les racines de la partition figurant sur le DSA local sur lequel le serveur a autorité. Les racines des partitions non expertes sont listées.
- altServer

Cet attribut ne répertorie pas les autres serveurs eDirectory qui partagent seulement des partitions non expertes avec le serveur local.

- superiorReference

  Cet attribut annonce le renvoi supérieur pour le DSA. Cette valeur est administrée par la mise à jour de l'attribut ldapReferral sur l'objet Serveur LDAP ou Groupe LDAP.

Recherche persistante : configuration d'événements eDirectory

NetIQ eDirectory dispose d'un service d'événements permettant de signaler aux applications les événements importants qui se produisent au sein de l'annuaire. Certains d'entre eux sont des événements généraux qui peuvent relever de n'importe quel service d'annuaire. D'autres événements sont spécifiques à eDirectory et à ses fonctions spéciales.

Les événements eDirectory sont exposés aux applications par l'intermédiaire de deux extensions distinctes du protocole LDAP :

- Une mise en oeuvre du contrôle de la recherche persistante

  La fonction Recherche persistante de NetIQ eDirectory est une opération de recherche qui se poursuit après le renvoi de la première série d'entrées correspondantes. La recherche persistante est une extension de l'opération de recherche LDAP v3 qui permet de faire basculer la tâche de recherche de mises à jour dans un ensemble de résultats du client vers le serveur. Le contrôle Recherche persistante permet au client d'effectuer une recherche LDAP normale (en spécifiant le DN de base, l'étendue et le filtre de la recherche, etc.) à l'issue de laquelle, au lieu d'un message `SearchResultDone` renvoyé par le serveur, une connexion est maintenue de sorte que le client puisse être informé à chaque modification d'une entrée dans les résultats. Ainsi, le client peut gérer un cache des entrées qui l'intéressent ou déclencher une opération logique dès qu'une mise à jour se produit.

  Le fichier « Persistent Search: A Simple LDAP Change Notification Mechanism » (http://www.ietf.org/proceedings/01mar/I-D/ldapext-psearch-03.txt) (Recherche persistante : un mécanisme de notification simple en cas de modification LDAP) décrit cette extension plus en détail.

- Surveillance des événements (une fonction LDAP étendue propre à eDirectory)

Les applications qui utilisent les services d'événements eDirectory peuvent représenter une lourde charge de traitement pour l'annuaire. Divers paramètres d'administration permettent de déterminer la manière dont les services d'événements sont employés sur chaque serveur eDirectory. Ces paramètres sont stockés dans l'objet Serveur LDAP. NetIQ iManager permet de définir ces paramètres.

Pour certaines applications qui emploient le service d'événements, il peut être nécessaire d'affecter des valeurs spécifiques à ces paramètres. La documentation de ces applications indique leurs besoins propres.

Pour plus d'informations, reportez-vous au document « Understanding and Using Persistent Search in eDirectory » (http://support.novell.com/techcenter/articles/dnd20030204.html) (Compréhension et utilisation de la recherche persistante dans eDirectory).

Gestion des recherches persistantes

iManager vous permet d'afficher ou de modifier les recherches persistantes.

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

3 Spécifiez le nom et le contexte de l'objet Serveur LDAP à modifier, ou cliquez sur pour rechercher ou accéder à l'objet Serveur LDAP.

4 Cliquez sur **OK**, puis sur **Recherches** sous l'onglet **Général**.

5 Activez les recherches persistantes.

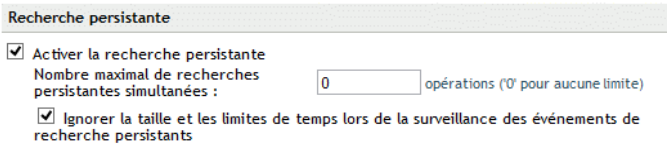
Par défaut, la case **Activer la recherche persistante** est cochée. Pour désactiver et empêcher les recherches persistantes sur ce serveur, désélectionnez la case à cocher.

REMARQUE : si vous désactivez une opération de recherche persistante précédemment établie, il se peut que la recherche continue, même après la désactivation de l'option et le rafraîchissement du serveur.

---

6 Déterminez le nombre de recherches persistantes simultanées à effectuer sur le serveur concerné.

Entrez une valeur dans le champ **Nombre maximal de recherches persistantes simultanées**. La valeur zéro autorise un nombre illimité de recherches persistantes simultanées.



7 Déterminez si vous souhaitez ignorer les limites de taille et de temps.

Pour déterminer si les limites de taille et de temps doivent être ignorées une fois que la recherche persistante a envoyé la première série de résultats, cochez la case **Ignorer la taille et les limites de temps lors de la surveillance des événements de recherche persistants**.

Si vous ne la cochez pas, toute la recherche persistante est soumise aux restrictions de la recherche. Si l'une des limites est atteinte, la recherche échoue et le message d'erreur correspondant s'affiche.

8 Cliquez sur **Appliquer**, puis sur **OK**.

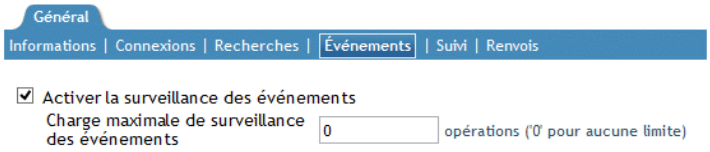
Contrôle de l'emploi de l'opération étendue de surveillance des événements

1 Dans iManager, cliquez sur le bouton **Rôles et tâches** .

2 Cliquez sur **LDAP** > **Options LDAP**.

3 Cliquez sur **Afficher les serveurs LDAP**, puis cliquez sur le nom d'un serveur LDAP.

4 Cliquez sur **Événements**.



5 Déterminez si les applications client peuvent surveiller les événements de ce serveur LDAP.

Pour permettre aux applications clientes de surveiller les événements sur ce serveur LDAP, cochez la case **Activer la surveillance des événements**.

Pour empêcher la surveillance des événements, désélectionnez cette case.

6 Déterminez la charge maximale que les applications de surveillance des événements peuvent placer sur le serveur.

Entrez une valeur dans le champ **Charge maximale de surveillance des événements**.

Le traitement de données et l'envoi de notifications d'événements à des applications de surveillance impliquent une importante charge de traitement pour le serveur LDAP. Pour chaque événement, la charge précise du serveur dépend de la fréquence à laquelle survient l'événement surveillé, des données associées à ce dernier et du nombre d'applications client qui le surveillent.

La charge maximale de surveillance des événements est une valeur relative indiquant la proportion de charge que l'extension de surveillance des événements est autorisée à placer sur le serveur. La valeur zéro indique qu'aucune limite n'a été définie. Pour déterminer la valeur appropriée de cet attribut, faites des essais.

7 Cliquez sur **Appliquer**, puis sur **OK**.

Obtention d'informations sur le serveur LDAP

Pour obtenir des informations sur un serveur LDAP, vous devez utiliser une recherche LDAP ou ICE. Les utilitaires correspondants ont besoin d'informations de rootDSE (Directory Service Agent, entrée spécifique).

rootDSE est un pseudo-objet d'une arborescence d'annuaire. Il s'agit d'une entrée sans nom à la racine de l'arborescence. RootDSE contient des informations propres au serveur auquel vous êtes connecté. À titre d'exemple, rootDSE sait où se trouvent les extensions et le schéma, et vérifie la prise en charge de ce dernier.

rootDSE n'étant pas une entrée dénommée de l'arborescence, un serveur LDAP ne le retourne pas au client dans le cadre d'une opération de recherche normale.

Le tableau ci-dessous liste les informations provenant de rootDSE.

Informations et description	Extrait
Emplacement du schéma : vous trouverez l'emplacement du schéma de l'arborescence ou du serveur LDAP en lisant subschemaSubentry. Pour eDirectory, cn=schema constitue la base de la recherche.	subschemaSubentry: cn=schema
Extensions prises en charge : les extensions permettent de gérer le serveur (par exemple, de créer ou de fusionner des contextes, d'ajouter de nouvelles répliques, de rafraîchir le serveur LDAP, de supprimer des répliques, de changer le type de la réplique maîtresse en Lecture-écriture ou Lecture seule) et les identités. Les extensions sont au format ASN.1OID. Pour les noms des extensions, reportez-vous à la rubrique LDAP Extensions (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a6ik7oi.html) (Extensions LDAP) de la documentation.	supportedExtension: 2.16.840.1.113719.1.27.100.12 supportedExtension: 2.16.840.1.113719.1.27.100.7 supportedExtension: 2.16.840.1.113719.1.27.100.8
Nom du fournisseur du serveur LDAP.	vendorName: NetIQ Corporation.
Version d'annuaire prise en charge par le serveur LDAP.	vendorVersion: eDirectory v8.7.0 (10410.29)
Version d'eDirectory en cours d'exécution.	vendorVersion: eDirectory v8.7.0 (10410.29)
Nom du serveur d'annuaire et nom de l'arborescence Annuaire.	dsaName: cn=WestWindNDS,o=westwind directoryTreeName: t=WESTWINDTREE
Mécanismes SASL pris en charge.	supported SASLMechanisms: EXTERNAL supported SASLMechanisms: DIGEST-MD5 supported SASLMechanisms: NMAS LOGIN
Version du serveur LDAP prise en charge.	supportedLDAPVersion: 2 supportedLDAPVersion: 3
Statistiques du serveur : RootDSE fournit une quantité de statistiques sur le serveur LDAP (par exemple, le nombre de liaisons d'authentification forte).	errors: 0 securityErrors: 0 chainings: 3 referralsReturned: 6 extendedOps: 0 abandonOps: 0 wholeSubtreeSearchOps: 1

Les informations fournies par rootDSE sont utiles aux développeurs d'application.

Scénario : développement d'une application— Henri écrit une application qui crée une nouvelle réplique. En lisant rootDSE, Henri trouve supportedExtension: 2.16.840.1.113719.1.27.100.7 dans la liste. Il sait que le serveur prend en charge l'appel de création d'une réplique.

De plus, NetIQ iManager vérifie quelles fonctionnalités sont disponibles dans rootDSE et adapte son comportement en conséquence.

Pour rechercher rootDSE, entrez les données suivantes sur un poste de travail :

```
ldapsearch -h nom_hôte -p 389 -b "" -s base "objectclass=*"
```

Cette recherche peut être effectuée par n'importe quelle application utilisant les API ldap_search.

La clé de la recherche est que la portée est la base (`-s base`). Notez également que la base est nulle et le filtre défini sur `objectclass=*`. Dans le cas de ce client, la base est `-b`.

Pour plus d'informations sur la lecture de rootDSE, reportez-vous à l'une des références suivantes :

- LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html)
- LDAP Classes for Java (http://developer.novell.com/documentation/jldap/jldapenu/data/bktitle.html)

Pour plus d'informations sur les filtres de recherche LDAP, reportez-vous à la section Filtres de recherche LDAP (http://developer.novell.com/ndk/doc/ldapover/ldap_enu/data/a3saoeg.html). Cette section figure dans la section relative à l'intégration LDAP et NDS de la documentation NDK.

Configuration de la prise en charge de l'heure au format généralisé

La prise en charge de l'heure au format généralisé permet d'afficher l'heure au format `AAAAMMJJHHmmSS.0Z`. Vous pouvez activer ou désactiver la prise en charge de l'heure au format généralisé LDAP à l'aide de l'utilitaire ldapconfig ou du plug-in LDAP iManager.

La prise en charge de l'heure au format généralisé peut être activée à l'aide de l'une des méthodes suivantes :

Plug-in LDAP iManager

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches**.
2. Cliquez sur **LDAP** > **Options LDAP** > **Afficher les serveurs LDAP**.
3. Cliquez sur l'objet Serveur LDAP > **Recherches**.
4. Faites défiler jusqu'à atteindre la section Comportements non standard, cliquez sur **Afficher l'heure au format Généralisé**, puis sur **OK**.

Utilitaire ldapconfig

```
ldapconfig set "ldapGeneralizedTime=yes/no" -a <admin-FDN> -w <admin-password">
```

Configuration du contrôle permissif des modifications

Il est possible d'étendre l'opération de modification LDAP en cours en définissant l'option ldapPermissiveModify sur TRUE. Si vous tentez de supprimer un attribut qui n'existe pas ou d'ajouter une valeur à un attribut existant, l'opération s'effectue sans afficher de message d'erreur.

Plug-in LDAP iManager

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches**.
2. Cliquez sur **LDAP** > **Options LDAP** > **Afficher les serveurs LDAP**.
3. Cliquez sur l'objet Serveur LDAP > **Recherches**.
4. Faites défiler jusqu'à atteindre la section Comportements non standard, cliquez sur **Activer le contrôle permissif des modifications**, puis sur **OK**.

Utilitaire ldapconfig

```
ldapconfig set "ldapPermissiveModify=yes/no" -a <admin-FDN> -w <admin-password">
```

Contrôle de l'autorisation par proxy

eDirectory offre la flexibilité de contrôler l'autorisation par proxy par le biais du protocole LDAP comme spécifié dans le fichier RFC 4370. Le contrôle de l'autorisation par proxy permet à un client de demander qu'une opération soit traitée avec une identité d'autorisation fournie au lieu de l'identité d'autorisation actuelle associée à la connexion. Cette fonction propose un mécanisme permettant de spécifier une identité d'autorisation pour chaque opération, ce qui est utile pour les clients qui doivent effectuer plusieurs opérations pour le compte de plusieurs utilisateurs.

Pour s'authentifier auprès du serveur eDirectory, un administrateur doit fournir le contrôle d'autorisation par proxy OID `2.16.840.1.113730.3.4.18` dans la requête cliente. Pour utiliser le contrôle d'autorisation par proxy, l'utilisateur authentifié doit disposer de droits Superviseur sur l'utilisateur représenté.

1. Créez une arborescence eDirectory et ajoutez-lui des objets Utilisateur.
2. Connectez-vous à **iManager > Rôles et tâches > Droits > Modifier les ayants droit** et sélectionnez un utilisateur.
3. Cliquez sur **OK**.
4. Cliquez sur **Ajouter un ayant droit** et sélectionnez un autre utilisateur dans la liste.
5. Cliquez sur **Droits assignés** pour l'utilisateur.
6. Sélectionnez **Superviseur** pour **Tous les droits d'attribut** et **Droits d'entrée** pour l'utilisateur.
7. Cliquez sur **Terminé**, puis sur **Appliquer**.

Pour effectuer l'autorisation par proxy pour `ldapsearch,` utilisez la commande suivante :

```
ldapsearch -x -h <SrvIP> -p <Port> -D <Admin DN> -w <Password> -e
'!authzid=dn:<Impersonate user> -b o=novell -s one
```

Pour effectuer d'autres opérations LDAP à l'aide du contrôle d'autorisation par proxy, indiquez l'OID `2.16.840.1.113730.3.4.18` dans la requête LDAP.

Audit des opérations d'autorisation par proxy

Pour auditer les opérations d'autorisation par proxy, eDirectory propose un nouvel événement appelé DSE_IMPERSONATE.

Contrôle du DN étendu LDAP

eDirectory propose un contrôle du DN étendu LDAP qui est utilisé avec une recherche LDAP étendue pour demander une forme étendue de l'objet `Distinguished Name` (Nom distinctif). La forme étendue inclut une représentation de chaîne de `Object GUID` (GUID d'objet) avec le nom distinctif (`Distinguished Name`) de l'objet.

Pour utiliser la fonction de contrôle du DN étendu LDAP avec le serveur eDirectory, un administrateur doit fournir l'OID de contrôle de DN étendu LDAP `1.2.840.113556.1.4.529` dans la requête de recherche LDAP étendue.

Le contrôle du DN étendu permet au client de demander que les résultats d'une recherche LDAP qui utilise ce contrôle renvoient les données GUID d'un objet ainsi que l'objet `distinguishedName`, avec la syntaxe suivante :

```
<GUID=xxxxxxxx>;distinguishedName
```

Où `xxxxxxxx` est une chaîne qui contient le `GUID` et `distinguishedName` est le nom distinctif (`DN`), comme dans l'exemple `cn=users,dc=fabrikam,dc=com`.

Le contrôle du DN étendu LDAP peut être transmis avec une valeur de drapeau entier. La valeur de drapeau transmise spécifie le format de chaîne de la valeur GUID renvoyée et est définie sur la séquence codée au format Ber suivante :

```
Sequence {
  Flag    INTEGER
}
```

Une valeur de drapeau 0 indique une valeur GUID renvoyée au format de chaîne hexadécimale telle que `<GUID=3BC72D2DEC5A704BBDC21F4EF97B7870>`.

Une valeur de drapeau 1 renvoie la valeur de GUID au format de chaîne standard telle que `<GUID = 098f2470-bae0-cd 11-b579-08002b30bfeb >`.

Il existe plusieurs types de données complexes d'eDirectory qui incluent le DN comme en faisant partie intégrante. eDirectory traite uniquement les types de données complexes suivants avec le contrôle du DN étendu LDAP :

- SYN_PATH (GUID est renvoyé pour `volumeDN`)
- SYN_DN
- SYN_TYPED_NAME

REMARQUE : les performances de recherche LDAP seront affectées lors de l'utilisation du contrôle de DN étendu avec les types de données complexes mentionnés ci-dessus.

Exemples :

Le code d'exemple C++ suivant montre comment formater manuellement les données de la séquence. La fonction `ber_printf` permet de créer les données de séquence. La partie des drapeaux contient l'indicateur du format de chaîne GUID :

```
LDAPControl *FormatExtDNFlags(int iFlagValue)
{
  BerElement *pber = NULL;
  LDAPControl *pLControl = NULL;
  berval *pldctrl_value = NULL;
  int success = -1;

  // Ensure that iFlagValue is either 0 or 1. Convert TRUE (-1) to a legal value.
  if(iFlagValue != 0)
         iFlagValue = 1;

  // Format and encode the SEQUENCE data in a BerElement.
  pber = ber_alloc_t(LBER_USE_DER);
  if(pber==NULL) return NULL;
  pLControl = new LDAPControl;
  if(pLControl==NULL) { ber_free(pber,1); return NULL; }
  ber_printf(pber,"{i}",iFlagValue);

  // Transfer encoded data into a BERVAL.
  success = ber_flatten(pber,&pldctrl_value);
  ber_free(pber,1);
  if(success != 0) {return NULL;}
```

```
  // Copy the BERVAL data to the LDAPControl structure.
  pLControl->ldctl_oid = LDAP_SERVER_EXTENDED_DN_OID;
  pLControl->ldctl_iscritical = true;
  pLControl->ldctl_value.bv_val = new char[pldctrl_value->bv_len];
  memcpy(pLControl->ldctl_value.bv_val,
         pldctrl_value->bv_val, pldctrl_value->bv_len);
  pLControl->ldctl_value.bv_len = pldctrl_value->bv_len;

  // Cleanup temporary berval.
  ber_bvfree(pldctrl_value);

  // Return formatted LDAPControl data.
  return pLControl;
}
```

L'exemple de code C++ suivant montre comment utiliser le contrôle du DN étendu avec la fonction `ldap_search_ext_s` :

```
        int err;
        LDAP *ldapConnection = NULL;
        LDAPControl *pExtDNControl;
        LDAPControl *controlArray[2];
        LDAPMessage *results = NULL;
        LDAPMessage *message = NULL;
        char *dn = NULL;

        // Connect to the default LDAP server.
        ldapConnection = ldap_open( NULL, 0 );
        if ( ldapConnection == NULL ) goto FatalExit0;

        // Bind to the server using default credentials.
        err = ldap_simple_bind_s( ldapConnection, NULL, NULL);
        if (LDAP_SUCCESS != err) goto FatalExit0;

        // Setup the extended DN control, requesting 'standard string' format.
        pExtDNControl = FormatExtDNFlags(1);
        if (pExtDNControl == NULL) goto FatalExit0;
        controlArray[0] = pExtDNControl;
        controlArray[1] = NULL;

        // Perform a synchronous search.
        err   = ldap_search_ext_s( ldapConnection,
                        "cn=users,dc=Fabrikam,dc=com",
                        LDAP_SCOPE_SUBTREE,
                        "objectClass=*",
                        NULL,          // Retrieve all attributes.
                        0,             // Retrieve attributes and values.
                        (LDAPControl **) &controlArray,
                        NULL,          // Client controls.
                        0,             // Timeout.
                        0,             // Sizelimit.
                        &results       // Receives identifier for results.
                        );
        if (LDAP_SUCCESS != err) goto FatalExit0;

        // Process the search results.
        message = ldap_first_entry( ldapConnection, results );
        while (message != NULL)
        {
```

```
                // Print the distinguished name of the object.
                dn = ldap_get_dn( ldapConnection, message );
                if (!dn) goto FatalExit0;
                printf( "  Distinguished Name is : %s\n", dn );
                ldap_memfree(dn);
                message = ldap_next_entry( ldapConnection, message );
        }

FatalExit0:
        if (ldapConnection)
                ldap_unbind( ldapConnection );
        if (results)
                ldap_msgfree( results );
}
```

Audit d’événements LDAP

L'audit LDAP permet aux applications de surveiller/auditer les opérations LDAP, notamment l'ajout, la modification et la recherche, et d'extraire du serveur LDAP des informations utiles telles que les informations de connexion, l'IP du client auquel le serveur était connecté au moment de l'opération LDAP, l'ID du message, le code de résultat de l'opération, etc.

Pour plus d'informations sur l'audit des événements LDAP, reportez-vous à la documentation LDAP Event Services (http://developer.novell.com/documentation/ldapover/ldap_enu/data/ag7bleo.html) (Services d'événements LDAP).

15 Sauvegarde et restauration de NetIQ eDirectory

NetIQ eDirectory est conçu pour assurer la tolérance aux pannes au moyen d'un système de réplication. Ainsi, si un serveur n'est pas disponible, d'autres serveurs peuvent fournir les accès requis. La réplication est la principale méthode de protection d'eDirectory.

Elle ne peut toutefois pas être mise en oeuvre dans un environnement qui comprend un seul serveur. De plus, la réplication ne garantit pas la restauration complète de serveurs individuels en cas de défaillance matérielle ou autre d'un serveur ou encore de sinistre tel qu'un incendie ou une inondation entraînant la perte de plusieurs machines. La sauvegarde d'eDirectory sur chaque serveur augmente la tolérance aux pannes de votre réseau.

L'outil de sauvegarde d'eDirectory permet de sauvegarder la base de données eDirectory sur des serveurs spécifiques. Ses avantages sont les suivants :

- **Même outil pour toutes les plates-formes.**
- **Sauvegarde continue à chaud.** Vous pouvez sauvegarder votre serveur sans fermer la base de données eDirectory, tout en disposant d'une sauvegarde complète.
- **Possibilité de restauration rapide d'un serveur individuel.** Ceci s'avère particulièrement utile en cas de défaillance matérielle.
- **Évolutivité.** Vous pouvez sauvegarder un serveur dont la base de données eDirectory contient des dizaines voire des centaines de millions d'objets. La vitesse du processus de sauvegarde est principalement limitée par la bande passante du canal d'E/S.
- **Capacité de restauration rapide de l'arborescence, en association avec la planification de répliques et les serveurs DSMASTER.** Même si vous n'utilisez pas des serveurs DSMASTER, vous devez être en mesure de restaurer une partie de l'arborescence. Reportez-vous à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre » page 456.
- **Possibilité de sauvegarder des fichiers connexes.** Vous pouvez sauvegarder des fichiers du serveur liés à la base de données, tels que les fichiers de sécurité NICI, les fichiers de flux, ainsi que tous ceux (tels que `autoexec.ncf`) spécifiés dans un fichier d'inclusion.
- **Possibilité de restaurer eDirectory dans l'état où il se trouvait avant son arrêt,** en utilisant la fonction de consignation continue de transactions individuelles par fichier. Reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.
- **Simplification de la mise à niveau du matériel.** En effectuant une sauvegarde à froid, puis en restaurant la base de données eDirectory, vous pouvez transférer facilement l'identité du serveur sur une nouvelle machine, ou la protéger pendant que vous effectuez des modifications telles qu'un ajout de mémoire vive. Reportez-vous à la « Mise à niveau du matériel ou remplacement d'un serveur » page 574.
- **Fonctionnement adapté à l'environnement distribué d'eDirectory.** Vous pouvez vous assurer qu'un serveur restauré possède l'état de synchronisation qu'attendent les autres serveurs de l'arborescence en activant la consignation continue de transactions individuelles par fichier.
- **Possibilité de sauvegardes sans surveillance.** Vous pouvez créer des fichiers de traitement par lots pour exécuter des sauvegardes sans surveillance au moyen du client DSBK.

L'outil de sauvegarde d'eDirectory est conçu pour effectuer une sauvegarde et une restauration complètes de la base de données et des fichiers associés présents sur un serveur spécifique. Il ne prend pas en charge la sauvegarde et la restauration d'objets individuels ou de sections de l'arborescence.

De plus, il doit être utilisé en association avec les sauvegardes du système de fichiers, afin d'enregistrer sur bande les fichiers de sauvegarde d'eDirectory, par mesure de sécurité.

Pour OES 2 Linux, vous pouvez sauvegarder eDirectory à l'aide de NetIQ Storage Management Services (SMS). SMS fournit un agent de service cible (TSA) pour la sauvegarde et la restauration d'eDirectory. Les services TSANDS garantissent une mise en oeuvre des API SMS pour les arborescences Annuaire. Les applications peuvent utiliser cette fonctionnalité pour sauvegarder et restaurer des objets eDirectory.

TSANDS prend en charge les fonctions suivantes dont les applications de sauvegarde peuvent tirer parti :

- Filtres pouvant être appliquées aux objets eDirectory.
- Restaurations sélectives des objets eDirectory à partir des données sauvegardées.
- Possibilité de renommer un ensemble spécifique de ressources.
- Prise en charge des sauvegardes incrémentielles et différentielles en fonction de la date de modification d'eDirectory.
- Enregistrement des données au format SIDF (System Independent Data Format), ce qui permet à n'importe quel logiciel compatible SIDF d'interpréter les données.

Pour plus d'informations sur l'utilisation de TSANDS, reportez-vous à la page du manuel TSANDS.

Ce chapitre comprend les rubriques suivantes :

- « Liste de contrôle pour la sauvegarde » page 445
- « Comprendre les services de sauvegarde et de restauration » page 447
- « Utilisation des fichiers journaux de transactions individuelles » page 458
- « Préparation d'une restauration » page 463
- « Utilisation de DSBK » page 466
- « Sauvegarde et restauration de NICI » page 483
- « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485
- « Scénarios de sauvegarde et de restauration » page 489
- « Utilisation de DSBK dans un plan de reprise après sinistre » page 496
- « Sauvegarde LDAP » page 498
- « Sauvegarde d'eDirectory avec SMS » page 499

Liste de contrôle pour la sauvegarde

Pour vous assurer que les objets d'une arborescence multiserveur sont accessibles, même lorsqu'un serveur est arrêté :

- ❒ Pour les arborescences multiserveurs, vérifiez que toutes les partitions eDirectory sont répliquées sur plusieurs serveurs, afin d'assurer la tolérance aux pannes.

  Pour plus d'informations sur la création de répliques, reportez-vous à la section « Ajout d'une réplique » page 156.

Pour permettre une restauration rapide et complète de serveurs individuels (après une défaillance matérielle, par exemple) :

- ❒ Effectuez régulièrement une sauvegarde complète de la base de données eDirectory (une fois par semaine, par exemple).
- ❒ Effectuez régulièrement une sauvegarde incrémentielle (toutes les nuits, par exemple).
- ❒ Veillez à sélectionner les attributs de flux et NICI lorsque vous effectuez une sauvegarde complète d'un serveur compatible EBA. Dans le cas contraire, l'opération de sauvegarde échoue.
- ❒ Effectuez des sauvegardes sur bande complètes et incrémentielles du système de fichiers peu après les sauvegardes complètes ou incrémentielles de la base de données eDirectory.

  L'outil de sauvegarde enregistre les fichiers de sauvegarde dans le répertoire du serveur que vous indiquez, mais ne peut pas les enregistrer directement sur bande. C'est pourquoi la sauvegarde du système de fichiers doit être configurée pour s'exécuter après la sauvegarde d'eDirectory, afin d'enregistrer les fichiers de sauvegarde de la base de données sur bande pour en assurer le stockage sécurisé.
- ❒ Activez et configurez la consignation de transactions individuelles par fichier, si elle est nécessaire dans votre environnement.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Dans le cas contraire, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas. Dans le cadre de la restauration par défaut, une base de données qui partage des répliques avec d'autres serveurs ne s'ouvre pas tant que son état au moment de l'arrêt du système n'a pas été restauré.

  Dans un environnement monoserveur, la consignation de transactions individuelles par fichier n'est pas nécessaire au processus de vérification de la restauration, mais vous pouvez l'utiliser si vous souhaitez pouvoir restaurer eDirectory dans l'état où il se trouvait avant son arrêt, au lieu de bénéficier simplement de l'état enregistré dans la dernière sauvegarde.

  Lorsque vous activez la fonction de consignation de transactions individuelles par fichier, vous devez avant tout prendre les précautions suivantes. Pour plus d'informations, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

  - Spécifiez un nouvel emplacement pour les journaux de transaction individuelle (n'utilisez pas la valeur par défaut).

    Les journaux doivent se trouver dans un répertoire local du serveur. Pour des raisons de tolérance aux pannes, ils ne doivent pas être stockés sur le même volume/partition de disque ou périphérique de stockage que eDirectory. Vous pouvez éventuellement réserver une partition/un volume aux fichiers journaux de transactions individuelles.
  - Prenez note de l'endroit où se trouvent les fichiers journaux de transactions individuelles, afin de pouvoir les retrouver en cas de défaillance.

Pour trouver cet emplacement lorsque le serveur est fonctionnel, reportez-vous à la « Emplacement des fichiers journaux de transactions individuelles » page 461. Toutefois, si le serveur connaît une défaillance affectant eDirectory (une panne matérielle, par exemple), vous ne pouvez pas rechercher l'emplacement des fichiers journaux de transaction individuelle.

- Surveillez l'espace disque sur la partition ou le volume qui reçoit les journaux de transactions individuelles, afin d'éviter une saturation.

  Si les fichiers journaux de transactions individuelles ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné.

- Limitez l'accès à l'emplacement où les journaux de transactions individuelles sont conservés, afin qu'ils ne puissent pas être vus par les utilisateurs non autorisés.
- Si une restauration est nécessaire, veillez à reconfigurer les fichiers journaux de transactions individuelles sur le serveur une fois la restauration terminée. En effet, les paramètres reprennent leur valeur par défaut durant une restauration. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

❒ Si vous utilisez NICI, assurez-vous que les sauvegardes d'eDirectory incluent les fichiers de sécurité NICI étant donné qu'eDirectory a besoin des mêmes fichiers NICI pour ouvrir la DIB et lire les données codées.

Pour plus d'informations, reportez-vous à la section Backing Up and Restoring NICI (Sauvegarde et restauration de NICI) du NICI Administration Guide (Guide d'administration de NICI).

❒ Pour les arborescences multiserveurs, si vous utilisez l'outil de sauvegarde pour sauvegarder un serveur, vous devez mettre à niveau tous les serveurs qui partagent des répliques avec ce dernier en installant eDirectory 8.5 ou une version ultérieure.

Le processus de vérification de la restauration est rétrocompatible avec eDirectory 8.5 et versions ultérieures uniquement. Pour plus d'informations sur la vérification de la restauration, reportez-vous à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.

❒ Vérifiez périodiquement le fichier journal des sauvegardes pour vous assurer de la réussite des sauvegardes sans surveillance.

❒ Supprimez les anciens fichiers du répertoire des fichiers journaux de transaction individuelle.

❒ Effectuez une sauvegarde à froid avant de mettre à niveau un serveur, comme expliqué à la « Mise à niveau du matériel ou remplacement d'un serveur » page 574.

❒ Pour les arborescences multiserveurs, vérifiez que toutes les partitions eDirectory sont répliquées sur plusieurs serveurs, afin d'assurer la tolérance aux pannes.

La réplication de vos partitions permet non seulement de rendre les objets disponibles lorsqu'un serveur est arrêté, à des fins de maintenance par exemple, mais aussi d'assurer une tolérance aux pannes pour protéger vos informations en cas de perte d'un serveur, à la suite d'une défaillance matérielle. Si un serveur d'une arborescence multiserveur contient une partition qui n'est pas répliquée, et s'il connaît une défaillance, vous risquez d'être dans l'impossibilité de récupérer la partition en question. Il est préférable de s'assurer que toutes les partitions sont répliquées. Pour plus d'informations sur les raisons pour lesquelles vous risquez de ne pas pouvoir récupérer une partition non répliquée dans une arborescence multiserveur, reportez-vous aux sections Présentation du processus de restauration avec l'outil de restauration, Utilisation des fichiers journaux de transactions individuelles et Récupération de la base de données en cas d'échec de la vérification de la restauration.

Pour plus d'informations sur la réplication, reportez-vous à la « Répliques » page 61 et au Chapitre 6, « Gestion des partitions et des répliques », page 151.

- ❒ Veillez à stocker en lieu sûr les bandes qui contiennent les sauvegardes d'eDirectory et du système de fichiers.
- ❒ Testez régulièrement votre stratégie de sauvegarde pour vous assurer qu'elle répond à vos objectifs.
- ❒ (Facultatif) Si vous envisagez d'accéder à distance aux serveurs pour effectuer des sauvegardes à froid (une sauvegarde complète avec la base de données fermée) ou des tâches avancées de sauvegarde et de restauration, installez DSBK sur la machine que vous prévoyez d'utiliser. Pensez également aux accès (accès par un réseau privé virtuel, par exemple) derrière le pare-feu.

  iManager vous permet d'effectuer des sauvegardes et des restaurations à distance, à l'extérieur du pare-feu, mais il ne prend en charge ni la sauvegarde à froid ni les tâches avancées.

  DSBK est installé avec eDirectory sur le serveur. Vous pouvez aussi l'utiliser sur des postes de travail avec Sun JVM 1.3.1. Pour plus d'informations sur l'installation et la configuration de DSBK, reportez-vous à la « Utilisation de DSBK » page 466.
- ❒ (Facultatif) Si vous envisagez d'accéder à distance aux serveurs pour effectuer des sauvegardes à froid (une sauvegarde complète avec la base de données fermée) ou des tâches avancées de sauvegarde et de restauration, installez eMBox sur la machine que vous prévoyez d'utiliser. Pensez également aux accès (accès VPN, par exemple) derrière le pare-feu. iManager vous permet d'effectuer des sauvegardes et des restaurations à distance, à l'extérieur du pare-feu, mais il ne prend en charge ni la sauvegarde à froid ni les tâches avancées.

  iManager vous permet d'effectuer des sauvegardes et des restaurations à distance, à l'extérieur du pare-feu, mais il ne prend en charge ni la sauvegarde à froid ni les tâches avancées.

  eMBox est installé avec eDirectory sur le serveur. Vous pouvez aussi l'utiliser sur des postes de travail avec Sun JVM 1.3.1. Pour plus d'informations sur l'installation et la configuration d'eMBox, reportez-vous à la « Utilisation du client eMBox pour la sauvegarde et la restauration » page 604.

Pour vous préparer à un sinistre dans lequel vous perdez plusieurs serveurs :

- ❒ Tenez compte des considérations ci-dessus.
- ❒ Pour les arborescences multiserveurs, prévoyez de créer des serveurs DSMASTER afin d'être prêt en cas de sinistre.

  Reportez-vous à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre » page 456.
- ❒ Testez régulièrement votre stratégie de reprise après sinistre afin de vous assurer qu'elle répond à vos objectifs.

Comprendre les services de sauvegarde et de restauration

- « À propos de l'outil de sauvegarde d'eDirectory » page 448
- « Différence entre sauvegarde et restauration dans l'utilitaire DSBK et TSA pour NDS » page 448
- « Présentation du processus de restauration avec l'outil de restauration » page 450
- « Format de l'en-tête des fichiers de sauvegarde » page 451
- « Format du fichier journal de sauvegarde » page 455

- « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre » page 456
- « Vecteurs de transition et processus de vérification de la restauration » page 458

À propos de l'outil de sauvegarde d'eDirectory

L'outil de sauvegarde permet d'effectuer une sauvegarde continue à chaud de la base de données eDirectory sur un serveur individuel. Si vous sauvegardez eDirectory sur votre serveur sans fermer la base de données, vous obtenez néanmoins d'une sauvegarde complète, image fidèle de l'état de la base au début de la sauvegarde. Grâce à cette fonction, vous pouvez lancer une sauvegarde à tout moment, eDirectory restant accessible tout au long du processus.

REMARQUE : la sauvegarde continue à chaud est adoptée par défaut. Vous pouvez, si nécessaire, demander une sauvegarde « à froid » lorsque la base de données est fermée.

La nouvelle fonction de sauvegarde permet également d'activer la consignation de transactions individuelles par fichier, pour conserver un enregistrement des transactions dans la base de données depuis la dernière sauvegarde. Vous pouvez ainsi restaurer un serveur dans l'état où il se trouvait avant son arrêt. Vous devez activer cette consignation pour les serveurs qui font partie d'un anneau de répliques, afin de rendre à un serveur l'état de synchronisation attendu par les autres serveurs. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas. La consignation de transactions individuelles par fichier est désactivée par défaut. Pour plus d'informations, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

L'outil de sauvegarde ne sauvegarde pas tous les objets d'eDirectory en même temps, mais seulement les partitions d'un serveur spécifique. Cela permet une meilleure restauration du serveur et des sauvegardes plus rapides qu'avec l'utilitaire de sauvegarde classique TSA pour NDS®. Celui-ci continue de fonctionner comme expliqué dans eDirectory 8.6. Vous pouvez l'employer avec la nouvelle fonction de sauvegarde, si nécessaire. Pour une comparaison, reportez-vous à la section « Différence entre sauvegarde et restauration dans l'utilitaire DSBK et TSA pour NDS » page 448.

L'outil de sauvegarde d'eDirectory doit être utilisé en association avec les sauvegardes du système de fichiers, afin d'enregistrer sur bande les fichiers de sauvegarde d'eDirectory, par mesure de sécurité. NetIQ a établi des partenariats avec plusieurs grands fournisseurs de solutions de sauvegarde. Pour obtenir la liste, consultez la section du site des produits partenaires de NetIQ eDirectory (NetIQ eDirectory Partner Products (http://www.novell.com/partnerguide/section/466.html)).

Pour une description du format des fichiers de sauvegarde et des fichiers journaux créés par l'outil de sauvegarde, reportez-vous aux sections « Format du fichier journal de sauvegarde » page 455 et « Format de l'en-tête des fichiers de sauvegarde » page 451.

Différence entre sauvegarde et restauration dans l'utilitaire DSBK et TSA pour NDS

Dans les versions précédentes d'eDirectory, les fonctions de sauvegarde et de restauration étaient axées sur la sauvegarde de l'arborescence, objet par objet.

L'outil de sauvegarde d'eDirectory 8.7 a introduit une méthode totalement différente, ainsi qu'une nouvelle architecture. Il est en effet axé sur le serveur, et non sur l'arborescence. Vous sauvegardez la base de données eDirectory individuellement sur chaque serveur. De plus, il est beaucoup plus rapide que l'utilitaire de sauvegarde classique TSA pour NDS.

Vous pouvez continuer d'utiliser celui-ci pour sauvegarder l'arborescence, mais nous vous conseillons d'employer le nouvel outil.

Pour plus d'informations, consultez le tableau ci-dessous.

Point	Sauvegarde TSA pour NDS existante	Outil de sauvegarde « Sauvegarde continue à chaud »
Objectif	Conçu pour sauvegarder l'arborescence, objet par objet.	Conçu pour sauvegarder la base de données eDirectory sur chaque serveur pris individuellement. La tolérance aux pannes de l'arborescence complète doit être en premier lieu assurée par la réplication, mais le fait de sauvegarder chaque serveur permet de la renforcer. Lorsque vous devez prévoir une stratégie de restauration de l'arborescence suite à un sinistre ayant entraîné la perte de nombreux serveurs, pensez à employer des serveurs DSMASTER avec la fonction de planification de répliques, comme expliqué à la section « Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre » page 456.
Vitesse	S/O	Considérablement accrue. La vitesse est l'une des caractéristiques les plus importantes du nouvel outil de sauvegarde.
Emplacement de la sauvegarde	Permet de placer la sauvegarde directement sur une bande magnétique.	Les fichiers de sauvegarde sont placés dans le système de fichiers. Vous devez sauvegarder ce dernier pour les enregistrer sur bande, afin de les stocker en lieu sûr.
Multi plate-forme	Fonctionne différemment sur chaque plate-forme.	Fonctionne de manière identique sur toutes les plates-formes.
Possibilité de restaurer des serveurs individuels	Non conçu pour cela.	Offre la possibilité de restaurer un serveur spécifique après une défaillance de disque dur, ou d'utiliser la sauvegarde pour transférer un serveur d'une machine vers une autre. Il est également possible de mettre en oeuvre la consignation de transactions individuelles par fichier afin de rendre à un serveur l'état qu'il avait avant son arrêt, de sorte qu'il retrouve l'état de synchronisation attendu par les autres serveurs dans un anneau de répliques. Permet de sauvegarder des fichiers liés à eDirectory sur un serveur individuel. Vous pouvez, par exemple, sauvegarder et restaurer des fichiers NICI. Vous pouvez aussi créer votre propre liste de fichiers à inclure dans la sauvegarde.

Point	Sauvegarde TSA pour NDS existante	Outil de sauvegarde « Sauvegarde continue à chaud »
Possibilité de restaurer des fichiers NICI pour un serveur	Non conçu pour cela.	Permet de sauvegarder et de restaurer les fichiers NICI, afin de pouvoir accéder aux données codées après une restauration. Vous pouvez ainsi gagner beaucoup de temps lors de la restauration.
Consignation de transactions individuelles par fichier pour un serveur individuel	Non conçu pour cela.	Permet de conserver un enregistrement des transactions dans la base de données depuis la dernière sauvegarde, afin de rétablir un serveur dans l'état où il se trouvait avant son arrêt. Dans un environnement multiserveur, cela vous permet de rendre à un serveur l'état de synchronisation attendu par les autres serveurs. La consignation de transactions individuelles par fichier est désactivée par défaut. Pour plus d'informations, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

Présentation du processus de restauration avec l'outil de restauration

Avant d'effectuer la restauration, vous devez collecter tous les fichiers de sauvegarde en suivant les instructions contenues dans la « Préparation d'une restauration » page 463. Lorsque vous demandez à l'outil de sauvegarde de commencer la restauration, à l'aide d'iManager ou de DSBK, celui-ci exécute la procédure suivante :

1. Il ferme l'agent DS.
2. Il transforme l'ensemble DIB (Data Information Base) actif nommé NDS en nouvel ensemble DIB nommé RST.

   REMARQUE : la base de données NDS existante est conservée sur le serveur. Si la vérification de la restauration échoue, elle redevient l'ensemble DIB actif.

3. Il effectue la restauration dans l'ensemble DIB nommé RST.
4. L'ensemble DIB est désactivé.

   L'attribut de connexion désactivée est paramétré sur le pseudo-serveur, empêchant ainsi l'agent DS de s'ouvrir avec cet ensemble DIB.

5. Il rétablit les paramètres par défaut des fichiers journaux de transactions individuelles. Vous pouvez l'en empêcher en utilisant le paramètre `-s`.

   Ainsi, après une restauration, la consignation de transactions individuelles par fichier est toujours désactivée. De plus, l'emplacement par défaut des fichiers journaux de transactions individuelles est rétabli.

   REMARQUE : Si vous souhaitez activer la consignation de transactions individuelles par fichier sur le serveur, vous devez prévoir de recréer la configuration appropriée après une restauration afin de vous assurer que cette fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

6. Il vérifie la base de données RST restaurée.

   Le serveur tente de vérifier la cohérence des données restaurées. Pour cela, il contacte chaque serveur avec lequel il partage une réplique et compare les vecteurs de transition.

   Le résultat de ce processus de vérification est enregistré dans le fichier journal.

   Si le vecteur de transition du serveur distant est en avance par rapport au vecteur local, il manque alors des données dans la restauration et la vérification échoue.

   Voici un exemple des informations enregistrées dans le fichier journal en cas d'échec de la vérification pour l'une des répliques. Il montre les vecteurs de transition qui ont été comparés :

```
Server: \T=LONE_RANGER\O=novell\CN=CHIP
   Replica: \T=LONE_RANGER\O=novell
      Status: ERROR = -6034
         Local TV             Remote TV
         s3D35F377 r02 e002   s3D35F3C4 r02 e002
         s3D35F370 r01 e001   s3D35F370 r01 e001
         s3D35F363 r03 e001   s3D35F363 r03 e001
         s3D35F31E r04 e004   s3D35F372 r04 e002
         s3D35F2EE r05 e001   s3D35F2EE r05 e001
         s3D35F365 r06 e003   s3D35F365 r06 e003
```

   Pour plus d'informations, reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration » page 458.

7. Si la vérification réussit, RST est renommé NDS et l'attribut de connexion désactivée est effacé, faisant ainsi de RST la base de données eDirectory active sur le serveur. Si la vérification échoue, l'ensemble DIB RST n'est pas renommé et NDS redevient l'ensemble DIB actif.

   En cas d'échec de la vérification, reportez-vous à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485 pour savoir comment récupérer le serveur.

REMARQUE : Il est possible de forcer l'activation et le déverrouillage de la base de données RST à l'aide des options de restauration avancées, mais cela n'est pas conseillé, sauf si NetIQ vous le propose.

Format de l'en-tête des fichiers de sauvegarde

Les fichiers de sauvegarde comportent un en-tête que vous pouvez lire pour accéder à des informations importantes, notamment :

- Le nom assigné au fichier de sauvegarde lors de sa création.

  Cela est utile si le fichier a été renommé depuis la création de la sauvegarde.

- Le nom du journal de transaction individuelle en service au moment de la sauvegarde.

  S'il s'agit de la dernière sauvegarde du jeu à partir duquel vous effectuez la restauration (par exemple, la dernière sauvegarde incrémentielle d'un ensemble constitué d'une sauvegarde complète et de trois sauvegardes incrémentielles), cette information vous est utile puisqu'elle indique le premier fichier journal de transaction individuelle dont vous avez besoin pour effectuer une restauration complète.

- Les répliques que contenait le serveur.

  Cette information est utile si vous n'avez pas noté l'emplacement de vos répliques. Si vous êtes confronté à un sinistre dans lequel de nombreux serveurs sont perdus, la liste des répliques figurant dans l'en-tête du fichier de sauvegarde peut vous aider à choisir les serveurs à restaurer en premier.

- Les noms des fichiers inclus dans la sauvegarde, listés dans un fichier d'inclusion utilisateur.
- Le nombre de fichiers figurant dans le jeu de sauvegarde.

Pour chaque sauvegarde individuelle, l'en-tête du fichier est au format XML. Immédiatement après l'en-tête viennent les données de sauvegarde de la base de données exprimées en code binaire.

REMARQUE : Étant donné que des données binaires sont incluses à la fin du fichier, l'analyse de ce dernier produirait des erreurs. Toutefois, l'en-tête est conforme au standard XML.

Si la sauvegarde s'étend sur plusieurs fichiers, les informations d'en-tête sont incluses dans chacun d'eux.

AVERTISSEMENT : lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car vous risqueriez de l'altérer. La plupart des applications n'enregistrent pas les données binaires correctement.

Voici la partie DTD de l'en-tête XML. Elle est incluse également dans l'en-tête du fichier de sauvegarde, pour référence.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
    backup_type (full|incremental) #REQUIRED
    idtag CDATA #REQUIRED
    time CDATA #REQUIRED
    srvname CDATA #REQUIRED
    dsversion CDATA #REQUIRED
    compression CDATA "none"
    os CDATA #REQUIRED
    current_log CDATA #REQUIRED
    number_of_files CDATA #IMPLIED
    backup_file CDATA #REQUIRED
    incremental_file_ID CDATA #IMPLIED
    next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
    name CDATA #REQUIRED
    encoding CDATA "base64"
    type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
    modification_time CDATA #REQUIRED
    replica_type (MASTER|SECONDARY|READONLY|SUBREF|
    SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
    replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
    CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
    BEGIN_ADD|MASTER_START|MASTER_DONE|
    FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
    Unknown) #REQUIRED>
]>
```

Le tableau ci-dessous décrit les attributs que contient cette partie.

Attribut	Explication
backup version	Version de l'outil de sauvegarde.

Attribut	Explication
backup backup_type	Type de sauvegarde exécuté (sauvegarde complète ou incrémentielle). Une sauvegarde à froid est une sauvegarde complète.
backup idtag	Identificateur GUID attribué selon l'heure de la sauvegarde. Il permet d'identifier la sauvegarde, même si le fichier de sauvegarde est renommé.
backup time	Date et heure à laquelle la sauvegarde a débuté.
backup srvname	Nom distinctif du serveur sauvegardé.
backup dsversion	Version d'eDirectory exécutée sur le serveur.
backup compression	Indique si l'outil de sauvegarde a comprimé les données de sauvegarde. La compression ne s'applique qu'aux données de sauvegarde. L'en-tête n'est jamais comprimé.
backup os	Système d'exploitation sur lequel la sauvegarde a été exécutée. Nous vous recommandons de ne restaurer que le même système d'exploitation.
backup current_log	Premier fichier journal de transaction individuelle nécessaire pour restaurer la sauvegarde. Cette information vous permet de collecter l'ensemble de fichiers approprié pour une restauration.
backup number_of_files	Nombre de fichiers faisant partie du jeu de sauvegarde. Cette valeur figure uniquement dans le premier fichier de sauvegarde.
backup backup_file	Nom de fichier de la sauvegarde actuelle. Si la sauvegarde s'étend sur plusieurs fichiers, l'en-tête de chaque fichier indique le nom du fichier ainsi que son numéro d'ordre dans le jeu de sauvegarde. Pour un exemple de noms de fichiers de sauvegarde, consultez la description de *-s taille_fichier*.
backup incremental_file_ID	S'il s'agit d'une sauvegarde incrémentielle, identificateur (ID) du fichier incrémentiel.
backup next_inc_file_ID	ID attribué au fichier de sauvegarde incrémentielle suivant lors de sa création. Cette information vous permet de collecter l'ensemble de fichiers approprié pour une restauration.
file size	Taille des données qui figurent entre les balises `<file>` du fichier.
file name	Nom et emplacement du fichier au moment de la sauvegarde.
file encoding	Algorithme de codage utilisé pour le fichier.
file type	Indique s'il s'agit d'un fichier NICI ou utilisateur.
Mot de passe	Spécifie le mot de passe de sauvegarde NICI. Le même mot de passe doit être spécifié pour restaurer les fichiers NICI.
replica partition_DN	Nom distinctif de la partition. Cette information est utile si vous n'avez pas noté l'emplacement de vos répliques. Si vous êtes confronté à un sinistre dans lequel de nombreux serveurs ont été perdus, la liste des répliques figurant dans l'en-tête du fichier de sauvegarde peut vous aider à choisir les serveurs à restaurer en premier.
replica modification_time	Vecteur de transition de la réplique au moment de la sauvegarde.

Attribut	Explication
replica replica_type	Type de réplique (maîtresse ou Lecture seule, par exemple).
replica_state	État de la réplique au moment de la sauvegarde (Active ou Nouvelle réplique, par exemple).

Voici un exemple d'en-tête de fichier de sauvegarde d'un serveur Windows. Les fichiers de sécurité NICI sont inclus dans la sauvegarde.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE backup [
<!ELEMENT backup (file|replica)*>
<!ELEMENT file (#PCDATA)>
<!ELEMENT replica EMPTY>
<!ATTLIST backup version CDATA #REQUIRED
    backup_type (full|incremental) #REQUIRED
    idtag CDATA #REQUIRED
    time CDATA #REQUIRED
    srvname CDATA #REQUIRED
    dsversion CDATA #REQUIRED
    compression CDATA "none"
    os CDATA #REQUIRED
    current_log CDATA #REQUIRED
    number_of_files CDATA #IMPLIED
    backup_file CDATA #REQUIRED
    incremental_file_ID CDATA #IMPLIED
    next_inc_file_ID CDATA #IMPLIED>
<!ATTLIST file size CDATA #REQUIRED
    name CDATA #REQUIRED
    encoding CDATA "base64"
    type (user|nici) #REQUIRED>
<!ATTLIST replica partition_DN CDATA #REQUIRED
    modification_time CDATA #REQUIRED
    replica_type (MASTER|SECONDARY|READONLY|SUBREF|
    SPARSE_WRITE|SPARSE_READ|Unknown) #REQUIRED
    replica_state (ON|NEW_REPLICA|DYING_REPLICA|LOCKED|
    CRT_0|CRT_1|TRANSITION_ON|DEAD_REPLICA|
    BEGIN_ADD|MASTER_START|MASTER_DONE|
    FEDERATED|SS_0|SS_1|JS_0|JS_1|MS_0|MS_1|
    Unknown) #REQUIRED>
]>

<backup version="2" backup_type="full" idtag="3D611DA2" time="2002-8-19'T10:32:35"
srvname="\T=MY_TREE\O=novell\CN=DSUTIL-DELL-NDS" dsversion="1041081"
compression="none" os="windows" current_log="00000003.log" next_inc_file_ID="2"
number_of_files="0000001" backup_file="c:\backup\header.bak"><replica
partition_DN="\T=MY_TREE" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" /><replica
partition_DN="\T=MY_TREE\O=part1" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" /><replica
partition_DN="\T=MY_TREE\O=part2" modification_time="s3D611D95_r1_e2"
replica_type="MASTER" replica_state="ON" /><replica
partition_DN="\T=MY_TREE\O=part3" modification_time="s3D611D96_r1_e2"
replica_type="MASTER" replica_state="ON" /><file size="190"
name="C:\WINDOWS\system32\novell\nici\bhawkins\XARCHIVE.001" encoding="base64"
type="nici">the data is included here</file>

<file size="4228" name="C:\WINDOWS\system32\novell\nici\bhawkins\XMGRCFG.KS2"
encoding="base64" type="nici">the data is included here</file>
```

```
<file size="168" name="C:\WINDOWS\system32\novell\nici\bhawkins\XMGRCFG.KS3"
encoding="base64" type="nici">the data is included here</file>

<file size="aaac" name="C:\WINDOWS\system32\novell\nici\nicintacl.exe"
encoding="base64" type="nici">the data is included here</file>

<file size="150" name="C:\WINDOWS\system32\novell\nici\NICISDI.KEY"
encoding="base64" type="nici">the data is included here
</file>

<file size="4228" name="C:\WINDOWS\system32\novell\nici\system\Xmgrcfg.ks2"
encoding="base64" type="nici">the data is included here
</file>

<file size="168" name="C:\WINDOWS\system32\novell\nici\system\Xmgrcfg.ks3"
encoding="base64" type="nici">the data is included here
</file>

<file size="1414" name="C:\WINDOWS\system32\novell\nici\xmgrcfg.wks"
encoding="base64" type="nici">the data is included here
</file>

</backup>
```

Les données binaires de la sauvegarde de la base de données sont ajoutées dans le fichier de sauvegarde à la suite de l’en-tête.

Format du fichier journal de sauvegarde

L'outil de sauvegarde d'eDirectory tient à jour un journal qui présente une vue d'ensemble de son activité et comporte des informations sur les sauvegardes antérieures. Le fichier journal contient un historique de toutes les sauvegardes et consigne l'heure de début et de fin de chacune d'entre elles. Il fournit également des informations sur les erreurs survenues éventuellement pendant le processus de sauvegarde. Ce fichier est complété à chaque sauvegarde. Il est également enregistré à l'emplacement que vous désignez.

Le fichier journal permet de s'assurer de la réussite des sauvegardes sans surveillance. Le résultat (réussite ou échec) est indiqué sur la dernière ligne avec le code d'erreur éventuel.

Le fichier journal de l'outil de sauvegarde mentionne également l'ID des sauvegardes qui ont été effectuées, ce qui facilite la collecte des fichiers de sauvegarde complète et incrémentielle corrects en vue d'une restauration. Les quatre premières lignes reprennent les informations de l'en-tête du fichier de sauvegarde.

Les autres fichiers inclus dans la sauvegarde de la base de données, tels que les fichiers NICI ou ceux listés dans un fichier d'inclusion, sont également consignés dans le fichier journal.

Pour une restauration, ce dernier enregistre également les fichiers inclus qui ont été restaurés.

Voici deux exemples d'entrées de fichier journal :

```
|==================DSBackup Log: Backup================|
Backup type: Full
Log file name: sys:/backup/backup.log
Backup started: 2002-6-21'T19:53:5GMT
Backup file name: sys:/backup/backup.bak
Server name: \T=VIRTUALNW_TREE\O=novell\CN=VIRTUALNW
Current Roll Forward Log: 00000001.log
DS Version: 1041072
Backup ID: 3D138421
Backing up security file: sys:/system/nici/INITNICI.LOG
Backing up security file: sys:/system/nici/NICISDI.KEY
Backing up security file: sys:/system/nici/XARCHIVE.000
Backing up security file: sys:/system/nici/XARCHIVE.001
Backing up security file: sys:/system/nici/XMGRCFG.KS2
Backing up security file: sys:/system/nici/XMGRCFG.KS3
Backing up security file: sys:/system/nici/XMGRCFG.NIF
Starting database backup...
Database backup finished
Completion time 00:00:03
Backup completed successfully

|==================DSBackup Log: Restore================|
Log file name: sys:/save/doc.log
Restore started: 2002-7-19'T19:1:34GMT
Restore file name: sys:/backup/backup.bak
Starting database restore...
Restoring file sys:/backup/backup.bak
Restoring file sys:/system/nici/INITNICI.LOG
Restoring file sys:/system/nici/NICISDI.KEY
Restoring file sys:/system/nici/XARCHIVE.000
Restoring file sys:/system/nici/XARCHIVE.001
Restoring file sys:/system/nici/XMGRCFG.KS2
Restoring file sys:/system/nici/XMGRCFG.KS3
Restoring file sys:/system/nici/XMGRCFG.NIF
Database restore finished
Completion time 00:00:15
Restore completed successfully
```

Utilisation de serveurs DSMASTER dans le cadre d'un plan de reprise après sinistre

Si vous possédez un environnement multiserveur et souhaitez planifier la reprise après un sinistre entraînant la perte de tous vos serveurs, vous pouvez utiliser des serveurs DSMASTER dans le cadre du plan de restauration de votre arborescence.

L'outil de sauvegarde permet de sauvegarder chaque serveur séparément. Il est axé sur le serveur et non sur l'arborescence. Si toutefois vous créez des serveurs DSMASTER, vous pouvez utiliser les fonctionnalités de l'outil de sauvegarde spécifiquement pour sauvegarder toute la structure de votre arborescence. Un exemple de sauvegarde impliquant des serveurs DSMASTER est présenté dans le scénario « Scénario : perte de tous les serveurs dans un environnement multiserveur » page 494.

Lors d'une restauration après un sinistre, l'un des principaux problèmes consiste à éviter de restaurer des répliques de la même partition qui ne concordent pas. Si, à la suite d'un sinistre, vous perdez les fichiers journaux de transaction individuelle de vos serveurs, vous ne pourrez pas restaurer tous vos serveurs au même point dans le temps. Sans ces fichiers journaux, les répliques qui se trouvent dans vos sauvegardes ne concordent pas. Cela entraîne des problèmes si elles sont toutes restaurées au même moment et intégrées ensemble à l'arborescence.

REMARQUE : le processus de vérification de la restauration a été conçu pour éviter ces problèmes. Par défaut, une base de données eDirectory restaurée ne s'ouvre pas après une restauration si elle ne concorde pas avec les autres répliques.

Vous pouvez recourir à des serveurs DSMASTER pour vous préparer à cette situation, en créant une copie maîtresse de l'arborescence que vous utiliserez comme point de départ.

Pour utiliser des serveurs DSMASTER en prévision d'un éventuel sinistre :

- Organisez vos répliques pour qu'un serveur contienne une réplique de chaque partition de l'arborescence. Ainsi, vous pouvez disposer d'une copie de l'ensemble de l'arborescence dans la base de données eDirectory d'un seul serveur (si l'arborescence est trop grande, vous pouvez utiliser deux serveurs clés). Ce type de serveur est souvent appelé serveur DSMASTER. Les répliques du serveur DSMASTER doivent être de type maîtresse ou Lecture/écriture.

  REMARQUE : si vous utilisez deux serveurs DSMASTER clés, gardez à l'esprit que chacun doit en principe disposer d'un ensemble unique de répliques de partitions. Il ne doit pas y avoir de chevauchement pour éviter les incohérences entre les répliques lors de la restauration après un sinistre.

  Si un sinistre entraîne la perte de vos serveurs, vous n'aurez pas accès aux derniers fichiers journaux de transactions individuelles pour la restauration ; en effet, ceux-ci sont enregistrés localement sur le serveur, de sorte qu'il sera probablement impossible de restaurer tous les serveurs DSMASTER au même point dans le temps. Si la même réplique est stockée sur deux serveurs DSMASTER, les deux copies ne seront probablement pas identiques, ce qui entraînera des incohérences dans l'arborescence. Pour préparer une reprise après sinistre, il est donc préférable qu'une même partition ne soit pas répliquée sur plusieurs serveurs DSMASTER.

  Pour obtenir des informations générales sur les répliques, reportez-vous à la « Répliques » page 61.

- Sauvegardez régulièrement les serveurs DSMASTER pour créer une copie de sauvegarde de votre arborescence. Il peut en outre être judicieux de prendre des précautions supplémentaires pour le stockage des sauvegardes des serveurs DSMASTER dans le cadre de votre plan de récupération en cas de sinistre.

Si vous concevez ainsi votre arborescence, vous pourrez, en cas de sinistre, rendre rapidement opérationnelle la structure arborescente en restaurant simplement le serveur (ou le petit groupe de serveurs clés) concerné et en vous assurant que les répliques qu'il contient sont désignées comme étant les répliques maîtresses.

Une fois la structure de l'arborescence redevenue opérationnelle, vous pourrez restaurer les autres serveurs perdus en utilisant uniquement les fichiers de sauvegarde complète et incrémentielle. Toutefois, comme vous ne disposez pas des fichiers journaux de transaction individuelle, la vérification de la restauration échoue pour ces autres serveurs. Pour les réintégrer dans l'arborescence, vous devrez les supprimer de l'anneau de répliques, changer en références externes toutes les informations concernant leurs répliques à l'aide de DSRepair, puis leur ajouter de nouveau les répliques en effectuant la réplication à partir de la copie figurant sur le serveur DSMASTER. Ces opérations sont décrites à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

Si, lors d'un sinistre, vous perdez une grande partie de vos serveurs, la procédure liée aux répliques risque d'être complexe. Dans ce cas, nous vous conseillons de contacter le support technique de NetIQ.

Vecteurs de transition et processus de vérification de la restauration

Un vecteur de transition est un tampon horaire pour une réplique. Ce tampon est constitué d'une représentation du nombre de secondes écoulées depuis un point de référence historique commun (1er janvier 1970), du numéro de réplique et du numéro d'événement en cours. Voici un exemple :

```
s3D35F377 r02 e002
```

Dans le contexte de la sauvegarde et de la restauration, le vecteur de transition est important, car il sert à vérifier que le serveur restauré est synchronisé avec l'anneau de répliques auquel il participe.

Les serveurs qui contiennent des répliques d'une même partition communiquent entre eux pour que celles-ci restent synchronisées en permanence. Chaque fois qu'un serveur communique avec un autre serveur de l'anneau de répliques, il conserve un enregistrement du vecteur de transition de l'autre serveur au moment de la communication. Les vecteurs de transition permettent aux serveurs d'un anneau de répliques de savoir quelles informations ils doivent envoyer à chacune des répliques de l'anneau pour assurer leur synchronisation. Lorsqu'un serveur s'arrête, il cesse de communiquer. Les autres serveurs ne lui envoient plus de mises à jour et ne modifient plus le vecteur de transition qu'ils ont enregistré pour lui jusqu'à ce qu'il recommence à communiquer.

Lorsque vous restaurez eDirectory sur un serveur, le processus de vérification de la restauration compare le vecteur de transition du serveur en cours de restauration et celui des autres serveurs de l'anneau de répliques. Cela permet de s'assurer que les répliques restaurées sont dans l'état attendu par les autres serveurs.

Si le vecteur de transition du serveur distant est en avance par rapport au vecteur local, il manque alors des données dans la restauration et la vérification échoue. Par exemple, des données peuvent être manquantes pour les raisons suivantes : vous n'avez pas activé la consignation continue de transactions individuelles par fichier avant la dernière sauvegarde complète ou incrémentielle, vous n'avez pas inclus les fichiers journaux de transactions individuelles dans la restauration ou l'ensemble de fichiers journaux que vous avez fourni pour la restauration est incomplet.

Par défaut, la base de données eDirectory restaurée n'est pas ouverte si elle est incohérente par rapport aux autres répliques.

Pour obtenir un exemple d'entrée de fichier journal lorsque des vecteurs de transition ne concordent pas, reportez-vous à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.

Pour plus d'informations sur la procédure à suivre en cas d'échec de la vérification de la restauration, reportez-vous à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

Utilisation des fichiers journaux de transactions individuelles

La consignation de transactions individuelles par fichier s'apparente à la journalisation dans d'autres produits de bases de données. Les fichiers journaux de transactions individuelles enregistrent toutes les modifications opérées dans la base de données.

L'intérêt de la consignation de transactions individuelles par fichier est qu'elle fournit un historique des modifications depuis la dernière sauvegarde complète ou incrémentielle, de sorte que vous pouvez restaurer eDirectory dans l'état où il se trouvait avant une défaillance. Sans les fichiers journaux de transactions individuelles, vous ne pouvez restaurer eDirectory que dans l'état où il se trouvait au moment de la dernière sauvegarde complète ou incrémentielle.

eDirectory enregistre les transactions dans un fichier journal avant de les appliquer à la base de données. Par défaut, ce fichier journal est réutilisé continuellement (occupant ainsi peu d'espace disque) et l'historique des changements apportés à la base de données eDirectory n'est pas enregistré.

Lorsque vous activez la consignation continue de transactions individuelles par fichier, l'historique des modifications est enregistré dans un jeu de fichiers journaux de transactions individuelles consécutifs. La consignation de transactions individuelles par fichier ne réduit pas les performances du serveur ; elle enregistre simplement les entrées du fichier journal qu'eDirectory est déjà en train de créer.

Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas. Dans le cadre de la restauration par défaut, une base de données qui partage des répliques avec d'autres serveurs ne s'ouvre pas tant que son état au moment de l'arrêt du système n'a pas été restauré. En l'absence de fichiers journaux de transaction individuelle, vous devez suivre une procédure distincte pour tenter de récupérer ce qui a été perdu, comme expliqué à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

La consignation de transactions individuelles par fichier est désactivée par défaut. Vous devez l'activer pour pouvoir l'utiliser sur un serveur. Elle est également désactivée lorsque vous restaurez un serveur, et les paramètres reprennent leur valeur par défaut. Après une restauration, vous devez donc la réactiver et recréer votre configuration.

REMARQUE : Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Dans un environnement monoserveur, la consignation de transactions individuelles par fichier n'est pas nécessaire. Vous pouvez néanmoins l'utiliser si vous souhaitez pouvoir restaurer eDirectory dans l'état où il se trouvait avant son arrêt, au lieu de bénéficier simplement de l'état enregistré dans la dernière sauvegarde.

Pensez à contrôler l'espace disque lorsque la consignation de transactions individuelles par fichier est activée. Pour plus d'informations, reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462.

Dans cette section :

- « Considérations utiles concernant la consignation de transactions individuelles par fichier » page 460
- « Emplacement des fichiers journaux de transactions individuelles » page 461
- « Sauvegarde et suppression des journaux de transactions individuelles » page 462
- « Avertissement : la suppression d'eDirectory entraîne également celle des fichiers journaux de transaction individuelle. » page 463

Vous pouvez activer et configurer la consignation de transactions individuelles par fichier à l'aide d'iManager ou de DSBK. Reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles avec iManager » page 615 ou à la section « Configuration des fichiers journaux de transaction individuelle avec DSBK » page 471.

Considérations utiles concernant la consignation de transactions individuelles par fichier

Si vous décidez d'utiliser la fonction de consignation de transactions individuelles par fichier, vous devez tenir compte des considérations suivantes :

- **Activez la fonction avant d'effectuer une sauvegarde** si vous souhaitez pouvoir l'utiliser pour restaurer la base de données.
- **Pour assurer une tolérance aux pannes, veillez à placer les journaux de transactions individuelles sur un ensemble de disques durs différent de celui d'eDirectory.** Par mesure de sécurité, veillez également à restreindre les droits d'accès aux fichiers journaux des utilisateurs. Pour plus d'informations, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles » page 461.
- **Notez l'emplacement des fichiers journaux de transactions individuelles.** Pour plus d'informations, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles » page 461.
- **Contrôlez l'espace disque disponible à l'emplacement de stockage des fichiers journaux.**

  Pour plus d'informations, reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462.
- **Si les fichiers journaux ont été désactivés ou perdus, réactivez-les, puis effectuez une nouvelle sauvegarde complète** afin de pouvoir effectuer une récupération totale. Cette opération est nécessaire dans les cas suivants :
  - Après une restauration. La consignation de transactions individuelles par fichier est désactivée et les paramètres reprennent leur valeur par défaut dans le cadre du processus de restauration.
  - Si vous perdez le répertoire contenant les fichiers journaux de transactions individuelles en raison de la défaillance d'un périphérique de stockage ou d'une autre panne.
  - Si les fichiers journaux de transactions individuelles ont été désactivés par inadvertance.
- **Si vous activez la consignation des fichiers de flux, les fichiers journaux de transactions individuelles consomment l'espace disque plus rapidement.** Lorsque vous activez la consignation des fichiers de flux (les scripts de connexion, par exemple), c'est tout le fichier de flux qui est copié dans le journal de transactions individuelles chaque fois qu'il subit une modification. La taille des fichiers journaux augmentera moins rapidement si vous désactivez la consignation des fichiers de flux et ne sauvegarder ces derniers que lors d'une sauvegarde complète ou incrémentielle.
- **La phase la plus lente de la restauration de la base de données est la lecture des fichiers journaux de transactions individuelles.** L'augmentation de la taille de ces fichiers journaux dépend du nombre de modifications apportées à l'arborescence et de la consignation éventuelle des fichiers de flux (tels que les scripts de connexion).

  Si votre base de données change fréquemment, vous pouvez envisager d'effectuer plus souvent des sauvegardes d'eDirectory pour traiter moins de changements à partir des journaux de transactions individuelles durant une restauration.
- **Ne modifiez pas le nom d'un fichier journal de transaction individuelle.** Si un fichier journal porte un nom différent de celui qu'il avait lors de sa création, il ne peut pas être utilisé dans une restauration.
- **N'oubliez pas que la suppression d'eDirectory entraîne celle de tous les fichiers journaux de transactions individuelles.** Si vous souhaitez pouvoir utiliser les fichiers journaux pour une restauration ultérieure, vous devez les copier à un autre emplacement avant de supprimer eDirectory.

- **Si une restauration est nécessaire, veillez à reconfigurer les fichiers journaux de transactions individuelles sur le serveur une fois la restauration terminée** afin de vous assurer qu'ils sont activés et qu'ils se trouvent à un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

  Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Emplacement des fichiers journaux de transactions individuelles

Si vous activez la consignation de transactions individuelles par fichier, veillez à changer l'emplacement du répertoire des journaux de transactions individuelles afin d'utiliser une unité de stockage différente de celle d'eDirectory.

Voici quelques points importants à prendre en compte lors du choix de l'emplacement :

- **Ne laissez pas les fichiers journaux à l'emplacement par défaut. Veillez à les enregistrer sur un autre périphérique de stockage qu'eDirectory.** Ainsi, si eDirectory est perdu en raison de la défaillance d'un périphérique de stockage, vous pouvez quand même accéder aux fichiers journaux de transactions individuelles pour le restaurer.

  Si votre serveur ne comprend qu'un seul périphérique de stockage, les fichiers journaux de transaction individuelle ne permettent pas d'assurer la tolérance aux pannes d'eDirectory en cas de défaillance de ce périphérique. Dans ce cas, il est préférable de ne pas les utiliser.

  Vous pouvez modifier l'emplacement des fichiers journaux de transaction individuelle à l'aide des options Configuration de la sauvegarde dans iManager ou setconfig dans DSBK. Ces fichiers journaux doivent se trouver dans un répertoire local du serveur.
- **Notez l'emplacement des fichiers journaux.** Vous devez noter l'emplacement de stockage des fichiers journaux de transactions individuelles de manière à pouvoir les retrouver si vous devez restaurer la base de données sur un serveur. Il est important de le faire lorsque le serveur est sain, avant qu'un incident ne survienne.

  Pour trouver cet emplacement lorsque le serveur est fonctionnel, vous pouvez utiliser l'option Configuration de la sauvegarde dans iManager ou `backup getconfig` dans DSBK. Toutefois, si le serveur connaît une défaillance affectant eDirectory (une panne matérielle, par exemple), vous ne pouvez pas rechercher l'emplacement des fichiers journaux de transaction individuelle.

  Si vous tentez de restaurer un serveur qui a déjà subi une défaillance, sachez qu'à chaque nouvelle installation d'eDirectory, c'est l'emplacement par défaut des fichiers journaux de transactions individuelles qui est indiqué. Par conséquent, si vous venez de réinstaller eDirectory lors de la première étape d'un processus de restauration, eDirectory n'indique pas l'emplacement où étaient stockés les fichiers journaux avant la défaillance du serveur. Vous devez vous reporter à vos notes pour savoir où ils se trouvent.

  La configuration des fichiers journaux de transaction individuelle est également enregistrée dans le fichier `_ndsdb.ini`, mais celui-ci figure sur le même volume/la même partition de disque qu'eDirectory. Par conséquent, si vous perdez le périphérique de stockage sur lequel se trouve eDirectory, vous ne pouvez pas employer ce fichier pour rechercher cet emplacement.

- **Limitez les droits d'accès pour l'emplacement de stockage des fichiers journaux de transactions individuelles.** C'est une question de sécurité. Les informations ne sont pas facilement lisibles, mais il est possible de décoder les fichiers journaux pour accéder à des données sensibles.
- **Contrôlez si l'espace disque disponible est suffisant.** Reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462.
- **Il est recommandé de réserver un volume/une partition de disque aux journaux de transactions individuelles.** Il est ainsi plus facile de contrôler les privilèges de sécurité et l'espace disque.
- **Le dernier répertoire du chemin d'accès est créé par eDirectory.** Il correspond au nom de la base de données eDirectory actuelle.

  Ainsi, si l'emplacement spécifié correspond à `d:\Novell\NDS\DIBFileset` le nom de votre base de données eDirectory à NDS, l'emplacement des fichiers journaux de transaction individuelle est alors `d:\Novell\NDS\DIBFiles\nds.rfl`. Si vous renommez la base de données NDS en ND1, le répertoire des fichiers journaux devient `d:\Novell\NDS\DIBFiles\nd1.rfl`.

  Le répertoire est créé immédiatement après le changement d'emplacement, mais aucun fichier journal de transaction individuelle n'est créé tant qu'aucune transaction n'a lieu dans la base de données.
- **Lors de la restauration, tous les journaux de transactions individuelles nécessaires doivent figurer dans le même répertoire.** Pour plus d'informations, reportez-vous à la « Préparation d'une restauration » page 463.

Sauvegarde et suppression des journaux de transactions individuelles

S'ils ne sont pas surveillés, les fichiers journaux de transactions individuelles peuvent saturer le volume/la partition de disque qui les reçoit. Si ces journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Il est conseillé de sauvegarder périodiquement les fichiers journaux et de supprimer du serveur ceux qui ne sont pas utilisés afin de libérer de l'espace disque.

Pour identifier, sauvegarder et supprimer les fichiers journaux de transactions individuelles dont la suppression ne pose pas de problème, procédez comme suit :

1. Notez le nom du dernier fichier journal de transaction individuelle inutilisé.

   Pour trouver le nom de ce fichier journal, vous avez plusieurs possibilités :

   - Dans iManager, cliquez sur **Maintenance** > **Configuration de la sauvegarde** et lisez le nom de fichier affiché.
   - Dans le client DSBK, entrez la commande `getconfig backup`. Reportez-vous à la section « Configuration des fichiers journaux de transaction individuelle avec DSBK » page 471 pour plus d'informations.

   Le dernier fichier journal de transaction individuelle inutilisé correspond au fichier le plus récent que la base de données a renseigné et qu'elle n'utilise plus pour enregistrer des transactions. Il s'agit du dernier fichier journal de transaction individuelle inutilisé puisque la base de données a fini d'y enregistrer des informations et a créé un nouveau fichier journal, de sorte qu'elle n'a plus besoin de le maintenir ouvert. Le fichier journal actuellement utilisé pour l'enregistrement des transactions est toujours nécessaire à la base de données.
2. Sauvegardez les fichiers journaux de transactions individuelles à partir du système de fichiers, afin de les enregistrer sur bande par mesure de sécurité.

3 Supprimez les fichiers journaux de transactions individuelles plus anciens que le dernier inutilisé.

AVERTISSEMENT : faites preuve de précaution lorsque vous supprimez des fichiers journaux de transactions individuelles du serveur. Assurez-vous que vous avez bien sauvegardé sur bande tous les fichiers journaux que vous supprimez.

Le dernier fichier journal de transaction individuelle inutilisé indique le nom du fichier que la base de données vient de compléter et de fermer. Il ne précise pas si vous pouvez supprimer ce fichier du serveur en toute sécurité. Veillez à ne supprimer que les fichiers que vous avez sauvegardés sur bande.

Si vous devez récupérer certains fichiers journaux de transactions individuelles sauvegardés sur bande afin de les utiliser dans une restauration, tenez compte des points suivants :

- Comme tous les fichiers journaux de transactions individuelles utilisés pour une restauration, ceux récupérés à partir d'une bande de sauvegarde du système de fichiers doivent être placés dans le même dossier que les autres fichiers journaux, sur le serveur en cours de restauration.
- Comparez les tampons horaires des fichiers dupliqués sur la bande et sur le serveur. Si les tampons horaires diffèrent, utilisez le fichier le plus récent, c'est-à-dire celui du serveur. Par exemple, le fichier journal de transaction individuelle que la base de données utilisait au moment de la sauvegarde du système de fichiers est incomplet sur la bande. La version complète et la plus récente de ce fichier figure sur le serveur.

Avertissement : la suppression d'eDirectory entraîne également celle des fichiers journaux de transaction individuelle.

Si vous supprimez eDirectory de votre serveur, le répertoire des fichiers journaux de transactions individuelles et son contenu sont également supprimés. Si vous souhaitez pouvoir utiliser les journaux ultérieurement pour restaurer le serveur, vous devez, avant de supprimer eDirectory, les copier à un autre emplacement.

Préparation d'une restauration

Lors de la restauration de la base de données eDirectory, le plus important est de s'assurer qu'elle est complète. Avant de restaurer une base de données eDirectory sur un serveur, assurez-vous que les conditions préalables ont été remplies, comme expliqué à la section « Conditions préalables à la restauration » page 463. Si vous ne savez pas vraiment comment collecter les fichiers de sauvegarde corrects, reportez-vous à la section « Localisation des fichiers de sauvegarde requis pour une restauration » page 464.

Conditions préalables à la restauration

- ❒ Tous les serveurs qui partagent une réplique avec le serveur à restaurer doivent être en service et communiquer. Le processus de vérification de la restauration peut ainsi effectuer un contrôle auprès de ces serveurs, qui font partie d'un même anneau de répliques.
- ❒ Vous avez collecté tous les fichiers de sauvegarde dont vous avez besoin :
  - Le fichier de sauvegarde complète et les fichiers incrémentiels consécutifs ont été copiés dans un répertoire du serveur à restaurer.

- Tous les fichiers journaux de transactions individuelles depuis la dernière sauvegarde se trouvent dans un répertoire du serveur à restaurer.

  Si le serveur fait partie d'un anneau de répliques, vous devez vous assurer que tous les fichiers journaux de transactions individuelles créés depuis la dernière sauvegarde figurent dans un même répertoire du serveur, sous le nom qu'ils avaient au moment de leur création.

Reportez-vous à la section « Localisation des fichiers de sauvegarde requis pour une restauration » page 464.

REMARQUE : si vous ne disposez pas de fichiers de sauvegarde pour le serveur, utilisez Xbrowse pour tenter de récupérer des informations sur ce dernier en sondant eDirectory. Effectuez cette opération avant de supprimer l'objet Serveur ou tout objet associé de l'arborescence.

Vous trouverez XBrowse ainsi que des informations supplémentaires sur le site Web du support NetIQ (http://support.novell.com/docs/Readmes/InfoDocument//2960653.html).

❒ Vous avez installé eDirectory dans une nouvelle arborescence temporaire.

Il est nécessaire, dans un premier temps, de mettre en service le serveur dans une nouvelle arborescence, car vous allez le créer sous le nom qu'il avait avant la défaillance, mais vous devez éviter la confusion qu'entraînerait son intégration dans l'arborescence originale avant que la restauration n'ait recréé son identité complète. Une fois le processus de restauration de la base de données terminé, le serveur est rétabli dans son arborescence d'origine.

❒ (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, prévoyez de recréer la configuration appropriée à l'issue de la restauration, afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

Le processus de restauration désactive la fonction de consignation et rétablit la configuration par défaut pour cette dernière.

Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

❒ (Conditionnel) Si des applications ou des objets doivent rechercher le serveur par son adresse IP, prévoyez d'utiliser la même adresse IP pour le serveur restauré.

L'outil de restauration d'eDirectory restaure d'abord la sauvegarde complète. Une fois cette opération terminée, il vous invite à saisir les noms des fichiers de sauvegarde incrémentielle. Il vous indique l'ID du fichier suivant. Une fois tous ces fichiers restaurés, l'outil de restauration passe aux fichiers journaux de transaction individuelle. Reportez-vous également à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.

Après avoir collecté tous les fichiers nécessaires, effectuez la restauration avec iManager ou le client DSBK. Reportez-vous à « Restauration à partir de fichiers de sauvegarde avec DSBK » page 472 ou à « Restauration à partir de fichiers de sauvegarde avec iManager » page 616.

Localisation des fichiers de sauvegarde requis pour une restauration

1. À partir de la bande de sauvegarde du système de fichiers, copiez les fichiers de la dernière sauvegarde complète d'eDirectory dans un répertoire du serveur.

Pour vérifier l'ID de la dernière sauvegarde complète, consultez le fichier journal de l'outil de sauvegarde.

2 À partir de la bande de sauvegarde du système de fichiers, copiez également chaque fichier de sauvegarde incrémentielle consécutif dans le même répertoire du serveur.

Pour vérifier que vous disposez des fichiers de sauvegarde incrémentielle appropriés, consultez l'en-tête du fichier de sauvegarde complète. Il contient l'ID du fichier de sauvegarde incrémentielle suivant, dans l'attribut `next_inc_file_ID`. L'ID mentionné dans `next_inc_file_ID` est identique à celui enregistré dans l'en-tête du fichier de sauvegarde incrémentielle, dans l'attribut `incremental_file_number`. Pour obtenir une description de l'en-tête, reportez-vous à la section « Format de l'en-tête des fichiers de sauvegarde » page 451.

AVERTISSEMENT : lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car vous risqueriez de l'altérer. La plupart des applications n'enregistrent pas les données binaires correctement.

Chaque fichier de sauvegarde incrémentielle contient également l'ID du prochain fichier de sauvegarde incrémentielle.

Vous pouvez aussi rechercher l'ID de sauvegarde incrémentielle dans le fichier journal de l'outil de sauvegarde.

Les ID sont importants car il se peut que vos fichiers de sauvegarde aient reçu le même nom au moment de leur création (par exemple, si vous utilisez le même fichier de traitement par lots pour les sauvegardes incrémentielles sans surveillance, le nom du fichier de sauvegarde spécifié est toujours identique). Il peut alors être nécessaire de changer les noms de fichiers afin de pouvoir enregistrer toutes les sauvegardes dans le même répertoire. L'ID qui figure dans l'en-tête vous permet de trouver les fichiers corrects, même si vous avez renommé les fichiers.

3 (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier, assurez-vous que tous les journaux de transactions individuelles créés depuis la dernière sauvegarde figurent dans un répertoire du serveur, sous le nom de fichier qu'ils avaient au moment de leur création.

Si votre serveur fait partie d'un anneau de répliques, vous devez le restaurer en utilisant tous les fichiers journaux de transactions individuelles. Si vous ne les incluez pas tous et si le serveur partage des répliques avec d'autres serveurs, le processus de vérification de la restauration échoue parce que les vecteurs de transition ne correspondent pas à ceux des autres répliques de l'anneau. Par défaut, la base de données eDirectory restaurée n'est pas ouverte à l'issue de la restauration si elle est incohérente par rapport aux autres répliques.

Identifiez le premier journal de transaction individuelle dont vous avez besoin en ouvrant le dernier fichier de sauvegarde dans un éditeur de texte et en consultant l'attribut current_log dans l'en-tête. Vous devez collecter ce fichier journal ainsi que tous les suivants.

AVERTISSEMENT : lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car vous risqueriez de l'altérer. La plupart des applications n'enregistrent pas les données binaires correctement.

Les fichiers journaux de transactions individuelles nécessaires peuvent ne pas tous figurer au même emplacement lorsque vous souhaitez les utiliser pour une restauration. Vous devez donc vous assurer que vous en avez collecté un jeu complet et les avez placés dans le même répertoire. Les fichiers journaux de transactions individuelles peuvent se trouver à différents emplacements pour les raisons suivantes :

- Vous avez modifié l'emplacement du répertoire des fichiers journaux de transactions individuelles depuis la dernière sauvegarde complète ou incrémentielle.
- Vous les avez enregistrés sur bande à l'aide de la sauvegarde du système de fichiers, puis supprimés du serveur pour libérer de l'espace disque.

Si vous devez récupérer des fichiers journaux de transactions individuelles à partir d'une sauvegarde sur bande, assurez-vous que vous disposez du jeu de fichiers le plus récent. Comparez les tampons horaires des fichiers dupliqués sur la bande et sur le serveur. Le fichier journal de transaction individuelle utilisé par la base de données au moment de la sauvegarde du système de fichiers est incomplet sur la bande. La version complète et la plus récente de ce fichier figure sur le serveur.

- Vous avez renommé la base de données eDirectory depuis la dernière sauvegarde (NDS est devenu ND1, par exemple). Cela modifie le dernier nom de répertoire dans le chemin d'accès aux fichiers journaux de transactions individuelles.

  Par exemple, si l'emplacement spécifié correspondait à `d:\novell\nds\dibfiles\` et le nom de votre base de données eDirectory à NDS, l'emplacement des fichiers journaux de transaction individuelle correspondait à `d:\novell\nds\dibfiles\nds.rfl\`. Si vous avez renommé la base de données NDS en ND1, le répertoire des fichiers journaux de transaction individuelle est devenu `d:\novell\nds\dibfiles\nd1.rfl\`.

IMPORTANT : veillez à fournir tous les fichiers journaux de transactions individuelles requis. L'outil de sauvegarde ne peut pas déterminer si le jeu de fichiers journaux dont vous disposez est complet. Il les ouvre et les utilise dans l'ordre. S'il ne trouve pas le fichier journal suivant dans le répertoire indiqué, il met fin au processus de restauration. Si vous n'avez pas fourni tous les fichiers journaux nécessaires, la restauration est incomplète.

Utilisation de DSBK

DSBK est un analyseur de ligne de commande léger qui effectue une sauvegarde d'eDirectory et vous permet de lancer une sauvegarde à partir de la console du serveur sans avoir à vous connecter au préalable ni à configurer les services RBS. Il s'exécute en tant que script sous Linux et qu'utilitaire de console sous Windows.

Au terme d'une opération DSBK, les résultats sont écrits dans un fichier (`dsbk.pipe` sous Linux) dont vous pouvez programmer l'ouverture et l'affichage des résultats. Les quatre premiers octets de ce fichier contiennent les éventuels codes d'erreur générés pendant l'opération. En l'absence d'erreurs, ces quatre octets contiennent des zéros.

REMARQUE : Veillez à avoir pris connaissance de toutes les instructions fournies par NetIQ avant de finaliser la configuration de votre sauvegarde/restauration.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la Liste de contrôle pour la sauvegarde pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Cette section traite des sujets suivants :

- « Conditions préalables » page 467
- « Utilisation de DSBK sur plusieurs plates-formes » page 467
- « Sauvegarde manuelle avec DSBK » page 470
- « Automatisation de la sauvegarde d'eDirectory » page 471
- « Configuration des fichiers journaux de transaction individuelle avec DSBK » page 471
- « Restauration à partir de fichiers de sauvegarde avec DSBK » page 472
- « Options de ligne de commande pour la sauvegarde et la restauration » page 474
- « Exécution de DSBK en tant que tâche cron » page 483

Conditions préalables

- ❒ Si vous prévoyez d'utiliser des fichiers journaux de transactions individuelles pour le serveur concerné, veillez à les activer avant d'effectuer une sauvegarde.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas.

  Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la Utilisation des fichiers journaux de transactions individuelles. Pour savoir comment les activer, reportez-vous à la section Configuration des fichiers journaux de transaction individuelle avec DSBK.

- ❒ Déterminez les autres fichiers à sauvegarder avec eDirectory et créez au besoin un fichier d'inclusion.

  Vous pouvez sauvegarder les fichiers de flux à l'aide de paramètres. Nous vous recommandons de sauvegarder systématiquement les fichiers NICI. Pour plus d'informations sur la sauvegarde de NICI, reportez-vous à la section Sauvegarde et restauration de NICI.

  Pour inclure d'autres fichiers, tels qu'`autoexec.ncf`, vous devez indiquer leurs noms et leurs chemins d'accès dans un fichier d'inclusion. Séparez les chemins d'accès et les noms de fichier par un point-virgule, sans inclure de retour chariot ni d'espace. Par exemple, `sys:\system\autoexec.ncf;sys:\etc\hosts;`.

- ❒ Prévoyez d'effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory pour enregistrer les fichiers de sauvegarde d'eDirectory sur bande. L'outil de sauvegarde les enregistre uniquement sur le serveur.

  SUGGESTION : pour faciliter le transfert des fichiers de sauvegarde sur un autre périphérique de stockage, vous pouvez spécifier la taille maximale de ces fichiers dans la commande de `sauvegarde`, à l'aide de l'option `-s` suivie d'un nombre indiquant la taille en octets. Vous pouvez également utiliser un logiciel tiers pour les compresser après leur création. Le taux de compression atteint environ 80 %.

- ❒ Consultez la description des options de la ligne de commande à la section Options de ligne de commande pour la sauvegarde et la restauration.

Utilisation de DSBK sur plusieurs plates-formes

- « Utilisation de DSBK sous Linux » page 467
- « Utilisation de DSBK sous Windows » page 469

Utilisation de DSBK sous Linux

Les commandes DSBK peuvent être exécutées directement sur le shell d'un serveur Linux sur lequel eDirectory est installé.

Le résultat de la commande est écrit dans le fichier journal spécifique de l'instance eDirectory (instance par défaut : `/var/opt/novell/eDirectory/log/ndsd.log`) :

```
DSBK HELP
To get help on a specific function type "help <function name>"
 Current functions:
  backup
  restore
  restadv
  getconfig
  setconfig
  cancel
```

Des commandes DSBK peuvent être entrées dans un outil `crontab` pour exécuter régulièrement des commandes `dsbk getconfig` et `dsbk backup`, afin d'effectuer des sauvegardes complètes une fois par semaine et des sauvegardes incrémentielles les autres jours, ou toute autre combinaison souhaitée.

À l'aide des fichiers journaux de transaction individuelle (RFL) dans DSBK

- Activez la fonctionnalité RFL à l'aide de la commande suivante :

  ```
  dsbk setconfig -L
  ```

  L'option `-L` démarre une nouvelle session de consignation de transactions individuelles par fichier.

- Définissez un emplacement pour les fichiers journaux de transaction individuelle à créer à l'aide de la commande suivante :

  ```
  dsbk setconfig -L -r <roll forward log directory>
  ```

- Obtenez un emplacement pour les fichiers journaux de transaction individuelle à créer à l'aide de la commande suivante :

  ```
  dsbk getconfig
  ```

- Supprimez les anciens fichiers journaux du répertoire des fichiers journaux de transaction individuelle au cours d'une sauvegarde à l'aide de l'option `- a` :

  ```
  backup -f <file name> -l <file name> [-s <size>] [-u <file name>] [-e
  <password>] [-t] [-w] [-a]
  [-b|-i|-c] [-o] [-d] [--config-file <configuration file>]
  ```

SUGGESTION : lorsque vous utilisez l'utilitaire DSBK de manière interactive, ouvrez une seconde fenêtre de terminal en veillant à ce que `tail -f <instance specific ndsd.log>` soit en cours d'exécution, afin que le résultat des commandes saisies soit immédiatement lisible.

Une fois la sauvegarde effectuée, enregistrez-la à l'aide des utilitaires de sauvegarde du système de fichiers standard.

REMARQUE : pour plus d'informations sur les options de ligne de commande DSBK, reportez-vous à la section Options de ligne de commande pour la sauvegarde et la restauration.

Utilisation de DSBK sous Windows

Cette section décrit le fonctionnement de base de l'utilitaire DSBK sur la plate-forme Windows.

Pour utiliser DSBK sur un serveur Windows qui héberge eDirectory, procédez comme suit :

1. Invoquez l'utilitaire via la console **NetIQ eDirectory Services**. **dsbk.dlm** est l'une des options disponibles dans la liste des services sous l'onglet Services. La sous-commande **dsbk** ainsi que tous les paramètres pour cette sous-commande sont spécifiés dans le champ **Paramètres de démarrage**.
2. Affichez la configuration actuelle de la sauvegarde à l'aide du paramètre `getconfig`. Le résultat de toutes les commandes DSBK est annexé au fichier `backup.out` situé dans le dossier d'installation d'eDirectory sous Windows.
3. Définissez un emplacement pour les fichiers journaux de transaction individuelle à créer à l'aide de la commande suivante :

   ```
   setconfig -r <roll forward log directory> -L
   ```

   L'option `-L` démarre une nouvelle session de consignation de transactions individuelles par fichier.
4. Démarrez une sauvegarde de l'arborescence en entrant la commande suivante :

   ```
   backup -f <backup file> -l <logfile> -t -w -b -e <password>
   ```

   Utilisez les options suivantes :

   - `-t` : effectue une sauvegarde des fichiers de flux.
   - `-w` : remplace un fichier de sauvegarde existant portant le même nom.
   - `-b` : effectue une sauvegarde complète.
   - `-e <mot_de_passe>` : effectue une sauvegarde NICI à l'aide du mot de passe fourni.
   - `-a` : supprime les anciens fichiers journaux du répertoire des fichiers journaux de transaction individuelle au cours d'une sauvegarde continue à chaud.

   Par exemple, démarrez la sauvegarde comme suit :

   ```
   backup -f c:\dsbk.bak -l c:\backup.log -t -w -b -e novell
   ```

   Vous pouvez vérifier l'état de la sauvegarde effectuée dans le fichier `backup.out`.

   REMARQUE : pour plus d'informations sur les options de ligne de commande DSBK, reportez-vous à la section Options de ligne de commande pour la sauvegarde et la restauration.

Vous pouvez activer la fonctionnalité RFL à l'aide de la commande suivante :

```
setconfig -r <roll forward log directory> -L
```

Sauvegarde manuelle avec DSBK

DSBK permet de sauvegarder les données d'une base de données eDirectory dans un fichier que vous indiquez, sur le serveur sur lequel la sauvegarde est en cours d'exécution. Le fichier de sauvegarde (ou le jeu de fichiers) contient les informations nécessaires pour restaurer eDirectory dans l'état où il se trouvait au moment de la sauvegarde. Le résultat du processus de sauvegarde est enregistré dans le fichier journal que vous spécifiez.

DSBK permet d'effectuer plusieurs tâches, notamment :

- effectuer une sauvegarde complète ou incrémentielle lorsque la base de données est ouverte (sauvegarde continue à chaud) ;

  Cela signifie que la base de données eDirectory est ouverte et accessible pendant le processus, mais que vous obtenez une sauvegarde complète qui constitue un instantané de la base au moment où la sauvegarde a commencé.
- effectuer une sauvegarde à froid (la base de données est fermée et une sauvegarde complète est créée) ;.

  Cette option est utile lors de la mise à niveau d'une machine, ou du déplacement d'un serveur vers une nouvelle machine équipée du même système d'exploitation (comme expliqué dans Mise à niveau du matériel ou remplacement d'un serveur).
- paramétrer la base de données pour qu'elle reste fermée et verrouillée après une sauvegarde ;.
- définir la taille maximale du fichier de sauvegarde.

Procédure

Pour sauvegarder la base de données eDirectory sur un serveur à l'aide de DSBK, procédez comme suit :

1. Entrez la commande `dsbk backup`, en suivant le modèle général ci-dessous :

   `dsbk backup -b -f nom_et_chemin_fichier_sauvegarde -l nom_et_chemin_fichier_sauvegarde -u nom_et_chemin_fichier_inclusion -t -w`

   Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

   Par exemple, sous Windows, entrez la commande suivante :

   `dsbk backup -b -f c:\backups\8_20_2001.bak -l c:\backups\backup.log -u c:\backups\myincludefile.txt -t -w`

   Cet exemple de commande permet d'effectuer une sauvegarde complète (`-b`), le fichier de sauvegarde étant enregistré sous `c:\backups\8_20_2001.bak` et le fichier journal correspondant sous `c:\backups\backup.log`. Cette commande indique que d'autres fichiers doivent être sauvegardés avec la base de données :

   - les fichiers mentionnés dans un fichier d'inclusion (`-u c:\backups\mon_fichier_inclusion.txt`) préalablement créé par l'administrateur ;
   - les fichiers de flux (`-t`).

   Cet exemple de commande indique que le fichier de sauvegarde doit être remplacé (`-w`). Par conséquent, si un fichier portant le même nom existe, l'outil de sauvegarde le remplace.

   Le résultat est consigné dans le fichier `dsbackup.out`, afin d'indiquer si la sauvegarde a réussi.

   Veillez à effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde sur bande par mesure de sécurité. L'outil de sauvegarde les enregistre uniquement sur le serveur.

Automatisation de la sauvegarde d'eDirectory

Pour automatiser la sauvegarde d'eDirectory, enregistrez la commande suivante dans un fichier de traitement par lots :

```
dhostcon.exe 192.168.1.1 load dsbk backup -b -f <Backup File> -l <Log File> -t -w
```

Par exemple,

```
c:\novell\nds\dhostcon.exe 192.168.1.1 load dsbk backup -b -f edirbackup.bak -l
c:\novell\edir-backup.log -t -w
```

Enregistrez ce fichier à l'emplacement où vous avez installé eDirectory.

Configuration des fichiers journaux de transaction individuelle avec DSBK

DSBK permet de modifier les paramètres des fichiers journaux de transaction individuelle. Vous pouvez effectuer les tâches suivantes :

- rechercher la configuration actuelle ;
- activer ou désactiver la fonction de consignation de transactions individuelles par fichier ;

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas.
- modifier le répertoire des fichiers journaux de transactions individuelles ;
- définir la taille minimale et maximale des fichiers journaux de transactions individuelles ;
- rechercher le fichier journal de transaction individuelle actuel ainsi que le dernier fichier journal inutilisé ;
- activer ou désactiver la consignation des fichiers de flux pour les fichiers journaux de transaction individuelle

Pour plus d'informations sur la consignation de transactions individuelles par fichier, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

Procédure

1. Recherchez la configuration actuelle en entrant

   ```
   dsbk getconfig
   ```

   Aucun paramètre n'est nécessaire.

   Voici un exemple des informations que vous recevez :

   ```
   Roll forward log status OFF
   Stream file logging status OFF
   Current roll forward log directory C:\rfl\nds.rfl
   Minimum roll forward log size (bytes) 104857600
   Maximum roll forward log size (bytes) 4294705152
   Last roll forward log not used 00000000.log
   Current roll forward log 00000001.log
   *** END ***
   ```

2. Modifiez les paramètres à l'aide de la commande `setconfig` et suivez le modèle général ci-dessous :

```
dsbk setconfig [-L|-l] [-T|-t] -r
chemin_fichiers_journaux_transactions_individuelles -n taille_minimale_fichier
-m taille_maximale_fichier
```

Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

En principe, vous devriez réserver un volume/une partition de disque à ces fichiers journaux, afin de faciliter le contrôle de l'espace disque et des droits.

AVERTISSEMENT : si vous activez la consignation de transactions individuelles par fichier, n'utilisez pas l'emplacement par défaut. Pour assurer une tolérance aux pannes, placez le répertoire sur un volume/une partition de disque et un périphérique de stockage différents de ceux d'eDirectory. Le répertoire des fichiers journaux de transactions individuelles doit résider sur le serveur us modifiez la configuration de sauvegarde.

IMPORTANT : si vous activez la consignation de transactions individuelles par fichier, vous devez surveiller l'espace disque sur le volume où vous placez les fichiers journaux de transactions individuelles. Si vous ne le surveillez pas, le répertoire des fichiers journaux s'étend jusqu'à saturer le volume/la partition de disque. Si ces journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Nous vous conseillons de sauvegarder et de supprimer périodiquement du serveur les fichiers journaux de transactions individuelles inutilisés. Reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462.

Restauration à partir de fichiers de sauvegarde avec DSBK

DSBK permet de restaurer une base de données eDirectory à partir des données stockées dans les fichiers de sauvegarde que vous avez créés manuellement. Les résultats de la restauration sont consignés dans le fichier journal que vous indiquez.

DSBK vous permet en outre d'utiliser des options de restauration avancées non disponibles dans iManager. Celles-ci sont présentées dans le tableau « Options de ligne de commande pour la sauvegarde et la restauration » page 474, sous restore et restadv.

Conditions supplémentaires

- ❒ Assurez-vous que eDirectory est installé et en service sur le serveur sur lequel vous effectuez la restauration.

  Par exemple, si la restauration est nécessaire en raison de la défaillance d'un périphérique de stockage, vous devez réinstaller eDirectory sur le nouveau périphérique. Si vous restaurez un serveur défaillant sur une nouvelle machine, ou transférez simplement un serveur d'une machine à une autre, vous devez installer le système d'exploitation ainsi que eDirectory sur la nouvelle machine.
- ❒ Consultez la description des options de la ligne de commande à la section « Options de ligne de commande pour la sauvegarde et la restauration » page 474.
- ❒ Consultez la description du processus de restauration dans la section « Présentation du processus de restauration avec l'outil de restauration » page 450.

Procédure

Pour restaurer une base de données eDirectory sur un serveur à l'aide de DSBK :

1. Vérifiez que vous avez collecté les fichiers de sauvegarde nécessaires, comme expliqué à la « Préparation d'une restauration » page 463.
2. Entrez la commande `dsbk restore`, en suivant le modèle général ci-dessous :

   `dsbk restore -r -a -o -f` *`chemin_et_nom_fichier_sauvegarde_complète`* `-d` *`emplacement_fichiers_journaux_transactions_individuelles`* `-l` *`chemin_et_nom_journal_restauration`*

   Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance. Veillez à utiliser le paramètre `-r` pour restaurer la base de données eDirectory proprement dite. Sinon, seuls les autres types de fichiers seront restaurés. Si vous souhaitez que la base de données soit ouverte et activée une fois la restauration terminée, veillez à spécifier les paramètres `-a` et `-o`.

   Si vous restaurez des fichiers journaux de transaction individuelle, veillez à inclure leur chemin d'accès complet, y compris le répertoire créé automatiquement par eDirectory, généralement dénommé `\nds.rfl`. Pour plus d'informations sur ce répertoire, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles » page 461.

   Par exemple :

   ```
   dsbk restore -r -a -o -f $HOME/backup/nds.bak -d $HOME/backup/rfldir/nds.rfl -
   l $HOME/backup/backup.log
   ```

   Cet exemple de commande indique que la base de données proprement dite doit être restaurée (`-r`), et qu'elle doit être activée (`-a`) et ouverte (`-o`) une fois la vérification de la restauration effectuée. Le paramètre `-f` indique où se trouve le fichier de sauvegarde complète, le paramètre `-d` désigne l'emplacement des fichiers journaux de transaction individuelle et le paramètre `-l`, le fichier journal dans lequel les résultats de la restauration sont consignés.

   DSBK restaure la sauvegarde complète. Le résultat est enregistré dans le fichier `ndsd.log`, lequel indique si la restauration a réussi.
3. (Conditionnel) Si la restauration échoue, consultez les erreurs dans le fichier journal.

   Si la vérification de la restauration échoue, reportez-vous à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

   REMARQUE : si le serveur que vous restaurez partage une réplique avec un serveur qui exécute une version d'eDirectory antérieure à 8.5, le journal de restauration indique l'erreur –666 (version DS incompatible) pour cette réplique.

   ---
4. (Conditionnel) Si vous avez restauré les fichiers de sécurité NICI, redémarrez le serveur pour réinitialiser NICI une fois la restauration terminée, puis restaurez DIB.
5. Vérifiez que le serveur fonctionne normalement.
6. (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, vous devez recréer la configuration de votre choix afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

La restauration est à présent terminée et NICI réinitialisé avec les fichiers correspondants restaurés, ce qui vous permet d'accéder aux informations codées. Si vous utilisez la fonction de consignation de transactions individuelles par fichier, vous vous êtes préparé contre toute nouvelle défaillance en réactivant cette fonction à l'issue de la restauration, puis en effectuant une nouvelle sauvegarde complète.

Options de ligne de commande pour la sauvegarde et la restauration

Les options de ligne de commande de l'outil de sauvegarde d'eDirectory sont réparties en six fonctions : backup, restore, restadv, getconfig, setconfig et cancel.

Les paramètres peuvent être introduits dans n'importe quel ordre dans la commande, après le nom de la fonction. Ils doivent cependant être séparés par un espace.

Option et paramètres	Description
`backup`	Effectue une sauvegarde de la base de données et des fichiers associés.
`-f` *`nom_fichier`*	(Obligatoire) Nom et chemin d'accès du fichier de sauvegarde Nom et emplacement du fichier de sauvegarde que l'outil de sauvegarde doit créer. Ce fichier doit figurer sur le serveur que vous sauvegardez. Par exemple, la commande `backup -f C:\backup\ndsbak.bak` permet de sauvegarder la base de données dans `C:\backup\ndsbak.bak`.
`-l` *`nom_fichier`*	(Obligatoire) Nom et chemin d'accès du fichier journal Indique le fichier journal dans lequel consigner les résultats de la sauvegarde.
`-b`	(Facultatif) Effectuer une sauvegarde complète. Effectue une sauvegarde complète de la base de données eDirectory. Il s'agit de l'option par défaut. Si vous ne spécifiez ni `-i` ni `-c`, une sauvegarde complète est effectuée.
`-i`	(Facultatif) Effectuer une sauvegarde incrémentielle. Effectue une sauvegarde incrémentielle de la base de données eDirectory. Toutes les modifications apportées à la base de données depuis la dernière sauvegarde complète ou incrémentielle sont sauvegardées.
`-t`	(Facultatif) Sauvegarder les fichiers de flux. Inclut les fichiers de flux lors de la sauvegarde de la base de données eDirectory.

Option et paramètres	Description
`-u` *`nom_fichier`*	(Facultatif) Nom et chemin d'accès du fichier d'inclusion utilisateur. Indique un fichier d'inclusion qui contient les fichiers supplémentaires à sauvegarder. Vous pouvez créer ce fichier de configuration afin d'inclure dans la sauvegarde d'autres fichiers importants pour la restauration de la base de données eDirectory du serveur. Dans le fichier d'inclusion, indiquez le chemin d'accès complet de chaque fichier à sauvegarder, suivi d'un point-virgule (;). N'insérez pas d'espaces ni de retours chariot dans la liste des fichiers. Pour vous assurer que les fichiers indiqués ont bien été sauvegardés, consultez le fichier journal de sauvegarde ou l'en-tête du fichier de sauvegarde. Reportez-vous aux sections « Format du fichier journal de sauvegarde » page 455 et « Format de l'en-tête des fichiers de sauvegarde » page 451. **AVERTISSEMENT :** lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car vous risqueriez de l'altérer. La plupart des applications n'enregistrent pas les données binaires correctement.

Option et paramètres	Description
`-s` *`taille_fichier`*	(Facultatif) Taille maximale du fichier de sauvegarde (Mo) Taille maximale (en Mo) du fichier de sauvegarde. Vous pouvez utiliser cette option si la taille des fichiers risque de poser un problème avec le support servant à enregistrer les fichiers de sauvegarde après leur création. Si la taille maximale est atteinte, un nouveau fichier de sauvegarde est créé avec le même nom, mais une extension de cinq chiffres hexadécimaux est ajoutée pour indiquer de quel fichier il s'agit. Cette extension est incrémentée pour chaque nouveau fichier. Par exemple, vous pouvez fixer la taille maximale des fichiers de sauvegarde à 10 Mo en utilisant les paramètres suivants dans la commande :`backup -f C:\backup\mydib.bak -s 10`. Si la taille de la base de données est de 35 Mo, vous obtenez les fichiers de sauvegarde suivants : `C:\backup\mydib.bak`, dont la taille s'élève à 9,6 Mo `C:\backup\mydib.bak.00001`, dont la taille s'élève à 9,6 Mo `C:\backup\mydib.bak.00002`, dont la taille s'élève à 9,6 Mo `C:\backup\mydib.bak.00003`, dont la taille s'élève à 5,6 Mo La plus petite taille possible est d'environ 1 Mo. Le premier fichier peut être plus volumineux, selon le nombre de fichiers inclus dans la sauvegarde. Le premier fichier contient, sous l'étiquette backup, un attribut nommé `number_of_files`. Il s'agit du nombre total de fichiers qui composent le jeu de sauvegarde. Dans l'exemple ci-dessus, ce nombre s'élèverait à 4. De plus, l'en-tête de chaque fichier de sauvegarde contient l'attribut `backup_file`. Il s'agit du nom original du fichier. Pour plus d'informations, reportez-vous à la section « Format de l'en-tête des fichiers de sauvegarde » page 451. Pour restaurer un ensemble de fichiers de sauvegarde comme dans l'exemple ci-dessus, la commande est la suivante : `restore -f C:/backup/mydib.bak -l` *`chemin_et_nom_du_fichier_journal`* L'outil de sauvegarde identifie la présence de plusieurs fichiers et les recherche dans le même répertoire que le premier, mais prend en compte les modifications de nom indiquées plus haut. **SUGGESTION :** en utilisant un logiciel de compression tiers, vous pouvez également réduire considérablement la taille des fichiers de sauvegarde. Le taux de compression atteint environ 80 %.

Option et paramètres	Description
`-w`	(Facultatif) Écraser le fichier de sauvegarde portant le même nom Écrase le fichier de sauvegarde spécifié avec le paramètre `-f` si un fichier du même nom existe déjà. En mode interactif, si cette option n'est pas utilisée et qu'un fichier du même nom existe déjà, l'outil de sauvegarde vous demande si vous souhaitez écraser ce fichier. En mode de traitement par lots, s'il existe un fichier du même nom et que le paramètre `-w` n'est pas spécifié, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. Si vous effectuez une sauvegarde du système de fichiers peu après chaque sauvegarde complète ou incrémentielle d'eDirectory, les fichiers de sauvegarde précédents doivent avoir été copiés sur une bande. Vous pouvez donc écraser le fichier de sauvegarde existant sans crainte. **IMPORTANT :** utilisez cette option dans vos fichiers de traitement par lots pour les sauvegardes sans surveillance. s'il existe déjà un fichier portant le même nom (ce qui est probable si vous utilisez régulièrement le même fichier de traitement par lots), votre sauvegarde aboutit uniquement si vous employez l'option `-w` pour écraser le fichier de sauvegarde existant. En mode de traitement par lots, s'il existe un fichier du même nom et que l'option `-w` n'est pas spécifiée, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. En mode interactif, si vous ne spécifiez pas le paramètre `-w`, DSBK vous demande si vous souhaitez écraser le fichier.
`-c`	(Facultatif) Effectuer une sauvegarde à froid Exécute une sauvegarde complète de la base de données fermée. Une fois la sauvegarde effectuée, la base de données est rouverte, sauf si les paramètres `-o` ou `-o` et `-d` sont spécifiés.
`-o`	(Facultatif) Laisser la base de données fermée après la sauvegarde à froid Ce paramètre ne peut être utilisé que si le paramètre `-c` est également spécifié. Laisse la base de données fermée après une sauvegarde à froid. Cette option est utile lors de la mise à niveau d'une machine, ou du déplacement d'un serveur vers une nouvelle machine équipée du même système d'exploitation (comme expliqué à la « Mise à niveau du matériel ou remplacement d'un serveur » page 574).
`-d`	(Facultatif) Désactiver l'agent DS après la sauvegarde à froid Ce paramètre ne peut être utilisé que si les paramètres `-c` et `-o` sont également spécifiés. Désactive l'agent DS après une sauvegarde à froid. Cette option est utile lors de la mise à niveau d'une machine, ou du déplacement d'un serveur vers une nouvelle machine équipée du même système d'exploitation (comme expliqué à la « Mise à niveau du matériel ou remplacement d'un serveur » page 574). Pour désactiver l'agent DS, l'attribut connexion désactivée doit être paramétré sur le pseudo-serveur. Cela aura pour conséquence l'apparition de l'erreur -663 au démarrage d'eDirectory.
`-e` *`mot_de_passe`*	Effectuer une sauvegarde de NICI *mot_de_passe* correspond au mot de passe à utiliser pour sauvegarder NICI. Ce même mot de passe doit être spécifié pour restaurer les fichiers NICI.

Option et paramètres	Description
`--config-file` *`fichier_configuration`*	(Facultatif) Permet de spécifier l'instance d'eDirectory à sauvegarder. *fichier_configuration* correspond au chemin absolu du fichier de configuration de l'instance d'eDirectory à sauvegarder. Par exemple : `--config-file /etc/opt/novell/eDirectory/conf/nds.conf` Ce paramètre s'applique uniquement aux environnements Linux.
`restore`	Effectue une restauration de la base de données et des fichiers associés.
`-f` *`nom_fichier`*	(Obligatoire) Nom et chemin d'accès du fichier de sauvegarde Indique la sauvegarde complète à partir de laquelle effectuer la restauration. Le fichier doit se trouver sur le serveur en cours de restauration. Par exemple, la commande `restore -f C:/backup/ndsbak.bak` permet d'effectuer la restauration à partir du fichier `C:/backup/ndsbak.bak`. Si la sauvegarde est constituée de plusieurs fichiers, tous les fichiers du jeu doivent être copiés dans le même répertoire du serveur.
`-l` *`nom_fichier`*	(Obligatoire) Nom et chemin d'accès du fichier journal Indique le fichier journal dans lequel consigner les résultats de la restauration.
`-r`	(Facultatif) Restaurer l'ensemble DIB Indique que la base de données eDirectory doit être restaurée. **AVERTISSEMENT :** si cette option n'est pas définie, la base de données eDirectory proprement dite n'est pas restaurée. Seuls les autres types de fichiers spécifiés seront restaurés.
`-d` *`nom_rép`*	(Facultatif) Répertoire des fichiers journaux de transactions individuelles Indique le répertoire où sont stockés les fichiers journaux de transactions individuelles. Le chemin d'accès complet doit être indiqué et le répertoire doit se trouver sur le serveur restauré. Tous les fichiers journaux de transactions individuelles doivent se trouver dans le répertoire spécifié et porter le même nom que lors de leur création. Une fois la base de données restaurée, les modifications enregistrées dans ces fichiers journaux sont réappliquées afin de mettre à jour la base de données. Si le paramètre `-d` n'est pas utilisé, l'outil de sauvegarde ne réapplique aucune modification, même si la consignation de transaction individuelle par fichier était activée au moment de la sauvegarde. Pour identifier le premier fichier journal de transaction individuelle requis, ouvrez dans un éditeur de texte le dernier fichier de sauvegarde restauré et lisez l'attribut `current_log` de l'étiquette `backup`. Le dernier fichier de sauvegarde restauré est le fichier de sauvegarde complète spécifié par l'option `-f` ou le dernier fichier de sauvegarde incrémentielle à appliquer pendant la restauration. Pour plus d'informations sur les attributs listés dans l'en-tête, reportez-vous à la section « Format de l'en-tête des fichiers de sauvegarde » page 451. **AVERTISSEMENT :** lorsque vous ouvrez un fichier de sauvegarde, contentez-vous de consulter l'en-tête. N'essayez pas d'enregistrer ni de modifier le fichier, car vous risqueriez de l'altérer. La plupart des applications n'enregistrent pas les données binaires correctement.

Option et paramètres	Description
`-u`	(Facultatif) Restaure les fichiers inclus par l'utilisateur Restaure les fichiers utilisateur inclus dans la sauvegarde de la base de données. Dans le cadre de la sauvegarde, vous pouvez créer un fichier texte contenant la liste des fichiers à sauvegarder avec la base de données, et le définir comme fichier d'inclusion utilisateur. Les fichiers concernés ne peuvent être restaurés que s'ils ont été inclus dans la sauvegarde.
`-a`	(Facultatif) Activer DIB après vérification Renomme la base de données RST en NDS une fois la restauration correctement vérifiée. Pour obtenir une vue d'ensemble du processus, reportez-vous à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.
`-o`	(Facultatif) Ouvrir la base de données à la fin de l'opération Ce paramètre indique à l'outil de sauvegarde d'ouvrir la base de données une fois l'opération terminée. Si la vérification se déroule correctement, la base de données restaurée s'ouvre. Sinon, cette option entraîne l'ouverture de la base de données présente sur le serveur avant la restauration. Pour obtenir une vue d'ensemble du processus, reportez-vous à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.
`-s`	Ce paramètre indique à l'outil de sauvegarde de ne pas réinitialiser le fichier journal de transaction individuelle une fois la restauration terminée. Il est principalement utilisé lorsque les fichiers RFL se trouvent à l'emplacement par défaut.
`-n`	(Facultatif) Ne pas vérifier la base de données après la restauration Ce paramètre indique à l'outil de sauvegarde de restaurer la base de données sans effectuer de vérification. Le vecteur de transition de ce serveur n'est pas comparé à celui qu'attendent les autres serveurs de l'anneau de répliques dont il fait partie. Pour plus d'informations sur les vecteurs de transition, reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration » page 458. La base de données RST n'est pas renommée en NDS, sauf si une autre option est définie à cet effet. **IMPORTANT :** nous vous recommandons de ne pas utiliser cette option à moins d'y être invité par le support technique de NetIQ.
`-v`	(Facultatif) Remplacer la restauration Renomme la base de données RST en base de données NDS sans tenter de vérification. **IMPORTANT :** nous vous recommandons de ne pas utiliser cette option à moins d'y être invité par le support technique de NetIQ.
`-k`	(Facultatif) Supprimer le verrouillage de la base de données Supprime le verrouillage de la base de données NDS.
`-i`	Liste de fichiers incrémentiels classés dans l'ordre et séparés par des virgules.

Option et paramètres	Description
`-e` *`mot_de_passe`*	Restaurer les fichiers NICI sauvegardés *`mot_de_passe`* correspond au mot de passe qui a été utilisé lorsque les fichiers NICI ont été sauvegardés. Si vous spécifiez un mot de passe erroné alors que vous tentez de restaurer les fichiers NICI, un message d'erreur s'affiche.
`--config-file` *`fichier_configuration`*	(Facultatif) Permet de spécifier l'instance d'eDirectory à restaurer. *fichier_configuration* correspond au chemin absolu du fichier de configuration de l'instance d'eDirectory à restaurer. Par exemple : `--config-file /etc/opt/novell/eDirectory/conf/nds.conf` Ce paramètre s'applique uniquement aux environnements Linux.
`restadv`	Options de restauration avancées. **REMARQUE :** l'agent DS est fermé pour toutes les options de restauration avancées.
`-l` *`nom_fichier`*	(Obligatoire) Nom et chemin d'accès du fichier journal Indique le fichier journal dans lequel consigner les résultats de la restauration.
`-o`	(Facultatif) Ouvrir la base de données à la fin de l'opération Ce paramètre indique à l'outil de sauvegarde d'ouvrir la base de données une fois l'opération terminée. Si la vérification se déroule correctement, la base de données restaurée s'ouvre. Sinon, cette option entraîne l'ouverture de la base de données présente sur le serveur avant la restauration. Pour obtenir une vue d'ensemble du processus, reportez-vous à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.
`-n`	(Facultatif) Tenter de vérifier une restauration qui a précédemment échoué Tente de vérifier une base de données RST restaurée précédemment.
`-m`	(Facultatif) Supprimer les fichiers DIB restaurés Supprime la base de données RST éventuellement présente.
`-v`	(Facultatif) Remplacer la restauration Renomme la base de données RST en base de données NDS sans tenter de vérification. **IMPORTANT :** nous vous recommandons de ne pas utiliser cette option à moins d'y être invité par le support technique de NetIQ.
`-k`	(Facultatif) Supprimer le verrouillage de la base de données Supprime le verrouillage de la base de données NDS.
`-i`	Liste de fichiers incrémentiels classés dans l'ordre et séparés par des virgules. **IMPORTANT :** cette option ne s'applique qu'à DSBK.
`getconfig`	Récupère la configuration actuelle des journaux de transactions individuelles.

Option et paramètres	Description

	Aucune option n'est nécessaire.
	
	Affiche la configuration actuelle. Par exemple, sur un serveur pour lequel la consignation de transactions individuelles par fichier est désactivée, la commande `getconfig` renvoie des informations semblables aux suivantes :
	
	`  Roll forward log status OFF`
	`Stream file logging status OFF`
	`Current roll forward log directory C:\rfl\nds.rfl`
	`Minimum roll forward log size (bytes) 104857600`
	`Maximum roll forward log size (bytes) 4294705152`
	`Last roll forward log not used 00000000.log`
	`Current roll forward log 00000001.log`
	`*** END ***`

`setconfig`	Définit la configuration des fichiers journaux de transactions individuelles.
`-L`	(Facultatif) Début de l'enregistrement des fichiers journaux de transactions individuelles. Active la consignation de transactions individuelles par fichier (désactivée par défaut). La consignation continue de transactions individuelles par fichier vous permet de rendre à un serveur l'état qu'il avait avant son arrêt, plutôt que celui de la dernière sauvegarde complète ou incrémentielle. Vous devez activer cette fonction pour les serveurs qui font partie d'un anneau de répliques afin de pouvoir rendre à un serveur l'état de synchronisation attendu par les autres serveurs. L'administrateur doit intervenir une fois que la consignation de transactions individuelles par fichier a été activée. Si vous ne les surveillez pas, les fichiers journaux de transactions individuelles s'étendent jusqu'au point de saturer le volume/la partition de disque. Si ces journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Il est donc nécessaire de sauvegarder et de supprimer périodiquement les fichiers journaux inutilisés. Reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462. Pour plus d'informations, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.
`-l`	(Facultatif) Arrêt de l'enregistrement des fichiers journaux de transactions individuelles Désactive la consignation de transactions individuelles par fichier (désactivée par défaut). La base de données réutilise le fichier journal de transaction individuelle actuel, au lieu d'enregistrer un ensemble de fichiers journaux consécutifs. Si la consignation de transactions individuelles par fichier est désactivée, vous ne pouvez restaurer eDirectory qu'au point de la dernière sauvegarde complète ou incrémentielle. Si elle a été désactivée par mégarde, vous devez la réactiver puis effectuer une nouvelle sauvegarde de la base de données pour être en mesure d'effectuer une restauration complète. Pour plus d'informations, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

Option et paramètres	Description
`-T`	(Facultatif) Début du chargement des fichiers de flux (Ne s'applique que si la fonction de consignation de transactions individuelles par fichier est activée.) Si un fichier de flux est modifié, il est intégralement copié dans le fichier journal de transaction individuelle. Les fichiers de flux sont des fichiers d'informations supplémentaires liés à la base de données. Les scripts de connexion en sont un exemple. Les fichiers journaux de transactions individuelles occupent l'espace disque plus rapidement lorsque les fichiers de flux sont consignés. Veillez, par conséquent, à contrôler l'espace libre sur le volume/la partition de disque où sont stockés les fichiers journaux de transactions individuelles. Si ces journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné.
`-t`	(Facultatif) Arrêt de l'enregistrement des fichiers de flux Arrête la copie du fichier de flux entier dans le fichier journal de transaction individuelle en cas de modification. Si la consignation des fichiers de flux est désactivée, vous pouvez utiliser les options de sauvegarde pour enregistrer ces fichiers lors des sauvegardes complètes et incrémentielles. Cette solution peut être suffisante si vos fichiers de flux ne changent pas fréquemment. Si vous désactivez la consignation des fichiers de flux, la taille des fichiers journaux de transactions individuelles augmentera moins rapidement.
`-r` *`nom_rép`*	(Facultatif) Définition du répertoire du fichier journal de transaction individuelle Modifie le répertoire où sont stockés les fichiers journaux de transactions individuelles. Par exemple, si la commande utilisée est `setconfig -r vol2:\rfl`, un répertoire est créé sous `vol2:\rfl` et les fichiers journaux de transaction individuelle y sont enregistrés. Le nom de ce répertoire est défini en fonction du nom de la base de données eDirectory actuelle. Pour les installations standard, il s'agit de « NDS ». Le nom du répertoire résultant est donc `vol2:\rfl\nds.rfl\`. Si vous renommez la base de données eDirectory NDS en ND1, le répertoire des fichiers journaux de transaction individuelle devient `vol2:\rfl\nd1.rfl\`. Vous pouvez trouver l'emplacement actuel des journaux en entrant la commande `getconfig`. Le répertoire est créé immédiatement après le changement d'emplacement, mais aucun fichier journal de transaction individuelle n'est créé tant qu'aucune transaction n'a lieu dans la base de données. **IMPORTANT :** l'outil de sauvegarde ne permet pas de suivre les modifications apportées au répertoire des fichiers journaux de transaction individuelle. Lorsque vous restaurez la base de données, vous devez collecter tous les fichiers journaux de transactions individuelles sur le serveur, dans un même répertoire. Pour plus d'informations, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

Option et paramètres	Description
`-n`	(Facultatif) Définition de la taille minimale du fichier journal de transaction individuelle Définit la taille minimale des fichiers journaux de transactions individuelles (en octets). Lorsque la taille minimale est atteinte, la base de données commence un nouveau fichier journal de transaction individuelle dès que la transaction en cours est terminée.
`-m` *`taille_fichier`*	(Facultatif) Définition de la taille maximale du fichier journal de transaction individuelle Définit la taille maximale des fichiers journaux de transactions individuelles (en octets). Si cette limite est atteinte et qu'une transaction est en cours, cette dernière se poursuit dans le fichier suivant. Cette valeur doit toujours être supérieure à la taille minimale.
`-s`	(Facultatif) Création d'un nouveau fichier journal de transaction individuelle Lance un nouveau fichier journal de transaction individuelle à la fin de la transaction en cours. Le nouveau fichier est créé au début de la transaction suivante.
`cancel`	Annule toute opération de sauvegarde ou de restauration en cours. Aucune option n'est nécessaire. **REMARQUE :** cette option ne s'applique pas à DSBK.
`--config-file` *`fichier_configuration`*	(Facultatif) Permet de spécifier l'instance d'eDirectory pour laquelle vous souhaitez définir la configuration des fichiers journaux de transaction individuelle. *fichier_configuration* correspond au chemin absolu du fichier de configuration de l'instance eDirectory pour laquelle vous souhaitez définir la configuration des fichiers journaux de transaction individuelle. Par exemple : `--config-file /etc/opt/novell/eDirectory/conf/nds.conf` Ce paramètre s'applique uniquement aux environnements Linux.

Exécution de DSBK en tant que tâche cron

Le script `dsbk` ne contient pas le chemin complet du fichier binaire DSTrace. Par conséquent, si vous exécutez le script en tant que tâche cron en utilisant les paramètres par défaut, le script échoue. Toutefois, ne modifiez pas le script `/opt/novell/eDirectory/bin/dsbk` pour ajouter le chemin d'accès, car les correctifs d'eDirectory qui seront appliqués par la suite écraseront ce fichier et annuleront toutes les modifications apportées au script.

Avant d'exécuter dsbk comme une tâche cron, définissez plutôt la variable d'environnement `PATH` du fichier `crontab` de manière à inclure le répertoire dans lequel se trouve `ndstrace`. La tâche cron peut alors localiser et exécuter l'application `ndstrace`.

Sauvegarde et restauration de NICI

L'infrastructure cryptographique internationale de Novell (NICI) stocke des clés et des données utilisateur dans le système de fichiers et dans les répertoires et fichiers spécifiques au système et à l'utilisateur. Pour protéger ces fichiers et répertoires, ils sont associés aux autorisations adéquates à

l'aide du mécanisme fourni par le système d'exploitation. Cette opération est effectuée par le programme d'installation de NICI. La sauvegarde et la restauration de NICI sont prises en charge uniquement pour les utilisateurs root, et non pour les utilisateurs non-root.

Désinstaller NICI du système ne supprime pas les fichiers et répertoires utilisateur ou système. Par conséquent, la seule raison justifiant la restauration de ces fichiers à un état antérieur est la récupération après une panne système catastrophique ou une erreur humaine. Il importe de comprendre que le fait d'écraser un ensemble existant de fichiers et de répertoires utilisateur NICI risque d'interrompre une application existante.

La clé de base de données nécessaire à l'ouverture du fichier DIB est encapsulée avec des clés NICI. Par conséquent, si la sauvegarde d'eDirectory est effectuée indépendamment de la sauvegarde NICI, elle n'est d'aucune utilité. La solution de sauvegarde d'eDirectory (DSBK et outil de sauvegarde eMBox) inclut un paramètre (`e -`) qui permet d'effectuer les opérations suivantes :

1. Sauvegarde des clés NICI lors de l'exécution d'une sauvegarde d'eDirectory
2. Restauration des clés NICI lors de l'exécution d'une restauration eDirectory

Pour plus d'informations sur la solution de sauvegarde d'eDirectory, reportez-vous à la « Utilisation de DSBK » page 466.

Sauvegarde de NICI

NICI peut être sauvegardé dans le cadre d'une sauvegarde complète ou incrémentielle d'eDirectory.

La commande permettant de sauvegarder NICI est la suivante :

```
dsbk backup -f nom_fichier -l nom_fichier_journal -e mot_de_passe
```

`-f` et `-l` sont des options obligatoires qui doivent être utilisées avec la commande de sauvegarde.

`-e` est le paramètre qui permet de sauvegarder les fichiers NICI.

`nom_fichier` correspond au nom et à l'emplacement du fichier de sauvegarde que l'outil de sauvegarde doit créer.

`nom_fichier_journal` correspond au nom et à l'emplacement du fichier journal créé pour consigner les résultats de l'opération de sauvegarde.

`mot_de_passe` correspond au mot de passe utilisé pour la sauvegarde de NICI. Le mot de passe peut être spécifié en texte clair. Sous Linux, le mot de passe peut également être transmis sous forme de fichier. Ce même mot de passe doit être spécifié pour restaurer les fichiers NICI.

REMARQUE : si un mot de passe de sauvegarde NICI n'est pas spécifié avec le paramètre `-e`, les messages d'erreur suivants s'affichent :

Dans DSBK :

```
Enter password along with the (-e) option!
DSBK error! 4
```

Restauration de NICI

1. Restaurez uniquement les fichiers NICI (pas la DIB).

   ```
   dsbk restore -f nom_fichier -l nom_fichier_journal -e mot_de_passe
   ```

`-f` et `-l` sont des options obligatoires qui doivent être utilisées avec la commande de restauration.

`-e` est le paramètre qui permet de restaurer les fichiers NICI.

`nom_fichier` correspond au nom et à l'emplacement du fichier de sauvegarde qui contient les informations à restaurer.`nom_fichier_journal` correspond au nom et à l'emplacement du fichier journal créé pour consigner les résultats de l'opération de restauration.`mot_de_passe` correspond au mot de passe qui a été utilisé lorsque les fichiers NICI ont été sauvegardés. Si vous spécifiez un mot de passe erroné alors que vous tentez de restaurer les fichiers NICI, un message d'erreur s'affiche.

2 Redémarrez le serveur ndsd.

3 Restaurez la DIB.

```
dsbk restore -f nom_fichier -l nom_fichier_journal -a -r -o
```

`-f` et `-l` sont des options obligatoires qui doivent être utilisées avec la commande de restauration.

`-a` active la DIB après la vérification, `-r` restaure l'ensemble DIB et `-o` ouvre la base de données une fois l'opération de restauration terminée.

Si vous avez sauvegardé NICI au cours d'une sauvegarde complète et d'une sauvegarde incrémentielle et si vous avez utilisé des mots de passe différents lors de ces sauvegardes, vous devez spécifier le mot de passe utilisé lors de la sauvegarde complète pour restaurer les fichiers NICI.

REMARQUE : si un mot de passe n'est pas spécifié avec le paramètre `-e`, les messages d'erreur suivants s'affichent :

Dans DSBK :

```
Enter password along with the (-e) option!
DSBK error! 4
```

Si un mot de passe erroné est spécifié lors de la restauration de l'infrastructure NICI, le message d'erreur suivant s'affiche :

```
NICI RESTORE: "NICI Files has not been restored(Check your parameters)" Error!: -32
```

Récupération de la base de données en cas d'échec de la vérification de la restauration

Le processus de restauration comprend une étape de vérification qui consiste à comparer la base de données eDirectory sur le serveur en cours de restauration et celles des autres serveurs de l'anneau de répliques, par rapprochement des vecteurs de transition. Pour plus d'informations sur le processus de restauration, reportez-vous aux sections « Présentation du processus de restauration avec l'outil de restauration » page 450 et « Vecteurs de transition et processus de vérification de la restauration » page 458.

Si les vecteurs de transition ne correspondent pas, la vérification échoue. Il faut généralement en déduire qu'il manque des données dans les fichiers utilisés pour la restauration. Les raisons peuvent être les suivantes, par exemple :

- Vous n'avez pas activé la consignation de transactions individuelles par fichier avant d'effectuer la dernière sauvegarde.

- Vous n'avez pas introduit les journaux de transactions individuelles dans l'opération de restauration.
- Le jeu de fichiers journaux de transactions individuelles fourni pour la restauration est incomplet.

Par défaut, la base de données eDirectory restaurée ne s'ouvre pas à l'issue de la restauration si elle est incohérente par rapport aux autres répliques.

Si vous possédez tous les fichiers de sauvegarde et tous les fichiers journaux de transactions individuelles nécessaires à une restauration complète, mais avez oublié de les fournir pendant le processus, vous pouvez vous contenter d'exécuter de nouveau la restauration avec l'ensemble complet de fichiers. Si la restauration est complète lors du second essai, la vérification réussit et la base de données restaurée s'ouvre.

Si vous ne possédez pas tous les fichiers de sauvegarde et fichiers journaux de transactions individuelles nécessaires pour effectuer une restauration complète et garantir la réussite de la vérification, vous devez suivre les instructions de cette section pour restaurer le serveur. Voici un récapitulatif des éléments récupérables en cas d'échec de la vérification :

- Vous pouvez toujours récupérer l'identité du serveur et les droits d'accès au système de fichiers.
- Vous ne pouvez pas récupérer les répliques qui figuraient sur le serveur à partir de la sauvegarde, mais vous pouvez utiliser ce dernier pour ces répliques après avoir exécuté la procédure de récupération présentée ici. Vous devez enlever le serveur de l'anneau de répliques et utiliser les options de restauration avancées ainsi que l'outil DSRepair pour remettre le serveur dans un état qui permette sa réintégration dans l'anneau de répliques. Vous pouvez ensuite réinstaller les répliques de votre choix.
- Néanmoins, si le serveur détenait l'unique copie d'une partition de la base de données (absence d'autres répliques), celle-ci ne peut pas être récupérée.

En cas d'échec de la vérification, suivez les instructions contenues dans cette section pour récupérer l'identité du serveur ainsi que les droits d'accès au système de fichiers, et pour enlever le serveur de l'anneau de répliques et l'y réintégrer. Une fois cette procédure exécutée et la réplication terminée, le serveur devrait fonctionner comme avant la défaillance (exception faite des partitions qui n'ont pas été répliquées et ne peuvent donc pas être récupérées).

Reportez-vous d'abord à la section « Nettoyage de l'anneau de répliques » page 486. Consultez ensuite la section « Réparation du serveur défaillant et réinstallation des répliques » page 488.

Nettoyage de l'anneau de répliques

Cette procédure vous explique comment effectuer les tâches suivantes :,

- **Réassigner des répliques maîtresses.** Si le serveur défaillant contient la réplique maîtresse d'une partition, utilisez DSRepair pour désigner une nouvelle réplique maîtresse sur un autre serveur de la liste des répliques.
- **Supprimer de la liste de répliques les références au serveur défaillant.** Tous les serveurs faisant partie de l'anneau de répliques qui incluait le serveur défaillant doivent être informés de l'indisponibilité de ce dernier.

Conditions préalables

- ❒ eDirectory est installé sur la machine sur laquelle vous tentez de restaurer le serveur défaillant.
- ❒ Une restauration a été tentée, mais la vérification a échoué.

- ❒ La base de données eDirectory est ouverte et opérationnelle, et la base de données RST se trouve toujours sur la machine (elle y a été laissée par le processus de restauration).
- ❒ Vous savez quelles partitions répliquées ont été stockées sur le serveur défaillant. Les répliques que contenait le serveur sont listées dans l'en-tête du fichier de sauvegarde.

Procédure

Pour nettoyer l'anneau de répliques :

1. Depuis la console de l'un des serveurs qui partageaient une réplique avec le serveur défaillant, chargez DSRepair avec le paramètre permettant d'accéder aux options avancées.
   - **Windows :** utilisez le paramètre `-a`.
   - **Linux :** utilisez le paramètre `-Ad`.

   Pour plus d'informations sur l'exécution de DSRepair avec le paramètre d'options avancées `-a` ou `-Ad`, reportez-vous à la « Options DSRepair » page 356.

   AVERTISSEMENT : si vous utilisez DSRepair avec le paramètre `-a` ou `-Ad`, certaines des options avancées peuvent endommager votre arborescence.

   ---

2. Sélectionnez **Opérations de partition et de réplique**.
3. Sélectionnez la partition à modifier, afin de pouvoir enlever le serveur défaillant de l'anneau de répliques pour cette partition.
4. Sélectionnez **Afficher l'anneau de répliques** pour afficher la liste des serveurs disposant de répliques de la partition.
5. (Conditionnel) Si le serveur défaillant contenait la réplique maîtresse, choisissez un autre serveur pour cette réplique en sélectionnant l'option **Désigner ce serveur en tant que nouvelle réplique maîtresse**.

   L'anneau de répliques comporte désormais une nouvelle réplique maîtresse. Toutes les répliques faisant partie de l'anneau sont informées de son existence.
6. Patientez pendant la mise en place de la réplique maîtresse. Avant de poursuivre, vérifiez que les autres serveurs de l'anneau ont bien enregistré le changement.
7. Revenez à l'écran **Afficher l'anneau de répliques**. Sélectionnez le nom du serveur défaillant, puis l'option **Supprimer ce serveur de l'anneau de répliques**.

   Si vous n'avez pas chargé DSRepair avec le paramètre `-a` ou `-Ad` (selon la plate-forme) pour accéder aux options avancées, cette option ne figure pas dans la liste.

   AVERTISSEMENT : veillez à ne pas effectuer cette opération si le serveur défaillant est désigné comme réplique maîtresse. Cette information est indiquée dans la liste des serveurs de l'anneau. S'il s'agit de la réplique maîtresse, désignez un autre serveur en tant que maître, comme expliqué à l'Étape 5. Revenez ensuite à cette étape et retirez le serveur défaillant de l'anneau de répliques.

   ---

8. Connectez-vous en tant qu'utilisateur Admin.
9. Après avoir lu le message d'explication, indiquez que vous souhaitez poursuivre.
10. Quittez DSRepair.

    Tous les serveurs qui font partie de l'anneau de répliques sont notifiés.
11. Répétez cette procédure sur un serveur pour chaque anneau de répliques dont le serveur défaillant faisait partie.

Pour terminer la préparation du serveur défaillant en vue de charger de nouvelles copies des répliques, consultez la procédure de la section suivante « Réparation du serveur défaillant et réinstallation des répliques » page 488.

Réparation du serveur défaillant et réinstallation des répliques

Cette procédure vous permet de changer en références externes les informations relatives aux répliques qui figurent sur le serveur, de sorte que celui-ci ne se considère plus comme faisant partie de l'anneau de répliques. Une fois que vous avez appliqué cette méthode pour enlever les répliques du serveur, vous pouvez déverrouiller la base de données.

Après avoir retiré les répliques, vous terminez la procédure en les réinstallant sur le serveur. Celui-ci reçoit ainsi une nouvelle copie actualisée de chaque réplique. Après la réinstallation de chaque réplique, le serveur doit fonctionner de la même façon qu'avant la défaillance.

Pour retirer les répliques à l'aide de DSRepair, puis les réinstaller à l'aide de la fonction de réplication :

1. Assurez-vous que vous avez terminé la procédure décrite à la section « Nettoyage de l'anneau de répliques » page 486.
2. Utilisez l'option de restauration avancée permettant de remplacer la restauration et précisez un nom de fichier journal :

   ```
   dsbk restadv -v -l nom_fichier_journal
   ```

   Cette option de restauration avancée renomme la base de données RST (la base de données qui a été restaurée, mais dont la vérification a échoué) en NDS, mais la laisse verrouillée.
3. Depuis la console du serveur, changez en références externes toutes les informations relatives aux répliques figurant sur le serveur, à l'aide des options avancées de DSRepair.
   - **Windows :** Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**. Sélectionnez **dsrepair.dlm**. Dans le champ Paramètres de démarrage, saisissez `-XK2 -rd`. Cliquez sur **Démarrer**.
   - **Linux :** Saisissez la commande suivante :

     ```
     ndsrepair -R -Ad -xk2
     ```

   Le paramètre `-rd` ou `R` permet de réparer la base de données locale et la réplique.

   AVERTISSEMENT : l'utilisation incorrecte des options avancées de DSREPAIR risque d'endommager votre arborescence.

   ---
4. Lorsque la réparation est terminée, supprimez le verrouillage et ouvrez la base de données à l'aide des options de restauration avancées suivantes du client eMBox :

   ```
   dsbk restadv -o -k -l logfilename
   ```

   Le paramètre `-o` permet d'ouvrir la base de données et le paramètre `-k` de supprimer le verrouillage.
5. Utilisez iManager pour réintroduire le serveur dans l'anneau de répliques :

   5a Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .

   5b Cliquez sur **Gestion des partitions et des répliques** > **Affichage des répliques**.

   5c Spécifiez le nom et le contexte de la partition à répliquer, puis cliquez sur **OK**.

5d Cliquez sur **Ajouter une réplique**.

5e En regard du champ **Nom du serveur**, cliquez sur le bouton Parcourir , puis sélectionnez le serveur que vous venez de restaurer.

5f Sélectionnez le type de réplique souhaité, cliquez sur **OK**, puis sur **Terminé**.

5g Répétez cette procédure pour chaque anneau de répliques dont le serveur faisait partie.

6 Attendez la fin du processus de réplication.

Le processus de réplication est terminé lorsque les répliques passent de l'état Nouveau à Actif. Vous pouvez vérifier l'état dans iManager. Pour plus d'informations, reportez-vous à la section « Affichage des informations concernant une réplique » page 163.

7 Pour restaurer les fichiers de sécurité NICI, commencez par restaurer uniquement les fichiers NICI, puis redémarrez le serveur NDSD et restaurez la DIB.

8 (Conditionnel) Si vous souhaitez utiliser la consignation de transactions individuelles par fichier sur le serveur, vous devez recréer votre configuration afin de vous assurer que cette fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

Scénarios de sauvegarde et de restauration

- « Scénario : perte d'un disque dur contenant eDirectory dans un réseau monoserveur » page 489
- « Scénario : perte d'un disque dur contenant eDirectory dans un environnement multiserveur » page 491
- « Scénario : perte d'un serveur complet dans un environnement multiserveur » page 493
- « Scénario : perte de plusieurs serveurs dans un environnement multiserveur » page 494
- « Scénario : perte de tous les serveurs dans un environnement multiserveur » page 494

Scénario : perte d'un disque dur contenant eDirectory dans un réseau monoserveur

Ingrid est l'administrateur d'un réseau monoserveur chez Stationery Supply, Inc. Elle ne peut pas recourir à la réplication pour la tolérance aux pannes, car son environnement ne comporte qu'un seul serveur. L'outil de sauvegarde constitue un moyen simple et efficace pour sauvegarder et restaurer eDirectory. Il s'agit d'une solution rapide, basée sur le serveur.

Sous eDirectory 8.7.3 ou une version ultérieure, Ingrid configure des sauvegardes sans surveillance pour son serveur, en utilisant des fichiers de traitement par lots pour exécuter l'outil de sauvegarde.

Ingrid souhaite effectuer une sauvegarde complète d'eDirectory chaque dimanche soir, et une sauvegarde incrémentielle chaque nuit, en semaine. Elle configure les sauvegardes sans surveillance pour qu'elles s'exécutent chaque nuit, peu avant ses sauvegardes complètes et incrémentielles du système de fichiers. Ainsi, les sauvegardes sur bande contiennent les fichiers de sauvegarde d'eDirectory en même temps que ceux du système de fichiers. Elle a passé un contrat avec une société de stockage de données à distance afin d'envoyer les sauvegardes sur bande hors site.

Tous les lundis matin, Indira vérifie le journal de sauvegarde pour s'assurer que la sauvegarde complète a abouti. Pendant la semaine, elle contrôle occasionnellement les fichiers journaux pour vérifier que les sauvegardes incrémentielles ont abouti.

Ingrid décide de ne pas activer les fichiers journaux de transactions individuelles pour les raisons suivantes :

- Comme elle ne possède pas de périphérique de stockage distinct sur son serveur, l'activation des fichiers journaux de transactions individuelles ne lui permet pas d'effectuer des sauvegardes supplémentaires d'eDirectory. Une défaillance du périphérique de stockage entraînerait la perte des fichiers journaux en même temps que celle d'eDirectory. La création de ces derniers ne présente donc aucun intérêt.
- L'arborescence ne change pas énormément. Ingrid se contente de pouvoir la restaurer dans l'état qu'elle avait au moment de la sauvegarde de la dernière nuit. Elle n'a pas besoin de pouvoir restaurer eDirectory dans l'état où il se trouvait avant la défaillance.
- Étant donné que le serveur ne fait pas partie d'un anneau de répliques comprenant d'autres serveurs, les fichiers journaux de transactions individuelles ne sont pas nécessaires à la réussite du processus de vérification de la restauration.

Stationery Supply, Inc. décide de réorganiser les ressources humaines. Ingrid fait donc une sauvegarde manuelle avant d'apporter des changements importants à l'arborescence et après les avoir appliqués. Sa stratégie consiste à faire une nouvelle sauvegarde des changements un jour de la semaine, lorsque cela s'avérera nécessaire, au lieu d'exécuter en permanence des fichiers journaux de transactions individuelles.

Pour s'assurer que sa stratégie de sauvegarde sera prête à fonctionner lorsqu'elle en aura besoin, Ingrid la teste de temps à autre. Comme elle ne dispose pas du budget nécessaire pour acquérir un second serveur afin d'effectuer les tests, elle passe un accord avec un laboratoire de test local. Sur un serveur du laboratoire comparable au sien, elle installe son système d'exploitation et son système de fichiers pour obtenir un environnement proche de celui de sa base de données eDirectory. Elle restaure ses sauvegardes et vérifie que la restauration d'eDirectory correspond à ses attentes.

Un mercredi matin, le disque dur qui contient eDirectory sur le serveur tombe en panne. Ingrid se procure un nouveau disque dur et réunit les fichiers de la sauvegarde complète du dimanche soir, de la sauvegarde incrémentielle du lundi soir et de celle du mardi soir. Elle met en place le nouveau disque dur et installe eDirectory sur ce dernier. Elle restaure ensuite les sauvegardes complète et incrémentielles. Les modifications apportées à l'arborescence le mercredi matin, avant la défaillance du disque dur, sont perdues puisque Ingrid n'effectuait pas de consignation de transactions individuelles par fichier sur le serveur. Toutefois, Ingrid se contente de pouvoir restaurer l'arborescence dans l'état où elle se trouvait lors de la sauvegarde de la nuit dernière. Elle estime qu'exécuter des fichiers journaux de transaction individuelle ne serait pas avantageux compte tenu de la surcharge administrative qui y est associée.

Scénario : perte d'un disque dur contenant eDirectory dans un environnement multiserveur

Chez Outdoor Recreation, Inc., Georges dispose de dix serveurs qui exécutent eDirectory. Il effectue des sauvegardes complètes chaque dimanche soir et des sauvegardes incrémentielles toutes les nuits. La sauvegarde d'eDirectory a lieu peu avant la sauvegarde sur bande du système de fichiers.

Tous les serveurs font partie d'un anneau de répliques. Georges utilise la consignation de transactions individuelles par fichier sur chacun d'eux. Pour chaque serveur, il a placé les fichiers journaux de transactions individuelles sur un périphérique de stockage différent de celui d'eDirectory. Il surveille l'espace disponible afin de s'assurer que les fichiers journaux de transaction individuelle ne le saturent pas. Il contrôle en outre les droits sur le périphérique de stockage. De temps à autre, il sauvegarde sur bande les fichiers journaux de transactions individuelles, puis les supprime tous, à l'exception de celui utilisé par eDirectory, afin de libérer de l'espace.

Pour Georges, la surcharge administrative liée à la mise en oeuvre de la consignation continue des transactions individuelles par fichier est compensée par le fait qu'il dispose d'une sauvegarde jusqu'à la dernière minute, ce qui est nécessaire pour des serveurs faisant partie d'un anneau de répliques. S'il doit restaurer un serveur, celui-ci se retrouve dans l'état de synchronisation qu'attendent les autres serveurs de l'anneau de répliques.

Dans son laboratoire de test, Georges teste périodiquement les fichiers de sauvegarde pour s'assurer que sa stratégie de sauvegarde répond à ses objectifs.

Un jeudi à 14 heures, le serveur Linux Stocks_DB1 subit une défaillance de disque dur, sur l'unité qui contient eDirectory.

Georges doit se procurer la dernière sauvegarde complète et les sauvegardes incrémentielles effectuées depuis celle-ci. Il peut ainsi restaurer la base de données dans l'état où elle se trouvait avant la sauvegarde incrémentielle réalisée la nuit précédente à une heure du matin. Les fichiers journaux de transaction individuelle ayant enregistré les modifications apportées à la base depuis la sauvegarde de la dernière nuit, Georges les introduit dans la restauration. Il peut ainsi restaurer la base dans l'état où elle se trouvait juste avant la défaillance du disque dur.

Georges procède de la façon suivante :

1. Il se procure un disque dur de rechange pour le serveur.
2. Il récupère la bande de la sauvegarde complète du serveur, effectuée le dimanche soir précédent.

   Le fichier de traitement par lots qu'il utilise pour effectuer des sauvegardes complètes chaque dimanche soir place le fichier de sauvegarde dans `/adminfiles/backup/backupfull.bk`.

   Comme il avait spécifié une taille limite de 200 Mo dans les paramètres de configuration de la sauvegarde, il y a deux fichiers de sauvegarde :

   `backupfull.bk.00001` (250 Mo)
   `backupfull.bk.00002` (32 Mo)
3. Il se procure également les bandes qui contiennent les sauvegardes incrémentielles de lundi, mardi et mercredi soir.

   Le fichier de traitement par lots qu'il utilise pour effectuer des sauvegardes incrémentielles tous les soirs de la semaine place le fichier de sauvegarde dans `/adminfiles/backup/backupincr.bk`.

Étant donné qu'il exécute le même fichier de traitement par lots chaque soir de la semaine pour les sauvegardes incrémentielles d'eDirectory, celles-ci ont toutes le même nom de fichier. Il doit leur assigner un nouveau nom lorsqu'il les recopie sur le serveur car elles doivent toutes être placées dans le même répertoire pendant la restauration.

4. Georges installe le disque dur de remplacement.

   Comme le système d'exploitation du serveur n'était pas sur le disque dur défaillant, il n'a pas besoin d'installer Linux.

5. Georges restaure le système de fichiers depuis la sauvegarde sur bande, pour les deux partitions de disque affectées.
6. Il réinstalle eDirectory et place le serveur dans une nouvelle arborescence temporaire (le processus de restauration le replace dans l'arborescence d'origine par la suite).
7. Georges crée un répertoire `/adminfiles/restore` sur le serveur, pour y stocker les fichiers à restaurer.
8. Il copie les deux fichiers de sauvegarde complète dans ce répertoire.
9. Ensuite, il y copie les sauvegardes incrémentielles de lundi, mardi et mercredi.

   Comme elles se nomment toutes `backupincr.bk`, lorsqu'il les copie dans le répertoire, il les renomme comme suit :

   ```
   backupincr.mon.bk
   backupincr.tues.bk
   backupincr.wed.bk
   ```

   REMARQUE : les sauvegardes complètes et incrémentielles ne doivent pas toutes se trouver dans le même répertoire. En revanche, toutes les sauvegardes incrémentielles doivent être placées dans le même répertoire.

10. Il utilise iManager pour restaurer eDirectory :
    a. Il ouvre iManager et clique sur **Maintenance** > **Restaurer**.
    b. Il se connecte au serveur, en utilisant le contexte de la nouvelle arborescence temporaire.
    c. Dans l'écran Assistant de restauration - Configuration du fichier, il effectue les opérations suivantes :

       Il spécifie `/adminfiles/restore` comme emplacement des fichiers de sauvegarde.

       Il spécifie `/adminfiles/restore/restore.log` comme emplacement du journal de restauration.

    d. Dans l'écran Assistant de restauration - Facultatif, il effectue les opérations suivantes :

       Il sélectionne l'option **Restaurer la base de données**.

       Il sélectionne aussi l'option **Restaurer les fichiers journaux de transaction individuelle**.

       Il entre l'emplacement des fichiers journaux de transactions individuelles.

       (Il s'agit de l'emplacement distinct qu'il a créé spécifiquement pour stocker les fichiers journaux de transactions individuelles. Comme il les a placés sur un disque dur différent de celui d'eDirectory, la panne qui s'est produite ne les a pas affectés et ils sont toujours disponibles.)

       Il sélectionne l'option **Restaurer les fichiers de sécurité**.

       Il sélectionne l'option **Activer la base de données restaurée après vérification**.

       Il sélectionne l'option **Ouvrir la base de données après restauration**.

       Il souhaite que eDirectory s'ouvre si la vérification de la restauration réussit.

11. Il lance la restauration et entre les noms des fichiers de sauvegarde incrémentielle lorsqu'il y est invité.
12. La vérification de la restauration réussit, de sorte que la base de données s'ouvre avec l'arborescence originale.

    Elle a réussi parce que les fichiers journaux de transactions individuelles étaient en service sur le serveur lors de la défaillance du disque dur, et que Georges les a inclus dans la restauration.
13. Une fois la restauration terminée, Georges recrée la configuration des fichiers journaux de transactions individuelles sur le serveur. Il effectue ensuite une nouvelle sauvegarde complète.

    Comme les paramètres reprennent leur valeur par défaut durant une restauration, la consignation de transactions individuelles par fichier est désactivée. Il doit la réactiver. Il doit, en outre, effectuer une nouvelle sauvegarde complète afin de se prémunir contre toute défaillance survenant avant la prochaine sauvegarde complète sans surveillance.

Georges vérifie le fonctionnement du serveur. Celui-ci semble être normal.

Scénario : perte d'un serveur complet dans un environnement multiserveur

Bob est l'administrateur de 15 serveurs chez GK Designs Company. Il effectue des sauvegardes complètes chaque samedi soir et des sauvegardes incrémentielles toutes les nuits. La sauvegarde d'eDirectory a lieu peu avant la sauvegarde sur bande du système de fichiers.

Tous les serveurs font partie d'un anneau de répliques. Bob utilise la consignation de transactions individuelles par fichier sur chacun d'eux.

Un incendie d'origine électrique détruit l'un des serveurs d'une succursale située de l'autre côté de la ville. Heureusement, toutes les partitions de ce serveur, sauf une, sont répliquées sur d'autres serveurs. Bob avait activé les fichiers journaux de transaction individuelle sur ce serveur, mais ils ont été perdus avec toutes les autres données. Il ne peut donc pas restaurer la base de données eDirectory du serveur dans l'état où elle se trouvait juste avant que le serveur ne tombe en panne.

En revanche, il peut recréer l'identité eDirectory du serveur en le restaurant à partir des fichiers de sauvegarde existants. Étant donné que Bob ne peut pas inclure les fichiers journaux de transaction individuelle dans la restauration, le serveur ne correspond pas à l'état de synchronisation attendu par les autres serveurs (reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration » page 458). Par conséquent, le processus de vérification de la restauration échoue. Cela signifie que, par défaut, la base de données eDirectory n'est pas ouverte après la restauration.

Pour résoudre ce problème, Bob supprime le serveur de l'anneau de répliques en utilisant DSRepair pour changer en références externes toutes les informations obsolètes relatives aux répliques qui figurent sur le serveur. Ensuite, il ajoute au serveur une nouvelle copie de chaque partition en effectuant une réplication à partir des autres serveurs contenant les répliques à jour. Ces opérations sont décrites à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

La seule partition du serveur que Bob n'avait pas répliquée était un conteneur dans lequel figuraient des objets Impression en réseau de la succursale, tels qu'un fax/imprimante et une imprimante couleur grand format. Les informations de cette partition ne peuvent pas être récupérées à l'aide de la méthode décrite ci-dessus, puisque aucun autre serveur ne dispose d'une réplique. Bob doit donc recréer les objets de la partition. Cette fois, il choisit de les répliquer sur d'autres serveurs pour assurer, à l'avenir, une meilleure tolérance aux pannes.

Bob recrée également la configuration des fichiers journaux de transactions individuelles après la remise en ligne du serveur (car la restauration désactive la fonction de consignation et rétablit les paramètres par défaut), puis il crée une nouvelle sauvegarde complète qui servira de point de départ.

Scénario : perte de plusieurs serveurs dans un environnement multiserveur

Julien administre 20 serveurs sur trois sites. Sur l'un de ces sites, la rupture d'une canalisation d'eau détruit cinq des huit serveurs.

Julien dispose de sauvegardes d'eDirectory pour tous les serveurs. Toutefois, ceux-ci font partie d'un anneau de répliques. Le problème est de les réinstaller dans l'arborescence sans fichiers journaux de transaction individuelle, puisque ces derniers ont aussi été perdus. Il ne sait pas sur quels serveurs il doit restaurer eDirectory d'abord, ni comment gérer les incohérences entre les répliques. En raison de la complexité de ces problèmes, il appelle le support de NetIQ afin d'être conseillé sur le choix de la méthode de restauration.

Scénario : perte de tous les serveurs dans un environnement multiserveur

Dolorès et son équipe de Human Resources Consulting, Inc. gèrent 50 serveurs sur un site.

Pour assurer la tolérance aux pannes dans les conditions normales d'exploitation, ils ont créé trois répliques de chaque partition de leur arborescence. Si un serveur est arrêté, les objets des partitions qu'il contient restent ainsi disponibles sur d'autres serveurs. Ils ont également pris les dispositions nécessaires pour pouvoir récupérer des serveurs individuels, en sauvegardant régulièrement tous leurs serveurs à l'aide de l'outil de sauvegarde, en activant la consignation de transactions individuelles par fichier et en stockant les bandes de sauvegarde sur un site distant.

Dans le cadre d'un plan de reprise après sinistre, Dolorès et son équipe ont également désigné deux de leurs serveurs comme serveurs DSMASTER. Deux serveurs sont nécessaires en raison de la taille de l'arborescence. Un seul serveur DSMASTER ne suffit pas à accueillir les répliques de toutes les partitions. Chaque partition de l'arborescence est répliquée sur l'un des deux serveurs DSMASTER. Les deux serveurs DSMASTER ne contiennent aucune réplique de la même partition, de sorte qu'il n'y a pas de chevauchement entre eux. Il s'agit là d'un aspect important du plan de reprise en cas de sinistre.

Dans leur laboratoire de test, Dolorès et son équipe testent périodiquement les sauvegardes afin de s'assurer que la stratégie de sauvegarde répond à leurs objectifs.

Une nuit, le bâtiment abritant Human Resources Consulting, Inc. est endommagé par un ouragan, et tous les serveurs de l'infocentre sont détruits.

À la suite de ce sinistre, Dolorès et son équipe commencent par restaurer les deux serveurs DSMASTER, qui contiennent les répliques de toutes les partitions. Ils utilisent la dernière sauvegarde complète et les sauvegardes incrémentielles consécutives, mais ils ne peuvent pas inclure les fichiers journaux de transaction individuelle dans la restauration car ils ont été perdus lors de la destruction des serveurs. Dolorès et son équipe ont configuré les serveurs DSMASTER afin qu'ils ne partagent pas de répliques. De ce fait, le processus de vérification de la restauration réussit sur les deux serveurs, même si les fichiers journaux de transactions individuelles ne sont pas inclus dans la restauration. Une fois les deux serveurs DSMASTER restaurés, tous les objets de l'arborescence de Human Resources Consulting, Inc. sont à nouveau disponibles.

Les serveurs DSMASTER sont importants car Dolorès et son équipe peuvent les utiliser pour recréer une arborescence sans incohérences à la suite d'un sinistre.

Ils utilisaient des journaux de transactions individuelles afin de pouvoir restaurer un serveur dans l'état où il se trouvait avant son arrêt et de rétablir l'état de synchronisation attendu par les autres serveurs de l'anneau de répliques. Le serveur peut ainsi reprendre les communications là où elles ont été interrompues, et recevoir des autres répliques les mises à jour requises afin que l'ensemble de l'anneau soit synchronisé.

Dans le cas du présent sinistre, cependant, Dolorès et son équipe ne disposent pas des fichiers journaux de transactions individuelles. Sans ces derniers, seul un serveur peut être restauré sans erreurs dans un anneau de répliques, à savoir le premier. Pour les autres serveurs, la vérification de la restauration échoue parce que les états de synchronisation ne correspondent pas à ce qu'attendent les autres serveurs (reportez-vous à la section « Vecteurs de transition et processus de vérification de la restauration » page 458). Si la vérification de la restauration échoue, le processus de restauration n'active pas la base de données eDirectory restaurée.

Dolorès et son équipe ont prévu cette situation et se sont organisés en conséquence. Ils utilisent comme point de départ les deux serveurs DSMASTER et ne disposent donc que d'une réplique de chaque partition. Il est possible de restaurer ces serveurs sans erreurs, et les répliques qu'ils contiennent peuvent servir de répliques maîtresses qui seront copiées sur tous les autres serveurs.

Après la restauration des serveurs DSMASTER, la restauration des autres serveurs nécessite quelques opérations supplémentaires. Dolorès et son équipe doivent restaurer chacun des serveurs restants en procédant comme suit :

- Ils vérifient que les répliques placées sur les serveurs DSMASTER sont désignées comme répliques maîtresses.
- Ils suppriment tous les serveurs de l'anneau de répliques, à l'exception des serveurs DSMASTER.
- Ils restaurent les sauvegardes complètes et incrémentielles pour chacun des autres serveurs.

  Dolorès et son équipe savent que le processus de vérification de la restauration va échouer pour le reste des serveurs parce qu'ils n'ont pas pu utiliser les fichiers journaux de transactions individuelles durant leur restauration. Ils obtiennent donc une base de données restaurée mais non activée.
- Ils activent la base de données restaurée, à l'aide des options de restauration avancées, mais ils la maintiennent verrouillée.
- Ils utilisent DSREPAIR pour modifier en références externes toutes les informations sur les répliques.
- Ils déverrouillent la base de données restaurée.

  À ce stade, le serveur a la même identité qu'auparavant, mais il ne tente pas de synchroniser les informations de réplique. Il est toutefois prêt à recevoir une nouvelle copie des répliques qu'il contenait précédemment.
- Ils réinstallent les répliques sur chacun des serveurs en les dupliquant à partir de la copie qui figure sur le serveur DSMASTER.

  Dolorès et son équipe savent assez précisément quelles répliques étaient détenues par chaque serveur, mais ils peuvent consulter l'en-tête des fichiers de sauvegarde de chacun d'eux pour voir la liste des répliques qu'ils contenaient au moment de la dernière sauvegarde.
- Ils recréent la configuration des journaux de transactions individuelles après la remise en ligne des serveurs (puisque la restauration désactive la fonction de consignation et rétablit les valeurs par défaut des paramètres), puis effectuent une nouvelle sauvegarde complète qui servira de base pour faire face aux défaillances susceptibles de survenir avant la prochaine sauvegarde complète sans surveillance.

(Ces étapes sont décrites plus en détail à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.)

Dolorès et son équipe ont beaucoup de travail en vue, mais ils peuvent remettre l'arborescence en service assez rapidement et peuvent s'attendre à récupérer l'identité eDirectory de tous leurs serveurs.

Utilisation de DSBK dans un plan de reprise après sinistre

Un plan de reprise après sinistre vous permet de restaurer votre disque dans l'état où il se trouvait juste avant qu'il ne soit altéré. Pour ce faire, vous devez sauvegarder le disque de votre serveur à un emplacement distant, afin que vous puissiez le restaurer même si le système d'exploitation est endommagé.

Cette section fournit un exemple de plan de reprise après sinistre pour un serveur eDirectory :

- « Plan de reprise après sinistre sous Linux » page 496
- « Plan de reprise après sinistre sous Windows » page 497

Plan de reprise après sinistre sous Linux

Pour effectuer une sauvegarde du disque du serveur :

1. Configurez DSBK :
   - **1a** Créez un fichier `dsbk.conf` dans `/etc`.
   - **1b** Créez un fichier temporaire. Par exemple, `/tmp/dsbk.tmp`.
   - **1c** Indiquez l'emplacement du fichier temporaire créé à l'étape précédente dans le fichier `/etc/dsbk.conf`.
2. Montez le disque du serveur sur une machine distante en mode lecture/écriture, afin de stocker tous les fichiers de sauvegarde sur un disque de machine distante.

   Par exemple, `eDirServer# mount <adresse_IP_machine_distante>:/home/backup/ /mnt/dsbkBkp`
3. Définissez l'emplacement pour la sauvegarde personnalisée à l'aide de la commande suivante :

   ```
   dsbk setconfig -L -T -r /mnt/dsbkBkp
   ```

   REMARQUE : veillez à exécuter DSBK à partir de l'emplacement suivant sur le serveur : `/opt/novell/eDirectory/bin`.
4. Effectuez une sauvegarde complète, y compris de NICI, et stockez-la sur le système de fichiers distant :

   ```
   dsbk backup -f <backup file location> -l <log file location> -e <password for NICI backup> -t -b
   ```

   Par exemple, `dsbk backup -f /mnt/dsbkBkp/fb1.bak -l /mnt/dsbkBkp/fb1.log -e novell -t -b`.

   REMARQUE : l'option `-e` permet de sauvegarder NICI. Dans l'exemple, `novell` est le mot de passe utilisé pour la sauvegarde de NICI. Vous pouvez choisir un autre mot de passe, mais n'oubliez pas que vous devez utiliser le même mot de passe lors de la restauration de NICI.
5. Effectuez des sauvegardes incrémentielles à l'aide de la commande suivante :

```
dsbk backup -f <incremental backup file location> -l <incremental log file
location> -t -i
```

Par exemple :

Jour 1: `dsbk backup -f /mnt/dsbkBkp/ib1.bak -l /mnt/dsbkBkp/ib1.log -t -i`

Jour 2: `dsbk backup -f /mnt/dsbkBkp/ib2.bak -l /mnt/dsbkBkp/ib2.log -t -i`

REMARQUE : lorsque vous effectuez une sauvegarde incrémentielle, vous n'êtes pas obligé de sauvegarder NICI.

Si le serveur eDirectory est endommagé, effectuez la procédure ci-dessous pour le restaurer à l'aide de la sauvegarde distante :

1. Si le système d'exploitation est endommagé, réinstallez-le.
2. Si seul eDirectory est endommagé, nettoyez le système en supprimant les RPM eDirectory.
3. Installez eDirectory comme auparavant et configurez une arborescence à serveur unique factice. Par exemple,

   ```
   ndsconfig new -t dummy_bkp_tree -n novell -a admin.novell -w novell
   ```

4. Restaurez NICI à partir du fichier de sauvegarde complète (sans les options `-d`, `- r`, `- a` et `o -`) :

   ```
   dsbk restore -f <emplacement_fichier_sauvegarde> -l
   <emplacement_fichier_journal> -e <mot_de_passe_sauvegarde_NICI>
   ```

   Par exemple, `dsbk restore -f /mnt/dsbkBkp/fb1.bak -l /mnt/dsbkBkp/restore1.log -e novell`

5. Une fois NICI restauré, redémarrez le serveur eDirectory.
6. Restaurez les fichiers de sauvegarde complète et incrémentielle. Par exemple,

   ```
   dsbk restore -f /mnt/dsbkBkp/fb1.bak -l /mnt/dsbkBkp/restore2.log -d /mnt/
   dsbkBkp/nds.rfl/ -r -a -e novell -o -i /mnt/dsbkBkp/ib1.bak, /mnt/dsbkBkp/
   ib2.bak
   ```

Pour plus d'informations sur les commandes de sauvegarde et de restauration, reportez-vous à la section « Utilisation de DSBK sous Linux » page 467.

Plan de reprise après sinistre sous Windows

Pour effectuer une sauvegarde du disque du serveur :

1. Assignez le disque du serveur à une machine distante en mode lecture/écriture. Par exemple, `O:\dsbkBkp`
2. Pour exécuter la commande DSBK :
   - **2a** Ouvrez la console du serveur eDirectory en exécutant le fichier `NDScons.exe`.
   - **2b** Cliquez sur **dsbk.dlm** sous l'onglet **Services**.
   - **2c** Entrez les commandes DSBK dans le champ **Paramètres de démarrage**.
3. Définissez l'emplacement pour la sauvegarde personnalisée à l'aide de la commande suivante :

   ```
   setconfig -L -T -r O:\dsbkBkp
   ```

4. Effectuez une sauvegarde complète, y compris de NICI, et stockez-la sur le système de fichiers distant :

```
backup -f <emplacement_fichier_sauvegarde> -l <emplacement_fichier_journal> -e
<mot_de_passe_sauvegarde_NICI> -t -b
```

REMARQUE : l'option `-e` permet de sauvegarder NICI. Dans l'exemple, `novell` est le mot de passe utilisé pour la sauvegarde de NICI. Vous pouvez choisir un autre mot de passe, mais n'oubliez pas que vous devez utiliser le même mot de passe lors de la restauration de NICI.

5 Effectuez des sauvegardes incrémentielles à l'aide de la commande suivante :

```
backup -f <emplacement_fichier_sauvegarde_incrémentielle> -l
<emplacement_fichier_journal_sauvegarde incrémentielle> -t -i
```

Par exemple :

Jour 1: `backup -f O:\dsbkBkp\ib1.bak -l O:\dsbkBkp\ib1.log -t -i`

Jour 2: `backup -f O:\dsbkBkp\ib2.bak -l O:\dsbkBkp\ib2.log -t -i`

REMARQUE : lorsque vous effectuez une sauvegarde incrémentielle, vous n'êtes pas obligé de sauvegarder NICI.

Si le serveur eDirectory est endommagé, effectuez la procédure ci-dessous pour le restaurer à l'aide de la sauvegarde distante :

1 Si le système d'exploitation est endommagé, réinstallez-le.

2 Si seul eDirectory est endommagé, nettoyez le système en supprimant les composants eDirectory.

3 Installez eDirectory comme auparavant et configurez une arborescence à serveur unique factice.

4 Restaurez NICI à partir du fichier de sauvegarde complète (sans les options `-d`, `- r`, `- a` et `o -`) :

Par exemple :

```
restore -f <emplacement_fichier_sauvegarde> -l <emplacement_fichier_journal> -
e <mot_de_passe_sauvegarde_NICI>
```

Par exemple, `restore -f O:\dsbkBkp\fb1.bak -l O:\dsbkBkp restore1.log -e novell`

5 Une fois NICI restauré, redémarrez le serveur eDirectory.

6 Restaurez les fichiers de sauvegarde complète et incrémentielle.

Par exemple :

```
restore -f O:\dsbkBkp\fb1.bak -l O:\dsbkBkp\restore2.log -d O:\dsbkBkp\nds.rfl\
-r -a -e novell -o -i O:\dsbkBkp\ib1.bak, O:\dsbkBkp\ib2.bak
```

Pour plus d'informations sur les commandes de sauvegarde et de restauration, reportez-vous à la section « Utilisation de DSBK sous Windows » page 469.

Sauvegarde LDAP

La fonction de sauvegarde LDAP permet de sauvegarder les attributs et valeurs d'attributs pour un objet à la fois.

Le tableau suivant liste les plates-formes prenant en charge cette fonction :

Fonction	Linux	Windows
Sauvegarde LDAP	✓	✓

Cette fonction permet d'effectuer une sauvegarde incrémentielle dans laquelle l'objet n'est sauvegardé que s'il est modifié.

Elle comprend une série d'interfaces pour la sauvegarde et la restauration d'objets eDirectory exposés via LDAP Libraries for C, via des opérations étendues LDAP.

Pour plus d'informations sur le SDK LDAP Libraries for C, reportez-vous à la documentation concernant LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

Pour savoir comment effectuer la sauvegarde et la restauration d'objets eDirectory via LDAP, consultez l'exemple de code backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

Avantage de la sauvegarde LDAP

La sauvegarde LDAP tente de résoudre les problèmes liés à la sauvegarde et restauration actuelles.

Les problèmes résolus par cette fonction sont les suivants :

- Intègre une interface cohérente permettant aux développeurs ou aux applications de sauvegarde tierces de sauvegarder eDirectory sur toutes les plates-formes prises en charge.
- Permet de sauvegarder les objets de manière incrémentielle.

Pour plus d'informations

Pour plus d'informations sur cette fonction, consultez les références suivantes :

- LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)
- Exemple de code : backup.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

Sauvegarde d'eDirectory avec SMS

La structure API Services de gestion de stockage (SMS) de Novell est utilisée par les applications de sauvegarde pour proposer une solution complète de sauvegarde. La structure SMS est implémentée par deux composants principaux :

- Requêteur de données de gestion de stockage (SMDR)
- Agent de service cible (TSA)

L'Agent de service cible (TSA) pour les services eDirectory (`tsands`) cible et fournit une implémentation de l'API Services de gestion de stockage (SMS) de Novell pour les arborescences de répertoires. Les applications peuvent être écrites sur l'`API SMS` pour fournir une solution de sauvegarde complète.

Le TSA pour NDS est pris en charge sous Linux.

16 Configuration d'eDirectory en mode SuiteB

SuiteB est un ensemble d'algorithmes de chiffrement normalisés par la NSA (National Security Agency) pour permettre à des produits commerciaux de protéger le trafic classé secret ou top secret. Les algorithmes SuiteB permettent de sécuriser les informations classées secrètes et non confidentielles qui sont transmises par le biais de réseaux publics.

REMARQUE : la norme SuiteB est sujette à modification. Notez que la NSA peut modifier ses recommandations à l'avenir. La prise en charge de SuiteB dans eDirectory est basée sur notre interprétation des recommandations de la NSA.

SuiteB inclut les algorithmes de chiffrement suivants :

- Chiffrement basé sur la norme AES (Advanced Encryption Standard) à l'aide de clés de 128 ou 256 bits
- Signatures numériques avec l'algorithme de signature ECDSA (Elliptic Curve Digital Signature Algorithm) sur les courbes P-256 et P-384
- Échange de clés pré-partagées ou dynamiques à l'aide de la méthode ECDH (Elliptic Curve Diffie-Hellman) sur les courbes P-256 et P-384
- Hachage (empreinte numérique) sur la base de l'algorithme Secure Hash Algorithm-2 (SHA-256 et SHA-384)

Pour plus d'informations sur SuiteB, reportez-vous à la section relative à la technologie de chiffrement SuiteB sur le site Web de la NSA.

eDirectory permet de configurer séparément les modules suivants en mode SuiteB :

Module	Description
NPKI (NetIQ Certificate Server)	Certificate Server propose des services de cryptographie à clé publique intégrés nativement dans eDirectory, qui permettent de créer, d'émettre et de gérer des certificats utilisateur et de serveur. Ces services permettent de protéger les transmissions de données confidentielles sur des canaux de communication publics tels qu'Internet. Lorsqu'il est configuré en mode SuiteB, Certificate Server respecte la convention RFC 5759 qui spécifie le profil de base pour les certificats et la liste de révocation de certificats SuiteB. Pour plus d'informations, reportez-vous à la « Activation de SuiteB dans Certificate Server » page 503.
Services LDAP et HTTP	Le service LDAP est une application serveur qui permet aux clients LDAP d'accéder aux informations stockées dans eDirectory. eDirectory fournit des fonctionnalités multi plate-formes de surveillance et de diagnostic pour tous les serveurs de votre arborescence eDirectory qui utilisent le service HTTP. Lorsqu'ils sont configurés en mode SuiteB, ces services prennent en charge les certificats ECDSA et appliquent l'utilisation des Ciphers TLS 1.2 et SuiteB, comme spécifié dans le fichier RFC 6460. Pour plus d'informations, reportez-vous à la « Configuration des services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB » page 504.

Module	Description
NICI	NICI est un module cryptographique qui fournit des clés, des algorithmes, différents mécanismes de stockage et d'utilisation de clés, ainsi qu'un système de gestion des clés à grande échelle. Pour aider les applications à stocker et à transférer des données et des clés en toute sécurité, NICI fournit trois types de clés, à savoir une clé de stockage de clé, une clé SDI (Security Domain Infrastructure) NICI et une clé de session. Lorsqu'un serveur est configuré en mode SuiteB, NICI sécurise les données sensibles de l'arborescence (par exemple, les mots de passe et les données des réponses de stimulations) en utilisant les clés AES 256 bits . En cas de mise à niveau vers NICI 3.0, les clés de stockage de clé et de session sont automatiquement recréées pour respecter les exigences de SuiteB. eDirectory utilise la clé SDI NICI, également appelée clé d'arborescence, pour chiffrer les clés qui chiffrent les données stockées localement ou à distance qui permettent aux serveurs de l'arborescence de décoder la clé. Les données restent sécurisées conjointement avec les droits eDirectory. La clé d'arborescence est disponible pour tous les serveurs de l'arborescence. Pour accéder aux mêmes données, les différents serveurs utilisent la même clé SDI NICI. C'est la raison pour laquelle cette clé n'est pas créée automatiquement lors de l'installation de NICI 3.0. Cette clé doit être créée manuellement. Pour plus d'informations, reportez-vous à la « Création d'une clé SDI AES 256 bits » page 507.
Mécanisme d'authentification en arrière-plan	NICI fournit un mécanisme d'authentification en arrière-plan basé sur les standards reposant sur TLS 1.2 pour l'authentification Single Sign-on avec eDirectory. Pour plus d'informations, reportez-vous à la « Activation de l'authentification en arrière-plan » page 507.

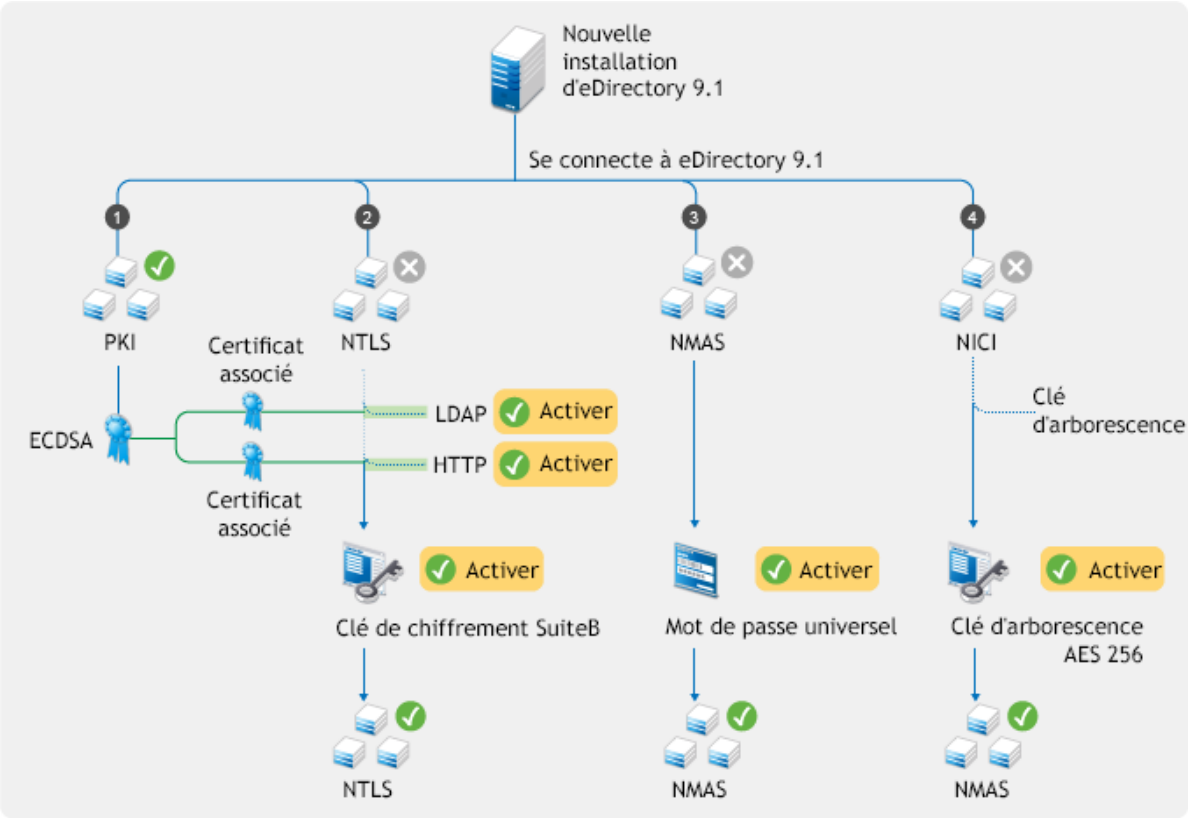
Les sections suivantes expliquent comment configurer les modules eDirectory en mode SuiteB :

- « Activation de SuiteB dans une nouvelle installation » page 502
- « Configuration de SuiteB sur des serveurs existants » page 507

Activation de SuiteB dans une nouvelle installation

La Figure 16-1 montre la série d'opérations à effectuer pour activer SuiteB sur les composants eDirectory dans le cadre d'une nouvelle installation.

Figure 16-1 *Activation de SuiteB dans une nouvelle installation*



Activation de SuiteB dans Certificate Server

Lorsque vous configurez une nouvelle arborescence, Certificate Server crée, en plus des certificats RSA traditionnels, un certificat ECDSA sur la courbe P-384 pour l'autorité de certification (CA) de l'arborescence. Si vous ajoutez de nouveaux serveurs à l'arborescence ou mettez à niveau d'anciens serveurs vers eDirectory 9.2, Certificate Server émet les certificats ECDSA pour ces serveurs.

REMARQUE : par défaut, NetIQ Certificate Server crée les certificats ECDSA sur la courbe P-384. Toutefois, vous pouvez également créer des certificats de serveur sur la courbe P-256.

Il est possible d'utiliser uniquement les certificats ECDSA sans activer SuiteB. L'activation de SuiteB est une étape supplémentaire pour respecter la convention RFC 5759.

Pour configurer le serveur de certificats de l'autorité de certification de manière à ce qu'il fonctionne en mode SuiteB, procédez comme suit :

1. Configurez l'authentification EBA (Enhanced Background Authentication) pour le serveur de certificats de l'autorité de certification.

   Pour plus d'informations, reportez-vous à la « Activation de l'authentification en arrière-plan » page 507.

2. Lancez iManager.
3. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

4 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ > Configurer l'autorité de certification**.

5 Sélectionnez **Activer le mode SuiteB**.

6 Cliquez sur **OK**.

Lorsque le serveur de certificats de l'autorité de certification est en mode SuiteB, l'autorité de certification ne vous autorise pas à créer des certificats RSA. En outre, la fonction d'auto-provisioning de serveur ne génère plus de certificats RSA. Si vous envisagez d'ajouter de nouveaux serveurs, assurez-vous qu'ils sont configurés pour exécuter l'authentification EBA.

Lorsque tous les serveurs de l'arborescence ou des services externes se connectant à l'arborescence commencent à utiliser les certificats de serveur ECDSA, vous pouvez révoquer et supprimer les certificats RSA, car ils ne sont plus nécessaires.

REMARQUE : la fonction d'algorithme de suivi de l'autorité de certification introduite dans eDirectory 8.8.8 Patch 6 n'est plus disponible à partir de la version 9.0 d'eDirectory. Au lieu de cette fonction, les serveurs eDirectory 9.2 utilisent par défaut l'algorithme SHA-256 pour les certificats RSA et SHA-384 pour les certificats ECDSA.

Configuration des services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB

NetIQ Transport Layer Security (NTLS) prend en charge les algorithmes de chiffrement TLS 1.2 et SuiteB via le module OpenSSL compatible FIPS. Ce module est utilisé par certains composants d'eDirectory, tels que le service LDAP, httpstk (iMonitor) et le moteur NCP. Pour plus d'informations, reportez-vous à la section Fonctionnement d'eDirectory en mode FIPS du *Guide d'installation de NetIQ eDirectory*.

Avant d'activer un mode SuiteB sur un serveur, assurez-vous que ce dernier de certificats ECDSA et de clients LDAP, et que les navigateurs LDAP et Web présents dans l'environnement eDirectory prennent en charge TLS 1.2, les certificats ECDSA et les Ciphers SuiteB. Pour configurer les interfaces LDAP et HTTPS en mode SuiteB, activez-les avec le mode SuiteB souhaité et associez-les à un certificat de serveur ECDSA approprié. Répétez cette procédure pour chaque serveur eDirectory de l'arborescence. Pour afficher le niveau de chiffrement et le certificat de serveur ECDSA d'un serveur, utilisez ses objets de configuration LDAP et httpstk, à savoir ldapServer et httpServer.

Pour configurer le serveur LDAP en mode SuiteB :

1 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

2 Dans le menu **Rôles et tâches**, cliquez sur **LDAP > Options LDAP > Afficher les serveurs LDAP**, puis sélectionnez l'objet Serveur LDAP que vous voulez configurer en mode SuiteB.

3 Cliquez sur **Connexions**.

4 Pour le paramètre **Certificat du serveur**, recherchez et cliquez sur le certificat à courbe elliptique que vous souhaitez utiliser avec l'objet Serveur LDAP.

5 Selon le mode SuiteB que vous voulez activer pour l'objet Serveur LDAP, sélectionnez une valeur dans la liste déroulante **Restrictions de liaison pour Cipher**.

Restrictions de liaison pour Cipher	Suite de chiffrement	Description
Utilisez un Cipher SuiteB (128 bits)	◆ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ◆ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Active un fonctionnement en mode SuiteB en utilisant un niveau de sécurité de 128 bits. Lorsque vous sélectionnez cette option, eDirectory autorise l'utilisation d'un niveau de sécurité de 128 bits et 192 bits par des homologues (tout client LDAP). Cette option permet d'utiliser des certificats ECDSA 256 ou ECDSA 384.
Utilisez un Cipher SuiteB (128 bits uniquement)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Active un fonctionnement en mode SuiteB en utilisant un niveau de sécurité de 128 bits. Lorsque vous sélectionnez cette option, eDirectory n'autorise pas l'utilisation du niveau de sécurité de 192 bits par des homologues (tout client LDAP). Tous les certificats d'une chaîne de certificats doivent utiliser des clés ECDSA sur la courbe P-256. Ceci est obligatoire pour les serveurs et applicable aux clients si la validation des certificats clients est activée.
Utilisez un Cipher SuiteB (192 bits)	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Active un fonctionnement en mode SuiteB en utilisant un niveau de sécurité de 192 bits. Lorsque vous sélectionnez cette option, eDirectory autorise uniquement l'utilisation du niveau de sécurité de 192 bits par des homologues (tout client LDAP). Tous les certificats d'une chaîne de certificats doivent utiliser des clés ECDSA sur la courbe P-384. Ceci est obligatoire pour les serveurs et applicable aux clients si la validation des certificats clients est activée.

eDirectory vous permet d'utiliser une combinaison de valeurs ldapbindrestrictions et de niveaux de chiffrement. Pour plus d'informations, reportez-vous au Tableau 14-1 page 406.

6 Cliquez sur **Appliquer**, puis sur **OK**.

7 Pour que les modifications soient appliquées, effectuez l'une des opérations suivantes :

- Redémarrez eDirectory.
- Déchargez et chargez le serveur LDAP.

Pour configurer l'interface HTTPS en mode SuiteB :

1 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

2 Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire > Modifier un objet**.

3 Sélectionnez l'objet Serveur HTTP à modifier, ou recherchez et cliquez sur l'objet Serveur HTTP que vous souhaitez afficher.

4 Cliquez sur **OK**.

5 Cliquez sur l'onglet **Autre**, puis sélectionnez httpBindRestrictions dans la liste **Attributs définis**.

6 Cliquez sur **Éditer**.

7 Selon le mode SuiteB que vous voulez activer pour l'objet Serveur HTTP, remplacez la valeur par 4, 5 ou 6 dans la boîte de dialogue qui s'affiche.

Restrictions de liaison pour Cipher	Suite de chiffrement	Description
4 - Utilisez un Cipher SuiteB (128 bits)	◆ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ◆ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Active un fonctionnement en mode SuiteB en utilisant un niveau de sécurité de 128 bits (Cipher SuiteB 128 bits). Lorsque vous sélectionnez cette option, eDirectory autorise l'utilisation d'un niveau de sécurité de 128 ou 192 bits par les clients (navigateurs Web). Cette option permet d'utiliser des certificats ECDSA 256 ou ECDSA 384.
5 - Utilisez un Cipher SuiteB (128 bits uniquement)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Active un fonctionnement en mode SuiteB en utilisant un niveau de sécurité de 128 bits (Cipher SuiteB 128 bits uniquement). Lorsque vous sélectionnez cette option, eDirectory n'autorise pas l'utilisation du niveau de sécurité de 192 bits par les clients (navigateurs Web). Tous les certificats d'une chaîne de certificats doivent utiliser des clés ECDSA sur la courbe P-256. Ceci est obligatoire pour les serveurs et applicable aux clients si la validation des certificats clients est activée.
6 - Utilisez un Cipher SuiteB (192 bits)	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Active un fonctionnement en mode SuiteB en utilisant un niveau de sécurité de 192 bits (Cipher SuiteB 192 bits). Lorsque vous sélectionnez cette option, eDirectory autorise uniquement l'utilisation d'un niveau de sécurité de 192 bits par les clients (navigateurs Web). Tous les certificats d'une chaîne de certificats doivent utiliser des clés ECDSA sur la courbe P-384. Ceci est obligatoire pour les serveurs et applicable aux clients si la validation des certificats clients est activée.

8 Cliquez sur **Appliquer.**

9 Sélectionnez httpKeyMaterialObject dans la liste **Attributs définis**, puis cliquez sur **Éditer**.

10 Recherchez et sélectionnez le certificat à courbe elliptique que vous souhaitez utiliser avec l'interface HTTPS, puis cliquez sur **OK**.

11 Cliquez sur **Appliquer**, puis sur **OK**.

12 Redémarrez eDirectory pour que les modifications soient appliquées.

Création d'une clé SDI AES 256 bits

Par défaut, la clé SDI NICI est une clé 3DES. Cependant, pour que les modes SuiteB soient pris en charge, vous devez créer manuellement la clé SDI NICI AES 256 bits. Ne créez cette clé que si tous les serveurs de l'arborescence exécutent eDirectory 9.0 ou une version ultérieure.

Lorsqu'un serveur contenant la réplique accessible en écriture du conteneur KAP.Security est mis à niveau vers eDirectory 9.2, la fonctionnalité de vérification de l'état de santé de la PKI crée un objet W1 dans ce conteneur. Lorsque tous les serveurs de l'arborescence sont mis à niveau vers eDirectory 9.2, l'administrateur de l'arborescence peut créer la clé SDI NICI AES 256 bits.

Pour créer la clé SDI NICI AES 256 bits, suivez les instructions de la section Creating an AES 256-Bit Tree Key (Création d'une clé d'arborescence AES 256 bits) du NICI Administration Guide (Guide d'administration de NICI).

Rechiffrement de données avec la clé SDI NICI AES 256 bits

NMAS utilise la clé SDI NICI pour stocker en toute sécurité les mots de passe et la configuration des questions/réponses de stimulations. NMAS dispose également d'un SecretStore pour la configuration spécifique de l'utilisateur et de la méthode qui utilise la clé SDI NICI. Pour rechiffrer les mots de passe de plusieurs utilisateurs dans le cadre de déploiements à grande échelle, utilisez l'utilitaire `diagpwd`. Pour plus d'informations, reportez-vous à la section « Utilitaire de diagnostic de mot de passe universel » page 817.

IMPORTANT : si votre environnement eDirectory intègre des serveurs utilisant des versions antérieures à eDirectory 9.0, ces serveurs ne peuvent pas déchiffrer les mots de passe ou les données secrètes chiffrés avec la clé d'arborescence AES 256 bits, ce qui entraîne l'échec de la connexion ces serveurs.

Activation de l'authentification en arrière-plan

eDirectory inclut un mécanisme d'authentification renforcée qui vérifie l'identité des utilisateurs qui tentent d'y accéder. Pour plus d'informations sur l'authentification EBA, reportez-vous au Chapitre 17, « Activation de l'authentification EBA (Enhanced Background Authentication) », page 509.

Configuration de SuiteB sur des serveurs existants

Pour activer SuiteB sur les serveurs présents dans votre arborescence eDirectory, procédez comme suit :

1. Mettez à niveau le serveur qui agit en tant qu'autorité de certification (CA) vers eDirectory 9.2.

   Lorsque le serveur d'autorité de certification est mis à niveau, il crée le certificat CA auto-signé ECDSA. Lorsque les autres serveurs sont mis à niveau vers eDirectory 9.2, la nouvelle autorité de certification émet des certificats ECDSA pour ces serveurs.

2. Mettez à niveau les serveurs de votre choix de l'arborescence vers eDirectory 9.2.

   Le processus de mise à niveau génère des certificats ECDSA pour les serveurs mis à niveau. Vous devez utiliser ces certificats pour activer les interfaces de pile de protocoles LDAP et HTTP en mode SuiteB. Pour plus d'informations, reportez-vous à la « Configuration des services LDAP et HTTP pour qu'ils utilisent les certificats ECDSA et les Ciphers SuiteB » page 504.

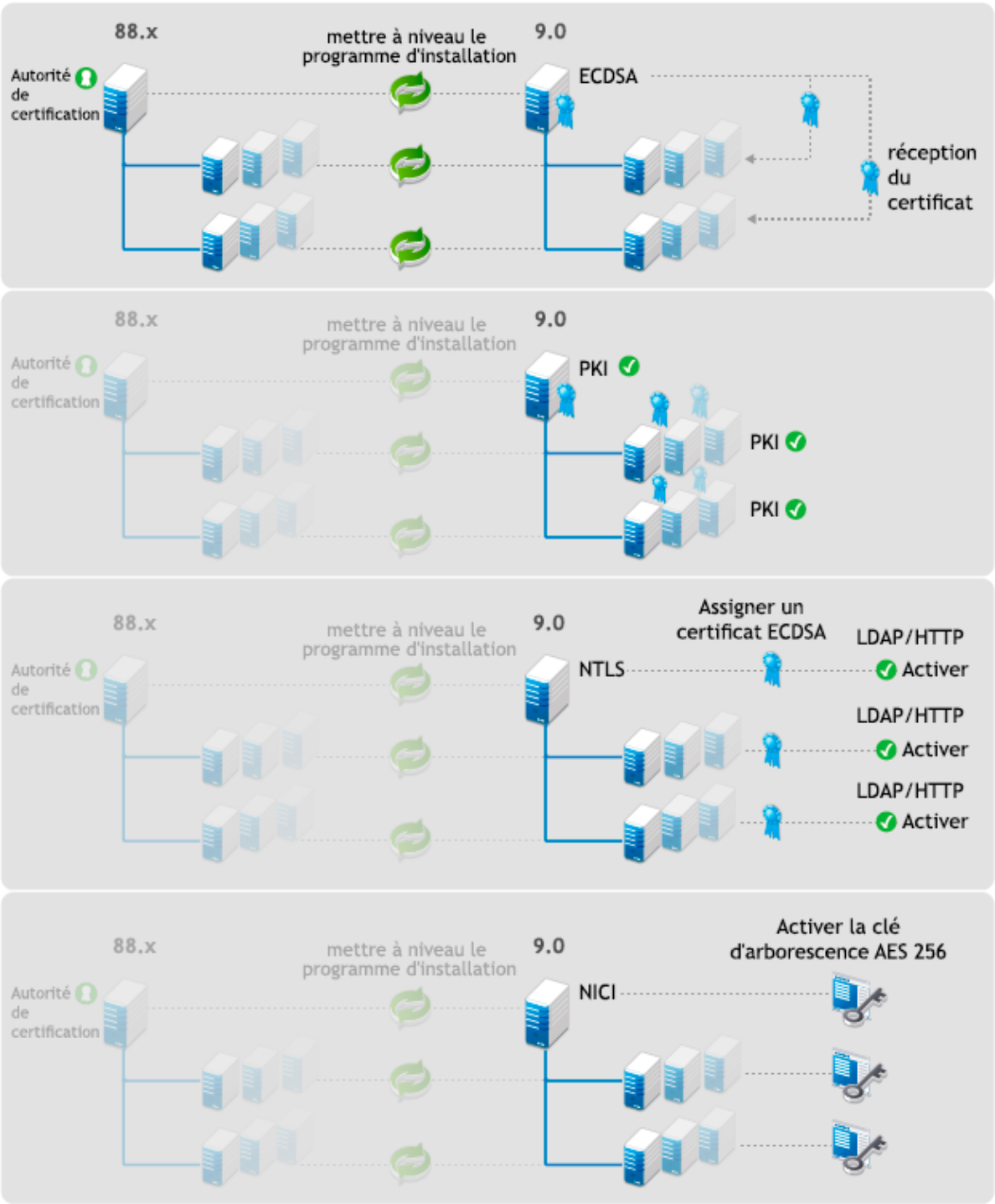
3. Créez une clé SDI AES 256 bits. Pour plus d'informations, reportez-vous à la « Création d'une clé SDI AES 256 bits » page 507.

4 Rechiffrez les données avec la clé SDI NICI AES 256 bits. Pour plus d'informations, reportez-vous à la « Création d'une clé SDI AES 256 bits » page 507.

5 Configurez l'authentification en arrière-plan. Pour plus d'informations, reportez-vous à la section « Activation de l'authentification EBA (Enhanced Background Authentication) » page 509.

La Figure 16-2 montre la série d'opérations à effectuer pour activer SuiteB lors de la mise à niveau d'eDirectory.

Figure 16-2 *Activation de SuiteB lorsqu'eDirectory est mis à niveau*



17 Activation de l'authentification EBA (Enhanced Background Authentication)

eDirectory inclut un mécanisme d'authentification renforcée qui vérifie l'identité des utilisateurs qui tentent d'y accéder. Le processus d'authentification comprend deux phases :

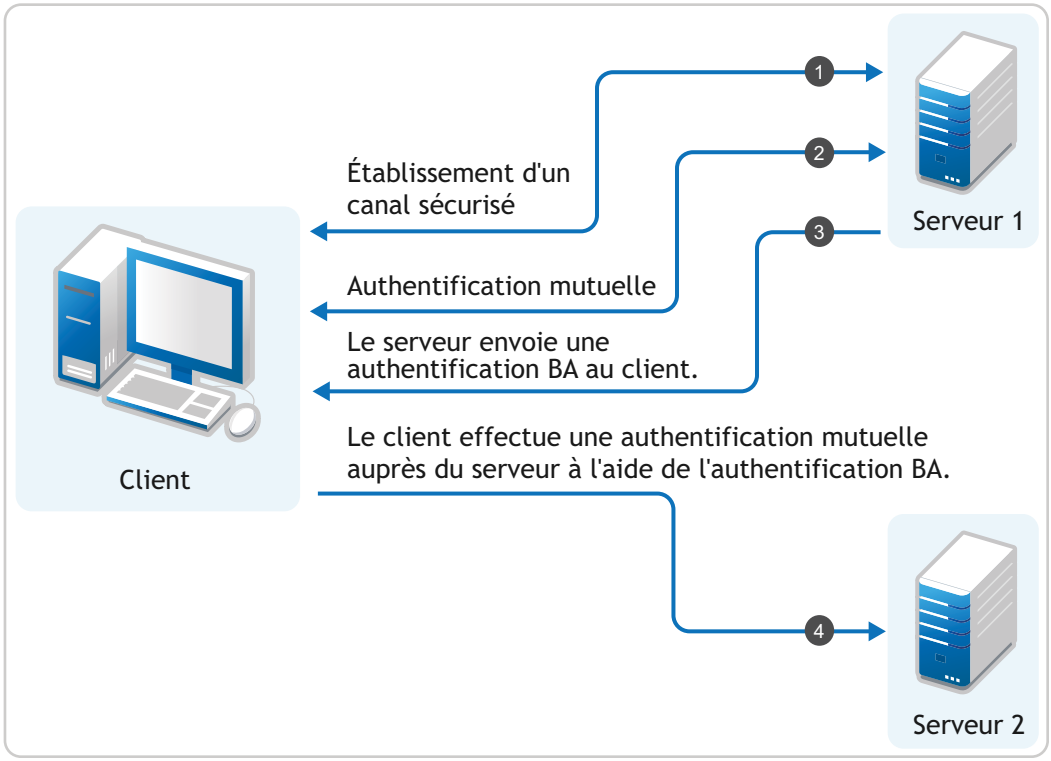
- Connexion
- Authentification en arrière-plan (BA)

Lorsqu'un utilisateur se connecte, NetIQ Modular Authentication Service (NMAS) vérifie ses références à long terme, telles que son mot de passe, et émet des données BA pour cet utilisateur.

Lorsqu'il s'authentifie auprès d'un autre serveur de l'arborescence, l'utilisateur utilise ces données BA. Cette fonction Single Sign-on d'eDirectory permet à l'utilisateur de s'authentifier auprès de n'importe quel serveur de l'arborescence sans devoir fournir à nouveau ses références à long terme.

eDirectory 9.0 introduit un protocole BA basé sur les standards, qui permet de surmonter les limites inhérentes au protocole BA propriétaire. Ce protocole se nomme EBA (Enhanced Background Authentication). Lorsqu'EBA est utilisé, NMAS émet pour les utilisateurs un certificat X.509 servant de données BA et le protocole BA utilise TLS 1.2 pour l'authentification mutuelle.

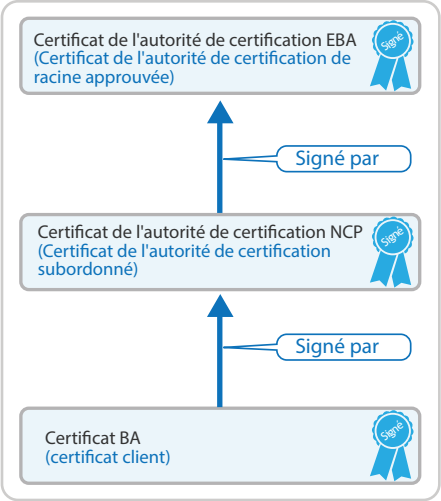
Figure 17-1 *Processus EBA*



Dans une arborescence eDirectory pour laquelle l'authentification EBA est activée, l'autorité de certification EBA est la CA racine approuvée pour EBA. L'autorité de certification EBA utilise un certificat auto-signé. Vous pouvez configurer comme autorité de certification EBA un des serveurs de

l'arborescence qui contiennent une réplique accessible en écriture de la partition root de l'arborescence. En règle générale, le premier serveur de l'arborescence qui héberge la réplique accessible en écriture de la partition root de l'arborescence et qui est configuré avec EBA fait office d'autorité de certification EBA. Vous pouvez également configurer un serveur eDirectory 9.2 qui héberge une réplique accessible en écriture de la partition racine de l'arborescence de manière à ce qu'il remplisse le rôle d'autorité de certification EBA.

Figure 17-2 *Autorité de certification EBA*



Chaque serveur de l'arborescence pour lequel l'authentification EBA est activée devient une autorité de certification subordonnée à la CA EBA et est appelé autorité de certification NCP. Une fois la connexion établie, NMAS renvoie un certificat BA émis par l'autorité de certification NCP pour l'utilisateur connecté.

REMARQUE : tout objet qui se connecte à eDirectory doit avoir un OID défini dans le schéma pour tous les attributs d'assignation de nom dans le DN de l'objet.

Pour utiliser EBA afin de s'authentifier auprès d'un serveur eDirectory, un client a besoin du certificat d'autorité de certification EBA de l'arborescence. Pour obtenir ce certificat, utilisez l'utilitaire ebaclientinit. Il s'agit d'un nouvel utilitaire de ligne de commande fourni avec eDirectory 9.0 et versions ultérieures. Cet utilitaire télécharge le certificat de l'autorité de certification EBA de l'arborescence et l'enregistre dans un fichier nommé `.eba.p12`. Ce fichier est stocké dans le répertoire privé de l'utilisateur sous Linux (`$HOME`) et dans le répertoire du profil utilisateur (`%USERPROFILE%`) sous Windows.

REMARQUE : pour que l'authentification EBA fonctionne correctement, synchronisez l'heure sur tous les clients et serveurs de votre environnement eDirectory pour lesquels EBA est activé.

Lorsque vous exécutez l'utilitaire ebaclientinit pour plusieurs arborescences, l'utilitaire ajoute les certificats d'autorité de certification EBA associés aux arborescences eDirectory dans le fichier `.eba.p12`. Pour obtenir les certificats d'autorité de certification EBA des arborescences eDirectory, exécutez l'utilitaire ebaclientinit pour chacune d'elles.

Activation de l'authentification EBA

Cette section explique comment activer l'authentification EBA sur eDirectory. Selon votre type d'installation, suivez les instructions d'une des sections suivantes :

- « Activation de l'authentification EBA sur une arborescence eDirectory » page 511
- « Activation de l'authentification EBA sur un serveur eDirectory » page 512
- « Désactivation de l'authentification EBA sur un serveur eDirectory » page 513

Activation de l'authentification EBA sur une arborescence eDirectory

- « Activation de l'authentification EBA sur une nouvelle arborescence eDirectory » page 511
- « Activation de l'authentification EBA sur une arborescence existante » page 511

Activation de l'authentification EBA sur une nouvelle arborescence eDirectory

Pour activer l'authentification EBA sur une nouvelle arborescence, suivez les instructions ci-dessous correspondant à votre plate-forme :

- **Linux :** pour activer l'authentification EBA lors de la configuration d'une nouvelle arborescence eDirectory, exécutez la commande `ndsconfig` avec l'argument `--configure-eba-now` dans la ligne de commande.

  Par exemple : `ndsconfig new --configure-eba-now` *`yes`*

  Si cet argument n'est pas transmis à la commande, vous êtes invité à activer l'authentification EBA. Selon vos préférences, entrez **yes** ou **no** lorsque vous y êtes invité.

- **Windows :** le programme d'installation offre la possibilité d'activer l'authentification EBA lors de la configuration d'eDirectory. Pour ce faire, sélectionnez l'option **Activer EBA** pendant le processus de configuration.

REMARQUE : eDirectory ne permet pas de configurer le démarrage automatique des modules `ebaext.dlm` et `ebassl_srv.dlm` sur un serveur pour lequel l'authentification EBA est activée, car le module DS les charge automatiquement lorsque vous activez l'authentification EBA sur un serveur eDirectory.

Si vous essayez de charger les modules `ebaext.dlm` et `ebassl_srv.dlm` sur un serveur pour lequel l'authentification EBA n'est pas activée, il se peut qu'ils soient chargés correctement mais que la fonction EBA ne fonctionne pas.

Activation de l'authentification EBA sur une arborescence existante

Pour activer l'authentification EBA sur une arborescence eDirectory existante, suivez les instructions ci-dessous correspondant à votre plate-forme :

- **Linux :** exécutez la commande `ndsconfig upgrade` avec l'argument `--configure-eba-now` sur l'un des serveurs qui hébergent une réplique accessible en écriture de la partition root de l'arborescence.

  Par exemple : `ndsconfig upgrade --configure-eba-now` *`yes`*

- **Windows :** exécutez le fichier `eDirectory_910_Windows_x86_64.exe` situé dans le dossier d'installation d'eDirectory 9.2 sur l'un des serveurs hébergeant une réplique accessible en écriture de la partition racine de l'arborescence et sélectionnez l'option **Activer EBA** pendant le processus de configuration d'eDirectory.

Activation de l'authentification EBA sur un serveur eDirectory

Lorsque vous activez l'authentification EBA sur un serveur eDirectory, une requête de signature de certificat (CSR) est envoyée à l'autorité de certification EBA. Cette dernière valide la CSR, effectue les vérifications de contrôle d'accès et émet le certificat d'autorité de certification NCP pour le serveur. Avant d'activer l'authentification EBA sur un serveur, vérifiez que :

- (Obligatoire) Une réplique accessible en écriture de la partition qui contient le DN de l'administrateur est présente sur le serveur de l'arborescence pour lequel l'authentification EBA est activée.
- (Facultatif) Une réplique accessible en écriture de la partition qui contient l'objet Serveur est présente sur un serveur de l'arborescence pour lequel l'authentification EBA est activée. Si le serveur ne remplit pas cette condition, l'autorité de certification EBA enregistre la CSR et n'émet pas le certificat d'autorité de certification NCP. Le cas échéant, la configuration d'eDirectory échoue et l'administrateur doit approuver la CSR à l'aide du plug-in EBA d'iManager. Pour plus d'informations, reportez-vous à la « Gestion de l'autorité de certification EBA à l'aide » page 515. Une fois la CSR approuvée, configurez l'authentification EBA en exécutant la commande `ndsconfig upgrade`. Par exemple : `ndsconfig upgrade --configure-eba-now yes`
- « Activation de l'authentification EBA lors de l'ajout d'un nouveau serveur » page 512
- « Activation de l'authentification EBA sur un serveur configuré » page 512

Activation de l'authentification EBA lors de l'ajout d'un nouveau serveur

Pour activer l'authentification EBA lorsqu'un nouveau serveur est ajouté à une arborescence, suivez les instructions ci-dessous correspondant à votre plate-forme :

- **Linux :** exécutez la commande `ndsconfig add` avec l'argument `--configure-eba-now yes`.

  Par exemple : `ndsconfig add --configure-eba-now yes`
- **Windows :** exécutez le fichier `eDirectory_910_Windows_x86_64.exe` situé dans le dossier d'installation d'eDirectory 9.2 et sélectionnez l'option **Activer EBA** pendant le processus de configuration d'eDirectory.

Activation de l'authentification EBA sur un serveur configuré

Pour activer l'authentification EBA sur un serveur configuré, suivez les instructions ci-dessous correspondant à votre plate-forme :

- **Linux :** exécutez la commande `ndsconfig upgrade` avec l'argument `--configure-eba-now yes`.

  Par exemple : `ndsconfig upgrade --configure-eba-now yes`
- **Windows :** exécutez le fichier `eDirectory_910_Windows_x86_64.exe` situé dans le dossier d'installation d'eDirectory 9.2 et sélectionnez l'option **Activer EBA** pendant le processus de configuration d'eDirectory.

IMPORTANT : NetIQ recommande de disposer, en plus du serveur servant d'autorité de certification EBA, d'au moins un autre serveur pour lequel l'authentification EBA est activée et qui héberge la réplique Lecture-écriture de la partition root de l'arborescence. En cas de défaillance du serveur faisant office d'autorité de certification EBA, l'autre serveur pour lequel l'authentification EBA est activée peut être configuré pour prendre le relais. Pour plus d'informations, reportez-vous à la « Déplacement du rôle d'autorité de certification EBA vers un nouveau serveur » page 518.

Désactivation de l'authentification EBA sur un serveur eDirectory

Pour désactiver l'authentification EBA sur un serveur configuré, suivez les instructions correspondant à votre plate-forme :

- **Linux:**
  - Exécutez les commandes suivantes pour redémarrer le serveur eDirectory avec l'authentification EBA désactivée :

    ```
    ndsmanage stopall
    export DISABLE_EBA=true
    ndsmanage startall
    ```

  - Exécutez les commandes suivantes pour redémarrer le serveur eDirectory avec l'authentification EBA activée :

    ```
    ndsmanage stopall
    unset DISABLE_EBA
    ndsmanage startall
    ```

  REMARQUE : vous devez ajouter toutes les variables d'environnement requises pour le service eDirectory dans le fichier `env` qui se trouve dans le répertoire `etc/opt/novell/eDirectory/conf` sur les plates-formes RHEL 7.x et SLES 12.x.

- **Windows :** accédez à **Panneau de configuration** > **Système** > **Paramètres système avancés** > **Variables d'environnement** > **Variables système** > **Nouvelle**. Ajoutez une nouvelle variable appelée `DISABLE_EBA` et la valeur 1, puis redémarrez le serveur.

IMPORTANT : ne désactivez EBA qu'à des fins de dépannage. Si l'authentification EBA est désactivée sur un serveur eDirectory faisant office d'autorité de certification EBA pendant 7 jours ou plus, la fonctionnalité EBA dans l'arborescence eDirectory sera interrompue. Pour plus d'informations, consultez le TID 7017232.

Affichage des informations relatives à l'authentification EBA

Le tableau ci-dessous répertorie les outils et utilitaires qui fournissent des informations à propos des différents aspects d'un serveur pour lequel l'authentification EBA est activée.

Utilitaire	Description
ndstrace	Fournit des informations sur les opérations EBA, telles que la gestion des requêtes EBA et l'émission des certificats d'autorité de certification NCP. Pour afficher ces informations : Sous Linux, activez la balise EBA de ndstrace. Sous Windows, chargez le module dstrace activé avec la balise EBA dans le fichier `NDSCons.exe`.
ndsd.log, dhost.log	Fournissent des informations à propos des messages de démarrage et d'arrêt d'EBA. Pour afficher ces informations : Sous Linux, consultez le fichier `ndsd.log` du serveur sur lequel vous avez configuré l'authentification EBA. Sous Windows, ces informations sont consignées dans le fichier `dhost.log`.
ndscheck	Indique l'état de l'authentification EBA sur un serveur, autrement dit si elle est activée sur ce serveur. Si l'authentification EBA est activée pour le serveur, le résultat de la commande indique la validité du certificat d'autorité de certification NCP, si le serveur fait office d'autorité de certification EBA, etc. Lorsque vous exécutez la commande `ndscheck` à distance, assurez-vous que le certificat d'autorité de certification EBA de l'arborescence a été téléchargé sur l'ordinateur local. Pour plus d'informations, reportez-vous à la « Exécution de l'utilitaire ebaclientinit » page 516.
ndslogin	Fournit des informations de dépannage à propos de la configuration de l'authentification EBA. Pour résoudre les problèmes de configuration de l'authentification EBA, connectez-vous à eDirectory à l'aide de la commande `ndslogin` avec l'argument -c. Par exemple : `ndslogin <DN_admin> –p <mot_de_passe> –c` Pour que la connexion réussisse, veillez à télécharger le certificat d'autorité de certification EBA de l'arborescence sur l'ordinateur local. Pour plus d'informations, reportez-vous à la « Exécution de l'utilitaire ebaclientinit » page 516.
schema.log	Le fichier `schema.log` du serveur sur lequel l'authentification EBA est configurée contient des informations à propos de l'extension du schéma pour EBA.
nioutput.log	Indique si l'authentification EBA a été sélectionnée lors de la configuration d'eDirectory.

Utilitaire	Description
iMonitor	iMonitor permet de surveiller les serveurs pour lesquels l'authentification EBA est activée, afin de : ◆ Déterminer si l'authentification EBA est activée pour un serveur est activé, en vérifiant le paramètre d'activation d'EBA sous l'onglet Infos sur la connexion de la page Configuration de l'agent. Si la valeur de ce paramètre est true, l'authentification EBA est activée pour le serveur. Dans le cas contraire, la valeur de ce paramètre est false. ◆ Afficher les mêmes informations de débogage que celles disponibles dans ndstrace sous Linux. La page de configuration de trace inclut une étiquette pour EBA qui permet d'afficher ces informations. ◆ Consulter des informations à propos de la validité du certificat d'autorité de certification EBA, du certificat d'autorité de certification NCP, et de l'état d'activation de l'authentification EBA pour le serveur sur la page État de santé de l'agent. Ces éléments apparaissent en vert si le certificat est valide et si les attributs EBA ne sont pas affectés. ◆ Consulter le verbe de requête EBA sur un serveur pour lequel l'authentification EBA est activée, sur la page Statistiques de verbe. ◆ Afficher la page Vérification de l'état de santé : Agent d'iMonitor, afin d'effectuer les opérations suivantes : ◆ vérifier si l'authentification EBA est activée pour le serveur ; ◆ vérifier si le serveur héberge l'autorité de certification EBA ; ◆ vérifier si le certificat d'autorité de certification EBA est valide ; ◆ vérifier si le certificat d'autorité de certification NCP est valide.

Gestion de l'autorité de certification EBA à l'aide

Pour accéder à eDirectory à partir du plug-in EBA d'iManager, le certificat de l'autorité de certification EBA doit se trouver dans la zone de stockage des certificats prenant en charge l'authentification EBA d'iManager. Pour télécharger le certificat d'autorité de certification EBA sur l'ordinateur qui exécute iManager, exécutez l'utilitaire ebaclientinit à partir du paquetage d'installation d'iManager. Pour plus d'informations, reportez-vous à la « Exécution de l'utilitaire ebaclientinit » page 516.

Pour ouvrir la page de gestion de l'autorité de certification EBA, connectez-vous à iManager, cliquez sur l'icône **Rôles et tâches** dans la barre supérieure pour vous assurer que vous vous trouvez dans la vue **Rôles et tâches**, puis sélectionnez **Enhanced Background Authentication (EBA)** dans le panneau de navigation de gauche. Cliquez sur **Gestion de l'autorité de certification EBA** pour ouvrir la page de gestion de l'autorité de certification EBA.

La page de gestion de l'autorité de certification EBA comprend les onglets ci-dessous, lesquels permettent de gérer les différents aspects de l'autorité de certification EBA :

- **Général :** Affiche l'adresse IP de l'autorité de certification EBA et son certificat.
- **Certificats émis:** Affiche les certificats de l'autorité de certification NCP, accompagnés de leur adresse et de leur port.

  Pour révoquer un certificat, sélectionnez-le et cliquez ensuite sur **Révoquer**. N'utilisez cette option que dans les cas extrêmes, car le serveur possédant le certificat d'autorité de certification NCP cessera de fonctionner si vous révoquez son certificat. En règle générale, un certificat doit être révoqué lorsqu'un serveur est endommagé.

- **Requête de signature de certificat (CSR) :** affiche la liste des requêtes de signature de certificat en attente d'approbation par l'administrateur. Pour approuver une requête de signature de certificat, sélectionnez le certificat dans la liste, puis cliquez sur **Approuver**.

Exécution de l'utilitaire ebaclientinit

Pour télécharger le certificat de l'autorité de certification EBA sur l'ordinateur, exécutez l'utilitaire `ebaclientinit`. Le tableau ci-dessous répertorie les options de ligne de commande disponibles avec l'utilitaire `ebaclientinit` :

Options de ligne de commande	Description
`--user-dn`	DN de l'utilisateur au format à points.
`--password`	Mot de passe de l'utilisateur pour lequel l'authentification EBA est activée.
`--address`	Adresse d'un serveur NCP existant dans l'arborescence. La syntaxe est `<adresse_IP>:<port>`.

Par exemple : `ebaclientinit --mechanism ebatls --user-dn john.foo.org --password p@$$w0rd --address 111.111.11.1:524`

En fonction de la plate-forme que vous utilisez, exécutez ebaclientinit à l'aide de l'une des méthodes suivantes :

Linux : sous Linux, iManager s'exécute en tant qu'utilisateur `novlwww`. Par conséquent, exécutez ebaclientinit en tant qu'utilisateur `novlwww` à l'aide de cette commande :

```
sudo -u novlwww -H LD_LIBRARY_PATH=/var/opt/novell/iManager/nps/WEB-INF/bin/linux/
:/opt/netiq/common/openssl/lib64/ /var/opt/novell/iManager/nps/WEB-INF/bin/linux/
ebaclientinit --mechanism ebatls
```

Windows : procédez comme suit :

1. Connectez-vous au serveur sur lequel iManager est installé.
2. Exécutez ebaclientinit à partir de `C:\Program Files\Novell\Tomcat\webapps\nps\WEBINF\bin\windows\ebaclientinit.exe --mechanism ebatls`.

   Le fichier `.eba.p12` est alors placé dans le répertoire privé de l'utilisateur.
3. Copiez le fichier `.eba.p12` dans `C:\Users\novlwww`.

   REMARQUE : Si vous utilisez iManager 3.0 SP1 ou une version antérieure, copiez le fichier `.eba.p12` à l'emplacement `C:\Windows\System32\config\systemprofile`. Cette action est nécessaire, car Tomcat est exécuté en tant qu'utilisateur `Système` sous Windows.

REMARQUE : si iManager ne trouve pas le certificat de l'autorité de certification EBA de l'arborescence dans le fichier `.eba.p12` ou si le fichier `.eba.p12` n'est pas présent, le plug-in EBA d'iManager vous invite à indiquer les références `sadmin` du serveur agissant comme autorité de certification EBA. Toutefois, NetIQ ne recommande pas d'utiliser les références `sadmin`.

Restrictions des opérations eDirectory en cas d'activation de l'authentification EBA

Si l'authentification EBA est activée pour un serveur hébergeant la réplique maîtresse Lecture-écriture d'une partition, on considère qu'elle l'est également pour la partition en question. eDirectory interdit toute opération entraînant la désactivation de l'authentification EBA pour une partition. Sur un serveur pour lequel l'authentification EBA est activée, eDirectory impose les restrictions suivantes concernant les opérations effectuées sur les partitions et les répliques :

- « Restrictions concernant la modification des types de réplique » page 517
- « Restrictions concernant la modification de la réplique maîtresse d'une partition » page 517
- « Restrictions concernant la fusion de partitions » page 517
- « Restrictions concernant la reconfiguration d'un serveur pour lequel l'authentification EBA est activée » page 518

Restrictions concernant la modification des types de réplique

- Si le serveur qui héberge l'autorité de certification EBA contient la réplique maîtresse de la partition root de l'arborescence, eDirectory ne permet pas de modifier son type de réplique.
- Si l'autorité de certification EBA est hébergée sur un serveur qui contient la réplique Lecture-écriture de la partition root de l'arborescence, veillez à ne pas remplacer le type de réplique par un autre type que Maîtresse. Si vous définissez le type de réplique sur Lecture seule/Lecture seule filtrée, l'authentification EBA risque de ne plus fonctionner correctement dans l'ensemble de l'arborescence. eDirectory applique cette restriction si l'authentification EBA est activée sur le serveur eDirectory qui héberge la réplique maîtresse de la partition root de l'arborescence.

REMARQUE : dans un environnement mixte comportant des serveurs exécutant la version 9.2 et des versions antérieures d'eDirectory, il se peut que vous puissiez modifier les types de répliques. Cela dit, cette opération est susceptible de nuire au fonctionnement de l'authentification EBA.

Restrictions concernant la modification de la réplique maîtresse d'une partition

Si la réplique maîtresse d'une partition est présente sur un serveur pour lequel l'authentification EBA est activée, les opérations suivantes échoueront :

- Transfert du rôle de maître vers un serveur pour lequel l'authentification EBA n'est pas activée.
- Transfert du rôle de maître vers tout autre serveur agissant en qualité d'autorité de certification EBA.

Restrictions concernant la fusion de partitions

Ne fusionnez pas deux partitions si l'authentification n'est pas activée pour la partition parente et est activée pour la partition enfant. Cette opération est susceptible de nuire au fonctionnement de l'authentification EBA.

Restrictions concernant la reconfiguration d'un serveur pour lequel l'authentification EBA est activée

Lorsqu'eDirectory est configuré sur un serveur pour lequel l'authentification EBA est activée, cette information est enregistrée dans le paramètre `n4u.server.eba_enabled` du fichier `nds.conf`. Si vous vous annulez la configuration d'eDirectory sur ce serveur, puis reconfigurez ce dernier, l'authentification EBA n'est pas activée par défaut. Pour configurer le serveur en mode non-EBA, supprimez ce paramètre du fichier nds.conf avant de configurer eDirectory sur le serveur.

Sauvegarde d'un serveur pour lequel l'authentification EBA est activée

Pour sauvegarder un serveur eDirectory pour lequel l'authentification EBA est activée, suivez les instructions de la section Sauvegarde et restauration de NetIQ eDirectory. Veillez à sélectionner les attributs de flux et NICI lorsque vous effectuez une sauvegarde incrémentielle ou complète d'un serveur pour lequel l'authentification EBA est activée, sinon vous ne pourrez pas restaurer le serveur.

Déplacement du rôle d'autorité de certification EBA vers un nouveau serveur

En cas de défaillance du serveur faisant office d'autorité de certification EBA, eDirectory permet de déplacer le rôle d'autorité de certification EBA vers un autre serveur de l'arborescence pour lequel l'authentification EBA est activée. Avant de déplacer le rôle d'autorité de certification EBA vers un nouveau serveur, assurez-vous que ce dernier :

- Est en mode Authentification EBA activée.
- Héberge une réplique accessible en écriture de la partition root de l'arborescence dans laquelle la réplique était déjà présente au moment de la défaillance de l'autorité de certification EBA.

Pour transférer le rôle d'autorité de certification EBA vers le nouveau serveur sous Linux, exécutez la commande ci-dessous à partir de votre shell bash sur le nouveau serveur :

```
ndstrace -c "config ebassl_srv seize_ebaca"
```

eDirectory affiche un message indiquant que le rôle d'autorité de certification EBA a été transféré correctement vers le nouveau serveur. Si vous tentez d'effectuer cette opération alors que le serveur d'origine fonctionne toujours, l'opération échoue.

Sous Windows, procédez comme suit :

1. Ouvrez `ndscons.exe`.
2. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > NetIQ eDirectory Services**.
3. Sous l'onglet **Services**, accédez à `ebassl_srv.dlm`, puis spécifiez `seize_ebaca` dans le champ **Paramètres de démarrage**.
4. Cliquez sur **Configurer**.

Pour afficher les messages relatifs au transfert du rôle d'autorité de certification EBA, exécutez `dstrace.dlm` avec la balise EBA activée lorsque l'opération de transfert du rôle d'autorité de certification EBA est en cours d'exécution. DSTrace affiche le message approprié selon que l'opération a réussi ou échoué. Si vous tentez d'effectuer cette opération alors que le serveur d'origine fonctionne toujours, l'opération échoue.

REMARQUE

- Pour déterminer si le rôle d'autorité de certification EBA a bien été transféré, exécutez ndscheck sur le nouveau serveur. Si le résultat affiche `EBACA=true`, le nouveau serveur est désormais l'autorité de certification EBA de l'arborescence.
- En cas de défaillance du serveur qui héberge l'autorité de certification EBA, désignez comme autorité de certification EBA un autre serveur appartenant à l'anneau de répliques de la partition root de l'arborescence. Si le serveur défaillant hébergeait une réplique maîtresse de la partition root de l'arborescence, il est recommandé pour transférer le rôle de maître vers le nouveau serveur agissant en tant qu'autorité de certification EBA. Pour transférer le rôle de maître, suivez les instructions de la « Réparation des répliques » page 344.

18 Prise en charge du protocole SNMP pour NetIQ eDirectory

Le protocole SNMP (Simple Network Management Protocol) correspond au protocole Internet standard d'exploitation et de maintenance. Il permet l'échange de données de gestion entre les applications de console de gestion et les périphériques qu'elles gèrent. Les applications de console de gestion incluent notamment IBM Tivoli NetView ou Solstice SunNet Manager. Les périphériques gérés comprennent les hôtes, les routeurs, les passerelles et les hubs ainsi que des applications réseau telles que NetIQ eDirectory.

Ce chapitre décrit les services SNMP pour NetIQ eDirectory. Elle contient les rubriques suivantes :

- « SNMP : définitions et terminologie » page 521
- « Présentation des services SNMP » page 522
- « eDirectory et SNMP » page 524
- « Installation et configuration des services SNMP pour eDirectory » page 526
- « Surveillance d'eDirectory à l'aide de SNMP » page 533
- « Dépannage » page 560

SNMP : définitions et terminologie

Le tableau suivant contient la terminologie employée dans ce chapitre.

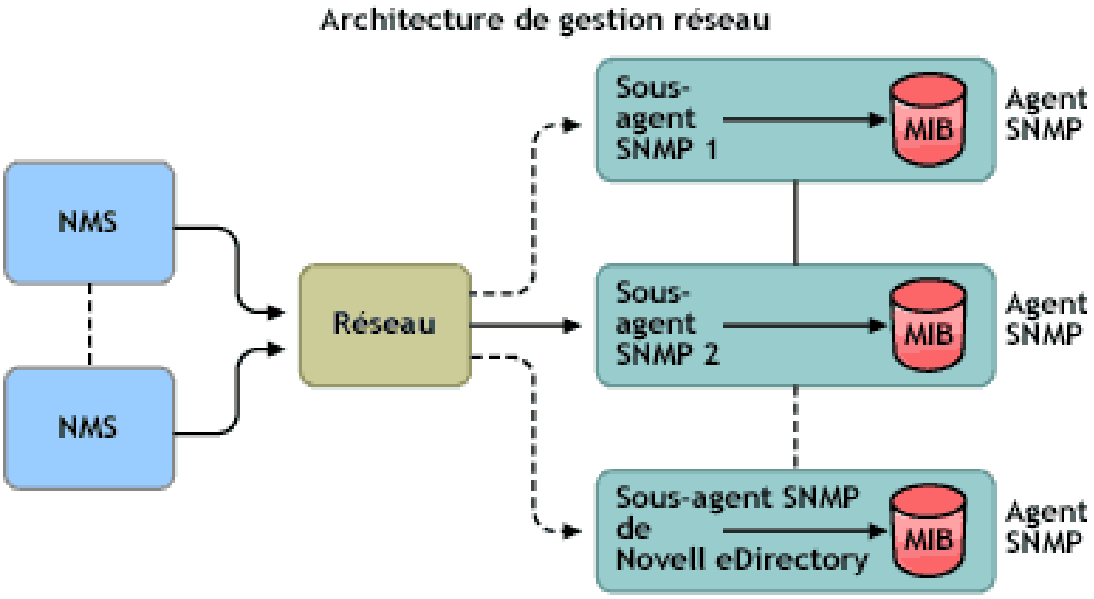
Terminologie	Définition
EMANATE	Enhanced Management Agent Through Extensions est un produit de SNMP Research International, Inc.
SNMP	Simple Network Management Protocol. Protocole utilisé pour l'échange de données sur l'activité du réseau.
NAA	Adaptateur d'agent natif
NMS	Network Management Station (Station d'administration réseau)
MA	Agent de gestion
SA	Sous-agent
MIB	Management Information Base (Base d'informations de gestion)
NCP	NetWare/Novell Core Protocol
NMA	Application de gestion réseau
edir.mib	MIB de surveillance du serveur NetIQ eDirectory qui contient les trappes et objets MIB appropriés pour NetIQ eDirectory.
Trappes	Alertes générées par des agents sur un périphérique géré lorsque des événements eDirectory se produisent sur le serveur. Ces conditions sont définies dans la MIB (base d'informations de gestion) fournie par NetIQ.

Présentation des services SNMP

SNMP repose sur une architecture gestionnaire/agent. L'architecture de gestion réseau SNMP comprend les éléments suivants :

- Station de gestion réseau (NMS)
- Périphérique géré
- Agent principal
- Sous-agent
- Base d'informations de gestion (MIB)
- Protocole de gestion réseau

Figure 18-1 *Architecture de gestion réseau*



Network Management Station (Station d'administration réseau)

Une station de gestion réseau est un poste de travail qui comporte une ou plusieurs applications de gestion réseau installées permettant d'afficher en mode graphique des informations sur les périphériques gérés.

Fonctions NMS :

- Elle fournit l'interface utilisateur à l'ensemble du système de gestion réseau et offre ainsi un outil de gestion réseau puissant, souple et simple à utiliser.
- Elle permet d'exécuter les opérations SNMP Get, Get Next, Get Response et Set. La station de gestion réseau permet également de capturer les trappes SNMP envoyées sur le réseau par les périphériques gérés.
- Elle surveille une ou plusieurs applications de gestion réseau (NMA) simultanément. La station de gestion réseau inclut des installations qui permettent de visualiser des informations à propos des périphériques gérés, de l'affichage des tables et de la consignation.
- Elle permet de compiler le fichier MIB à l'aide du compilateur MIB disponible dans la NMS.

Périphériques gérés

Un périphérique géré est un périphérique sur lequel est installé SNMP. Il peut s'agir d'un hôte, d'un routeur, d'une passerelle, d'un hub, etc. La NMS les surveille et communique avec eux.

Les informations circulant entre la NMS et le périphérique géré sont transférées via deux types d'agent : le sous-agent et l'agent principal.

Sous-agent

Le sous-agent collecte les informations relatives au périphérique géré et les transmet à l'agent principal.

Agent principal

L'agent principal prend en charge l'échange d'informations entre les différents sous-agents et la NMS. Il est exécuté sur la même machine hôte que les sous-agents avec lesquels il communique.

Management Information Base (Base d'informations de gestion)

SNMP permet d'échanger des informations sur le réseau sous forme de PDU (Protocol Data Units). Les PDU contiennent des informations sur les variables stockées sur le périphérique géré. Ces variables, appelées objets gérés, possèdent des valeurs et des intitulés qui sont renvoyés à la NMS. Tous les objets gérés sont définis dans la base d'informations de gestion. La MIB est une base de données virtuelle de type arborescence.

Protocole de gestion réseau SNMP

Le tableau ci-dessous liste les fonctions de base de SNMP.

Fonction	Description
Get	Commande utilisée par le gestionnaire pour demander des informations à un agent.
Get Next	Commande employée par le gestionnaire pour obtenir des informations depuis un tableau ou une table.
Get Response	Commande employée par l'agent interrogé pour répondre à la demande du gestionnaire.
Ensemble	Commande employée par le gestionnaire pour modifier la valeur de la variable qui réside dans la MIB de l'agent.
Trap	Notification utilisée par l'agent pour informer le gestionnaire qu'un événement donné s'est produit.

Pour plus d'informations sur SNMP, consultez les sites Web suivants :

- Page d'accueil de NET-SNMP (http://net-snmp.sourceforge.net)
- FAQ sur SNMP (http://www.faqs.org/faqs/snmp-faq/part1)
- RFC 1157 (http://www.ietf.org/rfc/rfc1157.txt)
- SNMPLink (http://www.snmplink.org)
- SNMPInfo (http://www.snmpinfo.com)

- SNMP RFC Standard MIBs and Informative Links (Liens d'information et MIB standard RFC SNMP) (http://www.wtcs.org/snmp4tpc/snmp_rfc.htm)
- RFC 2605 (http://www.ietf.org/rfc/rfc2605.txt?number=2605)

eDirectory et SNMP

eDirectory peut stocker et gérer des millions d'objets, tels que des utilisateurs, des applications, des périphériques réseau et des données. Plus les objets sont nombreux, plus il est nécessaire de suivre les ajouts et les modifications effectués dans eDirectory. SNMP apporte une solution à ce problème : il vous aide à surveiller les serveurs eDirectory en assurant le suivi des modifications.

Avantages de l'instrumentation de SNMP sur eDirectory

- Surveillance en temps réel d'un serveur eDirectory
- Surveillance d'eDirectory à partir d'un navigateur MIB SNMP tiers
- Suivi du statut d'eDirectory pour vérifier les opérations standard
- Identification et traitement des problèmes potentiels après leur détection
- Configuration de trappes et de statistiques en vue d'une surveillance sélective
- Définition d'une tendance pour l'accès à eDirectory
- Enregistrement et analyse des données historiques obtenues via SNMP
- Prise en charge des statistiques pour les opérations SNMP Get, GetNext
- Utilisation de l'agent principal natif SNMP sur l'ensemble de la plate-forme

Présentation du fonctionnement de SNMP avec eDirectory

L'implémentation de SNMP dans eDirectory fournit des informations utiles sur eDirectory en matière de statistiques sur les accès, les opérations, les erreurs et les performances du cache. Des trappes relatives à l'occurrence d'événements peuvent également être envoyées via une implémentation de SNMP. Les trappes et statistiques sont définies dans la MIB.

REMARQUE : Il se peut que vous deviez accéder aux attributs codés en utilisant un canal sécurisé, si vous avez spécifié qu'il convient d'utiliser un canal sécurisé pour accéder à ces attributs. Pour plus d'informations, reportez-vous à la « Attributs codés » page 315.

MIB de surveillance du service d'annuaire

La MIB eDirectory définit les statistiques et les trappes qui servent à surveiller eDirectory. Les OID suivants sont assignés à cette MIB :

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).novell(23).mibDoc(2).nd
sMIB(98)
```

Statistiques

La MIB eDirectory est divisée en quatre tables distinctes d'objets gérés :

- **Table Statistiques de la base de données mise en cache - ndsDbCacheTable :** contient une description des serveurs d'annuaire ainsi que des statistiques globales sur les entrées mises en cache par ces serveurs.
- **Table Statistiques de la base de données configurée - ndsDbConfigTable :** contient une description des serveurs d'annuaire ainsi que des statistiques globales sur les entrées configurées par ces serveurs.
- **Table Statistiques de protocole - ndsProtoIfOpsTable :** fournit des statistiques globales sur les accès, les opérations et les erreurs pour chaque interface de protocole d'application d'un serveur d'annuaire.
- **Table Statistiques d'interaction - ndsServerIntTable :** effectue un suivi du dernier serveur d'annuaire “N” avec lequel l'annuaire surveillé est entré ou a tenté d'entrer en interaction. “N” est une constante définie localement.

REMARQUE : pour plus d'informations sur les statistiques, reportez-vous à la section « Statistiques » page 555.

Trappes - ndsTrapVariables

La MIB eDirectory définit 119 trappes, dont 117 sont assignées à des événements eDirectory. Les deux trappes supplémentaires, `ndsServerStart` et `ndsServerStop`, sont directement générées par le sous-agent SNMP. Ces deux trappes ne peuvent pas être configurées.

REMARQUE : pour plus d'informations sur les trappes, reportez-vous à la section « Trappes » page 533.

Pour plus d'informations sur les statistiques et les trappes, reportez-vous au fichier `edir.mib`.

`Il réside dans les répertoires suivants :`

Windows : *`répertoire_installation`*`\SNMP`
Linux : `/etc/opt/novell/eDirectory/conf/ndssnmp/`

Objet Groupe SNMP

L'objet Groupe SNMP permet de configurer et de gérer les trappes SNMP eDirectory. Durant l'installation, un objet Groupe SNMP appelé “Groupe SNMP - *nom_serveur*” est créé (*nom_serveur* étant le nom du serveur sur lequel les services SNMP pour eDirectory sont installés). L'objet Groupe SNMP est créé dans le même conteneur que l'objet Serveur. Cet utilitaire de configuration SNMP permet de configurer les trappes SNMP.

Sous Windows

Pour créer un objet Groupe SNMP, entrez la commande suivante :

```
rundll32 snmpinst, snmpinst -c <createobj> -a <FDN_utilisateur> -p <mot_de_passe> -
h <nom_hôte ou adresse _IP>
```

Paramètre	Description
`-c <createobj>`	Commande de trappe spécifiant la création d'un objet
`-a <FDN_utilisateur>`	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
`-p <mot_de_passe>`	Mot de passe d'authentification du FDN utilisateur
`-h <nom_hôte ou adresse_IP>`	Nom d'hôte DNS ou adresse IP

Exemple :

```
rundll32 snmpinst, snmpinst -c createobj -a admin.mon_contexte -p mon_mot_de_passe
-h 160.98.146.26
```

Pour supprimer un objet Groupe SNMP, entrez la commande suivante :

```
rundll32 snmpinst, snmpinst -c <deleteobj> -a <FDN_utilisateur> -p <mot_de_passe> -
h <nom_hôte ou adresse_IP>
```

Pour plus d'informations, consultez le tableau ci-dessus.

Exemple :

```
rundll32 snmpinst, snmpinst -c deleteobj -a admin.mon_contexte -p mon_mot_de_passe
-h 160.98.146.26
```

Sous Linux

Pour créer un objet Groupe SNMP, entrez la commande suivante :

```
ndsconfig add -m <nom_module> -a <FDN_utilisateur>
```

Exemple :

```
ndsconfig add -m snmp -a admin.mon_contexte
```

Installation et configuration des services SNMP pour eDirectory

L'installation des services SNMP pour eDirectory s'effectue simultanément avec celle d'eDirectory. Vous pouvez modifier la configuration par défaut des services SNMP pour eDirectory à l'aide d'iManager. Pour plus d'informations, reportez-vous à la section « Configuration dynamique » page 529.

Un nouvel objet appelé Groupe SNMP est ajouté à l'arborescence Annuaire lors de l'installation d'eDirectory. Cet objet permet de configurer et de gérer les trappes SNMP de NetIQ eDirectory. Pour plus d'informations, reportez-vous à la section « Objet Groupe SNMP » page 525.

Installation de SNMP après l'installation d'eDirectory sous Windows

Si les services SNMP ne sont pas implémentés lors de l'installation d'eDirectory, le programme d'installation d'eDirectory copie uniquement les fichiers de sous-agents SNMP et ne met pas à jour le registre.

Si vous souhaitez par la suite utiliser les services SNMP sur eDirectory, vous pouvez en effectuer l'installation et mettre à jour le registre via la commande suivante :

```
rundll32 snmpinst, snmpinst -c createreg
```

Chargement et déchargement du module serveur SNMP

Vous pouvez charger et décharger manuellement le module serveur SNMP. Par défaut, ce module est chargé automatiquement sur toutes les plates-formes. Toutefois, vous pouvez le charger manuellement sous Windows et Linux.

Pour charger le module serveur SNMP, entrez les commandes suivantes :

Serveur	Commande
Windows	Dans l'écran DHost (NDSCONS), sélectionnez **ndssnmp.dlm**, puis cliquez sur **Démarrer**.
Linux	Pour charger le serveur de trappes SNMP, sur la page de gestion à distance DHost, cliquez sur l'icône Serveur de trappes SNMP pour NetIQ eDirectory pour démarrer. ou Lorsque vous y êtes invité, saisissez les informations suivantes : `/opt/novell/eDirectory/bin/ndssnmp -l`

Pour décharger le module serveur SNMP, entrez les commandes suivantes :

Serveur	Commande
Windows	Dans l'écran DHost (NDSCONS), sélectionnez **ndssnmp.dlm**, puis cliquez sur **Arrêter**.
Linux	Pour décharger le serveur de trappes SNMP, sur la page de gestion à distance DHost, cliquez sur l'icône **Serveur de trappes SNMP pour NetIQ eDirectory 9.2** pour arrêter. ou Lorsque vous y êtes invité, saisissez les informations suivantes : `/opt/novell/eDirectory/bin/ndssnmp -u`

Configuration du sous-agent

- « Configuration statique » page 527
- « Configuration dynamique » page 529

Configuration statique

La configuration statique est employée avant la mise en service du sous-agent. Vous pouvez le configurer manuellement en modifiant le fichier `ndssnmp.cfg` sous Windows ou Linux. Le fichier `ndssnmp.cfg` réside dans les répertoires suivants :

Windows : *`répertoire_installation`*`\SNMP\`

Linux : `/etc/opt/novell/eDirectory/conf/ndssnmp/`

REMARQUE : si vous apportez des modifications au fichier `ndssnmp.cfg`, vous devez redémarrer le sous-agent.

Vous pouvez fournir au sous-agent des informations de configuration telles que :

- `INTERACTIVE` *`état`*

  Où *état* peut correspondre à « on » (activé) ou « off » (désactivé). Si l'état est « on », vous êtes invité à entrer le nom d'utilisateur et le mot de passe au démarrage du sous-agent. Si l'état est « off », le nom d'utilisateur et le mot de passe sont extraits de l'emplacement de stockage sécurisé. Par défaut=désactivé.

  Exemples :

  ```
  INTERACTIVE on
  ```

  ```
  INTERACTIVE off
  ```

- `INTERACTION` *`valeur`*

  Où le paramètre *`valeur`* correspond au nombre d'entrées de la table d'interaction. Plage = 1 à 10. Valeur par défaut = 4.

  Exemples :

  ```
  INTERACTION 4
  ```

  ```
  INTERACTION 2
  ```

- `MONITOR` *`état`*

  Où *`état`* peut correspondre à « on » (activé) ou « off » (désactivé). Par défaut=activé.

  Exemples :

  ```
  MONITOR on
  ```

  ```
  MONITOR off
  ```

- `SSLKEY` *`fichier_certificat`*

  Où le paramètre *`fichier_certificat`* correspond au certificat exporté avec son chemin d'accès. Vous devez spécifier le chemin de ce certificat exporté.

  Exemples :

  `SSLKEY /home/guest/snmp-cert.der` (Linux)

  `SSLKEY c:\home\guest\snmp-cert.der` (Windows)

  REMARQUE : cette option n'est pas prise en charge si plusieurs instances à surveiller n'acceptent pas un certificat commun.

- `SERVER` *`nom_hôte/adresse_IP:port_NCP`*

  Où *`nom_hôte`* correspond au nom de l'hôte sur lequel le serveur eDirectory est installé et configuré. Seul le serveur installé en local est pris en charge. Il s'agit d'une commande obligatoire dans le fichier. Dans le cas contraire, aucun des serveurs n'est surveillé. Valeur par défaut : nom d'hôte du serveur local.

  Exemples :

  ```
  SERVER myserver
  ```

  ```
  SERVER myserver:1524
  ```

Sous Linux, si vous disposez de plusieurs instances d'eDirectory, vous pouvez inclure tous les serveurs eDirectory à surveiller comme suit :

```
SERVER myserver:1524
SERVER myserver:2524
SERVER myserver:6524
```

REMARQUE : n'insérez pas d'espace avant ou après «:» dans la commande du serveur.

Configuration dynamique

Une fois le service d'annuaire activé et en cours d'exécution, la configuration dynamique peut s'effectuer à tout moment à l'aide des méthodes suivantes :

Ligne de commande

Vous pouvez faire appel à un utilitaire de ligne de commande de configuration des trappes afin de configurer les trappes SNMP d'eDirectory.

L'utilitaire de ligne de commande de configuration permet d'effectuer les opérations suivantes :

- activer ou désactiver des trappes ;
- définir l'intervalle entre les trappes ;
- activer ou désactiver des trappes d'échec ;
- répertorier les trappes activées/désactivées ou l'ensemble des trappes.

REMARQUE : Pour plus de détails, reportez-vous à la section « Configuration des trappes » page 547.

Plug-in iManager

Vous pouvez également configurer des trappes à l'aide de NetIQ iManager, un outil basé sur un navigateur qui permet d'administrer, de gérer et de configurer les objets eDirectory. NetIQ iManager permet d'assigner aux utilisateurs des tâches ou responsabilités particulières, et de mettre à leur disposition uniquement les outils (et les droits correspondants) nécessaires pour accomplir ces tâches.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **SNMP** > **Présentation de SNMP**.
3. Cliquez sur **Afficher des objets Groupe SNMP**, puis sur le nom de l'objet Groupe SNMP à configurer.
4. Entrez les paramètres configurables dans la page Général/Trappes.
5. Cliquez sur **Appliquer**, puis sur **OK** pour enregistrer les nouveaux paramètres de configuration.

REMARQUE : pour plus d'informations, reportez-vous à l'aide en ligne de NetIQ iManager.

Configuration des services SNMP pour eDirectory

Cette section explique comment configurer les services SNMP pour eDirectory sur les plates-formes suivantes :

- « Windows » page 530
- « Linux » page 531

Pour configurer les services SNMP pour eDirectory, exécutez la procédure suivante :

1. Configuration de l'agent principal
2. Démarrage de l'agent principal
3. Configuration du sous-agent
4. Démarrage du sous-agent

Windows

- « Configuration de l'agent principal » page 530
- « Démarrage de l'agent principal » page 530
- « Arrêt de l'agent principal » page 531
- « Démarrage du sous-agent » page 531

Configuration de l'agent principal

REMARQUE : l'agent principal SNMP doit être installé avant eDirectory. Pour plus d'informations, reportez-vous à l'article Microsoft SNMP Services (http://technet.microsoft.com/en-us/library/bb726977.aspx).

---

1 Dans la boîte de dialogue SNMP Properties (Propriétés de SNMP) de Microsoft, cliquez sur l'onglet **Agent**.

2 Entrez les informations relatives au contact et à l'emplacement.

3 Cliquez sur l'onglet Trappes, puis entrez les informations relatives au nom de communauté et à la destination des trappes.

- **3a** Spécifiez le nom de communauté, puis cliquez sur **Ajouter**.
- **3b** Entrez l'adresse IP ou le nom d'hôte de l'ordinateur cible pour lequel sont générées les trappes.
- **3c** Cliquez sur **Ajouter** pour ajouter l'adresse IP ou le nom d'hôte.

4 Activez l'option **Autoriser le service à interagir avec le Bureau**.

Si vous n'activez pas cette option, vous ne pourrez pas vous connecter à SNMP sous Windows.

Sous Windows, cliquez sur **Démarrage** > **Paramètres** > **Panneau de configuration** > **Outils d'administration** > **Services**. Cliquez ensuite avec le bouton droit de la souris sur **SNMP** et sélectionnez **Propriétés**. Dans l'onglet de **connexion**, sélectionnez l'option **Autoriser le service à interagir avec le Bureau**.

Démarrage de l'agent principal

1 Pour démarrer l'agent principal, procédez comme suit :

Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **Outils d'administration** > **Services** > **SNMP** > **Démarrer**.

2 À l'invite, saisissez la commande suivante :

```
Net start SNMP
```

Arrêt de l'agent principal

Pour arrêter l'agent principal, procédez comme suit :

1 Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **Outils d'administration** > **Services** > **SNMP** > **Arrêter**.

2 À l'invite, saisissez la commande suivante :

```
Net stop SNMP
```

Démarrage du sous-agent

Lorsque l'agent principal démarre sous Windows, le sous-agent démarre également.

IMPORTANT : Le dernier Service Pack mis à jour doit être installé après l'installation du service SNMP

Linux

Sous Linux, la suite `net-snmp` doit être installée. Par défaut, elle est installée sur la plupart des systèmes Linux.

Configuration des services SNMP sous Linux

- « Configuration de l'agent principal » page 531
- « Démarrage de l'agent principal » page 532
- « Démarrage du sous-agent » page 532
- « Arrêt du sous-agent » page 532

Configuration de l'agent principal

Pour configurer l'agent principal sous Linux, modifiez le fichier `snmpd.conf` comme expliqué à la section « Modification du fichier snmpd.conf » page 531.

Le fichier `snmpd.conf` se trouve dans le répertoire `/etc/snmp` sous SLES, et dans le répertoire `/etc` sur les autres plates-formes Linux.

Modification du fichier snmpd.conf

Dans le fichier `snmpd.conf`, entrez la ligne suivante :

```
trapsink myserver public
```

Où *`mon_serveur`* correspond au nom d'hôte de l'emplacement cible des trappes.

Dans le fichier `snmpd.conf`, ajoutez la ligne suivante :

```
master agentx
```

Apportez également les modifications suivantes :

Texte original	Texte modifié
`com2sec notConfigUser default public`	`com2sec demouser default public`
`group notConfigGroup v1 notConfigUser`	`group demogroup v1 demouser`
`view systemview included system`	view all included .1
`access notConfigGroup "" any noauth exact systemview none none`	`access demogroup "" any noauth exact all all all`

Si le texte ci-dessus ne figure pas dans le fichier `snmpd.conf`, ajoutez-le.

IMPORTANT : si des fichiers de configuration sont modifiés, il convient de redémarrer l'agent principal et le sous-agent.

Démarrage de l'agent principal

Pour démarrer l'agent principal, exécutez la commande suivante :

```
/usr/sbin/snmpd -C -c /etc/snmpd.conf
```

REMARQUE : exécutez la commande `/etc/init.d/snmpd start` pour démarrer l'agent maître sous SLES 12 et versions ultérieures.

Démarrage du sous-agent

Pour démarrer le sous-agent, exécutez la commande suivante :

```
/etc/init.d/ndssnmpsa start
```

Entrez le nom d'utilisateur et le mot de passe lorsque vous y êtes invité. Une fois l'authentification effectuée, le message suivant s'affiche si le paramètre `INTERACTION a la valeur ON` dans le fichier `/etc/opt/novell/eDirectory/conf/ndssnmp/ndssnmp.cfg` :

```
Do you want to remember password? (Y/N)
```

Entrez `o` pour le mémoriser. Au prochain lancement du sous-agent, vous ne serez plus invité à entrer le mot de passe.

Si vous entrez `n`, vous devrez indiquer le mot de passe au prochain démarrage du sous-agent.

REMARQUE : en cas de défaillance du serveur, l'agent principal et le sous-agent s'arrêtent également. Dès lors, pour démarrer l'agent principal et le sous-agent au moment du redémarrage du serveur, exécutez les commandes suivantes :

```
chkconfig snmpd on
chkconfig ndssnmpsa on
```

Arrêt du sous-agent

Pour arrêter le sous-agent, exécutez la commande suivante :

```
/etc/init.d/ndssnmpsa stop
```

Surveillance d'eDirectory à l'aide de SNMP

eDirectory est surveillé à l'aide des trappes et de la fonctionnalité de statistiques de SNMP.

Pour surveiller un serveur eDirectory à l'aide de SNMP, vous devez disposer des droits suivants sur les objets Serveur NCP, Groupe LDAP et Serveur LDAP :

- droits Superviseur sur l'objet Serveur NCP ;
- Droits de lecture sur l'attribut LDAP Autoriser les mots de passe en texte clair de l'objet Groupe LDAP
- Droits de lecture sur les attributs LDAP Port TCP et Port SSL de l'objet Serveur LDAP

Par défaut, un utilisateur qui s'est connecté avec les droits d'administrateur ne rencontre aucun problème pour surveiller un serveur eDirectory via SNMP.

Trappes

Le composant SNMP génère au total 119 trappes dont ndsServerStart (2001) et ndsServerStop (2002) qui ne peuvent pas être configurées. Ces trappes sont activées par défaut.

Vous pouvez utiliser un navigateur MIB pour vérifier les trappes générées.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
1	ndsCreateEntry	Un nouvel objet est ajouté dans l'annuaire. Exemple : Création d'un objet à l'aide des outils LDAP, ICE ou iManager.
2	ndsDeleteEntry	Un objet existant est supprimé. Exemple : Création d'un objet à l'aide des outils LDAP, ICE ou iManager.
3	ndsRenameEntry	Un objet existant est renommé. Exemple : Attribution d'un nouveau nom à un objet à l'aide des outils LDAP, ICE ou iManager.
4	ndsMoveSourceEntry	Un objet est déplacé vers un autre contexte. La trappe donne alors le contexte de l'objet avant son déplacement. Exemple : Déplacement d'un objet via ldapmodrdn ou ldapsdk.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
5	ndsAddValue	Une valeur est ajoutée à un attribut d'objet. Exemple : Ajout de nouvelles valeurs à des attributs à l'aide des outils LDAP, ICE ou iManager. **REMARQUE :** si la valeur renvoyée est nulle, vous devrez peut-être accéder au répertoire via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés » page 547
6	ndsDeleteValue	Une valeur est supprimée d'un attribut d'objet. Exemple : Suppression de nouvelles valeurs d'attribut à l'aide des outils LDAP, ICE ou iManager. **REMARQUE :** si la valeur renvoyée est nulle, vous devrez peut-être accéder au répertoire via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés » page 547
7	ndsCloseStream	Un attribut de flux est modifié.
8	ndsDeleteAttribute	Une valeur est supprimée d'un attribut à valeur unique. Exemple : Suppression d'un attribut à l'aide des outils LDAP, ICE ou iManager. **REMARQUE :** si la valeur renvoyée est `NULL`, vous devrez peut-être accéder au répertoire via un canal sécurisé. Pour plus d'informations, reportez-vous à la section « Accès aux attributs codés » page 547.
9	ndsCheckSecurityEquiv	Le vecteur d'équivalence de sécurité d'une entrée spécifique est contrôlé. Exemple : Modification de l'attribut d'équivalence de sécurité à l'aide des outils LDAP, ICE ou iManager.
10	ndsUpdateSecurityEquiv	Le vecteur d'équivalence de sécurité d'une entrée spécifique est modifié. Exemple : Modification de l'attribut d'équivalence de sécurité à l'aide des outils LDAP, ICE ou iManager.
11	ndsMoveDestEntry	Un objet est déplacé vers un autre contexte. La trappe donne alors le contexte vers lequel l'objet est déplacé. Exemple : Déplacement d'objets via ldapmodrdn ou ldapsdk.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
12	ndsDeleteUnusedExtref	Un objet Lien en amont est supprimé.
13	ndsAgentOpenLocal	L'agent Annuaire local est ouvert. Exemple : Exécution d'une réparation sans surveillance.
14	ndsAgentCloseLocal	L'agent Annuaire local est fermé. Exemple : Exécution d'une réparation sans surveillance.
15	ndsDSABadVerb	Un numéro de verbe incorrect est associé à une requête DSAgent. Exemple : Envoi d'une requête de verbe erronée à eDirectory à l'aide d'appels DClient.
16	ndsMoveSubtree	Un conteneur et son objet subordonné sont déplacés. Exemple : déplacement d'une partition vers un autre contexte via les outils LDAP, ICE ou iManager.
17	ndsNoReplicaPointer	Aucun pointeur de réplique n'est associé à une réplique donnée.
18	ndsSyncInEnd	La synchronisation entrante est terminée.
19	ndsBacklinkSecurEquiv	Une opération de liaison en amont a mis à jour le vecteur d'équivalence de sécurité d'un objet. Exemple : Modification de l'attribut d'équivalence de sécurité à l'aide des outils LDAP, ICE ou iManager.
20	ndsBacklinkOperPrivChg	Une opération de liaison en amont a modifié les privilèges de l'opérateur de la console d'un objet.
21	ndsDeleteSubtree	Un conteneur et ses objets subordonnés ont été supprimés.
22	ndsReferral	Un renvoi est créé.
23	ndsUpdateClassDef	Une définition de classe de schéma est mise à jour. Exemple : Cette trappe est générée lorsqu'une nouvelle classe ou un nouvel attribut sont ajoutés à un objet primaire, lui-même synchronisé avec un objet secondaire à l'aide des outils LDAP, ICE ou iManager.
24	ndsUpdateAttributeDef	Une définition d'attribut de schéma est mise à jour. Exemple : Cette trappe est générée lorsqu'un nouvel attribut est ajouté à un objet primaire, lui-même synchronisé avec un objet secondaire à l'aide des outils LDAP, ICE ou iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
25	ndsLostEntry	eDirectory identifie une entrée perdue. Une entrée perdue est une entrée pour laquelle vous recevez des mises à jour bien qu'elle n'existe pas sur le serveur local.
26	ndsPurgeEntryFail	L'opération de purge a échoué.
27	ndsPurgeStart	L'opération de purge a commencé. Exemple : Exécutez DSTrace et `Set ndstrace=*j`.
28	ndsPurgeEnd	L'opération de purge est terminée. Exemple : Exécutez DSTrace et `Set ndstrace=*j`.
29	ndsLimberDone	L'opération de contrôle de connectivité est terminée. Exemple : Configuration de DSTrace en vue du lancement du contrôleur de connectivité (limber) après une période donnée.
30	ndsPartitionSplitDone	L'opération de division de la partition est terminée. Exemple : Création d'une partition à l'aide d'iManager.
31	ndsSyncServerOutStart	La synchronisation sortante à partir d'un serveur particulier est lancée. Exemple : Configuration de DSTrace en vue du lancement de la synchronisation sortante après une période donnée.
32	ndsSyncServerOutEnd	La synchronisation sortante à partir d'un serveur particulier est terminée. Exemple : Configuration de DSTrace en vue de l'arrêt de la synchronisation sortante après une période donnée.
33	ndsSyncPartitionStart	La synchronisation de la partition est lancée. Exemple : Première partition des conteneurs.
34	ndsSyncPartitionEnd	La synchronisation de la partition est terminée. Exemple : Première partition des conteneurs.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
35	ndsMoveTreeStart	Le déplacement d'une sous-arborescence est lancé. Une sous-arborescence est déplacée en même temps qu'une partition. Exemple : Création et déplacement d'une partition vers un autre conteneur à l'aide d'iManager.
36	ndsMoveTreeEnd	Le déplacement d'une sous-arborescence est terminé. Une sous-arborescence est déplacée lors de la fusion d'une partition. Exemple : Création et déplacement d'une partition vers un autre conteneur à l'aide d'iManager.
37	ndsJoinPartitionDone	La jonction des partitions est terminée. Exemple : Création et fusion d'une partition à l'aide d'iManager.
38	ndsPartitionLocked	Une partition est verrouillée (par exemple, avant la fusion des partitions). Exemple : Création d'une partition à l'aide d'iManager.
39	ndsPartitionUnlocked	Une partition est déverrouillée (par exemple, après la fusion des partitions). Exemple : Création d'une partition à l'aide d'iManager.
40	ndsSchemaSync	Les schémas sont synchronisés. Exemple : Planification de la synchronisation des schémas à l'aide de `ldapsdk schsync`.
41	ndsNameCollision	Deux objets résidant sur des serveurs différents portent le même nom (ils **entrent en collision**). Exemple : désactivation de la synchronisation sortante des serveurs primaire et secondaire d'une arborescence via iMonitor. Ajoutez des objets Utilisateur aux deux serveurs à l'aide des outils LDAP. Puis, activez la synchronisation sortante des deux serveurs via iMonitor.
43	ndsChangeModuleState	Un module eDirectory (NLM/DLM) est chargé ou déchargé. Exemple : Chargement ou déchargement du module nldap.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
44	ndsLumberDone	Le processus en arrière-plan de contrôle de la connectivité est lancé.
45	ndsBacklinkProcDone	Le processus de liaison en amont est terminé. Exemple : Configuration de DSTrace en vue du lancement de la liaison en amont après une période donnée.
46	ndsServerRename	Un serveur est renommé. Exemple : Utilisation de ldapmodrdn ou ldapsdk pour renommer le serveur.
47	ndsSyntheticTime	Des objets sont créés avec des tampons horaires futurs. Pour synchroniser les serveurs eDirectory, il convient d'utiliser l'heure synthétique. Exemple : Ajout d'un serveur secondaire à l'arborescence via ndsconfig.
48	ndsServerAddressChange	Le contrôleur de connectivité (limber) modifie une adresse de renvoi du serveur. Exemple : modification de l'adresse IP du serveur et redémarrage de ndsd.
49	ndsDSARead	Une entrée est lue. Cette trappe est générée pour toutes les opérations exécutées sur eDirectory. Exemple : Utilisation de ldapsearch pour générer des trappes.
50	ndsLogin	Un utilisateur se connecte à eDirectory. Exemple : Connexion à l'arborescence via ndslogin.
51	ndsChangePassword	Un mot de passe est modifié. Exemple : Modification du mot de passe d'un objet Utilisateur via ldapmodify.
52	ndsLogout	Un utilisateur se déconnecte d'eDirectory. Exemple : Déconnexion de l'arborescence à l'aide du client Novell.
53	ndsAddReplica	Une réplique est ajoutée à une partition de serveur. Exemple : Ajout d'une réplique à l'arborescence via ndsconfig.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
54	ndsRemoveReplica	Une réplique est supprimée. Exemple : Suppression d'une réplique de l'un des serveurs à l'aide d'iManager.
55	ndsSplitPartition	Une partition est divisée. Exemple : Création d'une partition à l'aide d'iManager.
56	ndsJoinPartition	Une partition parente est associée à une partition enfant. Exemple : Création et jonction d'une partition à l'aide d'iManager.
57	ndsChangeReplicaType	Le type d'une réplique de partition est modifié. Exemple : Modification du type de réplique de « réplique maîtresse » en « réplique de type Lecture-écriture ».
58	ndsAddEntry	Un nouvel objet est ajouté. Exemple : Ajout d'un objet Utilisateur à l'aide d'iManager.
59	ndsAbortPartitionOp	Une opération de partition est abandonnée. Exemple : Partitionnement d'un conteneur et abandon de l'opération de partitionnement.
60	ndsRecvReplicaUpdates	Une réplique reçoit une mise à jour lors de la synchronisation. Exemple : Un serveur eDirectory dans une configuration d'arborescence multiserveur demande des mises à jour sur la réplique qu'il détient. Cette opération peut s'effectuer à l'aide d'iManager.
61	ndsRepairTimeStamps	Les tampons horaires d'une réplique sont réparés. Exemple : Exécution d'une opération de réparation de la DIB pour les tampons horaires à l'aide de DSRepair (ndsrepair sous Linux ou NDSCons sous Windows).
62	ndsSendReplicaUpdates	Une réplique est mise à jour lors de la synchronisation. Exemple : un serveur eDirectory dans une configuration d'arborescence multiserveur envoie des mises à jour sur la réplique qu'il détient. Cette opération peut s'effectuer à l'aide d'iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
63	ndsVerifyPass	Un mot de passe est vérifié. Exemple : Lorsque le mot de passe expire, saisissez-le de nouveau pour confirmation à l'invite de modification du mot de passe.
64	ndsBackupEntry	Une entrée est sauvegardée. Exemple : Sauvegarde d'objets Annuaire à l'aide de l'utilitaire de sauvegarde (ndsbackup sous Linux ou NDSCons sous Windows).
65	ndsRestoreEntry	Une entrée est restaurée. Exemple : Restauration des objets Annuaire sauvegardés à l'aide de l'utilitaire de sauvegarde (ndsbackup sous Linux ou NDSCons sous Windows).
66	ndsDefineAttributeDef	Une définition d'attribut est ajoutée au schéma. Exemple : Extension du schéma de l'arborescence eDirectory par l'ajout d'une définition d'attribut. Le schéma peut être étendu lors de l'installation d'une application dépendante d'eDirectory, telle que ZENWorks® ou NMAS™. L'extension de schéma peut également s'effectuer à l'aide d'iManager ou de l'utilitaire d'extension de schéma ndssch sous Linux.
67	ndsRemoveAttributeDef	Une définition d'attribut est supprimée du schéma. Exemple : Suppression d'une définition d'attribut du schéma de l'arborescence eDirectory. La suppression de l'attribut peut également s'effectuer à l'aide d'iManager ou de l'utilitaire d'extension de schéma ndssch sous Linux.
68	ndsRemoveClassDef	Une définition de classe est supprimée du schéma. Exemple : Suppression d'une définition de classe d'objet du schéma de l'arborescence eDirectory. La suppression peut s'effectuer à l'aide d'iManager ou de l'utilitaire d'extension de schéma ndssch sous Linux.
69	ndsDefineClassDef	Une définition de classe est ajoutée au schéma. Exemple : Extension du schéma de l'arborescence eDirectory par l'ajout d'une classe. Le schéma peut être étendu lors de l'installation d'une application dépendante d'eDirectory, telle que ZENWorks ou NMAS. L'extension du schéma peut également s'effectuer à l'aide d'iManager ou de l'utilitaire d'extension de schéma ndssch sous Linux.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
70	ndsModifyClassDef	Une définition de classe est modifiée. Exemple : Modification d'une classe d'objet ou de définitions d'attribut.
71	ndsResetDSCounters	Les compteurs internes d'eDirectory sont réinitialisés.
72	ndsRemoveEntryDir	Un répertoire de fichiers associé à une entrée est supprimé.
73	ndsCompAttributeValue	Les valeurs des attributs sont comparées. Exemple : Comparaison d'une valeur d'attribut à un objet. Exécution d'une opération de recherche LDAP par rapport à un objet `Utilisateur` pour vérifier si son numéro de téléphone correspond à la valeur entrée.
74	ndsOpenStream	Un attribut de flux est ouvert ou fermé. Exemple : Création ou ouverture d'un flux pour des opérations de lecture ou d'écriture. Création d'un script de connexion pour un objet `Utilisateur`. La génération de cette trappe résulte de la création d'un fichier sous le répertoire DIB.
75	ndsListSubordinates	Une opération consistant à lister les entrées subordonnées est exécutée sur un objet Conteneur. Il s'agit d'une recherche sur un niveau. Exemple : À l'aide d'iManager, cliquez sur un objet Conteneur pour répertorier les objets qu'il contient.
76	ndsListContainerClasses	Une opération Répertorier les classes pouvant être contenues est exécutée sur une entrée. Exemple : pour un objet donné, énumération des classes de conteneurs susceptibles de contenir l'objet. Lorsque la requête porte sur un objet Utilisateur, les classes de conteneurs listées peuvent être les suivantes : Organisation, Unité organisationnelle et Domaine.
77	ndsInspectEntry	Une opération Inspecter l'entrée est exécutée sur une entrée. Exemple : Inspection d'une entrée pour obtenir des informations la concernant et vérifier si des erreurs se sont produites à ce niveau. Cet événement est généré dans le cadre du processus en arrière-plan Gestionnaire d'attributs (Flat Cleaner) d'eDirectory, qui entraîne la génération de cette trappe.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
78	ndsResendEntry	Une opération Envoyer à nouveau l'entrée est exécutée sur une entrée. Exemple : Durant une opération de réplication, lors du renvoi d'une entrée en raison de l'échec de l'envoi précédent à cause de la connexion entre les serveurs.
79	ndsMutateEntry	Une opération Muter l'entrée est exécutée sur une entrée. Exemple : Mutation d'une classe d'objet Bindery en classe d'objet `Utilisateur`.
80	ndsMergeEntries	Deux entrées sont fusionnées. Exemple : Fusion de deux objets `Utilisateur`. Fusion d'`Entry2` (`ndsEntryName2`) avec `Entry` (`ndsEntryName`).
81	ndsMergeTree	Deux arborescences eDirectory sont fusionnées. Exemple : Fusion de deux arborescences eDirectory à l'aide de DSMerge (ndsmerge sous Linux ou NDSCons sous Windows).
82	ndsCreateSubref	Une référence subordonnée est créée. Exemple : Lorsque vous supprimez la réplique de la partition enfant d'un serveur, la réplique de référence subordonnée est créée automatiquement, ce qui entraîne la génération de cette trappe.
83	ndsListPartitions	Une opération Répertorier les partitions est exécutée. Exemple : À l'aide d'iManager, dans la vue Partition et schéma, cliquez sur l'objet Serveur eDirectory pour répertorier les partitions que contient le serveur.
84	ndsReadAttribute	Une valeur d'attribut est lue. Exemple : Exécution d'une opération de recherche sur l'arborescence.
85	ndsReadReferences	Les références d'une entrée sont lues.
86	ndsUpdateReplica	Une opération Mettre à jour la réplique est exécutée sur une réplique de partition. Exemple : Si vous supprimez un utilisateur de l'un des serveurs, l'autre réplique est mise à jour de façon à prendre en compte l'opération de suppression.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
87	ndsStartUpdateReplica	Une opération Début de la mise à jour de la réplique est exécutée sur une réplique de partition. Exemple : Si vous supprimez un utilisateur de l'un des serveurs, l'autre réplique est mise à jour de façon à prendre en compte l'opération de suppression.
88	ndsEndUpdateReplica	Une opération Fin de la mise à jour de la réplique est exécutée sur une réplique de partition. Exemple : Si vous supprimez un utilisateur de l'un des serveurs, l'autre réplique est mise à jour de façon à prendre en compte l'opération de suppression.
89	ndsSyncPartition	Une opération Sync. - Partition est exécutée sur une réplique de partition. Exemple : Suppression d'un utilisateur de l'une des partitions, La synchronisation peut être observée à l'aide de DSTrace.
90	ndsSyncSchema	La réplique maîtresse de la racine est invitée à synchroniser son schéma avec le serveur. Exemple : Ajout d'une nouvelle classe à l'aide d'iManager, des outils LDAP ou des utilitaires ndssch.
91	ndsCreateBackLink	Un lien en amont est créé. Un lien en amont est créé lorsqu'un objet qui n'est pas présent en local est référencé. Exemple : Dans un scénario multiserveur, créez une partition contenant quelques utilisateurs. Si vous supprimez cette partition de l'un des serveurs, une référence subordonnée est créée. Un lien en amont est créé pour tous les utilisateurs présents dans la partition supprimée.
93	ndsChangeTreeName	Le nom de l'arborescence est modifié. Exemple : Exécution de l'utilitaire de fusion DSMerge/ndsmerge pour renommer l'arborescence.
94	ndsStartJoinPartition	Une opération Début de la jonction est exécutée pour fusionner des partitions. Exemple : Fusion ou jonction de partitions à l'aide des outils LDAP.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
95	ndsAbortJoinPartition	Une opération Joindre les partitions est abandonnée pour arrêter la fusion des partitions. Exemple : Fusion ou jonction de partitions à l'aide des outils LDAP.
96	ndsUpdateSchema	Une opération Mettre à jour le schéma est exécutée. Exemple : Ajout d'une nouvelle classe à l'aide d'iManager, des outils LDAP ou de ndssch.
97	ndsStartUpdateSchema	Une opération Début de la mise à jour du schéma est exécutée. Exemple : Ajout d'une nouvelle classe à l'aide d'iManager, des outils LDAP ou de ndssch.
98	ndsEndUpdateSchema	Une opération Fin de la mise à jour du schéma est exécutée. Exemple : Ajout d'une nouvelle classe à l'aide d'iManager, des outils LDAP ou de ndssch.
99	ndsMoveTree	Une opération Déplacer l'arborescence est exécutée. Exemple : déplacement d'une partition d'un conteneur à un autre.
101	ndsConnectToAddress	Une connexion est établie avec une adresse particulière. Exemple : Navigation dans l'arborescence à l'aide d'iManager.
102	ndsSearch	Une opération Rechercher est exécutée. Exemple : Exécution de ldapsearch sur l'arborescence à l'aide des outils LDAP.
103	ndsPartitionStateChange	Une partition est créée ou supprimée. Exemple : Création d'une partition.
104	ndsRemoveBacklink	Des références externes inutilisées sont supprimées et le serveur envoie une requête de suppression de lien en amont au serveur contenant l'objet.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
105	ndsLowLevelJoinPartition	Une jonction de faible niveau est exécutée durant les opérations de fusion des partitions. Exemple : Fusion ou jonction de partitions à l'aide d'iManager ou des outils LDAP.
106	ndsCreateNameBase	Une base de noms eDirectory est créée.
107	ndsChangeSecurityEquals	L'attribut Équivalents de sécurité est modifié. Exemple : Modification de l'équivalent de sécurité d'un utilisateur pour le rendre équivalent à `admin` à l'aide d'iManager.
108	ndsRemoveEntry	Une entrée est supprimée d'eDirectory. Exemple : Suppression d'un utilisateur à l'aide d'iManager.
109	ndsCRCFailure	Un échec CRC se produit au cours de la reconstitution de requêtes NCP fragmentées.
110	ndsModifyEntry	Une entrée d'eDirectory est modifiée. Exemple : Modification des attributs d'un utilisateur à l'aide d'iManager.
111	ndsNewSchemaEpoch	Le schéma est réinitialisé via DSRepair. Exemple : Création d'une période de schéma à l'aide de `ndsrepair -S -Ad` sous Linux.
112	ndsLowLevelSplitPartition	Une division de faible niveau est exécutée lors de la création d'une partition. Exemple : Création d'une partition à l'aide d'iManager ou des outils LDAP.
113	ndsReplicaInTransition	Une réplique est ajoutée ou supprimée.
114	ndsAclModify	L'ayant droit d'un objet est modifié (un objet Liste de contrôle d'accès (ACL) est modifié). Exemple : Ajout, modification ou suppression de l'ayant droit d'un objet via les outils LDAP, ICE ou iManager.
115	ndsLoginEnable	Le serveur reçoit une requête visant à activer le compte utilisateur. Exemple : Activation de l'attribut Compte désactivé via les outils LDAP, ICE ou iManager.

Numéro de la trappe	Nom de la trappe	Génération de la trappe quand
116	ndsLoginDisable	Le serveur reçoit une requête visant à désactiver le compte utilisateur. Exemple : Désactivation de l'attribut Compte désactivé via les outils LDAP, ICE ou iManager.
117	ndsDetectIntruder	Un compte utilisateur est verrouillé suite à la détection d'un intrus. Exemple : Verrouillage au moyen de l'attribut Intrus via les outils LDAP, ICE ou iManager.
2001	ndsServerStart	Le sous-agent réussit à se reconnecter au serveur eDirectory. Cette trappe comporte deux variables : ◆ `ndsTrapTime` : variable contenant le nombre total de secondes qui se sont écoulées entre le 1er janvier 1970 à minuit (24:00) GMT (TU), moment auquel le sous-agent a réussi à se reconnecter au serveur eDirectory. ◆ `ndsServerName` : serveur eDirectory auquel le sous-agent a réussi à se reconnecter. Exemple : arrêt et démarrage du serveur eDirectory alors que le sous-agent est en cours d'exécution.
2002	ndsServerStop	Le sous-agent perd sa connexion au serveur eDirectory. Cette trappe comporte deux variables : ◆ `ndsTrapTime` : variable contenant le nombre total de secondes qui se sont écoulées entre le 1er janvier 1970 à minuit (24:00) GMT (TU), moment auquel la connexion entre le sous-agent et le serveur eDirectory a été interrompue. ◆ `ndsServerName` : serveur eDirectory dont le sous-agent a été déconnecté. Exemple : arrêt du serveur eDirectory alors que le sous-agent est en cours d'exécution.

Accès aux attributs codés

eDirectory permet de chiffrer des données sensibles spécifiques pour les protéger lorsqu'elles sont stockées sur le disque et lorsque vous tentez d'y accéder sur le réseau. Vous pouvez spécifier si vous souhaitez toujours accéder aux attributs codés via un canal sécurisé. Pour plus d'informations, reportez-vous à la « Accès aux attributs codés » page 322.

Si vous avez spécifié que vous n'avez besoin que de canaux sécurisés pour accéder aux attributs chiffrés, les événements de valeur NDS sont bloqués. Le cas échéant, les trappes associées à des événements de valeur auront des données de valeur telles que `NULL` et vous recevrez un message d'erreur -6089 indiquant que vous avez besoin d'un canal sécurisé pour obtenir la valeur des attributs chiffrés. Les trappes qui auront les données de valeur `NULL` sont les suivantes :

- ndsAddValue
- ndsDeleteValue
- ndsDeleteAttribute

Configuration des trappes

La méthode de configuration des trappes diffère d'une plate-forme à une autre.

Plate-forme	Utilitaire
Windows	ndssnmpcfg
Linux	ndssnmpconfig

Windows

L'utilitaire ndssnmpcfg permet de configurer les trappes sous Windows. Il réside dans le répertoire *`chemin_installation`*`\`. Cet utilitaire permet d'activer et de désactiver les trappes, de définir l'intervalle de temps des trappes individuelles, de définir un intervalle de temps par défaut, d'activer des trappes pour les opérations en échec et de lister toutes les trappes.

Utilisation :

`ndssnmpcfg -h [`*`nom_hôte`*`[:`*`port`*`]] -p `*`mot_de_passe`*` -a `*`FDN_utilisateur`*` -c `*`commande`*

Paramètre	Description
`-h`	Nom d'hôte DNS ou adresse IP
`-p`	Mot de passe d'authentification du FDN utilisateur
`-a`	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
`-c`	Commandes de trappes (Reportez-vous à la section « Commandes de trappes Windows » page 548.)

Commandes de trappes Windows

Commandes de trappes	Description	Utilisation

`DISABLE`	La désactivation d'une trappe signifie que la NMS ne reçoit pas de trappes, bien que ces dernières soient générées.	Pour désactiver des trappes spécifiques, par exemple les trappes 10, 11 et 100 :
		`ndssnmpcfg "DISABLE 10, 11, 100"`
		Pour désactiver toutes les trappes, excepté les trappes 10, 11 et 100 :
		`ndssnmpcfg "DISABLE ID != 10, 11, 100"`
		Pour désactiver toutes les trappes comprises dans la plage allant de 20 à 30 :
		`ndssnmpcfg "DISABLE 20-29"`
		Pour désactiver toutes les trappes :
		`ndssnmpcfg "DISABLE ALL"`

`ENABLE`	L'activation d'une trappe signifie que la NMS reçoit les trappes lorsqu'elles sont générées.	`ndssnmpcfg "ENABLE` *`Spécification_trappe`*`"`
		`Il peut s'agir de l'une des spécifications suivantes :`
		Pour activer des trappes spécifiques, par exemple les trappes 10, 11 et 100 :
		`ndssnmpcfg "ENABLE 10, 11, 100"`
		Pour activer toutes les trappes, excepté les trappes 10, 11 et 100 :
		`ndssnmpcfg "ENABLE ID != 10, 11, 100"`
		Pour activer toutes les trappes comprises dans la plage allant de 20 à 30 :
		`ndssnmpcfg "ENABLE 20-29"`
		Pour activer toutes les trappes :
		`ndssnmpcfg "ENABLE ALL"`

Commandes de trappes	Description	Utilisation

`INTERVAL`	Cet utilitaire permet de définir et d'afficher l'intervalle de temps.
	
	Celui-ci correspond au nombre de secondes précédant l'envoi de trappes en double.
	
	Sa valeur doit être comprise entre 0 et 2 592 000 secondes.
	
	Si tel n'est pas le cas, l'intervalle de temps par défaut est adopté.
	
	S'il présente la valeur zéro, toutes les trappes sont envoyées.
		Pour afficher l'intervalle de temps :
		
		`ndssnmpcfg "213,240,79 INTERVAL"`
		
		Pour définir l'intervalle de temps entre plusieurs trappes (par exemple, pour définir un intervalle de temps de 5 entre les trappes 12, 17 et 101) :
		
		`ndssnmpcfg "12 17 101 INTERVAL 5"`
		
		Pour afficher l'intervalle de temps par défaut :
		
		`ndssnmpcfg "DEFAULT INTERVAL"`
		
		Pour définir l'intervalle de temps par défaut :
		
		`ndssnmpcfg "DEFAULT INTERVAL=10"`

Commandes de trappes	Description	Utilisation

`LIST`	Cet utilitaire permet d'afficher des listes de numéros de trappe répondant à des critères spécifiés.	`ndssnmpcfg LIST` *`Spécification_trappe`*
		
		`La valeur` Spécification_trappe permet de spécifier des groupes de numéros de trappe et peut être suivie de l'un des mots-clés suivants :
		
		`ALL`, `ENABLED`, `DISABLED`, `FAILED` ou une expression logique
		
		Exemples :
		
		Pour lister toutes les trappes activées par leur nom :
		
		`ndssnmpcfg LIST ENABLED`
		
		Pour lister toutes les trappes désactivées par nom :
		
		ndssnmpcfg LIST DISABLED
		
		Pour lister toutes les trappes (117) par nom :
		
		`ndssnmpcfg LIST ALL`
		
		Pour lister des trappes spécifiques telles que 12, 224 et 300 par nom :
		
		`ndssnmpcfg LIST ID = 12,224,300`
		
		Pour lister toutes les trappes, excepté celles sélectionnées, telles que 12, 224 et 300 par nom :
		
		`ndssnmpcfg LIST ID != 12,224,300`
		
		Pour lister toutes les trappes mises en échec par nom :
		
		`ndssnmpcfg LIST FAILED`

Commandes de trappes	Description	Utilisation
READ_CFG	Cette commande permet de modifier la configuration de l'annuaire à partir du fichier de configuration ndstrap.cfg. Toutes les modifications spécifiées dans ce fichier sont alors appliquées. Cet utilitaire sert principalement à regrouper plusieurs commandes dans le fichier ndstrap.cfg et à exécuter l'opération en une fois. Le fichier ndstrap.cfg se trouve dans *répertoire_installation*\SNMP. Le fichier ndstrap.cfg indique les paramètres opérationnels à utiliser pour configurer les trappes et permet de configurer le fonctionnement des trappes SNMP. Ce fichier est lu à chaque fois que l'utilitaire de configuration de trappes ndssnmpcfg est exécuté avec la commande READ_CFG.	ndssnmpcfg "READ_CFG"
FAILURE	Cette commande permet de lister toutes les trappes activées pour être mises en échec. Lorsqu'un événement échoue, une trappe d'échec est générée. **REMARQUE :** si la trappe est mise en échec, puis désactivée avant d'être à nouveau activée via la commande enable trapid, elle est alors activée en cas de réussite, et non d'échec.	ndssnmpcfg "FAILURE *Spécification_trappe*" *La valeur* Spécification_trappe comporte un ou plusieurs numéros de trappe séparés par une virgule ou un espace, du mot-clé ALL ou d'une expression logique. Exemples : Pour mettre plusieurs trappes en échec : ndssnmpcfg "FAILURE 10,11,100" Pour mettre toutes les trappes en échec, à l'exception de celles mentionnées : ndssnmpcfg "FAILURE ID != 24,30" Pour mettre toutes les trappes en échec : ndssnmpcfg "FAILURE ALL"

Linux

L'utilitaire ndssnmpconfig permet de configurer des trappes sous Linux. Il réside dans le répertoire /etc/ndssnmp/. Cet utilitaire permet d'activer et de désactiver les trappes, de définir l'intervalle de temps des trappes individuelles, de définir un intervalle de temps par défaut, d'activer des trappes pour les opérations en échec et de lister toutes les trappes.

Utilisation :

ndssnmpconfig -h [*nom_hôte*[*:port*]] -p *mot_de_passe* -a *FDN_utilisateur* -c *commande*

Paramètre	Description
`-h`	Nom d'hôte DNS ou adresse IP
`-p`	Mot de passe d'authentification du FDN utilisateur
`-a`	Nom distinctif complet d'un utilisateur disposant de droits d'administrateur
`-c`	Commandes de trappes (Reportez-vous à la section « Commandes de trappes sous Linux » page 552.)

Commandes de trappes sous Linux

Commandes de trappes	Description	Utilisation

`DISABLE`	La désactivation d'une trappe signifie que la NMS ne reçoit pas de trappes, bien que ces dernières soient générées.	Pour désactiver des trappes spécifiques, par exemple les trappes 10, 11 et 100 :
		`ndssnmpconfig "DISABLE 10, 11, 100"`
		Pour désactiver toutes les trappes, excepté les trappes 10, 11 et 100 :
		`ndssnmpconfig "DISABLE ID != 10, 11, 100"`
		Pour désactiver toutes les trappes comprises dans la plage allant de 20 à 30 :
		`ndssnmpconfig "DISABLE 20-29"`
		Pour désactiver toutes les trappes :
		`ndssnmpconfig "DISABLE ALL"`

Commandes de trappes	Description	Utilisation

`ENABLE`	L'activation d'une trappe signifie que la NMS reçoit les trappes lorsqu'elles sont générées.	`ndssnmpconfig "ENABLE` *`Spécification_trappe`*`"`
		
		Il peut s'agir de l'une des spécifications suivantes :
		
		Pour activer des trappes spécifiques, par exemple les trappes 10, 11 et 100 :
		
		`ndssnmpconfig "ENABLE 10, 11, 100"`
		
		Pour activer toutes les trappes, excepté les trappes 10, 11 et 100 :
		
		`ndssnmpconfig "ENABLE ID != 10, 11, 100"`
		
		Pour activer toutes les trappes comprises dans la plage allant de 20 à 30 :
		
		`ndssnmpconfig "ENABLE 20-29"`
		
		Pour activer toutes les trappes :
		
		`ndssnmpconfig "ENABLE ALL"`

`INTERVAL`	Cet utilitaire permet de définir et d'afficher l'intervalle de temps.
	
	Celui-ci correspond au nombre de secondes précédant l'envoi de trappes en double.
	
	Sa valeur doit être comprise entre 0 et 2 592 000 secondes.
	
	Si ce n'est pas le cas, l'intervalle de temps par défaut est pris en compte.
	
	S'il présente la valeur zéro, toutes les trappes sont envoyées.
		Pour afficher l'intervalle de temps :
		
		`ndssnmpconfig "213,240,79 INTERVAL"`
		
		Pour définir l'intervalle de temps entre plusieurs trappes (par exemple, pour définir un intervalle de temps de 5 entre les trappes 12, 17 et 101) :
		
		`ndssnmpconfig "12 17 101 INTERVAL 5"`
		
		Pour afficher l'intervalle de temps par défaut :
		
		`ndssnmpconfig "DEFAULT INTERVAL"`
		
		Pour définir l'intervalle de temps par défaut :
		
		`ndssnmpconfig "DEFAULT INTERVAL=10"`

Commandes de trappes	Description	Utilisation

`LIST`	Cet utilitaire permet d'afficher des listes de numéros de trappe répondant à des critères spécifiés.	ndssnmpconfig LIST <*Spécification_trappe*>
		
		La valeur Spécification_trappe permet de spécifier des groupes de numéros de trappe et peut être suivie de l'un des mots-clés suivants :
		
		`ALL`, `ENABLED`, `DISABLED`, `FAILED` ou une expression logique
		
		Exemples :
		
		Pour lister toutes les trappes activées par leur nom :
		
		`ndssnmpconfig LIST ENABLED`
		
		Pour lister toutes les trappes désactivées par nom :
		
		`ndssnmpconfig LIST DISABLED`
		
		Pour lister toutes les trappes (117) par nom :
		
		`ndssnmpconfig LIST ALL`
		
		Pour lister des trappes spécifiques telles que 12, 224 et 300 par nom :
		
		`ndssnmpconfig LIST ID = 12,224,300`
		
		Pour lister toutes les trappes, excepté celles sélectionnées, telles que 12, 224 et 300 par nom :
		
		`ndssnmpconfig LIST ID != 12,224,300`
		
		Pour lister toutes les trappes mises en échec par nom :
		
		`ndssnmpconfig LIST FAILED`

Commandes de trappes	Description	Utilisation
`READ_CFG`	Cette commande permet de modifier la configuration de l'annuaire à partir du fichier de configuration `ndstrap.cfg`. Toutes les modifications spécifiées dans ce fichier sont alors appliquées. Cet utilitaire sert principalement à regrouper plusieurs commandes dans le fichier `ndstrap.cfg` et à exécuter l'opération en une seule fois. Ce fichier est enregistré dans `/etc/ndssnmp/`. Le fichier `ndstrap.cfg` indique les paramètres opérationnels à utiliser pour configurer les trappes et permet de configurer le fonctionnement des trappes SNMP. Ce fichier est lu à chaque fois que l'utilitaire de configuration de trappes ndssnmpcfg est exécuté avec la commande `READ_CFG`.	`ndssnmpconfig "READ_CFG"`

`FAILURE`	Cette commande permet de lister toutes les trappes activées pour être mises en échec.
	
	Lorsqu'un événement échoue, une trappe d'échec est générée.
	
	REMARQUE : si la trappe est mise en échec, puis désactivée avant d'être à nouveau activée via la commande enable trapid, elle est alors activée en cas de réussite, et non d'échec.
		`ndssnmpconfig "FAILURE` *`Spécification_trappe`*`"`
		
		La valeur *`Spécification_trappe`* comporte un ou plusieurs numéros de trappe séparés par des virgules ou des espaces, du mot-clé `ALL` ou d'une expression logique.
		
		Exemples :
		
		Pour mettre plusieurs trappes en échec :
		
		`ndssnmpconfig "FAILURE 10,11,100"`
		
		Pour mettre toutes les trappes en échec, à l'exception de celles mentionnées :
		
		`ndssnmpconfig "FAILURE ID != 24,30"`
		
		Pour mettre toutes les trappes en échec :
		
		`ndssnmpconfig "FAILURE ALL"`

Statistiques

- « ndsDbCache » page 556
- « ndsDbConfig » page 557
- « ndsProtoIfOps » page 557
- « ndsServerInt » page 559

ndsDbCache

Objets gérés dans l'Annuaire	Description
ndsDbSrvApplIndex	Index permettant d'identifier de façon unique l'application serveur eDirectory.
ndsDbDibSize	Taille actuelle de la base de données eDirectory en Ko.
ndsDbBlockSize	Taille des blocs de la base de données eDirectory en Ko.
ndsDbEntryCacheMaxSize	Informations relatives à la taille maximum du cache d'entrées en Ko.
ndsDbBlockCacheMaxSize	Informations relatives à la taille maximum du cache de blocs en Ko.
ndsDbEntryCacheCurrentSize	Informations relatives à la taille actuelle du cache d'entrées.
ndsDbBlockCacheCurrentSize	Informations relatives à la taille actuelle du cache de blocs.
ndsDbEntryCacheCount	Informations relatives au nombre d'entrées du cache.
ndsDbBlockCacheCount	Informations relatives au nombre de blocs du cache.
ndsDbEntryCacheOldVerCount	Informations relatives au nombre d'entrées de la version précédente mises en cache.
ndsDbBlockCacheOldVerCount	Informations relatives au nombre de blocs de la version précédente mis en cache.
ndsDbEntryCacheOldVerSize	Informations relatives à la taille de la version précédente du cache d'entrées.
ndsDbBlockCacheOldVerSize	Informations relatives à la taille de la version précédente du cache de blocs.
ndsDbEntryCacheHits	Informations relatives au nombre d'occurrences d'entrées.
ndsDbBlockCacheHits	Informations relatives au nombre d'occurrences de blocs.
ndsDbEntryCacheHitLooks	Informations relatives au nombre d'entrées examinées pour trouver des occurrences.
ndsDbBlockCacheHitLooks	Informations relatives au nombre de blocs examinés pour trouver des occurrences.
ndsDbEntryCacheFaults	Informations relatives au nombre de pannes d'entrées.
ndsDbBlockCacheFaults	Informations relatives au nombre de pannes de blocs.
ndsDbEntryCacheFaultLooks	Informations relatives au nombre d'entrées examinées pour déterminer les occurrences manquantes.
ndsDbBlockCacheFaultLooks	Informations relatives au nombre de blocs examinés pour déterminer les occurrences manquantes.

ndsDbConfig

Objets gérés dans l'Annuaire	Description
ndsDbCfgSrvApplIndex	Index permettant d'identifier de façon unique l'application serveur eDirectory.
ndsDbCfgDynamicCacheAdjust	Informations indiquant si l'ajustement dynamique du cache est activé ou désactivé. 0 = désactivé, 1 = activé
ndsDbCfgDynamicCacheAdjustPercent	Informations sur le paramètre de pourcentage d'ajustement dynamique du cache de mémoire disponible.
ndsDbCfgDynamicCacheAdjustMin	Informations sur le paramètre de valeur minimale d'ajustement dynamique du cache. Il s'agit des valeurs de contraintes relatives à la taille du cache exprimées en Ko.
ndsDbCfgDynamicCacheAdjustMinToLeave	Informations relatives à la valeur minimale de l'ajustement dynamique du cache exprimée en Ko à soustraire de la taille totale de la mémoire disponible exprimée en Ko.
ndsDbCfgHardLimitCacheAdjust	Informations indiquant si l'ajustement de la limite stricte du cache est activé ou désactivé. 0 = désactivé, 1 = activé
ndsDbCfgHardLimitCacheAdjustMax	Information relative à la taille maximum du cache en Ko. Il s'agit d'un paramètre de limite stricte.
ndsDbCfgBlockCachePercent	Informations relatives au pourcentage du cache de blocs.
ndsDbCfgCacheAdjustInterval	Informations relatives à l'intervalle d'ajustement du cache en secondes.
ndsDbCfgCacheCleanupInterval	Information relative à l'intervalle de nettoyage du cache en secondes.
ndsDbCfgPermanentSettings	Informations indiquant si les paramètres permanents sont activés ou désactivés. 0 = désactivé, 1 = activé

ndsProtoIfOps

Objets gérés dans l'Annuaire	Description
ndsProtoIfSrvApplIndex	Index permettant d'identifier de façon unique l'application serveur eDirectory.
ndsProtoIfIndex	Index permettant d'identifier de façon unique une entrée correspondant à une interface de protocole du serveur eDirectory.
ndsProtoIfDescription	Informations relatives au port utilisé par l'interface de protocole DS.
ndsProtoIfUnauthBinds	Nombre de requêtes de liaison non authentifiées/anonymes reçues.

Objets gérés dans l'Annuaire	Description
ndsProtoIfSimpleAuthBinds	Nombre de requêtes de liaison authentifiées à l'aide de procédures d'authentification simples dans lesquelles le mot de passe est envoyé sur le réseau, au format chiffré ou en texte clair.
ndsProtoIfStrongAuthBinds	ndsProtoIfStrongAuthBinds Nombre de requêtes de liaison authentifiées à l'aide des procédures d'authentification supérieures SASL et X.500. Ceci englobe les liaisons qui ont été authentifiées à l'aide de procédures d'authentification externes.
ndsProtoIfBindSecurityErrors	Nombre de requêtes de liaison rejetées en raison d'une authentification erronée ou de références non valides.
ndsProtoIfInOps	Nombre de requêtes reçues des agents utilisateurs d'annuaire ou d'autres serveurs eDirectory.
ndsProtoIfReadOps	Nombre de requêtes de lecture reçues.
ndsProtoIfCompareOps	Nombre de requêtes de comparaison reçues.
ndsProtoIfAddEntryOps	Nombre de requêtes addEntry reçues.
ndsProtoIfRemoveEntryOps	Nombre de requêtes removeEntry reçues.
ndsProtoIfModifyEntryOps	Nombre de requêtes modifyEntry reçues.
ndsProtoIfModifyRDNOps	Nombre de requêtes modifyRDN reçues.
ndsProtoIfListOps	Nombre de requêtes de liste reçues.
ndsProtoIfSearchOps	Nombre de requêtes de recherche reçues (portant sur un objet de base, sur un niveau ou sur l'ensemble de la sous-arborescence).
ndsProtoIfOneLevelSearchOps	Nombre de requêtes de recherche portant sur un niveau reçues.
ndsProtoIfWholeSubtreeSearchOps	Nombre de requêtes de recherche reçues portant sur l'ensemble de la sous-arborescence.
ndsProtoIfExtendedOps	Nombre d'opérations avancées.
ndsProtoIfReferrals	Nombre de renvois renvoyés en réponse aux requêtes pour des opérations.
ndsProtoIfChainings	Nombre d'opérations transmises par ce serveur eDirectory aux autres serveurs eDirectory.
ndsProtoIfSecurityErrors	Nombre de requêtes reçues qui ne répondent pas aux conditions de sécurité requises.
ndsProtoIfErrors	Nombre de requêtes qui n'ont pas pu être traitées en raison d'erreurs non liées à la sécurité et aux renvois. Une opération partiellement traitée n'est pas comptabilisée comme une erreur. Les erreurs en question incluent les erreurs d'assignation de nom, de mise à jour, d'attribut et de service.
ndsProtoIfReplicationUpdatesIn	Nombre de mises à jour de réplications récupérées ou reçues par les serveurs Serveurs.
ndsProtoIfReplicationUpdatesOut	Nombre de mises à jour de réplication envoyées aux serveurs eDirectory ou exécutées par les Serveurs.

Objets gérés dans l'Annuaire	Description
ndsProtoIfInBytes	Trafic entrant, en octets, sur l'interface. Il inclut les requêtes envoyées par les agents utilisateurs d'annuaire ainsi que les réponses d'autres serveurs eDirectory.
ndsProtoIfOutBytes	Trafic sortant, en octets, sur l'interface. Comprend les réponses aux agents utilisateurs d'annuaire et aux serveurs eDirectory ainsi que les requêtes adressées à d'autres serveurs eDirectory.

ndsServerInt

Objets gérés dans l'Annuaire	Description
ndsSrvIntSrvApplIndex	Index permettant d'identifier de façon unique une application serveur eDirectory.
ndsSrvIntProtoIfIndex	Index permettant d'identifier de façon unique une entrée correspondant à une interface de protocole du serveur eDirectory.
ndsSrvIntIndex	Associé à ndsSrvIntSrvApplIndex et ndsSrvIntProtoIfIndex, cet objet constitue la clé unique permettant d'identifier la ligne conceptuelle qui contient des informations utiles sur l'interaction (tentative) entre le serveur eDirectory (correspondant à applIndex) et un serveur eDirectory homologue à l'aide d'un protocole particulier.
ndsSrvIntURL	URL du serveur eDirectory parent.
ndsSrvIntTimeOfCreation	Nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle cette ligne a été créée.
ndsSrvIntTimeOfLastAttempt	Nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle la dernière tentative de contact avec le serveur eDirectory parent a été effectuée.
ndsSrvIntTimeOfLastSuccess	Nombre total de secondes depuis minuit (24:00) du 1er janvier 1970 GMT (TU), date à laquelle la dernière tentative de contact avec le serveur eDirectory parent a abouti.
ndsSrvIntFailuresSinceLastSuccess	Nombre d'échecs depuis la dernière tentative réussie de contact avec le serveur eDirectory homologue. Si aucune tentative n'a abouti, ce compteur totalise le nombre d'échecs depuis que cette entrée a été créée.
ndsSrvIntFailures	Échecs cumulés des tentatives de contact du serveur eDirectory parent depuis la création de cette entrée.
ndsSrvIntSuccesses	Réussites cumulées des tentatives de contact du serveur eDirectory parent depuis la création de cette entrée.

Dépannage

Les fichiers journaux sont mis à jour et permettent ainsi de résoudre les problèmes qui se présentent. Ils contiennent des informations sur les erreurs qui se produisent et peuvent vous aider à résoudre les problèmes. Pour plus d'informations, reportez-vous à la section « Dépannage du protocole SNMP » page 951.

Le Tableau 18-1 indique l'emplacement par défaut des fichiers journaux du serveur pour les plates-formes Linux. Pour connaître l'emplacement du fichier `ndsd.log`, exécutez la commande `ndsconfig get n4u.server.log-file` sur l'instance d'eDirectory.

Tableau 18-1 *Emplacement du fichier journal*

Plate-forme	Sous-agent	Serveur	Maîtresse
Windows	*répertoire_installation*\nds\snmp\dssnmpsa.log	*répertoire_installation*\nds\snmp\dssnmpsrv.log	NA
Linux	/var/opt/novell/eDirectory/log/ndssnmpsa.log	/var/opt/novell/eDirectory/log/ndsd.log	/var/log/messages

19 Maintenance de NetIQ eDirectory

Pour que NetIQ eDirectory fonctionne de manière optimale, il est impératif de procéder à la maintenance de l'annuaire en vérifiant régulièrement son état de santé et en mettant à niveau ou en remplaçant le matériel lorsque cela s'avère nécessaire.

Ce chapitre traite des sujets de gestion suivants :

Performances

- « Évaluation avancée des coûts de renvoi » page 561

Vérifications de l'état de santé

- « Préservation de l'état de santé d'eDirectory » page 570
- « Ressources de surveillance » page 573

Remplacements de matériel

- « Mise à niveau du matériel ou remplacement d'un serveur » page 574

Récupération

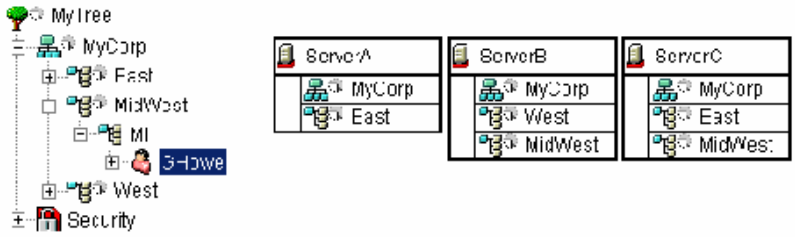
- « Restauration d'eDirectory après une panne matérielle » page 580

Évaluation avancée des coûts de renvoi

Les applications serveur communiquent souvent avec d'autres serveurs via un client intégré (Dclient), car un seul serveur ne contient pas toutes les données eDirectory nécessaires au fonctionnement d'une application. Un exemple est le protocole NLDAP, lorsqu'il est configuré pour chaîner les requêtes.

Lorsqu'une application serveur demande des données que le serveur local n'héberge pas, le serveur identifie un autre serveur qui contient les données demandées et les récupère pour le client. Ce procédé est appelé « navigation dans l'arborescence ». Évidemment, un serveur mettra plus de temps à exécuter une requête via la navigation dans l'arborescence. Même si les meilleures pratiques relatives à la conception de l'arborescence eDirectory permettent de réduire le besoin de recourir à la navigation dans l'arborescence, il est parfois encore nécessaire d'avoir recours à ce procédé.

Figure 19-1 *Évaluation avancée des coûts de renvoi*



La Figure 19-1 illlustre une recherche du nom commun `cn=GHowe` dans une sous-arborescence LDAP adressée au serveur A. La recherche commence à partir de `O=MyCorp`. Toutefois, l'objet `cn=GHowe` se trouve sur la partition `ou=MidWest`, laquelle n'est pas représentée sur le serveur A.

Pour localiser un serveur contenant les données nécessaires pour répondre à la demande du client, le serveur A doit récupérer les données sur le serveur B ou C. Pour ce faire, le serveur A doit envoyer la requête au serveur B ou C. Dans le cas présent, le serveur A choisit le serveur B. Notez que le processus de sélection du serveur est imprévisible. Le serveur B est disponible sur le réseau et accepte la requête, mais ne peut pas l'exécuter rapidement. Le serveur A attend que le serveur B traite la requête, alors que le serveur C pourrait également fournir les données requises. La requête envoyée par le serveur A est mise en attente jusqu'à ce que le serveur B l'exécute ou ne soit plus disponible sur le réseau.

Les sections suivantes expliquent comment améliorer les performances des serveurs eDirectory :

- « Amélioration de la connexion entre les serveurs » page 562
- « Avantages de la fonction d'évaluation des coûts de renvoi » page 564
- « Déploiement de l'évaluation avancée des coûts de renvoi » page 565
- « Activation de l'évaluation avancée des coûts de renvoi » page 566
- « Optimisation de l'évaluation avancée des coûts de renvoi » page 567
- « Surveillance de l'évaluation avancée des coûts de renvoi » page 568

Amélioration de la connexion entre les serveurs

Le système d'évaluation avancée des coûts de renvoi (ARC) est un algorithme d'évaluation des coûts amélioré. Il sert principalement à empêcher les pannes de serveur et peut offrir les avantages suivants :

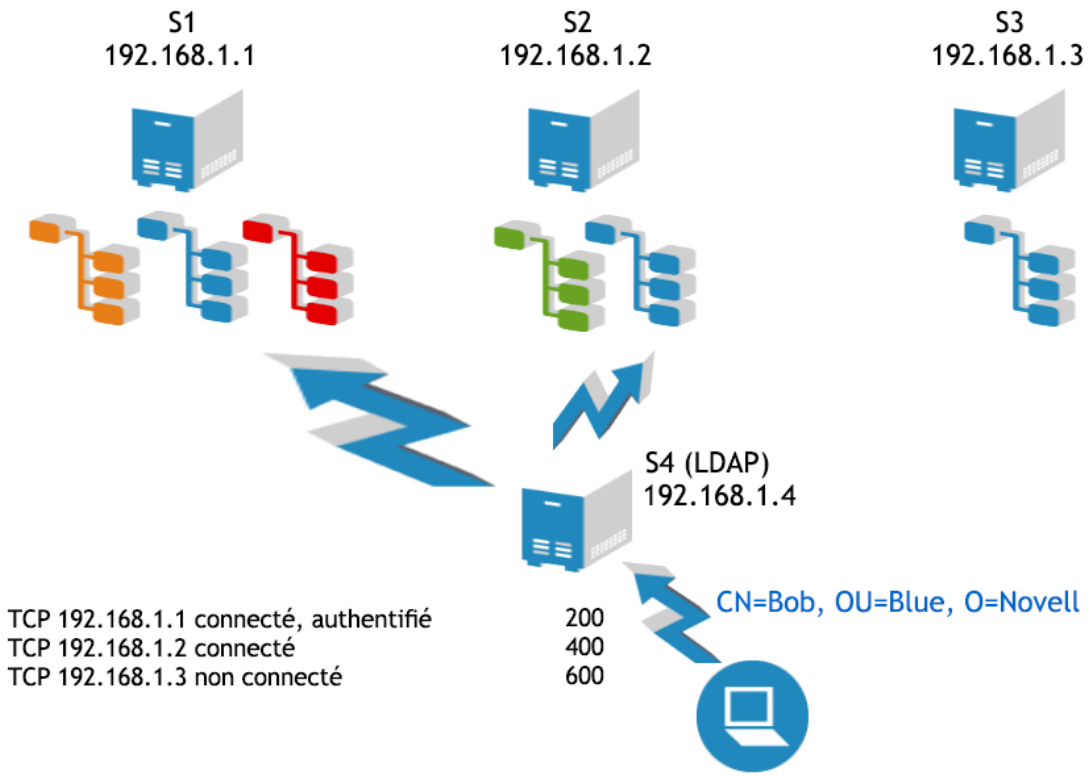
- Amélioration des performances et de la tolérance aux pannes des serveurs
- Amélioration de la communication entre les serveurs
- Distribution de la charge
- Surveillance à distance de l'état de santé des serveurs
- Distinction et identification plus aisées des problèmes de communication

À qui profite l'évaluation avancée des coûts de renvoi ?

L'évaluation avancée des coûts de renvoi est utile pour les serveurs qui n'hébergent pas une copie locale d'un objet ou d'un service et doivent parcourir l'arborescence pour trouver ces informations, car ils communiquent fréquemment avec les autres serveurs. L'évaluation avancée des coûts de renvoi est très efficace dans les environnements LDAP, en particulier lorsque le chaînage est privilégié.

La Figure 19-2 illustre le cas d'un serveur qui est parfois submergé par les demandes d'autres serveurs, qui lui adressent systématiquement leurs requêtes.

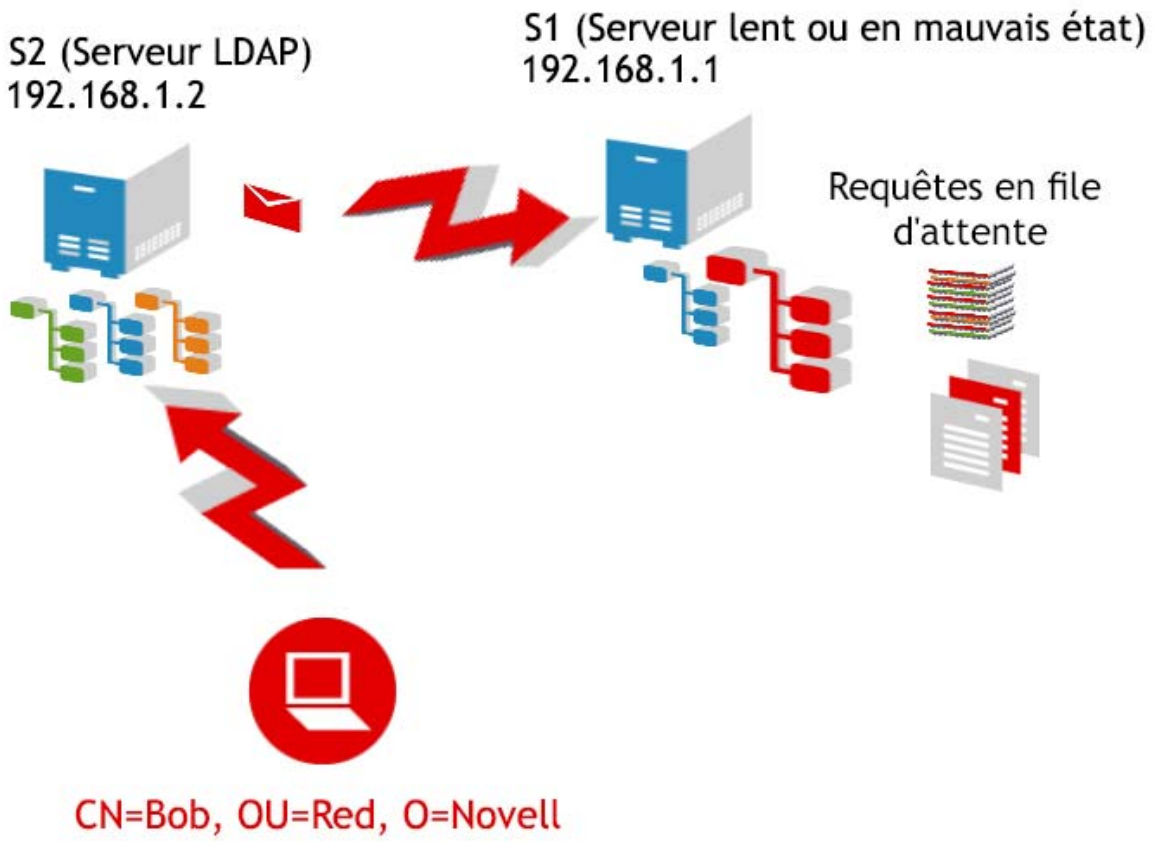
Figure 19-2 *Effet du serveur unique*



Bien que d'autres serveurs hébergeant des répliques des objets requis soient disponibles, ce serveur est systématiquement privilégié. Ceci s'explique par le fait que les serveurs qui ont besoin d'un service ou d'une réplique spécifique sont déjà connectés à ce serveur, si bien qu'ils ont tendance à lui envoyer toutes les requêtes qu'il peut traiter. La Figure 19-2 montre que toutes les requêtes émanant de S4 sont adressées à S1. S4 étant déjà connecté et authentifié auprès de S1, il continue à lui envoyer toutes les requêtes pour la partition bleue, alors que S2 et S3 pourraient aussi répondre à ces requêtes. L'évaluation avancée des coûts de renvoi permet d'éviter ces situations en répartissant la charge entre les serveurs qui répondent plus rapidement. Cette fonctionnalité doit être activée sur les serveurs distants (S4) qui sollicitent ce serveur ou peut être activée sur tous les serveurs.

La Figure 19-3 illustre un autre scénario, à savoir l'effet du « serveur en cascade ». Dans ce cas-ci, il arrive souvent que le serveur S1 ne réponde pas, sans pour autant qu'il soit hors service. S'il était hors service, les requêtes expireraient et la communication serait interrompue. Si le serveur est toujours fonctionnel au niveau du transport, mais que la base de données est lente ou occupée, le serveur continue à accepter les nouvelles requêtes provenant d'autres serveurs et les place en file d'attente. Le cas échéant, les autres serveurs (S2) peuvent finir par manquer de threads. Chaque requête en suspens prend un thread sur le serveur distant et lorsqu'il est à court de threads, le serveur ne répond plus. L'évaluation avancée des coûts de renvoi résout ce problème en répartissant les requêtes entre les serveurs les plus rapides, car le coût de traitement des requêtes est plus élevé lorsqu'un serveur est lent ou défaillant.

Figure 19-3 *Effet du serveur en cascade*



L'évaluation avancée des coûts de renvoi constitue également un excellent moyen d'améliorer la tolérance aux pannes, puisqu'elle permet d'identifier facilement les problèmes de communication des serveurs.

Avantages de la fonction d'évaluation des coûts de renvoi

- Elle prévoit/achemine la plupart des requêtes de résolution de nom vers des serveurs distants au moment où elles sont soumises.
- Elle calcule la moyenne des temps de traitement (en millisecondes) des requêtes de résolution de nom sur chaque adresse. Cela lui permet d'être plus précise et d'ajuster plus activement le coût du renvoi. Elle est également capable de détecter rapidement un serveur lent, car les temps de traitement sont calculés en millisecondes, et non en secondes.
- Elle assure le suivi des requêtes en suspens, de manière à déterminer rapidement si une requête met trop de temps à être traitée. Elle ne doit pas attendre que la requête soit traitée pour savoir que le serveur est lent.
- Elle assure le suivi des temps de réponse pour chaque adresse. Pour un serveur, il est normal d'avoir de nombreuses connexions à la même adresse. Grâce au suivi par adresse et non par connexion, une connexion peut profiter des statistiques collectées à partir d'autres connexions.

REMARQUE : pour évaluer les requêtes LDAP, la fonction d'évaluation avancée des coûts de renvoi tient également compte de la réactivité des connexions privées.

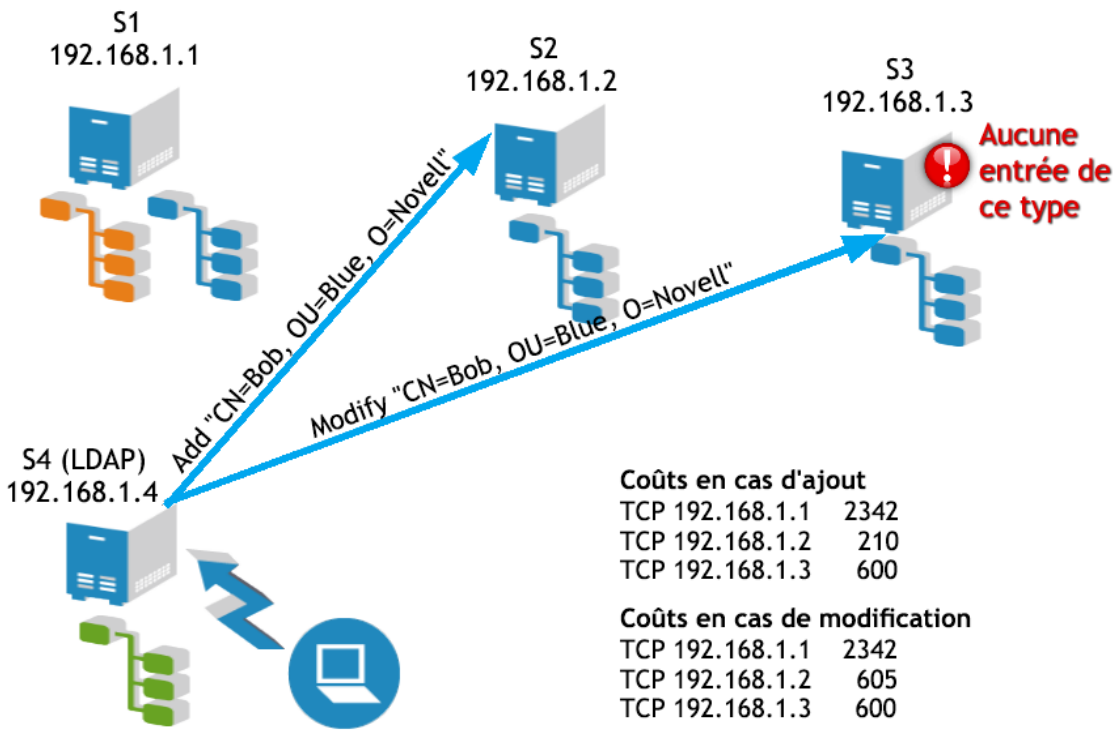
Déploiement de l'évaluation avancée des coûts de renvoi

L'évaluation avancée des coûts de renvoi est généralement déployée sur une base Serveur à serveur. Les serveurs sur lesquels l'évaluation avancée des coûts de renvoi est activée peuvent être informés des nouvelles informations relatives à l'évaluation des coûts. Vous devez activer l'évaluation avancée des coûts de renvoi sur chaque serveur de l'environnement.

Considérations sur le déploiement

Il n'est pas utile d'activer l'évaluation avancée des coûts de renvoi sur tous les serveurs. La Figure 19-4 illustre une situation susceptible de nuire à l'efficacité des serveurs LDAP. Sur la figure, le serveur S4 héberge une copie de la partition verte, mais pas de la partition bleue. Pour être exécutée, toute requête LDAP de chaînage qui requiert des informations issues de la partition bleue doit être adressée au serveur S1, S2 ou S3. L'évaluation avancée des coûts de renvoi a été précisément conçue pour faire face ce genre de situation et se révèle efficace dans la plupart des cas.

Figure 19-4 *Considérations relatives au déploiement de l'évaluation avancée des coûts de renvoi*



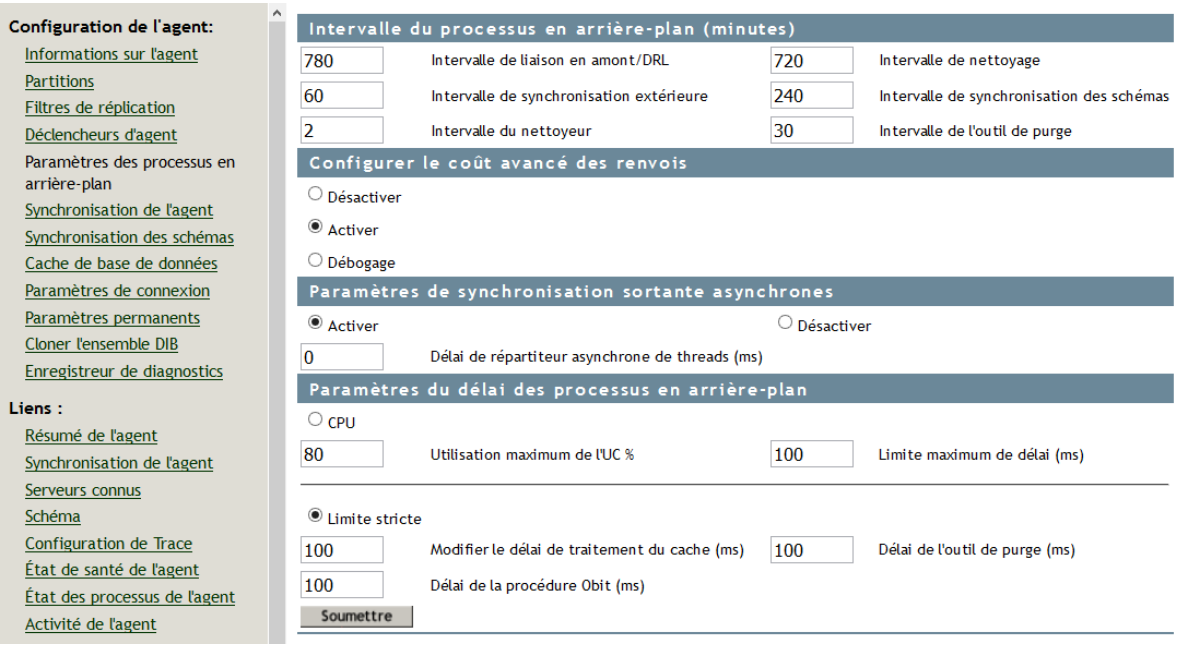
Cependant, effectuer certaines opérations LDAP peut s'avérer difficile. Ainsi, même s'il est possible d'ajouter un utilisateur, par exemple, Bob.Blue.Novell, il se peut que l'opération échoue si vous essayez immédiatement de le modifier. La figure montre que Bob a bien été ajouté sur S2, mais que sa modification sur S3 a échoué, car S3 n'a pas encore été synchronisé avec S2 ou n'a pas encore reçu Bob. L'évaluation avancée des coûts de renvoi a la capacité de vous diriger vers un autre serveur, car elle est plus dynamique que la méthode standard d'évaluation des coûts.

Cette configuration fonctionne bien lorsque les serveurs présentent des coûts qui ne varient pas énormément et n'ont pas de problèmes de synchronisation. La désactivation de l'évaluation avancée des coûts de renvoi sur S4 permet de résoudre ce problème.

Activation de l'évaluation avancée des coûts de renvoi

L'évaluation avancée des coûts de renvoi est activée par défaut pour eDirectory. Pour la configurer à l'aide de NDS iMonitor, cliquez sur **Configuration de l'agent**, puis sur **Paramètres des processus en arrière-plan**. Les options **Activer**, **Désactiver** et **Débogage** sont également disponibles.

Figure 19-5 *Écran de configuration d'agent de NDS iMonitor*



NDSTrace

Pour activer l'évaluation avancée des coûts de renvoi sur toutes les plates-formes UNIX, utilisez l'outil NDSTrace.

Tableau 19-1 *Activation de l'évaluation avancée des coûts de renvoi sous UNIX*

`set NDSTRACE =!ARC`	Affiche le tableau gv_ResolveTimesTable à des fins de débogage.
`set NDSTRACE =!ARC0`	Désactive l'évaluation avancée des coûts de renvoi.
`set NDSTRACE =!ARC1`	Active l'évaluation avancée des coûts de renvoi.
`set NDSTRACE =!ARC2`	Active l'évaluation avancée des coûts de renvoi en mode débogage et affiche les coûts occasionnés par chaque renvoi sur le drapeau DSTrace de résolution de nom à chaque fois qu'une décision est prise en matière d'évaluation des coûts.

Optimisation de l'évaluation avancée des coûts de renvoi

Par défaut, l'évaluation avancée des coûts de renvoi ne doit pas être optimisée. Toutefois, il est possible de configurer des paramètres pour modifier le fonctionnement de l'évaluation avancée des coûts de renvoi, ou pour désactiver ou activer certaines fonctions. L'évaluation avancée des coûts de renvoi inclut 3 composants majeurs.

Évaluation avancée des coûts

Pour évaluer les coûts d'une adresse donnée, le système d'évaluation avancée des coûts de renvoi utilise les informations connues à propos de la connexion pour calculer le coût du renvoi en question. Si la fonction ARC est activée, l'évaluation avancée des coûts est toujours utilisée pour calculer le coût d'un renvoi.

Surveillance en arrière-plan

Un thread d'arrière-plan vérifie régulièrement les informations de l'horloge pour s'assurer qu'elles sont à jour. Lorsqu'un serveur est lent, son coût augmente et il est fort probable que la communication soit interrompue. Le thread d'arrière-plan vérifie régulièrement (par défaut, toutes les minutes) si un serveur présent dans le tableau n'a pas été mis à jour. Si le serveur n'a pas été mis à jour au cours des trois dernières minutes, le serveur effectue, en son nom, une demande de résolution de nom afin de vérifier son état de santé. Cette opération permet de créer une évaluation actualisée des coûts du serveur et de déterminer si ce dernier est maintenant moins occupé, ou en bonne santé, afin qu'un client ne doive pas subir des effets néfastes pour vérifier l'état de santé du serveur. Deux paramètres de configuration permanents peuvent être modifiés pour le thread d'arrière-plan :

- **ARC_MAX_WAIT :** délai de péremption d'une horloge avant qu'une requête de vérification d'état de santé ne soit envoyée au serveur (par défaut, 180 secondes).
- **ARC_BG_INTERVAL :** fréquence d'exécution du thread d'arrière-plan (par défaut, 60 secondes ; si ce paramètre est défini sur 0, il est désactivé et le thread ne s'exécute pas).

Pour plus d'informations, reportez-vous à la section 8.4.24 relative à la définition de paramètres de configuration permanents.

Informations d'état de santé distantes

Les serveurs utilisant l'évaluation avancée des coûts de renvoi demandent périodiquement des informations d'état de santé à un serveur distant. Il ne s'agit pas de requêtes supplémentaires sur le réseau, mais d'informations d'état de santé complémentaires renvoyées dans les requêtes de résolution de nom standard régulièrement envoyées par les serveurs. Ces informations sont ensuite utilisées par l'algorithme d'évaluation des coûts afin d'améliorer les réactions par rapport aux serveurs qui présentent une charge importante. Lorsqu'une demande de résolution de nom est envoyée à un serveur distant, si plus de 15 secondes se sont écoulées depuis la dernière mise à jour, les informations d'état de santé sont demandées au serveur distant et sont ajoutées à la réponse à la demande de résolution de nom.

Un paramètre peut être réglé pour la surveillance de l'état de santé à distance :

- **ARC_DS_INFO_INTERVAL :** fréquence à laquelle les informations de verrouillage (état de santé) sont demandées dans le cadre de l'évaluation avancée des coûts de renvoi (par défaut, 15 secondes).

Surveillance de l'évaluation avancée des coûts de renvoi

Pour assurer le suivi de l'évaluation avancée des coûts de renvoi, vous pouvez imprimer le tableau des temps de résolution.

Pour ce faire, utilisez les commandes suivantes :

- `set DSTRACE = +DBG`
- `set DSTRACE = !ARC`

Ces commandes permettent d'imprimer le tableau des temps de résolution et les informations actuellement stockées pour chaque serveur. Ce tableau indique l'adresse de transport, le nombre de millisecondes écoulées depuis la dernière utilisation de l'adresse, le dernier coût utilisé dans une décision de renvoi et le nombre de requêtes en suspens pour cette adresse.

Un grand nombre de requêtes en suspens n'est pas nécessairement problématique. Cela peut simplement signifier que ce serveur est fréquemment utilisé.

Utilisation de l'évaluation avancée des coûts de renvoi à des fins de dépannage

L'une des fonctions les plus utiles de l'évaluation avancée des coûts de renvoi est sa capacité à identifier rapidement les problèmes de communication des serveurs.

Le tableau ci-dessous est un exemple de tableau des temps de résolution au format imprimé.

L'évaluation avancée des coûts de renvoi est actuellement activée.

Tableau 19-2 *Coûts associés aux temps de résolution*

Slot	Transport Address	Cost	LastUse	Checked	#Req	Waiters	LockTime
1	tcp:151.155.134.27:524	214	14	14	0	0	0
2	tcp:151.155.134.11:524	0	0	0	0	0	0
3	udp:151.155.134.11:524	0	0	0	0	0	0
4	cp:151.155.134.13:524	554 759	280	0	0	27	582
5	tcp:151.155.134.59:524	0	179	179	0	0	0
6	udp:151.155.134.59:524	0	119	119	0	0	0
7	tcp:151.155.134.28:524	1 543	119	119	0	0	0
8	tcp:151.155.134.15:524	124	14	14	0	0	0

La version imprimée du tableau montre que du point de vue de ce serveur, l'adresse 151.155.134.13 rencontre des difficultés. On peut également voir que le problème vient très probablement du serveur, et non du transport. Le serveur compte 27 demandes d'accès à la base de données qui sont en attente, et les requêtes prennent énormément de temps à obtenir le verrouillage de la base de données. Ce serveur compte deux requêtes qui n'ont jamais reçu de réponse de la part du serveur distant.

On peut également voir que les serveurs 151.155.134.11 et 151.155.134.59 sont très rapides, ne sont pas fortement sollicités ou les deux. On voit que les serveurs 151.155.134.59 et 151.155.134.11 ont tous deux eu des problèmes de communication via le protocole TCP à un moment donné, mais

qu'il sont désormais en bonne santé, car ils disposent tous deux de connexions UDP. Les connexions UDP à un serveur ne sont utilisées qu'en cas de problème de communication avec ce serveur via le protocole TCP.

Les différents champs du tableau sont expliqués ci-dessous :

Transport Address : adresse du serveur distant.

Cost : coût actuel du serveur distant.

Last Use : nombre de secondes écoulées depuis la dernière communication avec le serveur.

Checked : nombre de secondes écoulées depuis la dernière fois que des informations d'état de santé ont été obtenues de la part du serveur distant.

#Req : nombre de requêtes en suspens adressées au serveur distant.

Waiters : nombre de requêtes adressées au serveur distant en attente du verrouillage de la base de données.

LockTime : période pendant laquelle un processus a maintenu la base de données verrouillée sur le serveur distant.

Le tableau ci-après montre bien que l'évaluation avancée des coûts de renvoi permet d'identifier rapidement un problème de communication, car on peut voir que le serveur ne peut pas communiquer actuellement avec 151.155.134.13 via le protocole TCP.

L'évaluation avancée des coûts de renvoi est actuellement activée.

Tableau 19-3 *Coûts associés aux temps de résolution*

Slot	Transport Address	Cost	LastUse	Checked	#Req	Waiters	LockTime
1	tcp:151.155.134.27:524	394	92	14	0	0	0
2	tcp:151.155.134.11:524	0	0	0	0	0	0
3	udp:151.155.134.11:524	0	0	0	0	0	0
4	tcp:151.155.134.13:524	5 000 000	180	180 est dans le CACHE DES ADRESSES INCORRECTES.			

Lorsque vous consultez ces tableaux, gardez ceci à l'esprit :

- Les requêtes en suspens ne sont pas nécessairement problématiques. En effet, il se peut que le serveur ait simplement de nombreuses requêtes à traiter. En revanche, elles constituent un problème lorsqu'elles sont adressées à un serveur dont le coût est élevé.
- Le premier indicateur de l'état de santé d'un serveur est le coût actuel, lequel permet d'identifier facilement les serveurs problématiques.

REMARQUE : le temps d'aller-retour et la durée d'attente sont mesurés pour toutes les requêtes. Autrement dit, les temps de transport sont également pris en compte dans le calcul du coût. Si un serveur semble problématique selon ce tableau, mais fonctionne correctement indépendamment d'autres serveurs et ne présente manifestement aucun problème, le problème est peut être lié au transport.

Traces de thread d'arrière-plan

Le message ci-dessous est une trace montrant l'exécution de la tâche ARCBackgroundResolveTimerThread :

```
ARCBackGroundResolveTimerThread started Interval = 60 MaxWait = 180000

Updating timer info for tcp:151.155.134.11:524

Updating timer info for udp:151.155.134.11:524

Updating timer info for tcp:151.155.134.13:524 ARCBackGroundResolveTimerThread
error -635 in DCConnectToAddress for tcp:151.155.134.59:524

ARCBackGroundResolveTimerThread completed in 0 seconds

8-total timers 4-stale timers 3-timers updated
```

La trace ci-dessus révèle que :

- l'adresse TCP:151.155.134.11 n'a pas été utilisée pendant plus de 3 minutes ;
- l'adresse UDP:151.155.134.11 n'a pas été utilisée pendant plus de 3 minutes ;
- l'adresse TCP:151.155.134.13 n'a pas été utilisée pendant plus de 3 minutes.

Les informations de l'horloge ont été mises à jour pour tous les serveurs ci-dessus, avec les résultats suivants :

- l'adresse TCP:151.155.134.59 n'est toujours pas accessible à partir de ce serveur.

La nouvelle évaluation des coûts est très dynamique et change très fréquemment. Pour suivre son évolution, vous pouvez définir le paramètre d'évaluation avancée des coûts de renvoi (ARC) en mode Débogage.

REMARQUE : une fois que vous avez fini de surveiller l'évaluation des coûts, veillez à désactiver le mode Débogage pour le paramètre ARC en exécutant la commande `set NDSTRACE = !ARC1`. S'ils ne sont pas indispensables, mieux vaut éviter des frais généraux d'impression.

Si les paramètres ARC et +RSLV sont activés, vous pouvez voir les coûts de renvoi individuels dans l'utilitaire DSTrace ou NDSTrace. Les balises restantes sont désactivées à l'aide de la commande `set NDSTrace =nodebug`.

```
Sorted results from DCAdjustCostAndSort follow:

137.65.10.3 cost of 217

137.65.10.9 cost of 222

137.65.10.10 cost of 400
```

Si un serveur distant est lent ou surchargé, les chiffres changent rapidement. L'évaluation des coûts du serveur ExRef s'ajuste dynamiquement toutes les secondes. Pour suivre l'évolution des coûts au fil du temps, il est donc recommandé de publier la trace dans un fichier journal.

Préservation de l'état de santé d'eDirectory

Le bon fonctionnement des services Annuaire est essentiel à toute organisation. Des vérifications régulières de l'état de santé d'eDirectory à l'aide de NetIQ iMonitor assurent le bon fonctionnement de votre annuaire et facilitent considérablement les mises à niveau et les opérations de dépannage.

Fréquence des vérifications de l'état de santé

En règle générale, si votre réseau ne change pas souvent (si vous n'ajoutez des serveurs et des partitions que tous les deux ou trois mois et ne réalisez habituellement que de simples modifications), il est recommandé de procéder à ces vérifications une fois par mois.

En revanche, si votre réseau est plus dynamique (si vous ajoutez toutes les semaines des partitions ou des serveurs, ou que votre entreprise est en pleine restructuration), il est recommandé de réaliser ce contrôle une fois par semaine.

Définissez la fréquence des vérifications de l'état de santé au fur et à mesure de l'évolution de votre environnement. Les facteurs qui ont une influence sur la planification des vérifications d'état de santé sont notamment les suivants :

- Nombre de partitions et de répliques
- Stabilité des serveurs hébergeant les répliques
- Quantité d'informations dans une partition eDirectory
- la taille et la complexité des objets ;
- le nombre d'erreurs lors de précédentes exécutions de DSRepair.

Lorsque vous effectuez une vérification de l'état de santé, iMonitor rassemble des informations provenant de tous les serveurs, en fonction de droits donnés. Sachez que l'exécution de rapports sur l'état de santé augmente le trafic réseau et consomme de l'espace disque.

Présentation de la vérification de l'état de santé

La vérification complète de l'état de santé porte sur les éléments suivants :

- Version d'eDirectory

  L'exécution de différentes versions de NDS ou d'eDirectory sur le même serveur peut causer des problèmes de synchronisation. Si votre version de NDS ou d'eDirectory est obsolète, téléchargez le dernier correctif logiciel à partir du site Web relatif à la sécurité et aux correctifs (http://support.novell.com/patches.html).
- Synchronisation horaire

  Tous les serveurs eDirectory doivent prendre en charge l'heure exacte. Des tampons horaires associés à chaque objet et propriété garantissent que les mises à jour de ces objets et propriétés sont classées dans le bon ordre. Ils permettent à eDirectory de déterminer les répliques qui doivent être synchronisées.
- Tolérances de synchronisation

  Périodes depuis lesquelles un serveur s'est synchronisé en intégrant les changements de données entrantes et sortantes, les quantités de données en attente, etc.
- Processus en arrière-plan

  Processus qui effectuent différentes tâches, notamment la réplication des changements et la mise à jour des informations système.
  - Références externes
  - Notices nécrologiques
  - Schéma eDirectory

Pour connaître la procédure détaillée permettant d'effectuer ces vérifications, reportez-vous à la « Contrôle de l'état de santé d'eDirectory à l'aide d'iMonitor » page 572.

Contrôle de l'état de santé d'eDirectory à l'aide d'iMonitor

En fonction de vos préférences, vous pouvez effectuer une vérification de l'état de santé du serveur eDirectory en utilisant l'une ou l'autre des méthodes proposées dans iMonitor :

- Utilisation du cadre du navigateur
- Utilisation du cadre de l'assistant

Utilisation du cadre du navigateur

1. Accédez à iMonitor.

   Reportez-vous à la « Accès à iMonitor » page 241.

2. Dans le cadre du navigateur, cliquez sur l'icône de rapport .
3. Dans le cadre de l'assistant, cliquez sur le lien **Configuration du rapport**.

   La liste des rapports pouvant être exécutés s'affiche dans le cadre des données.

4. Cliquez sur l'icône Configurer le rapport pour définir les informations que vous souhaitez obtenir sur les serveurs.

   Un rapport d'information sur le serveur s'affiche dans le cadre des données. Utilisez-le pour sélectionner les options souhaitées pour votre rapport.

5. Cochez la case **Sous-rapport de santé**.
6. Pour exécuter le rapport à intervalles donnés, sélectionnez les options requises dans la section Planifier le rapport du cadre des données.

   IMPORTANT : si vous exécutez un rapport planifié, il s'exécutera comme public et risque de ne pas rassembler autant d'informations qu'il le ferait s'il s'exécutait comme utilisateur authentifié.

7. Cliquez sur **Exécuter le rapport** pour le traiter.

Utilisation du cadre de l'assistant

1. Accédez à iMonitor.

   Reportez-vous à la « Accès à iMonitor » page 241.

2. Dans le cadre de l'assistant, cliquez sur **État de santé de l'agent**.

   Les informations sur la vérification de l'état de santé s'affichent dans le cadre des données correspondant au serveur sur lequel iMonitor lit ces informations (qui n'est pas nécessairement celui auquel vous êtes connecté).

Étude des informations du rapport

Une fois le rapport généré, le cadre des données affiche les résultats. Si l'état de santé de certains serveurs de votre arborescence laisse à désirer, le rapport est divisé en trois catégories (en commençant par les serveurs en moins bonne santé) :

- Serveurs avec signalement d'avertissements
- Serveurs présentant des signes suspects
- Serveurs en bonne santé

Si aucun de vos serveurs n'affiche d'avertissement ou ne présente de signes suspects, ces catégories n'apparaissent pas.

Pour les serveurs qui ne sont pas en bonne santé, vous pouvez cliquer sur le lien Sous-rapport d'état de santé de l'agent situé en regard de chaque serveur. Utilisez l'aide contextuelle en ligne pour résoudre les problèmes. Cette aide vous permet de connaître la signification et l'importance de chacune des options, de résoudre les problèmes éventuels, d'ajuster les plages et de déterminer si vous souhaitez inclure certaines options dans la vérification de l'état de santé.

IMPORTANT : si des avertissements sont signalés pour un serveur, il est vivement recommandé de résoudre les problèmes correspondants. Cela s'applique également aux serveurs qui présentent des signes suspects.

Pour plus d'informations

Les techniques et outils utilisés pour préserver l'état de santé d'eDirectory sont décrits dans la formation 3007 relative au diagnostic et aux outils d'eDirectory. Dans ce cours, vous apprendrez à :

- effectuer des vérifications de l'état de santé ;
- effectuer convenablement les opérations eDirectory ;
- diagnostiquer, dépanner et résoudre les problèmes eDirectory ;
- exécuter les outils et utilitaires de dépannage ;

Pour plus d'informations sur ce cours, visitez le site Web des services de formation NetIQ (https://www.netiq.com/training/).

Ressources de surveillance

L'utilitaire NetIQ DSTrace s'exécute sous Windows et Linux. Cet outil permet de surveiller les nombreuses ressources d'eDirectory. Pour plus d'informations sur DSTrace, reportez-vous aux sources suivantes :

- « Configuration des paramètres Trace » page 253
- Looking Into the Directory Services Trace (DSTrace) Options (http://support.novell.com/techcenter/articles/anp20010801.html) (Recherche dans les options de DSTrace)
- More on Using the DSTrace Command (http://support.novell.com/techcenter/articles/anp20010901.html) (Complément d'information sur l'utilisation de la commande DSTrace)

Vous pouvez également investir dans des produits tiers qui offrent des solutions de gestion complémentaires pour votre environnement eDirectory. Pour plus d'informations, visitez les sites Web suivants :

- Symantec (http://www.symantec.com/compliance/)
- Blue Lance (http://www.bluelance.com)
- Quest (http://www.quest.com/active-directory/)

Si vous devez surveiller ou auditer certaines caractéristiques d'eDirectory non proposées par nos partenaires, les services NetIQ Consulting peuvent vous aider à utiliser le système d'événements NetIQ pour procéder à une évaluation ou à un audit personnalisé.

Mise à niveau du matériel ou remplacement d'un serveur

Cette section explique comment transférer et protéger eDirectory sur un serveur spécifique, lorsque vous effectuez une mise à niveau du matériel ou remplacez celui-ci. Elle se fonde sur des informations figurant à la section « Sauvegarde et restauration de NetIQ eDirectory » page 443.

L'outil Backup eMTool vous permet de préparer les informations eDirectory sur un serveur pour effectuer les opérations suivantes :

- « Mise à niveau planifiée du matériel ou d'un périphérique de stockage sans remplacement du serveur » page 574
- « Remplacement planifié d'un serveur » page 577

Mise à niveau planifiée du matériel ou d'un périphérique de stockage sans remplacement du serveur

Si vous envisagez de mettre à niveau le matériel, par exemple un périphérique de stockage ou de la mémoire RAM, commencez par effectuer une sauvegarde à froid d'eDirectory à l'aide de Backup eMTool, ainsi qu'une sauvegarde du système de fichiers. Vous pourrez ainsi sauvegarder l'identité eDirectory et les données du système de fichiers du serveur, ce qui présente les avantages suivants :

- Si vous remplacez des périphériques de stockage, les sauvegardes vous permettent de transférer des informations des anciens périphériques vers les nouveaux.
- Si vous remplacez le périphérique de stockage qui contient le volume/la partition de disque où est stocké eDirectory, les informations de sauvegarde vous permettent également d'utiliser le processus de restauration pour recréer la base de données eDirectory sur le nouveau périphérique.
- En effectuant une sauvegarde à froid d'eDirectory et en gardant la base de données fermée ensuite, vous pouvez mettre à niveau le matériel et transférer la base de données sans vous préoccuper de savoir si elle a changé depuis la dernière sauvegarde.
- En cas de problème, vous disposez de sauvegardes pour la récupération des données.

Pour la sauvegarde à froid d'eDirectory, vous devez utiliser les options de verrouillage et de désactivation d'eDirectory sur le serveur pour empêcher toute modification des données après la sauvegarde. Pour les autres serveurs qui communiquent normalement avec ce serveur, le serveur semble être arrêté. Toutes les informations eDirectory qui sont normalement envoyées au serveur sont stockées dans l'arborescence jusqu'à ce que les communications avec le serveur reprennent. Les informations stockées servent à synchroniser le serveur lors de sa remise en ligne.

REMARQUE : étant donné que d'autres serveurs de l'arborescence eDirectory attendent la remise en ligne rapide du serveur, vous devez effectuer la mise à niveau et restaurer les informations eDirectory du serveur dès que possible.

Pour effectuer une mise à niveau planifiée du matériel, procédez comme suit :

1. Si vous pensez que la mise à niveau risque d'entraîner un problème pour votre serveur, vous pouvez préparer une autre machine pour l'utiliser, si nécessaire.

   Reportez-vous à l'étape « 1. Préparation du remplacement d'un serveur » page 577.

2. Utilisez une commande client similaire à celle ci-dessous pour effectuer une sauvegarde à froid de la base de données eDirectory et maintenir celle-ci fermée et verrouillée une fois l'opération terminée. Si vous utilisez NICI, veillez à sauvegarder aussi les fichiers de sécurité.

```
backup -f backup_filename_and_path
-l log_filename_and_path -t -c -o -d
```

Si vous utilisez NICI, veillez à sauvegarder les fichiers NICI. Pour plus d'informations sur l'utilisation du client et des paramètres, reportez-vous aux sections « Sauvegarde manuelle avec DSBK » page 470 et « Options de ligne de commande pour la sauvegarde et la restauration » page 474.

La base de données eDirectory est à présent verrouillée. Vous devez la laisser verrouillée pour empêcher toute modification des données sur ce serveur tant que vous n'avez pas terminé la procédure.

Terminez rapidement la procédure afin de réduire au maximum le temps d'indisponibilité du serveur.

3 Sauvegardez le système de fichiers au moyen de l'outil de votre choix.

Il est important d'effectuer cette opération *après* avoir sauvegardé la base de données, afin que les fichiers de sauvegarde d'eDirectory soient enregistrés sur bande avec le reste du système de fichiers.

4 Arrêtez le serveur et remplacez le matériel.

5 Après avoir remplacé le matériel, suivez les instructions correspondant à la modification apportée :

Si vous…	Exécutez ces procédures générales
N'avez pas modifié les unités de stockage	Démarrez le serveur et déverrouillez la base de données.
Avez remplacé des unités de stockage, mais sans modifier la partition de disque/le volume contenant eDirectory	1. Démarrez le serveur et eDirectory. 2. Restaurez le système de fichiers uniquement pour les partitions de disque/les volumes qui se trouvaient sur les unités de stockage que vous avez remplacées. 3. Déverrouillez la base de données eDirectory.

Si vous…	Exécutez ces procédures générales
Avez remplacé le périphérique de stockage qui contenait eDirectory	1. Installez le système d'exploitation, si nécessaire. 2. Restaurez le système de fichiers sur les volumes concernés par le changement d'unité de stockage. 3. Installez eDirectory sur la nouvelle unité de stockage, dans une nouvelle arborescence temporaire. 4. Restaurez eDirectory à partir de la sauvegarde (ce qui rétablit l'arborescence d'origine), en spécifiant l'option qui permet de le maintenir fermé et verrouillé après la restauration. Utilisez une commande similaire à la suivante : `restore -r -f` *`nom_fichier_et_chemin_sauvegarde`* `-l` *`nom_fichier_et_chemin_journal`*. Si vous avez sauvegardé les fichiers répertoriés dans un fichier d'inclusion et que vous restaurez des fichiers NICI séparément, ajoutez l'option `-u`. 5. Déverrouillez la base de données eDirectory. 6. Si vous avez restauré les fichiers de sécurité NICI, après avoir terminé la restauration, redémarrez le serveur pour réinitialiser le système de sécurité. 7. Vérifiez si le serveur répond normalement. Utilisez iMonitor pour contrôler le serveur et sa synchronisation. 8. Si vous avez utilisé la consignation de transactions individuelles par fichier sur ce serveur, veillez à recréer la configuration des fichiers journaux de transactions individuelles, une fois la restauration terminée. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète. Comme ces paramètres reprennent leur valeur par défaut après une restauration, la consignation de transactions individuelles par fichier est désactivée. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Si le serveur ne répond pas comme d'habitude, vous devrez peut-être procéder à une récupération en appliquant l'une des deux méthodes ci-après :

- Recréez la configuration matérielle précédente, puisqu'elle fonctionnait avant le changement.
- Transférez l'identité du serveur vers une autre machine au moyen des sauvegardes du système de fichiers et d'eDirectory que vous avez effectuées. Reportez-vous à la section « Remplacement planifié d'un serveur » page 577.

Remplacement planifié d'un serveur

Les instructions suivantes concernent les cas où le remplacement du serveur s'opère par le déplacement de son identité eDirectory et des données de son système de fichiers vers une autre machine. L'ancien serveur est appelé serveur A et le nouveau serveur, ou serveur de remplacement, serveur B.

Il convient, au préalable, d'effectuer une sauvegarde à froid d'eDirectory (c'est-à-dire pendant que la base de données est fermée) à l'aide de l'outil Backup eMTool, ainsi qu'une sauvegarde du système de fichiers à l'aide de l'outil de votre choix. Ces données de sauvegarde vous permettent d'utiliser le processus de restauration pour recréer le serveur sur la nouvelle machine.

Pour la sauvegarde à froid d'eDirectory, vous devez utiliser les options de verrouillage et de désactivation d'eDirectory sur le serveur A pour empêcher toute modification des données après la sauvegarde. Pour les autres serveurs qui communiquent normalement avec ce serveur, le serveur semble être arrêté. Toutes les informations eDirectory qui sont normalement envoyées au serveur sont stockées dans l'arborescence jusqu'à ce que les communications avec le serveur reprennent. Les informations stockées servent à synchroniser le serveur lorsque vous le remettez en ligne sur la nouvelle machine, à savoir le serveur B.

REMARQUE : étant donné que d'autres serveurs de l'arborescence eDirectory attendent la remise en ligne rapide du serveur, vous devez effectuer le changement et la restauration des informations eDirectory sur le serveur dès que possible.

Suivez la procédure générale suivante pour remplacer un serveur :

1. Pour réduire le temps d'arrêt du serveur A durant son remplacement, il est préférable de préparer le serveur B du mieux possible avant de commencer la procédure, en installant le système d'exploitation, etc., comme indiqué à l'étape « 1. Préparation du remplacement d'un serveur » page 577.
2. Effectuez les sauvegardes d'eDirectory et du système de fichiers sur le serveur A, comme expliqué à l'étape « 2. Création d'une sauvegarde d'eDirectory » page 578.
3. Transférez les informations vers le serveur B, comme décrit à l'étape « 3. Restauration des informations eDirectory pour le remplacement d'un serveur » page 579.

1. Préparation du remplacement d'un serveur

Utilisez, pour les serveurs A et B, les listes de contrôle suivantes afin de déterminer si vous êtes prêt à remplacer le serveur A. En préparant préalablement le serveur B, vous réduirez le temps d'inactivité du serveur durant le transfert d'une machine vers l'autre.

Préparation du serveur A

- ❒ Assurez-vous que la dernière version du système d'exploitation est installée sur le serveur A.
- ❒ Vérifiez l'état de santé de l'arborescence du serveur A en exécutant DSRepair sur le serveur contenant la réplique maîtresse de la partition racine et en exécutant une synchronisation horaire.
- ❒ Exécutez DSRepair sur la base de données du serveur A. Vérifiez que celui-ci est entièrement synchronisé.

Préparation du serveur B

- ❒ Installez la dernière version du système d'exploitation. Il doit s'agir du même système d'exploitation que celui du serveur A.
- ❒ Installez eDirectory en plaçant le serveur B dans une nouvelle arborescence temporaire.

  (Si vous restaurez eDirectory durant l'étape « 3. Restauration des informations eDirectory pour le remplacement d'un serveur » page 579, le serveur B sera placé dans l'arborescence d'origine qui était celle du serveur A.)

Passez à l'étape « 2. Création d'une sauvegarde d'eDirectory » page 578 ci-dessous.

2. Création d'une sauvegarde d'eDirectory

Vous devez créer une sauvegarde d'eDirectory avant de remplacer un serveur. Après avoir effectué l'étape « 1. Préparation du remplacement d'un serveur » page 577, utilisez le client pour effectuer une sauvegarde à froid de la base de données eDirectory sur le serveur A, au moyen des options avancées pour désactiver et verrouiller cette base après la sauvegarde.

Pour effectuer une sauvegarde à froid d'eDirectory (c'est-à-dire pendant que la base de données est fermée) et maintenir ensuite la base de données fermée, procédez comme suit :

1. Assurez-vous d'avoir terminé l'étape « 1. Préparation du remplacement d'un serveur » page 577.
2. Utilisez une commande de `sauvegarde` similaire à celle ci-dessous dans le client, en précisant les paramètres `-c`, `-o` et `-d` pour effectuer une sauvegarde à froid de la base de données eDirectory sur le serveur A et la maintenir fermée et verrouillée une fois l'opération terminée :

   ```
   backup -f nom_et_chemin_fichier_sauvegarde -l nom_et_chemin_fichier_journal -t
   -c -o -d
   ```

   Si vous utilisez NICI, veillez à sauvegarder les fichiers NICI. Pour plus d'informations sur l'utilisation du client et des paramètres, reportez-vous aux sections « Sauvegarde manuelle avec DSBK » page 470 et « Options de ligne de commande pour la sauvegarde et la restauration » page 474.

   La base de données eDirectory du serveur A est à présent verrouillée. Vous devez la maintenir verrouillée afin que les nouvelles modifications apportées aux données soient reportées sur ce serveur jusqu'à ce que vous le replaciez dans l'arborescence en le restaurant sur le serveur B.

   Terminez rapidement la procédure de mise à niveau/restauration du serveur afin de réduire au maximum le temps d'indisponibilité de ce dernier.
3. Effectuez une sauvegarde complète du système de fichiers du serveur A.

   Il est important d'effectuer cette opération *après* avoir sauvegardé la base de données, afin que les fichiers de sauvegarde d'eDirectory soient enregistrés sur bande avec le reste du système de fichiers.

   Pour plus d'informations sur l'utilisation de SMS, reportez-vous au *Storage Management Services Administration Guide* (http://www.novell.com/documentation/oes/smsadmin/data/hjc2z4tu.html) (Guide d'administration de SMS).
4. Verrouillez la base de données eDirectory sur le serveur A et déconnectez celui-ci du réseau.

   Passez à l'étape « 3. Restauration des informations eDirectory pour le remplacement d'un serveur » page 579.

3. Restauration des informations eDirectory pour le remplacement d'un serveur

Pour transférer l'identité eDirectory et le système de fichiers d'un serveur A vers un serveur B :

1. Assurez-vous d'avoir terminé les étapes « 1. Préparation du remplacement d'un serveur » page 577 et « 2. Création d'une sauvegarde d'eDirectory » page 578.
2. Vérifiez que le serveur B et eDirectory fonctionnent.
3. Utilisez la fonction de restauration pour transférer l'identité eDirectory et le système de fichiers du serveur A vers le serveur B :

   3a Copiez les fichiers de sauvegarde à froid eDirectory du serveur A vers le serveur B.

   En utilisant un outil de compression tiers, vous pouvez sensiblement réduire la taille des fichiers de sauvegarde, car ceux-ci offrent un taux de compression élevé. Cela peut vous aider à accélérer la copie.

   3b Restaurez la base de données eDirectory du serveur A vers le serveur B à l'aide des fichiers de sauvegarde que vous avez copiés. Sur la ligne de commande du client, entrez une commande similaire à la suivante :

   `restore -r -f` *`nom_et_chemin_fichier_sauvegarde`* `-l` *`nom_et_chemin_fichier_journal`*

   Si vous utilisez NICI, veillez à restaurer les fichiers NICI. Si vous avez sauvegardé des fichiers répertoriés dans un fichier d'inclusion, ajoutez l'option `-u`. Pour plus d'informations sur l'utilisation du client et des paramètres, reportez-vous aux sections « Restauration à partir de fichiers de sauvegarde avec DSBK » page 472 et « Options de ligne de commande pour la sauvegarde et la restauration » page 474.

   Il est inutile d'inclure des fichiers journaux de transactions individuelles dans la restauration, puisque vous avez effectué une sauvegarde à froid et maintenu ensuite la base de données fermée. Aucune transaction n'est intervenue dans la base de données, puisque celle-ci était fermée ; aucun fichier journal de transaction individuelle n'a donc été créé depuis la sauvegarde.

   3c Transférez le système de fichiers du serveur A vers le serveur B à partir de la sauvegarde.
4. Si vous utilisez NICI, redémarrez le serveur pour réinitialiser NICI afin qu'il utilise les fichiers de sécurité restaurés.
5. Déverrouillez la base de données eDirectory.
6. Une fois la restauration terminée, vérifiez que le serveur B a adopté l'identité du serveur A et qu'il répond normalement. Utilisez iMonitor pour contrôler le serveur et sa synchronisation.

   Si le serveur répond normalement, la procédure de remplacement est terminée. Vous pouvez maintenant désinstaller eDirectory du serveur A en supprimant l'identité eDirectory de ce dernier, puis utiliser la machine à d'autres fins. Ne refaites pas fonctionner le serveur A tant que vous n'avez pas supprimé eDirectory. Sinon, la synchronisation d'eDirectory risquerait de perturber le réseau, car les serveurs A et B entreraient en concurrence pour obtenir la même identité.
7. (Conditionnel) Si vous avez utilisé la consignation de transactions individuelles par fichier sur ce serveur, veillez à recréer la configuration des fichiers journaux de transactions individuelles, une fois la restauration terminée. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

   Comme ces paramètres reprennent leur valeur par défaut après une restauration, la consignation de transactions individuelles par fichier est désactivée. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Si le serveur B ne fonctionne pas correctement et que l'identité et le système de fichiers du serveur A doivent être immédiatement disponibles, procédez comme suit :

1. Débranchez le câble réseau du serveur B ou arrêtez le serveur.
2. Reconnectez le serveur A au réseau, démarrez-le, puis ouvrez la base de données eDirectory.

   Ignorez les messages système vous invitant à exécuter DSREPAIR.
3. Supprimez eDirectory du serveur B et tentez à nouveau la mise à niveau.

Modification de l'adresse IP du serveur

L'adresse IP du serveur est généralement statique. Si vous la modifiez, vous devez mettre à jour le fichier `nds.conf` pour toutes les instances d'eDirectory associées à la nouvelle adresse IP. Si l'adresse IP change fréquemment, il est préférable que le fichier `nds.conf` utilise le nom d'interface au lieu de l'adresse IP.

Par exemple : `n4u.server.interfaces=eth0@1524`

Après un changement d'adresse IP, les objets KMO (Key Material Object) basés sur l'adresse IP du serveur ne sont pas mis à jour automatiquement. Même s'il n'est pas nécessaire de supprimer les anciens objets KMO (dont le nom comporte l'adresse IP), cette opération permet de nettoyer l'arborescence. Pour recréer vos objets KMO et les associer aux objets Serveur NCP et Serveur LDAP, exécutez la commande `ndsconfig upgrade`.

REMARQUE : l'exécution de la commande `ndsconfig upgrade` entraîne le redémarrage de votre instance d'eDirectory.

Le serveur continue désormais à écouter sur la nouvelle adresse. Si l'arborescence compte plusieurs serveurs, exécutez les options de réparation réseau DSRepair :

```
ndsrepair -N
```

Après avoir exécuté les options de réparation, redémarrez le serveur eDirectory.

Pour plus d'informations sur les modifications d'adresse IP du serveur, reportez-vous au document TID 3201067 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3201067&sliceId=SAL_Public&dialogID=36008849&stateId=0%200%2036014447).

Restauration d'eDirectory après une panne matérielle

Une panne de disque dur impliquant le volume/la partition de disque contenant eDirectory correspond à une suppression d'eDirectory du serveur. Heureusement, dans un environnement multiserveur, un serveur peut s'arrêter, alors que les autres serveurs de l'anneau de répliques restent intacts.

Pour restaurer eDirectory après une panne affectant le volume/la partition de disque où celui-ci réside, suivez les procédures de restauration à partir des fichiers de sauvegarde décrites à la « Préparation d'une restauration » page 463 ainsi qu'à la section « Restauration à partir de fichiers de sauvegarde avec iManager » page 616 (ou à la section « Restauration à partir de fichiers de sauvegarde avec DSBK » page 472).

Durant la nouvelle installation, suivez les instructions du fabricant pour vérifier le bon fonctionnement des disques durs du serveur. Le nouveau disque dur doit avoir une capacité de stockage au moins égale à celle du disque qu'il remplace. Utilisez les fichiers contenant les informations locales du serveur pour vérifier les informations de configuration.

REMARQUE

- Il est recommandé d'exclure le répertoire DIB présent sur votre serveur eDirectory de la portée de tout antivirus ou processus de logiciel de sauvegarde. Utilisez l'outil de sauvegarde d'eDirectory pour sauvegarder votre répertoire DIB. Pour plus d'informations sur la sauvegarde d'eDirectory, reportez-vous à la section « Sauvegarde et restauration de NetIQ eDirectory » page 443.
- Si vous ne disposez d'aucun fichier de sauvegarde pour le serveur, utilisez l'outil XBrowse pour interroger eDirectory et ainsi récupérer les informations du serveur. Effectuez cette opération avant de supprimer l'objet Serveur ou tout objet associé de l'arborescence. Vous trouverez XBrowse ainsi que des informations supplémentaires sur le site Web du support NetIQ (http://support.novell.com/docs/Readmes/InfoDocument//2960653.html).

Amélioration des performances de recherche dans les sous-arborescences

Les performances de recherche dans les sous-arborescences d'eDirectory demeurent piètres dans les arborescences de grande taille présentant une structure fortement imbriquée, et ce quel que soit le DN de base de la recherche. Ce problème a été résolu par l'utilisation de l'attribut `AncestorID`. L'attribut `AncestorID` répertorie les ID d'entrée de tous les ancêtres, associés à chaque entrée. Utilisé en interne pendant la recherche dans les sous-arborescences, l'attribut `AncestorID` limite l'étendue de la recherche.

Il est complété lors de l'ajout d'une entrée et après une mise à niveau pour toutes les entrées de la DIB, et est recomplété pour toutes les entrées de la sous-arborescence après le déplacement de celle-ci. Toutefois, la recherche dans les sous-arborescences n'utilise pas l'attribut `AncestorID` pendant que l'attribut est complété après une mise à niveau et un déplacement de sous-arborescence. Les performances de recherche dans les sous-arborescences restent donc similaires à celles qui existaient avant eDirectory

Pour vérifier si les attributs `AncestorID` sont actualisés après une mise à niveau :

Une fois les attributs `AncestorID` complétés, la version de mise à niveau de l'objet NDS passe à 6 ou plus. Pour le vérifier, utilisez iMonitor dans la section **Historique de la DIB** de la page Informations sur les agents.

Pour vérifier si les attributs `AncestorID` sont actualisés après le déplacement d'une sous-arborescence :

Pendant que les attributs `AncestorID` sont complétés, l'attribut `UpdateInProgress` dans l'objet `Pseudo serveur` détient la liste des ID d'entrée de la racine de partition de la sous-arborescence. Une fois les attributs `AncestorID` complétés, l'attribut est absent de l'objet `Pseudo serveur`.

DSRepair met à jour l'attribut `AncestorID` s'il n'est pas valide.

Préparation des conteneurs

Pour garantir une utilisation optimale du cache d'entrée ainsi qu'une amélioration des performances des opérations de recherche d'attributs, FLAIM enregistre les attributs dont les valeurs sont plus élevées ou contenant un nombre supérieur de valeurs à un autre emplacement, à savoir, le conteneur d'attributs. Par défaut, les attributs seront déplacés automatiquement vers le conteneur lorsque l'attribut :

- contient plus de 25 valeurs ;
- sa valeur est supérieure à 2 048 octets.

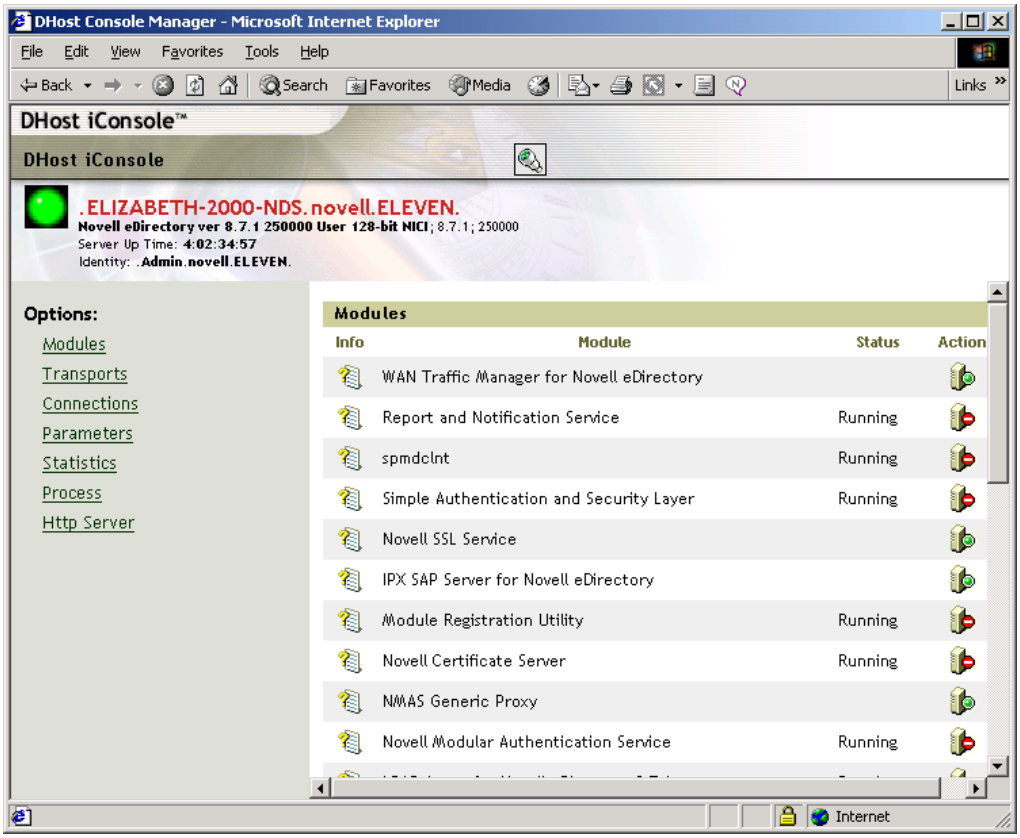
eDirectory offre désormais la possibilité de contrôler les mouvements d'attributs vers des conteneurs distincts. Un administrateur peut ainsi planifier le déplacement d'un attribut comme il le souhaite. Pour plus d'informations, reportez-vous à la section Mise en conteneur des attributs FLAIM du Guide d'optimisation de NetIQ eDirectory.

20 Gestionnaire DHost iConsole

Outil d'administration basé sur le Web, le gestionnaire DHost iConsole est un navigateur qui permet de :

- gérer les modules Dhost ;
- rechercher les paramètres de configuration Dhost ;
- consulter les informations de connexion Dhost ;
- visualiser les statistiques de réserves de threads ;
- consulter des informations détaillées sur les protocoles enregistrés auprès du gestionnaire de piles de protocoles Dhost.

Figure 20-1 *Gestionnaire DHost iConsole*



Ce chapitre développe les informations suivantes :

- « Définition de DHost » page 584
- « Exécution de DHost iConsole » page 584
- « Gestion des modules eDirectory » page 585
- « Demande d'informations DHost » page 587
- « Pile de processus » page 589

Définition de DHost

Les logiciels NetIQ eDirectory pour Windows et Linux reposent tous deux sur le même code de base. Pour pouvoir interagir correctement avec les autres versions d'eDirectory, ces logiciels prennent en charge un sous-ensemble de services NCP (NetWare Core Protocol) géré par le programme DHost. DHost s'exécute sous eDirectory et offre des fonctionnalités que le protocole NCP fournit naturellement.

DHost fournit les services suivants :

Service	Description
Moteur NCP	Protocole basé sur des paquets qui permet à un client d'envoyer des requêtes à un serveur eDirectory et de recevoir les réponses de ce dernier. Pour plus d'informations, reportez-vous à la documentation relative au NDK des protocoles NetWare (http://developer.novell.com/documentation/ncp/index.html).
Surveillance (watchdog)	Paquets utilisés pour s'assurer que les postes de travail sont toujours connectés au serveur eDirectory. Pour plus d'informations, reportez-vous à la documentation Watchdog Packet Spoofing (Simulation de paquets de surveillance).
Table de connexions	Numéro unique assigné à un processus, à un serveur d'impression, à une application, à un poste de travail ou à toute autre entité connectée à un serveur eDirectory. Ce numéro peut être différent pour chaque attache. Les numéros de connexion sont utilisés pour mettre en oeuvre la sécurité et la facturation réseau. Ils indiquent la place des objets dans la table de connexions des serveurs de fichiers. De plus, ils facilitent l'identification et l'obtention d'informations concernant les objets connectés sur le réseau.
Système d'événements	Permet aux applications de surveiller l'activité d'un serveur.
Réserve de threads	Séquence d'instructions exécutée comme une entité indépendante et programmée par le logiciel système.
Extensions NCP	Ces extensions permettent aux développeurs d'applications serveur d'écrire des logiciels NLM™ à implémenter en tant que NCP. Pour plus d'informations, reportez-vous à la section NCP Extension (http://developer.novell.com/documentation/ncp/ncp__enu/data/alne6tm.html) (Extension NCP) de la documentation relative au NDK des protocoles NCP.
Message Digest	Forme compressée ou condensée d'un document, ou extrait d'un document, qui sert d'« empreinte digitale numérique » pour un document de plus grande taille. Un message digest sert à créer une signature numérique spécifique à un document en particulier.

Exécution de DHost iConsole

- « Exécution de DHost iConsole sous Windows » page 585
- « Exécution de DHost iConsole sous Linux » page 585

Exécution de DHost iConsole sous Windows

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   par exemple :

   `http://MyServer:80/dhost`

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   `http://137.65.135.150:80/dhost`
3. Indiquez un nom d'utilisateur, un contexte et un mot de passe.

Exécution de DHost iConsole sous Linux

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   Par exemple :

   `http://MyServer:80/dhost`

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   `http://137.65.135.150:80/dhost`
3. Indiquez un nom d'utilisateur, un contexte et un mot de passe.

Gestion des modules eDirectory

La page Modules de DHost iConsole fournit des informations sur les services eDirectory disponibles et sur leurs états. Elle permet également de démarrer et d'arrêter (de charger et de décharger) ces services.

Vous pouvez uniquement charger ou décharger des modules non interactifs tels que LDAP, SNMP et HTTPSTK.

La page Modules comporte les attributs suivants :

Attribut	Description
Informations	Cliquez sur pour afficher la description, le nom de fichier, l'identificateur, les attributs et le nom d'objet partagé du module sélectionné.
Module	Affiche le nom du module.
État	Indique si le module est en cours d'exécution ou non.
Action	Indique si le module peut être démarré ou non. Les trois états possibles d'un module sont les suivants : • indique que le module est un module système qui ne peut pas être déchargé. • indique que le module est prêt pour le chargement. • indique que le module est en cours d'exécution.

- « Chargement et déchargement de modules sous Windows » page 586
- « Chargement et déchargement de modules sous Linux » page 586

Pour plus d'informations sur l'utilisation de NetIQ iManager pour charger et décharger des services eDirectory, reportez-vous à la « Gestionnaire de services eDirectory » page 207.

Chargement et déchargement de modules sous Windows

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   par exemple :

   `http://MyServer:80/dhost`

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   `http://137.65.135.150:80/dhost`
3. Indiquez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur **Modules**.
5. Cliquez sur pour charger un module, ou sur pour décharger un module.

Chargement et déchargement de modules sous Linux

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   par exemple :

```
http://MyServer:80/dhost
```

Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

```
http://137.65.135.150:80/dhost
```

3 Indiquez un nom d'utilisateur, un contexte et un mot de passe.

4 Cliquez sur **Modules**.

5 Cliquez sur pour charger un module, ou sur pour décharger un module.

Demande d'informations DHost

Grâce au gestionnaire DHost iConsole, vous pouvez demander les informations suivantes :

- Paramètres de configuration
- Protocoles enregistrés avec le gestionnaire PSTACK
- Propriétés de connexion
- Résumé des réserves de threads

Affichage des paramètres de configuration

Les paramètres de configuration sont propres à Linux.

Dans le gestionnaire DHost iConsole, cliquez sur **Paramètres**. Pour plus d'informations, reportez-vous à la section « Exécution de DHost iConsole sous Linux » page 585.

Les paramètres de configuration affichent les informations suivantes :

Option	Description
Nom du paramètre	Affiche le nom du paramètre de configuration.
Default value (Valeur par défaut)	Affiche la valeur par défaut du paramètre.
Set value (Valeur définie)	Affiche la valeur actuellement définie.
Valeur minimum	Affiche la valeur minimale qui peut être définie pour le paramètre.
Maximum value (Valeur maximum)	Affiche la valeur maximale qui peut être définie pour le paramètre.
Type	Affiche le type de valeur qui peut être défini pour le paramètre.

Pour plus d'informations, reportez-vous à la section « Paramètres de configuration » du *Guide d'installation de NetIQ eDirectory*.

Affichage des informations sur le protocole

Dans le gestionnaire DHost iConsole, cliquez sur **Transports**.

Les informations de protocole suivantes s'affichent :

- ID
- Protocole
- Transports

Affichage des propriétés de connexion

Dans le gestionnaire DHost iConsole, cliquez sur **Connexions**.

Les propriétés de connexion suivantes s'affichent :

- Conn
- Drapeaux
- Identité
- Nom d'affichage
- Transport
- Authentication Name (Nom d'authentification)
- SEV Count (Nombre SEV)
- Dernier accès
- Verrouillée

Affichage des statistiques de réserves de threads

Dans le gestionnaire DHost iConsole, cliquez sur **Statistiques**.

Les statistiques de réserves de threads s'affichent :

- Spawned Threads (Threads générés)
- Dead Threads (Threads morts)
- Idle Threads (Threads inactifs)
- Worker Thread (Thread de travail)
- Peak Worker Thread (Thread de travail maximum)
- Ready for Work Thread (Thread prêt pour le travail)
- Ready Queue Peak Worker Threads (Threads de travail maximum prêts dans la file d'attente)
- Ready Queue Max Wait Time (Délai d'attente maximal prêt dans la file d'attente)
- Schedule Delay Minimum Time (Durée d'attente minimale planifiée)
- Schedule Delay Maximum Time (Durée d'attente maximale planifiée)
- Schedule Delay Average Time (Durée d'attente moyenne planifiée)
- Waiting For Work (En attente de travail)
- Peaking Waiting For Work (Attente de travail maximale)

Pile de processus

La pile de processus contient la liste des threads en cours d'exécution dans l'espace de processus DHost. Vous pouvez obtenir des informations détaillées sur un thread en cliquant sur son ID. Cette fonctionnalité est généralement utilisée comme un outil de débogage de bas niveau par les ingénieurs et le support technique de NetIQ.

Cette option n'est disponible que sous Windows.

1. Ouvrez un navigateur Web.
2. Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   par exemple :

   `http://MyServer:80/dhost`

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   `http://137.65.135.150:80/dhost`
3. Indiquez un nom d'utilisateur, un contexte et un mot de passe.
4. Cliquez sur **Processus**.
5. Pour afficher la pile d'appel d'un thread, cliquez sur l'ID de ce dernier.

21 Définition du mot de passe de l'utilisateur sadmin

Vous pouvez définir un administrateur préconfiguré permettant d'accéder à HTTPSTK (pile de protocole HTTP) lorsqu'eDirectory n'est pas chargé. Cet administrateur préconfiguré (`sadmin`) dispose de droits équivalents à ceux de l'objet Utilisateur Admin eDirectory. Si l'état du serveur ne permet pas à eDirectory de fonctionner correctement, vous pouvez vous connecter au serveur avec l'identité de cet utilisateur et effectuer toutes les tâches requises de diagnostic et de débogage qui ne requièrent pas eDirectory.

REMARQUE : le nom d'utilisateur de sadmin respecte la casse.

L'utilitaire `ndspassstore` permet de définir le mot de passe de l'utilisateur sadmin sur les systèmes Windows et Linux.

Saisissez les lignes suivantes sur la console du serveur :

```
ndspassstore -a sadmin -w <mot_de_passe>
```

`sadmin` (contexte Admin) correspondant au nom distinctif complet d'un utilisateur disposant de droits d'administrateur, et `mot_de_passe` au mot de passe d'authentification. En présence de plusieurs instances, sélectionnez une instance adéquate.

Exemple : `ndspassstore -a sadmin -w pass`

ndspassstore est disponible par défaut dans les répertoires **C:\Novell\NDS** sous Windows et **/opt/novell/eDirectory/bin** sous UNIX.

22 eDirectory Management Toolbox

L'outil NetIQ eMBox (eDirectory Management Toolbox) permet d'accéder à tous les principaux utilitaires d'eDirectory, à distance comme sur le serveur.

Combiné à NetIQ iManager, eMBox fournit un accès via le Web à des utilitaires tels que DSRepair, DSMerge, Service Manager, ainsi qu'à l'utilitaire de sauvegarde et de restauration.

IMPORTANT : pour tous les utilisateurs, y compris l'administrateur, les services basés sur le rôle doivent être configurés avec l'étendue, via iManager, sur l'arborescence qui doit être administrée pour les tâches à exécuter.

Des services basés sur le rôle doivent être configurés pour les tâches ci-dessous, lesquelles se trouvent sous le menu de maintenance d'eDirectory dans iManager :

- Configuration de la sauvegarde
- Greffe d'arborescence
- Réparer eDirectory
- Réparer le serveur
- Réparer la synchronisation
- Réparation des répliques
- Réparation des anneaux de répliques
- Restauration
- Maintenance du schéma
- Gestionnaire de services
- Fusionner l'arborescence
- Renommer l'arborescence

Toutes les fonctions sont accessibles, sur le serveur local ou à distance, via un client à ligne de commande. Grâce au client, vous pouvez effectuer des tâches pour plusieurs serveurs à partir d'un seul serveur ou poste de travail.

Pour exécuter tous les outils eMTools (eDirectory Management Tools), tels que Backup, DSRepair, DSMerge, Schema Operations et eDirectory Service Manager, eMBox doit être chargé et exécuté sur le serveur eDirectory.

REMARQUE : pour plus d'informations sur l'utilisation des outils eMTools, reportez-vous à la « Utilitaires de dépannage sous Linux » page 973.

Dans cette section :

- « Utilisation du client à ligne de commande » page 594
- « Utilisation de l'enregistreur » page 603
- « Utilisation du client eMBox pour la sauvegarde et la restauration » page 604
- « Sauvegarde et restauration à l'aide de NetIQ iManager » page 613

Utilisation du client à ligne de commande

L'un des moyens d'accéder à consiste à utiliser son client Java à ligne de commande. Le client à ligne de commande propose deux modes : interactif et traitement par lots. En mode interactif, vous exécutez une commande à la fois. En mode de traitement par lots, vous pouvez exécuter automatiquement un groupe de commandes. Le client à ligne de commande possède un service de consignation pour les deux modes.

Le client à ligne de commande est une application Java. Pour l'exécuter, vous devez installer la dernière version d'Azul ZuluOpenJDK (1.8 ou version ultérieure). Vous devez également veiller à mettre à niveau toute version antérieure de Java en installant les mises à niveau de correctif disponibles. Une fois que la dernière version de Java est installée, exportez les variables d'environnement suivantes souhaitées :

- `EDIR_JAVA_HOME`
- `JAVA_HOME`
- `JRE_HOME`

REMARQUE

- Sous Linux, si aucune des variables d'environnement mentionnées n'est détectée, le client de ligne de commande recherche le fichier binaire Java dans la variable d'environnement `PATH` par défaut.
- eDirectory 9.1 SP2 et les versions ultérieures prennent en charge Azul ZuluOpenJDK 1.8.0_192.

Exemples

Quelques exemples de variables d'environnement sont présentés ci-dessous :

- **Linux**
  - `EDIR_JAVA_HOME=/usr/java/java1.8.0_131`
  - `JAVA_HOME= /usr/java/java1.8.0_131`
  - `JRE_HOME= /usr/java/java1.8.0_131/jre`
- **Windows**
  - `EDIR_JAVA_HOME= C:\Program Files\Java\jdk1.8.0_131`
  - `JAVA_HOME= C:\Program Files\Java\jdk1.8.0_131`
  - `JRE_HOME= C:\Program Files\Java\jdk1.8.0_131\jre`

Vous devez aussi pouvoir accéder derrière le pare-feu aux serveurs que vous voulez gérer. Vous pouvez effectuer des tâches pour plusieurs serveurs à partir d'un même serveur ou poste de travail.

REMARQUE : l'outil eDirectory Management Toolbox prend uniquement en charge l'anglais, que ce soit dans le client à ligne de commande ou dans l'aide de la ligne de commande.

Dans cette section :

- « Affichage de l'aide sur la ligne de commande » page 595
- « Exécution du client à ligne de commande en mode interactif » page 595
- « Exécution du client à ligne de commande en mode de traitement par lots » page 599

- « Options du client à ligne de commande eMBox » page 601
- « Établissement d'une connexion sécurisée avec le client » page 602
- « Recherche des numéros de port eDirectory » page 602

Affichage de l'aide sur la ligne de commande

Pour afficher l'aide générale sur la ligne de commande avant d'accéder au client, procédez comme suit :

- Linux : entrez `edirutil -?` dans la ligne de commande.
- Windows : exécutez *`unité`*`\novell\nds\\edirutil.exe -?`.

Pour afficher l'aide interactive sur la ligne de commande en mode interactif, entrez un point d'interrogation (?) à l'invite du client. Par exemple, `Client> ?`

L'aide affiche des informations sur les options de ligne de commande similaires à celles de la section « Options du client à ligne de commande eMBox » page 601.

Exécution du client à ligne de commande en mode interactif

Le mode interactif permet d'exécuter les commandes l'une après l'autre.

Dans cette section :

- « Exécution du client sur un serveur eDirectory » page 595
- « Exécution du client sur un poste de travail » page 596
- « Configuration du chemin et du chemin de classe pour le client » page 596
- « Connexion à un serveur » page 597
- « Définition des préférences de langue, de timeout et de fichier journal » page 597
- « Liste des outils eMTools et de leurs services » page 597
- « Exécution d'un service spécifique » page 598
- « Déconnexion du serveur en cours » page 598
- « Fermeture du client » page 599

Exécution du client sur un serveur eDirectory

Le client et JVM 1.3.1 de Sun sont installés avec eDirectory. Pour ouvrir le client en mode interactif sur un serveur eDirectory, procédez comme suit :

- Linux : entrez `edirutil -i` dans la ligne de commande.
- Windows : exécutez *`unité`*`\novell\nds\edirutil.exe -i`.

Le fichier `edirutil` est un raccourci pour l'exécution du client. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client est installé avec eDirectory. Vous pouvez également entrer les informations manuellement, comme expliqué à la section « Configuration du chemin et du chemin de classe pour le client » page 596.

L'utilisation du client à ligne de commande nécessite un accès derrière le pare-feu pour les serveurs que vous voulez gérer. Si vous êtes à distance, vous devez donc disposer d'un accès VPN.

Exécution du client sur un poste de travail

Pour exécuter le client sur un ordinateur autre qu'un serveur eDirectory :

- Copiez le fichier `eMBoxClient.jar` d'un serveur eDirectory vers votre machine.
  - Windows : `\novell\nds\\eMBoxClient.jar`
  - Linux : `/opt/novell/eDirectory/lib/nds-modules//eMBoxClient.jar`
- Assurez-vous que JVM 1.3.1 de Sun est installé sur la machine.
- Vérifiez que l'accès derrière le pare-feu est possible afin d'utiliser le client à ligne de commande pour les serveurs que vous voulez gérer.

Contrairement à un serveur, un poste de travail ne permet pas d'employer la commande `edirutil` comme raccourci pour accéder au client en mode interactif. Vous devez soit configurer l'environnement après avoir accédé à votre chemin et votre chemin de classe, soit l'entrer chaque fois manuellement. Reportez-vous à la section « Configuration du chemin et du chemin de classe pour le client » page 596.

Configuration du chemin et du chemin de classe pour le client

Si vous exécutez le client sur un serveur eDirectory sans avoir changé l'emplacement de Java ou du fichier `eMBoxClient.jar`, vous pouvez utiliser `edirutil` comme raccourci pour exécuter le client. Reportez-vous à la section « Exécution du client sur un serveur eDirectory » page 595.

En revanche, si vous avez modifié les emplacements par défaut, si vous exécutez le fichier `eMBoxClient.jar` sur une autre machine qu'un serveur ou si vous voulez entrer le chemin de classe manuellement, vous devez configurer le chemin et le chemin de classe pour le client conformément aux indications de cette section.

Vous pouvez exécuter le client à partir de n'importe quel emplacement sur votre ordinateur si vous suivez la procédure ci-après :

- Ajoutez à votre chemin l'emplacement de l'exécutable Java (par exemple `java.exe`) ou assurez-vous que Java est déjà en cours d'exécution.

  Si vous êtes sur un serveur, cette opération a probablement déjà été effectuée. Sur des serveurs Windows, Linux et UNIX, le répertoire doit se trouver dans votre chemin.

  Sur un poste de travail, vous devrez peut-être le définir vous-même. Par exemple, sous Windows, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **Système**. Sous l'onglet **Avancé**, cliquez sur **Variables d'environnement** et ajoutez le chemin à la variable **Path**.

  Pour procéder manuellement : Si le chemin d'accès à l'exécutable Java n'a pas été ajouté à votre chemin, vous devez d'abord passer, sur la ligne de commande, au répertoire contenant cet exécutable avant de lancer. Par exemple, sous Windows, entrez `cd c:\novell\nds\\jre\bin`.
- Ajoutez le chemin d'accès au fichier `eMBoxClient.jar` à votre chemin de classe.

  Serveur ou poste de travail Windows : `set CLASSPATH=`*`chemin`*`\eMBoxClient.jar`

  Serveur ou poste de travail Linux : `export CLASSPATH=`*`chemin/`*`eMBoxClient.jar`

  Pour procéder manuellement : un autre moyen de spécifier le chemin de classe consiste à utiliser le drapeau `-cp` pour Java chaque fois que vous voulez exécuter :

  `java -cp` *`path/`*`eMBoxClient.jar -i`

  Par exemple, sous Windows, entrez `java -cp c:\novell\nds\\eMBoxClient.jar -i`.

Une fois ces deux opérations effectuées, vous pouvez exécuter le client en mode interactif à partir de n'importe quel emplacement de votre machine en utilisant la commande suivante :

```
java  -i
```

Pour plus d'informations sur les commandes Java, reportez-vous à la documentation Java sur le site Web d'Oracle (http://www.oracle.com/technetwork/java/).

Connexion à un serveur

Pour vous connecter à un serveur, vous devez indiquer son nom ou son adresse IP ainsi que le numéro du port de connexion. Il n'est pas nécessaire de spécifier un nom d'utilisateur et un mot de passe pour les connexions publiques.

Par exemple, une fois que le client est ouvert en mode interactif, entrez

```
login -s 137.65.123.244 -p 8008 -u admin.mycompany
-w mypassword -n
```

Pour plus d'informations sur les numéros de port, reportez-vous à la section « Recherche des numéros de port eDirectory » page 602.

Définition des préférences de langue, de timeout et de fichier journal

La langue par défaut est la langue du système client. Ainsi, dans la plupart des cas, vous n'avez pas besoin de définir explicitement une langue. De même, le timeout par défaut convient le plus souvent. Pour définir le fichier journal, indiquez son nom et le mode d'ouverture (annexer ou écraser).

Le tableau ci-après fournit des exemples de commandes.

Commande	Description
`set -L en,de`	Définit l'anglais et l'allemand comme langues préférées (dans cet ordre).
`set -T 100`	Définit un timeout de 100 secondes. Le paramètre de timeout indique le délai d'attente des réponses du serveur.
`set -l mylog.txt -o`	Utilise `mylog.txt` comme fichier journal et l'écrase à l'ouverture. Valeur par défaut = append (annexer)

Liste des outils eMTools et de leurs services

Une fois connecté à un serveur, vous pouvez utiliser la commande list pour afficher la liste des services disponibles.

La commande list affiche dynamiquement tous les outils eMTools suivants et leurs services.

eMTool	Description
Sauvegarde	NetIQ eDirectory Backup eMTool
DSMerge	NetIQ eDirectory Merge eMTool
DSRepair	NetIQ eDirectory Repair eMTool
DSSchema	NetIQ eDirectory Schema Operations eMTool
service	NetIQ eDirectory Service Manager eMTool

Utilisez l'option `-r` pour forcer le rafraîchissement de la liste. Utilisez l'option `-t` pour répertorier les détails des services. Utilisez l'option `-f` pour afficher uniquement le format de commande.

Le tableau ci-après fournit des exemples de commandes.

Commande	Description
`list`	Liste les outils eMTools disponibles sur le serveur.
`list -r`	Rafraîchit la liste des outils eMTools.
`list -t backup`	Liste les services de sauvegarde (Backup) de manière détaillée.
`list -t dsrepair`	Liste les services DSRepair de manière détaillée.
`list -t dsmerge -f`	Liste les services DSMerge de manière détaillée.

Exécution d'un service spécifique

Une fois connecté à un serveur, vous pouvez effectuer des tâches au moyen des différents services eMTool. Par exemple :

Commande	Description
`dsrepair.rld`	Réparer la base de données locale
`backup.getconfig`	Obtenir des informations sur la configuration de la sauvegarde.

Pour plus d'informations, reportez-vous aux points suivants :

- « Utilisation du client eMBox pour la sauvegarde et la restauration » page 604
- « Utilisation du client pour fusionner des arborescences » page 311
- « Utilisation du client pour réparer une base de données » page 361
- « Utilisation de l'outil Service Manager eMTool du client » page 208

Déconnexion du serveur en cours

Pour vous déconnecter de la session en cours, utilisez la commande suivante :

```
Déconnexion
```

Si vous vous connectez à un autre serveur, vous ne devez pas utiliser cette commande. Vous êtes automatiquement déconnecté du serveur actuel.

Fermeture du client

Pour quitter le client, utilisez l'une des commandes suivantes :

`exit`

ou

`quit`

Exécution du client à ligne de commande en mode de traitement par lots

Il existe trois méthodes d'exécution du client en mode de traitement par lots :

- « Tâches uniques » page 599
- « Fichier interne de traitement par lots » page 599
- « Fichier système de traitement par lots » page 600

Pour une souplesse accrue et pour organiser et réutiliser les commandes fréquemment exécutées, vous pouvez combiner des fichiers de traitement par lots internes et propres au système.

Tâches uniques

Dans la ligne de commande, vous pouvez n'exécuter qu'une seule tâche en mode de traitement par lots. Pour ce faire, il suffit d'entrer la commande avec l'option `-t` pour spécifier l'outil et la tâche sans sélectionner l'option `-i` (mode interactif). Par exemple :

```
java -s 137.65.123.244 -p 8008 -u admin.mycompany
-w mypassword -l mylog.txt -t dsrepair.rld -n
```

Pour des tâches multiples sur plusieurs serveurs, ou des tâches que vous exécutez fréquemment, il est recommandé d'utiliser un fichier interne de traitement par lots. Pour plus d'informations, reportez-vous à la section « Fichier interne de traitement par lots » page 599.

Fichier interne de traitement par lots

Pour exécuter le client en mode de traitement par lots à l'aide d'un fichier de traitement par lots interne au client, vous devez créer un fichier contenant le groupe des commandes que vous exécuteriez en mode interactif.

Un fichier de traitement par lots interne au client permet d'exécuter automatiquement toutes les commandes qu'il contient. Vous pouvez effectuer plusieurs tâches sur le même serveur au moyen des différents outils sans avoir à vous connecter et déconnecter à chaque fois. À partir d'un serveur, vous pouvez également exécuter plusieurs tâches au moyen d'outils sur plusieurs serveurs.

Les fichiers de traitement par lots internes aident à organiser et à réutiliser les commandes fréquemment exécutées, ce qui évite de les entrer à chaque fois manuellement dans la ligne de commande.

Vous pouvez accéder à la ligne de commande et exécuter le fichier de traitement par lots interne au moyen d'une commande client. Par exemple, la commande ci-dessous permet de se connecter à un serveur et d'exécuter les commandes répertoriées dans le fichier `mybatch.mbx` :

```
java -s 137.65.123.244 -p 8008 -u admin.mycompany -w mypassword -l mylog.txt -o -b
mybatch.mbx -n
```

Une autre solution consiste à inclure le même type de commande dans un fichier système de traitement par lots, ce qui permet de planifier l'exécution sans surveillance de ce fichier sur le serveur. Reportez-vous à la section « Fichier système de traitement par lots » page 600.

Voici un exemple de fichier interne de traitement par lots Il contient des exemples de commandes exécutables et un exemple de connexion à un autre serveur. Dans cet exemple, nous partons du principe que vous vous êtes connecté à un serveur lorsque vous avez ouvert le client Chaque commande doit figurer sur une ligne distincte. Les lignes qui commencent par le signe # sont des commentaires.

```
# This file is named mybatch.mbx.
# This is an example of commands you could use in
# an internal command batch file.

# Backup commands
backup.getconfig
backup.backup -b -f mybackup.bak -l backup.log -t -w

# DSRepair commands
dsrepair.rld

# Log in to a different server
login -s 137.65.123.255 -p 8008 -u admin.mycompany -w mypassword -n

# DSMerge commands
dsmerge.pr -u admin.mycompany -p admin.mycompany -n mypassword # Schema Operations
dsschema.rst
dsschema.dse
dsschema.rls
dsschema.gsu
dsschema.scc
dsschema.irs -n LocalTree

# DSService commands
service.serviceList

# End of example.
```

Fichier système de traitement par lots

Comme avec d'autres outils de ligne de commande, vous pouvez créer des fichiers système de traitement par lots qui contiennent des commandes du client , et les exécuter manuellement dans la ligne de commande ou planifier leur exécution sans surveillance sur le serveur. Par exemple, vous pouvez effectuer des sauvegardes sans surveillance en utilisant des fichiers système de traitement par lots similaires à ceux des exemples décrits à la section « Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox » page 607.

À partir d'un seul serveur, vous pouvez exécuter des tâches multiples à l'aide de plusieurs outils sur différents serveurs.

Dans un fichier système de traitement par lots, vous pouvez combiner des commandes individuelles du client et des fichiers de traitement par lots internes pour bénéficier d'une souplesse accrue et pour organiser et réutiliser les commandes que vous exécutez fréquemment. Pour plus d'informations, reportez-vous à la section « Fichier interne de traitement par lots » page 599 ci-dessus.

Pour des instructions sur l'exécution de fichiers de traitement par lots sans surveillance, consultez la documentation de votre système d'exploitation ou de votre logiciel de planification tiers.

Options du client à ligne de commande eMBox

Option	Description
`-? ou -h`	affiche les informations d'aide
`-i`	Exécute les commandes l'une après l'autre en mode interactif.
`-s` *`serveur`*	Nom ou adresse IP du serveur Valeur par défaut : `127.0.0.1`
`-p` *`port`*	Numéro de port du serveur Valeur par défaut : `8008`
`-u` *`utilisateur`*	DN utilisateur. Par exemple : `admin.masociété`. Valeur par défaut : `anonyme`
`-w` *`mot de passe`*	Mot de passe associé à l'utilisateur spécifié au moyen de l'option `-u`.
`-m` *`mode`*	Mode de connexion. Valeur par défaut : `dclient`
`-n`	Ne tente pas d'établir une connexion SSL sécurisée. Utilisez une connexion non sécurisée. Si vous n'utilisez pas cette option, le client tente d'établir une connexion SSL et une erreur est renvoyée si vous ne disposez pas des fichiers JSSE dans votre chemin de classe. Pour plus d'informations, reportez-vous à la section « Établissement d'une connexion sécurisée avec le client » page 602.
`-l` *`fichier_journal`*	Nom du fichier journal.
`-o`	Écrase le fichier journal à son ouverture.
`-T` *`timeout`*	Délai d'attente (en secondes) des réponses du serveur.
`-L` *`langue`*	Liste des langues admises (séparées par des virgules) par ordre de préférence, par exemple `en-US,de_DE`. L'option par défaut est la langue du système client.
`-t` `[`*`outil`*`.]`*`options tâche`*	Exécute un service unique avec cette connexion. La chaîne qui suit l'option `-t` doit être une commande valide.
`-b` *`fichier de traitement par lots`*	Exécute un groupe de services tel qu'il est spécifié dans le fichier de traitement par lots. Les commandes du fichier de traitement par lots doivent être placées sur des lignes distinctes. Les lignes précédées du signe # sont des commentaires.

Établissement d'une connexion sécurisée avec le client

Si vous utilisez une connexion non sécurisée, toutes les informations que vous entrez, telles que les noms d'utilisateur et mots de passe, sont envoyées en texte clair sur le réseau.

Si vous voulez établir une connexion sécurisée au moyen de SSL, procédez comme suit :

- Veillez à ne pas utiliser l'option `-n` dans votre commande lorsque vous vous connectez à un serveur. Cette option spécifie en effet une connexion non sécurisée. La valeur par défaut est une connexion sécurisée.
- Vérifiez que les fichiers JSSE (Java Secure Socket Extension) suivants figurent dans votre chemin d'accès de classe :
  - `jsse.jar`
  - `jnet.jar`
  - `jcert.jar`

  Si ce n'est pas le cas, le client renvoie un message d'erreur indiquant qu'il ne parvient pas à établir de connexion sécurisée.

  Pour obtenir ces fichiers, ainsi que des informations sur JSSE, reportez-vous au site Web d'Oracle (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html).

Recherche des numéros de port eDirectory

Lorsque vous vous connectez à un serveur sur le client , vous devez spécifier un numéro de port.

Si vous avez déjà indiqué un numéro de port lors de l'installation d'eDirectory, utilisez ce numéro.

Pour toutes les plates-formes, le port non sécurisé par défaut est 8008, et le port sécurisé par défaut 8030.

Les sections suivantes fournissent des conseils supplémentaires pour trouver le port assigné à eDirectory :

- « Sous Windows » page 602
- « Sous Linux » page 602

Sous Windows

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.
2. Double-cliquez sur l'icône **Services NetIQ eDirectory**, puis cliquez sur l'onglet **Transport**.
3. Recherchez le port sécurisé ou non sécurisé.
   - Pour le port non sécurisé, cliquez sur le signe plus placé en regard de HTTP.
   - Pour le port sécurisé, cliquez sur le signe plus placé en regard de HTTPS.

   Cliquez sur le signe plus (+) situé en regard de **Bound Transports** (Transports liés) pour afficher le numéro de port.

Sous Linux

Vous pouvez utiliser la commande suivante pour afficher une liste de ports :

```
ndsconfig get | grep http
```

Recherchez les lignes qui contiennent http.server.interface suivi d'un numéro de port.

Utilisation de l'enregistreur

L'enregistreur est un module d'infrastructure qui consigne tous les événements pour l'ensemble des outils eMTools tels que DSBackup, DSMerge et DSRepair. Cette version est livrée avec un seul fichier journal dans lequel tous les outils eMTools consignent leurs opérations.

L'enregistreur diffère du service de consignation du client, qui est fourni via les fichiers journaux spécifiés lors de l'exécution du client. Par exemple, lorsque vous spécifiez `-l mylogfile.txt` dans une commande client ou que vous entrez `mylogfile.txt` comme nom de fichier journal dans iManager. L'enregistreur consigne de manière plus détaillée tous les messages du serveur pour les tâches exécutées par eMTools. Quant à lui, le service de consignation client enregistre les messages envoyés et reçus par le client, ce qui permet d'obtenir un rapport général d'avancement.

La consignation est asynchrone et toutes les opérations sont consignées par défaut.

Cette version de l'outil de consignation présente les caractéristiques suivantes :

- Possibilité de changer le nom et l'emplacement du fichier journal.

  Par défaut, les fichiers journaux sont créés dans le répertoire `\log` situé dans le répertoire d'installation d'eDirectory.
- Possibilité de changer la taille maximale du fichier journal, après quoi ce fichier est réinitialisé.

  La taille maximale du fichier est 8 Mo.
- Possibilité de changer de mode de consignation.

  Vous pouvez choisir d'annexer tous les nouveaux messages au fichier journal ou d'écraser un fichier journal existant. L'option d'annexion est sélectionnée par défaut.
- Possibilité de lancer et d'arrêter la consignation.

  Par défaut, l'enregistreur est en mode Démarrage au lancement de En mode Arrêté, aucun message n'est consigné.
- Possibilité de réinitialiser le contenu du fichier journal.
- Possibilité de lire le fichier journal à partir d'un ordinateur client.

Contenu de cette section :

- « Utilisation du client à ligne de commande « outil de consignation » page 603
- « Utilisation de la fonction Enregistreur dans NetIQ iManager » page 604

Utilisation du client à ligne de commande « outil de consignation

Le tableau suivant liste les options du client à ligne de commande « outil de consignation

Option	Description
`logstart`	Démarre l'enregistreur.
`logstop`	Arrête l'enregistreur.
`readlog`	Affiche le fichier journal en cours.

Option	Description
`getlogstate`	Affiche l'état actuel de l'outil de consignation (Démarrage/Arrêt).
`getloginfo`	Affiche le nom, le mode de consignation (annexion/écrasement), ainsi que les tailles maximale et actuelle du fichier journal.
`setloginfo [-f nom_fichier] [-s taille_en_kilo-octets] [-a | -o]`	Permet de définir le nom, la taille et le mode de consignation (Annexer/Écraser) du fichier journal à l'aide des paramètres suivants : ◆ `-f nom_fichier` Nom du fichier journal ◆ `-s taille_en_Ko` Taille maximale du fichier journal. ◆ `-a` Les nouveaux messages de journal sont annexés au journal actuel. ◆ `-o` Le fichier journal est écrasé.
`emptylog`	Efface le contenu du fichier journal du serveur.

Utilisation de la fonction Enregistreur dans NetIQ iManager

1. Dans iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Fichier journal**.
3. Spécifiez le serveur qui effectuera l'opération de fichier journal, puis cliquez sur **Suivant**.
4. Authentifiez-vous auprès du serveur, puis cliquez sur **Suivant**.
5. Sélectionnez l'opération de fichier journal à effectuer.

   Pour obtenir plus d'informations, cliquez sur **Aide**.

Utilisation du client eMBox pour la sauvegarde et la restauration

Le client eMBox est un client Java à ligne de commande qui donne accès aux outils eMBox tels que eDirectory Backup eMTool. Il vous permet d'effectuer, à partir d'une seule machine, des tâches de sauvegarde, de restauration et de configuration de la consignation de transactions individuelles par fichier pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu. Il permet d'exécuter à distance la plupart des tâches de sauvegarde et de restauration dans un navigateur à l'aide d'iManager, que ce soit derrière le pare-feu ou au-delà de celui-ci. Il est également possible d'exécuter des tâches avancées à distance, à l'aide du client eMBox, client Java à ligne de commande qui permet un accès derrière le pare-feu ou au moyen d'un réseau privé virtuel (VPN).

Dans iManager, vous pouvez employer toutes les fonctions, exception faite de la sauvegarde à froid, des sauvegardes sans surveillance et des options de restauration avancées, comme expliqué à la « Sauvegarde et restauration à l'aide de NetIQ iManager » page 613.

L'outil de sauvegarde d'eDirectory fait partie de l'ensemble d'outils eMBox. Installé sur le serveur, eMBox est un service qui fait partie d'eDirectory.

L'outil de sauvegarde comprend les fichiers suivants :

Nom de fichier	Description
`backupcr`	Bibliothèque principale contenant toutes les fonctionnalités de sauvegarde et de restauration. Cette bibliothèque ne possède pas d'interface utilisateur. Elle est chargée et liée dynamiquement par le programme backuptl.
`backuptl`	Interface de l'outil avec la bibliothèque backupcr. Offre des fonctionnalités de sauvegarde et de restauration par le biais de l'architecture DSBK. Ce fichier est accessible via le plug-in iManager ou DSBK, le client à ligne de commande Java.
`dsbackup_en.xlf`	Fichier de langue contenant les messages renvoyés par l'outil de sauvegarde.

IMPORTANT : Le processus de vérification de la restauration est rétrocompatible avec eDirectory 8.5 et versions ultérieures uniquement. Si vous souhaitez utiliser le nouvel outil de sauvegarde et de restauration sur des serveurs qui font partie d'un anneau de répliques, veillez à les mettre à niveau vers eDirectory 8.5 ou une version ultérieure.

Étant donné que le client eMBox peut être exécuté en mode de traitement par lots, vous pouvez l'utiliser pour effectuer des sauvegardes sans surveillance à l'aide de l'outil Backup eMTool d'eDirectory.

Le fichier `eMBoxClient.jar` est installé sur votre serveur dans le cadre de l'installation d'eDirectory. Vous pouvez également copier ce fichier et l'exécuter sur toute machine équipée de Sun JVM 1.3.1. Pour plus d'informations, reportez-vous aux sections « eDirectory Management Toolbox » page 593 et « Exécution du client sur un poste de travail » page 596.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde » page 445 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

- « Conditions préalables » page 605
- « Sauvegarde manuelle à l'aide du client eMBox » page 606
- « Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox » page 607
- « Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox » page 609
- « Restauration à partir de fichiers de sauvegarde avec le client eMBox » page 611

Conditions préalables

❒ Assurez-vous que le fichier `eMBoxClient.jar` se trouve sur la machine à partir de laquelle vous souhaitez lancer la sauvegarde.

Ce fichier est installé sur votre serveur dans le cadre de l'installation d'eDirectory. Vous pouvez le copier afin de l'utiliser sur un autre ordinateur équipé de Sun JVM 1.3.1. Il vous permet d'effectuer à partir d'une même machine des sauvegardes pour plusieurs serveurs, si vous disposez d'un accès derrière le pare-feu. Pour plus d'informations, reportez-vous à la « Utilisation du client à ligne de commande » page 594.

- ❒ Si vous prévoyez d'utiliser des fichiers journaux de transactions individuelles pour le serveur concerné, veillez à les activer avant d'effectuer une sauvegarde.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas.

  Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458. Pour savoir comment les activer, reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox » page 609.

- ❒ Consultez la description des options de la ligne de commande à la section « Options de ligne de commande pour la sauvegarde et la restauration » page 474.

- ❒ Pour les arborescences multiserveurs, nous vous conseillons de mettre à niveau tous les serveurs qui partagent des répliques avec le serveur concerné en installant eDirectory 8.5 ou une version ultérieure.

Sauvegarde manuelle à l'aide du client eMBox

Le client eMBox vous permet de sauvegarder les données d'une base de données eDirectory dans un fichier que vous indiquez, sur le serveur sur lequel la sauvegarde est en cours d'exécution. Le fichier de sauvegarde (ou le jeu de fichiers) contient les informations nécessaires pour restaurer eDirectory dans l'état où il se trouvait au moment de la sauvegarde. Le résultat du processus de sauvegarde est enregistré dans le fichier journal que vous spécifiez.

Pour sauvegarder la base de données eDirectory sur un serveur à l'aide du client eMBox, procédez comme suit :

1. Lancez le client eMBox en mode interactif.
   - Linux : entrez `edirutil -i` dans la ligne de commande.
   - Windows : exécutez *`unité`*`\novell\nds\edirutil.exe -i`.

   Le fichier `edirutil` constitue un raccourci pour exécuter le client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory. Vous pouvez aussi entrer les informations manuellement, comme expliqué à la section « Configuration du chemin et du chemin de classe pour le client » page 596.

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : client eMBox>

2. Connectez-vous au serveur à sauvegarder en entrant

   `login -s` *`nom_ou_adresse_IP_serveur`* `-p` *`numéro_port`* `-u` *`nom_utilisateur.contexte`* `-w` *`mot_de_passe`*

   Par exemple, sous Windows, spécifiez

   ```
   login -s 151.155.111.1 -p 8009 -u admin.ma_société -w mon_mot_de_passe
   ```

   Si un message d'erreur indique qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE listés à la section « Établissement d'une connexion sécurisée avec le client » page 602.

Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory » page 602.

Le client eMBox indique si la connexion a abouti.

3 Entrez la commande de sauvegarde à l'invite du client eMBox, en suivant le modèle général ci-dessous :

```
backup -b -f nom_et_chemin_fichier_sauvegarde -l
nom_et_chemin_fichier_journal_sauvegarde -u nom_et_chemin_fichier_inclusion -t
-w -a
```

Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

Par exemple, sous Windows, spécifiez

```
backup -b -f c:\backups\8_20_2001.bak -l c:\backups\backup.log -u
c:\backups\fichierinclusion.txt -t -w -a
```

Cet exemple de commande permet d'effectuer une sauvegarde complète (`-b`), le fichier de sauvegarde étant enregistré sous `c:\backups\8_20_2001.bak` et le fichier journal correspondant sous `c:\backups\backup.log`. Cette commande indique que d'autres fichiers doivent être sauvegardés avec la base de données :

- les fichiers mentionnés dans un fichier d'inclusion (`-u c:\backups\mon_fichier_inclusion.txt`) préalablement créé par l'administrateur ;
- les fichiers de flux (`-t`).

  Cet exemple de commande indique que le fichier de sauvegarde doit être remplacé (`-w`). Par conséquent, si un fichier portant le même nom existe, Backup eMTool le remplace.
- L'option `-a` permet de supprimer les anciens fichiers journaux du répertoire des fichiers journaux de transaction individuelle au cours d'une sauvegarde continue à chaud.

Le client eMBox indique si la sauvegarde a réussi.

4 Déconnectez-vous du serveur. Pour ce faire, entrez la commande suivante :

```
Déconnexion
```

5 Quittez le client eMBox en entrant la commande suivante :

```
exit
```

6 Veillez à effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde sur bande par mesure de sécurité. Backup eMTool les place uniquement sur le serveur.

Pour plus d'informations sur les sauvegardes manuelles, reportez-vous à la « Sauvegarde manuelle avec DSBK » page 470.

Sauvegardes sans surveillance à l'aide d'un fichier de traitement par lots et du client eMBox

Pour exécuter des sauvegardes sans surveillance d'd'eDirectory avec le client eMBox, vous devez utiliser un fichier de traitement par lots. Supposons que vous souhaitiez effectuer une sauvegarde complète d'eDirectory toutes les semaines et une sauvegarde incrémentielle toutes les nuits.

Vous pouvez, dans ce cas, exécuter le client eMBox en mode de traitement par lots en utilisant un fichier système, un fichier propre au client eMBox, ou encore une combinaison des deux. Pour plus d'informations, reportez-vous à la section « Exécution du client à ligne de commande en mode de traitement par lots » page 599.

La procédure ci-dessous met en oeuvre un fichier système de traitement par lots:

1. Créez un fichier système de traitement par lots pour sauvegarder les serveurs et suivez le modèle général ci-dessous, c'est-à-dire avec une ligne par serveur.

   Dans les environnements Windows et Linux, il s'agit du modèle général suivant :

   ```
   java -cp path/eMBoxClient.jar embox -s server_name -p port_number -u
   username.context -w password -t backup.backup -b -f backup_filename_and_path -
   l backup_log_filename_and_path -u include_file_filename_and_path -t -w
   ```

   Pour obtenir des exemples et des explications supplémentaires, reportez-vous à la section « Exemple de fichier système de traitement par lots pour les sauvegardes sans surveillance » page 608.

   Pour les sauvegardes incrémentielles nocturnes, vous pouvez utiliser le même fichier que celui employé pour les sauvegardes complètes, en remplaçant toutefois l'option `-b` par l'option `-i`. Il est également judicieux d'utiliser des noms de fichiers de sauvegarde différents pour les sauvegardes incrémentielles et complètes.

   Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory » page 602. Si vous voulez utiliser une connexion sécurisée, reportez-vous à la section « Établissement d'une connexion sécurisée avec le client » page 602. Pour toute information sur l'utilisation d'un fichier de traitement par lots propre au client eMBox, reportez-vous à la section « Exécution du client à ligne de commande en mode de traitement par lots » page 599.

2. Exécutez les fichiers de traitement par lots sans surveillance, conformément aux instructions de la documentation de votre système d'exploitation ou du logiciel tiers.

3. Prévoyez d'effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, afin de placer les fichiers de sauvegarde d'eDirectory en sécurité, en les enregistrant sur une bande.

   Backup eMTool les place uniquement sur le serveur.

4. Vérifiez périodiquement les résultats enregistrés dans le fichier journal que vous avez spécifié, pour vous assurer que les sauvegardes sans surveillance aboutissent.

Exemple de fichier système de traitement par lots pour les sauvegardes sans surveillance

Un exemple de fichier système de traitement par lots est fourni ci-dessous.

Exemple de fichier de traitement par lots pour Windows

```
java -cp c:\novell\nds\embox\eMBoxClient.jar embox -s myserver -p 8008 -u
admin.myorg -w mypassword -n -t backup.backup -b -f c:\backup\backup.bak -u
c:\backup\includes\includefile.txt -l c:\backup\backup.log -t -w
```

Les options suivantes figurent dans cet exemple de fichier de traitement par lots.

- Une sauvegarde complète est spécifiée (`-b`).
- Un fichier d'inclusion est spécifié `-u`. Cette option est facultative. Le fichier d'inclusion vous permet d'introduire dans la sauvegarde d'autres fichiers de votre choix. Il doit avoir été créé auparavant.
- Les fichiers de flux (`-t`) sont également sauvegardés.
- L'option permettant d'écraser un fichier de sauvegarde du même nom est spécifiée (`-w`).

IMPORTANT : s'il existe déjà un fichier portant le même nom (ce qui est probable si vous utilisez régulièrement le même fichier de traitement par lots), votre sauvegarde aboutit uniquement si vous employez l'option `-w` pour écraser le fichier de sauvegarde existant.

En mode de traitement par lots, s'il existe un fichier du même nom et que l'option `-w` n'est pas spécifiée, le comportement par défaut consiste à ne pas écraser le fichier, ce qui empêche la création d'une sauvegarde. En mode interactif, si vous n'utilisez pas l'option `-w`, le client eMBox vous demande si vous souhaitez écraser le fichier.

Si vous effectuez une sauvegarde du système de fichiers peu après chaque sauvegarde complète ou incrémentielle d'eDirectory, les fichiers de sauvegarde précédents doivent avoir été copiés sur une bande. Vous pouvez donc écraser le fichier de sauvegarde existant sans crainte.

- Comme un port non sécurisé est utilisé dans cet exemple (`-p 8008`), une connexion non sécurisée est spécifiée (`-n`).

Configuration des fichiers journaux de transactions individuelles à l'aide du client eMBox

Le client eMBox vous permet de modifier les paramètres des fichiers journaux de transactions individuelles. Vous pouvez effectuer les tâches suivantes :

- rechercher la configuration actuelle ;
- activer ou désactiver la fonction de consignation de transactions individuelles par fichier ;

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas.
- modifier le répertoire des fichiers journaux de transactions individuelles ;
- définir la taille minimale et maximale des fichiers journaux de transactions individuelles ;
- rechercher le fichier journal de transaction individuelle actuel ainsi que le dernier fichier journal inutilisé ;
- activer ou désactiver la consignation des fichiers de flux pour les fichiers journaux de transaction individuelle

Pour plus d'informations sur la consignation de transactions individuelles par fichier, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

1. Lancez le client eMBox en mode interactif :
   - Linux : entrez `edirutil -i` dans la ligne de commande.
   - Windows : exécutez *`unité`*`\novell\nds\edirutil.exe -i`.

   Le fichier `edirutil` constitue un raccourci pour exécuter le client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory, et inclut l'option `-ns` nécessaire. Vous pouvez également entrer les options manuellement, comme expliqué à la section « Exécution du client sur un poste de travail » page 596.

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : client eMBox>
2. Connectez-vous au serveur sur lequel vous souhaitez configurer la consignation de transactions individuelles par fichier, en entrant

   `login -s` *`nom_ou_adresse_IP_serveur`* `-p` *`numéro_port`* `-u` *`nom_utilisateur.contexte`* `-w` *`mot_de_passe`*

   Par exemple, sous Windows, spécifiez

```
login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
```

Si un message d'erreur indique qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE listés à la section « Établissement d'une connexion sécurisée avec le client » page 602.

Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory » page 602.

Le client eMBox indique si la connexion a abouti.

3 (Facultatif) Affichez les paramètres actuels en entrant la commande suivante :

```
getconfig
```

Aucun paramètre n'est nécessaire.

Voici un exemple des informations que vous recevez :

```
Roll forward log status OFF
Stream file logging status OFF
Current roll forward log directory C:\rfl\nds.rfl
Minimum roll forward log size (bytes) 104857600
Maximum roll forward log size (bytes) 4294705152
Last roll forward log not used 00000000.log
Current roll forward log 00000001.log
*** END ***
```

4 Modifiez les paramètres à l'aide de la commande setconfig et suivez le modèle général ci-dessous :

```
setconfig [-L|-l] [-T|-t] -r chemin_journaux_transactions_individuelles -n
taille_minimale_fichier -m taille_maximale_fichier
```

Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance.

En principe, vous devriez réserver un volume/une partition de disque à ces fichiers journaux, afin de faciliter le contrôle de l'espace disque et des droits.

AVERTISSEMENT : si vous activez la consignation de transactions individuelles par fichier, n'utilisez pas l'emplacement par défaut. Pour assurer une tolérance aux pannes, placez le répertoire sur un volume/une partition de disque et un périphérique de stockage différents de ceux d'eDirectory. Le répertoire des fichiers journaux de transactions individuelles doit résider sur le serveur us modifiez la configuration de sauvegarde.

IMPORTANT : si vous activez la consignation de transactions individuelles par fichier, vous devez surveiller l'espace disque sur le volume où vous placez les fichiers journaux de transactions individuelles. Si vous ne le surveillez pas, le répertoire des fichiers journaux s'étend jusqu'à saturer le volume/la partition de disque. Si ces journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Nous vous conseillons de sauvegarder et de supprimer périodiquement du serveur les fichiers journaux de transactions individuelles inutilisés. Reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462.

---

5 Déconnectez-vous du serveur. Pour ce faire, entrez la commande suivante :

```
Déconnexion
```

6 Quittez le client eMBox en entrant la commande suivante :

```
exit
```

Restauration à partir de fichiers de sauvegarde avec le client eMBox

Le client eMBox vous permet de restaurer une base de données eDirectory à partir des données stockées dans les fichiers de sauvegarde que vous avez créés manuellement ou à l'aide d'un fichier de traitement par lots. Les résultats de la restauration sont consignés dans le fichier journal que vous indiquez.

Le client eMBox vous permet en outre d'utiliser des options de restauration avancées qui ne sont pas disponibles dans iManager. Celles-ci sont présentées dans le tableau « Options de ligne de commande pour la sauvegarde et la restauration » page 474, sous restore et restadv.

Pour restaurer une base de données eDirectory sur un serveur à l'aide du client eMBox, procédez comme suit :

1. Vérifiez que vous avez collecté les fichiers de sauvegarde nécessaires, comme expliqué à la « Préparation d'une restauration » page 463.
2. Lancez le client eMBox en mode interactif :
   - Linux : entrez `edirutil -i` dans la ligne de commande.
   - Windows : exécutez *unité*`\novell\nds\edirutil.exe -i`.

   Le fichier `edirutil` constitue un raccourci pour exécuter le client eMBox. Il pointe vers l'exécutable Java et l'emplacement par défaut où le client eMBox est installé avec eDirectory, et inclut l'option -ns nécessaire. Vous pouvez également entrer les informations manuellement, comme expliqué à la section « Exécution du client sur un poste de travail » page 596.

   Lorsque le client eMBox s'ouvre, l'invite correspondante s'affiche : client eMBox>
3. Connectez-vous au serveur à restaurer. Pour ce faire, entrez

   `login -s` *`nom_ou_adresse_IP_serveur`* `-p` *`numéro_port`* `-u` *`nom_utilisateur.contexte`* `-w` *`mot_de_passe`*

   Par exemple, sous Windows, spécifiez

   ```
   login -s 151.155.111.1 -p 8009 -u admin.mycompany -w mypassword
   ```

   Si un message d'erreur indique qu'il est impossible d'établir une connexion sécurisée, vérifiez si votre machine possède les fichiers JSSE listés à la section « Établissement d'une connexion sécurisée avec le client » page 602.

   Pour savoir quel numéro de port utiliser, reportez-vous à la section « Recherche des numéros de port eDirectory » page 602.

   Le client eMBox indique si la connexion a abouti.
4. Entrez la commande `restore` à l'invite du client eMBox, en suivant le modèle général ci-dessous :

   `restore -r -a -o -f` *`chemin_et_nom_fichier_sauvegarde_complète`* `-d` *`emplacement_journaux_transactions_individuelles`* `-l` *`chemin_et_nom_journal_restauration`*

   Chaque paramètre doit être délimité par un espace. L'ordre des paramètres n'a pas d'importance. Veillez à utiliser le paramètre `-r` pour restaurer la base de données eDirectory proprement dite. Sinon, seuls les autres types de fichiers seront restaurés. Si vous souhaitez que la base de données soit ouverte et activée une fois la restauration terminée, veillez à spécifier les paramètres `-a` et `-o`.

Si vous restaurez des fichiers journaux de transaction individuelle, veillez à inclure leur chemin d'accès complet, y compris le répertoire créé automatiquement par eDirectory, généralement dénommé `\nds.rfl`. Pour plus d'informations sur ce répertoire, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles » page 461.

Par exemple :

```
restore -r -a -o -f sys:/backup/nds.bak -d $HOME/rfldir/nds.rfl -l $HOME/
backups/backup.log
```

Cet exemple de commande indique que la base de données proprement dite doit être restaurée (`-r`), et qu'elle doit être activée (`-a`) et ouverte (`-o`) une fois la vérification de la restauration effectuée. Le paramètre `-f` indique où se trouve le fichier de sauvegarde complète, le paramètre `-d` désigne l'emplacement des fichiers journaux de transaction individuelle et le paramètre `-l`, le fichier journal dans lequel les résultats de la restauration sont consignés.

Le client eMBox restaure la sauvegarde complète, puis vous invite à indiquer les fichiers de sauvegarde incrémentielle.

5 (Conditionnel) Si vous restaurez des fichiers de sauvegarde incrémentielle, indiquez le chemin d'accès et le nom de chaque fichier lorsque le client eMBox vous invite à désigner le fichier incrémentiel suivant.

Il vous fournit l'ID du fichier suivant, que vous pouvez trouver dans l'en-tête du fichier de sauvegarde incrémentielle.

Le client eMBox indique si la restauration a réussi.

6 (Conditionnel) Si la restauration échoue, consultez les erreurs dans le fichier journal.

Si la vérification de la restauration échoue, reportez-vous à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

REMARQUE : si le serveur que vous restaurez partage une réplique avec un serveur qui exécute une version d'eDirectory antérieure à 8.5, le journal de restauration indique l'erreur –666 (version DS incompatible) pour cette réplique.

---

7 Déconnectez-vous du serveur. Pour ce faire, entrez la commande suivante :

```
Déconnexion
```

8 Quittez le client eMBox en entrant la commande suivante :

```
exit
```

9 (Conditionnel) Si vous avez restauré les fichiers de sécurité NICI, redémarrez le serveur pour réinitialiser NICI une fois la restauration terminée, puis restaurez DIB.

10 Vérifiez que le serveur fonctionne normalement.

11 (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, vous devez recréer la configuration de votre choix afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

La restauration est à présent terminée et NICI réinitialisé avec les fichiers correspondants restaurés, ce qui vous permet d'accéder aux informations codées. Si vous utilisez la fonction de consignation de transactions individuelles par fichier, vous vous êtes préparé contre toute nouvelle défaillance en réactivant cette fonction à l'issue de la restauration, puis en effectuant une nouvelle sauvegarde complète.

Sauvegarde et restauration à l'aide de NetIQ iManager

Les tâches de sauvegarde, de configuration de la sauvegarde et de restauration de NetIQ iManager vous donnent accès à la plupart des fonctions de l'outil de sauvegarde d'eDirectory. En outre, iManager vous permet d'effectuer des tâches sur vos serveurs à partir d'un navigateur, même si vous n'êtes pas derrière le pare-feu. Pour plus d'informations sur NetIQ iManager, reportez-vous au *Guide d'administration de NetIQ iManager* (https://www.netiq.com/documentation/imanager-3/imanager_admin/).

Les tâches non disponibles dans iManager sont la sauvegarde à froid (sauvegarde complète lorsque la base de données est fermée), la sauvegarde sans surveillance et les options de restauration avancées. Pour effectuer ces tâches, vous devez utiliser DSBK, comme expliqué à la « Utilisation de DSBK » page 466.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde » page 445 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Dans cette section :

- « Sauvegarde manuelle avec iManager » page 613
- « Configuration des fichiers journaux de transactions individuelles avec iManager » page 615
- « Restauration à partir de fichiers de sauvegarde avec iManager » page 616

Sauvegarde manuelle avec iManager

Utilisez la fonction Sauvegarder d'iManager à partir d'un navigateur pour sauvegarder les données d'une base de données eDirectory dans un ou plusieurs fichiers du serveur sur lequel la sauvegarde a lieu. Vous pouvez exécuter une sauvegarde complète ou incrémentielle.

Les fichiers de sauvegarde contiennent les informations nécessaires pour restaurer eDirectory dans l'état où il se trouvait au moment de la sauvegarde. Le résultat du processus de sauvegarde est enregistré dans le fichier journal que vous spécifiez.

Les sauvegardes effectuées à l'aide d'iManager sont des sauvegardes continues à chaud. Cela signifie que la base de données eDirectory est ouverte et accessible pendant le processus, mais que vous obtenez quand même une sauvegarde complète qui constitue un instantané de la base au moment où la sauvegarde a commencé.

Notez que pour effectuer une sauvegarde à froid (avec la base de données fermée) ou sans surveillance, vous devez utiliser DSBK. Reportez-vous à la section « Sauvegarde manuelle avec DSBK » page 470.

Avant d'exécuter des tâches de sauvegarde et de restauration, consultez la « Liste de contrôle pour la sauvegarde » page 445 pour une vue d'ensemble des éléments à considérer lors de la préparation d'une stratégie de sauvegarde efficace pour eDirectory.

Conditions préalables

- Déterminez les autres fichiers à sauvegarder avec eDirectory et créez au besoin un fichier d'inclusion.

  Vous pouvez sauvegarder les fichiers NICI et de flux en cochant les cases correspondantes dans iManager. Nous vous recommandons de sauvegarder systématiquement les fichiers NICI.

  Pour inclure d'autres fichiers, tels qu'`autoexec.ncf`, vous devez indiquer leurs noms et leurs chemins d'accès dans un fichier d'inclusion. Séparez les chemins d'accès et les noms de fichier par un point-virgule, sans inclure de retour chariot ni d'espace. Par exemple, `sys:\system\autoexec.ncf;sys:\etc\hosts;`.

- Prévoyez d'effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, si vous devez enregistrer les fichiers de sauvegarde d'eDirectory sur bande. L'outil de sauvegarde les enregistre uniquement sur le serveur.

  SUGGESTION : pour faciliter le transfert des fichiers de sauvegarde sur un autre périphérique de stockage, vous pouvez spécifier la taille maximale de ces fichiers. Vous pouvez également utiliser un logiciel tiers pour les compresser après leur création. Le taux de compression atteint environ 80 %.

- Si vous prévoyez d'utiliser des fichiers journaux de transactions individuelles pour le serveur concerné, veillez à les activer avant d'effectuer une sauvegarde.

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas.

  Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458. Pour savoir comment les activer, reportez-vous à la section « Configuration des fichiers journaux de transactions individuelles avec iManager » page 615.

- Pour les arborescences multiserveurs, nous vous conseillons de mettre à niveau tous les serveurs qui partagent des répliques avec le serveur concerné en installant eDirectory 8.5 ou une version ultérieure.

Procédure

Pour sauvegarder la base de données eDirectory sur un serveur à l'aide d'iManager, procédez comme suit :

SUGGESTION : l'aide en ligne fournit une description des options disponibles dans iManager.

1. Cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Maintenance** > **Sauvegarder**.
3. Spécifiez le serveur qui effectuera la sauvegarde, puis cliquez sur **Suivant**.
4. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel la sauvegarde doit être effectuée, puis cliquez sur **Suivant**.
5. Spécifiez les options relatives au fichier de sauvegarde, puis cliquez sur **Suivant**.

   Pour ne sauvegarder que les modifications apportées à la base de données depuis la dernière sauvegarde, cliquez sur **Effectuer une sauvegarde incrémentielle**.

6 Pour supprimer les anciens fichiers journaux du répertoire des fichiers journaux de transaction individuelle au cours d'une sauvegarde continue à chaud, sélectionnez **Supprimer les anciens fichiers RFL**.

7 Désignez d'autres fichiers à sauvegarder.

Si aucun fichier supplémentaire n'est désigné, seule la base de données eDirectory est sauvegardée.

Nous vous conseillons de sauvegarder systématiquement les fichiers de sécurité NICI.

8 Suivez les instructions en ligne pour terminer la sauvegarde.

9 Veillez à effectuer une sauvegarde du système de fichiers peu après avoir sauvegardé eDirectory, afin d'enregistrer les fichiers de sauvegarde sur bande par mesure de sécurité. L'outil de sauvegarde les enregistre uniquement sur le serveur.

Configuration des fichiers journaux de transactions individuelles avec iManager

Utilisez l'option Configuration de la sauvegarde à partir d'un navigateur pour modifier les paramètres des fichiers journaux de transactions individuelles. Vous pouvez effectuer les tâches suivantes :

- activer ou désactiver la fonction de consignation de transactions individuelles par fichier ;

  Vous devez activer la fonction de consignation de transactions individuelles par fichier pour les serveurs faisant partie d'un anneau de répliques. Faute de quoi, des messages d'erreur s'afficheront lorsque vous tenterez de procéder à une restauration à partir des fichiers de sauvegarde et la base de données ne s'ouvrira pas.
- modifier le répertoire des fichiers journaux de transaction individuelle ;
- définir les tailles minimale et maximale des fichiers journaux de transaction individuelle ;
- déterminer le fichier journal de transaction individuelle actuel ainsi que le dernier fichier journal inutilisé ;
- activer ou désactiver la consignation des fichiers de flux pour les fichiers journaux de transaction individuelle.

Pour plus d'informations sur les fichiers journaux de transactions individuelles, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

SUGGESTION : l'aide en ligne fournit une description des options disponibles dans iManager.

---

1 Cliquez sur le bouton **Rôles et tâches**  .

2 Cliquez sur **Maintenance** > **Configuration de la sauvegarde**.

3 Spécifiez le serveur dont la configuration sera modifiée, puis cliquez sur **Suivant**.

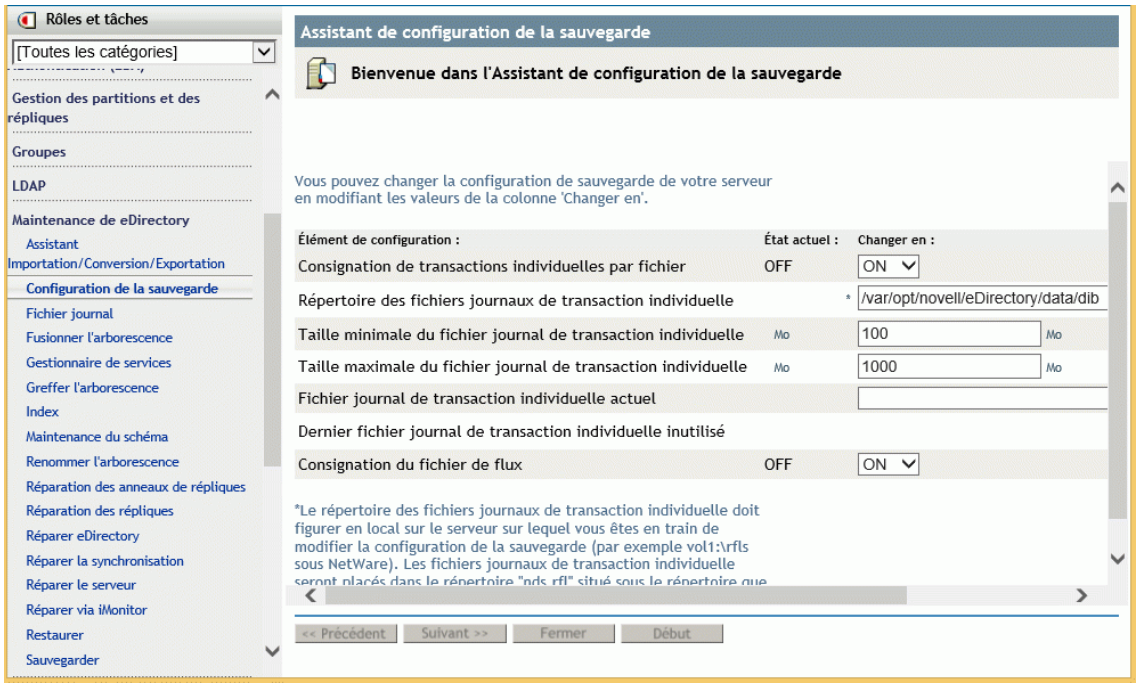
4 Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur dont vous souhaitez modifier la configuration, puis cliquez sur **Suivant**.

5 Apportez les modifications requises à la configuration de sauvegarde du serveur.

AVERTISSEMENT : si vous activez la consignation de transactions individuelles par fichier, n'utilisez pas l'emplacement par défaut. Pour assurer une tolérance aux pannes, placez le répertoire sur un volume/une partition de disque et un périphérique de stockage différents de ceux d'eDirectory. Le répertoire des fichiers journaux de transactions individuelles doit résider sur le serveur us modifiez la configuration de sauvegarde.

IMPORTANT : si vous activez la consignation de transactions individuelles par fichier, vous devez surveiller l'espace disque sur le volume où vous placez les fichiers journaux de transactions individuelles. Si vous ne le surveillez pas, le répertoire des fichiers journaux s'étend jusqu'à saturer le volume/la partition de disque. Si ces journaux ne peuvent pas être créés par manque d'espace disque, eDirectory cesse de fonctionner sur le serveur concerné. Nous vous conseillons de sauvegarder et de supprimer périodiquement du serveur les fichiers journaux de transactions individuelles inutilisés. Reportez-vous à la section « Sauvegarde et suppression des journaux de transactions individuelles » page 462.

Voici un exemple d'écran.



6 Suivez les instructions en ligne pour terminer l'opération.

Restauration à partir de fichiers de sauvegarde avec iManager

Utilisez l'option Restaurer dans un navigateur pour restaurer une base de données eDirectory à partir des données enregistrées dans des fichiers de sauvegarde. Les résultats de la restauration sont consignés dans le fichier journal que vous indiquez.

Pour la description du processus de restauration, reportez-vous à la section « Présentation du processus de restauration avec l'outil de restauration » page 450.

Notez que pour accéder aux options de restauration avancées, vous devez utiliser DSBK, comme expliqué à la section « Utilisation de DSBK » page 466.

Conditions préalables

❒ Placez tous les fichiers de sauvegarde dont vous avez besoin pour la restauration dans un répertoire du serveur sur lequel vous effectuez cette opération.

Reportez-vous aux sections « Préparation d'une restauration » page 463 et « Localisation des fichiers de sauvegarde requis pour une restauration » page 464.

❒ Vérifiez que eDirectory est déjà installé sur le serveur sur lequel vous effectuez la restauration, et qu'il fonctionne.

Par exemple, si la restauration est nécessaire en raison de la défaillance d'un périphérique de stockage, vous devez réinstaller eDirectory sur le nouveau périphérique. Si vous restaurez un serveur défaillant sur une nouvelle machine, ou transférez simplement un serveur d'une machine à une autre, vous devez installer le système d'exploitation ainsi que eDirectory sur la nouvelle machine.

❒ Consultez la description du processus de restauration dans la section « Présentation du processus de restauration avec l'outil de restauration » page 450.

Procédure

SUGGESTION : l'aide en ligne fournit une description des options disponibles dans iManager.

Pour restaurer la base de données eDirectory sur un serveur à l'aide d'iManager, procédez comme suit :

1. Vérifiez que vous avez collecté les fichiers de sauvegarde nécessaires, comme expliqué à la « Préparation d'une restauration » page 463.
2. Cliquez sur le bouton **Rôles et tâches**  .
3. Cliquez sur **Maintenance** > **Restaurer**.
4. Sélectionnez le serveur qui effectuera la restauration, puis cliquez sur **Suivant**.
5. Spécifiez un nom d'utilisateur, un mot de passe et un contexte pour le serveur sur lequel la restauration doit être effectuée, puis cliquez sur **Suivant**.
6. Indiquez les noms des fichiers de sauvegarde et des fichiers journaux à utiliser, puis cliquez sur **Suivant**.
7. Spécifiez les autres options de restauration, puis cliquez sur **Suivant**.

   Dans la plupart des cas, vous devez au moins cocher les cases suivantes :

   - **Restaurer la base de données**
   - **Activer la base de données restaurée après vérification**
   - **Ouvrir la base de données après restauration**
   - **Restaurer les fichiers de sécurité** (fichiers NICI)

   Nous vous recommandons de sauvegarder systématiquement les fichiers NICI afin de pouvoir lire les informations codées après une restauration.

   Si vous restaurez des fichiers journaux de transaction individuelle, veillez à inclure leur chemin d'accès complet, y compris le répertoire créé automatiquement par eDirectory, généralement dénommé `\nds.rfl`. Pour plus d'informations sur ce répertoire, reportez-vous à la section « Emplacement des fichiers journaux de transactions individuelles » page 461.
8. Suivez les instructions en ligne pour terminer la restauration.

   Si la vérification de la restauration échoue, reportez-vous à la « Récupération de la base de données en cas d'échec de la vérification de la restauration » page 485.

REMARQUE : si le serveur que vous restaurez partage une réplique avec un serveur qui exécute une version d'eDirectory antérieure à 8.5, le journal de restauration indique l'erreur –666 (version DS incompatible) pour cette réplique.

9 Si vous avez restauré les fichiers de sécurité NICI, redémarrez le serveur pour réinitialiser NICI une fois la restauration terminée.

10 Vérifiez que le serveur fonctionne normalement.

11 (Conditionnel) Si vous utilisez la consignation de transactions individuelles par fichier sur ce serveur, vous devez recréer la configuration de votre choix afin d'être certain que la fonction est activée et que les fichiers journaux sont enregistrés dans un emplacement assurant la tolérance aux pannes. Après avoir activé les journaux de transactions individuelles, vous devez également effectuer une nouvelle sauvegarde complète.

   Cette opération est nécessaire car, au cours d'une restauration, la consignation de transactions individuelles par fichier reprend sa configuration par défaut, autrement dit elle est désactivée et l'emplacement par défaut est rétabli. Vous devez effectuer une nouvelle sauvegarde complète afin de vous protéger contre toute défaillance susceptible de survenir avant la prochaine sauvegarde complète sans surveillance planifiée.

   Pour plus d'informations sur les fichiers journaux de transactions individuelles et leur emplacement, reportez-vous à la « Utilisation des fichiers journaux de transactions individuelles » page 458.

La restauration est à présent terminée et NICI réinitialisé avec les fichiers correspondants restaurés, ce qui vous permet d'accéder aux informations codées. Si vous utilisez la fonction de consignation de transactions individuelles par fichier, vous vous êtes préparé contre toute nouvelle défaillance en réactivant cette fonction à l'issue de la restauration, puis en effectuant une nouvelle sauvegarde complète.

23 Audit des événements eDirectory

Vous pouvez auditer les événements eDirectory de l'une des manières suivantes :

- « Audit avec Novell Audit » page 619
- « Audit avec XDAS » page 629
- « Audit à l'aide de CEF » page 651
- « Caching des événements de journal » page 670
- « Audit LDAP » page 671

Audit avec Novell Audit

Grâce au paquetage Novell Audit, vous pouvez envoyer des événements générés par eDirectory à un client d'audit externe à des fins de surveillance.

eDirectory Instrumentation est fourni avec eDirectory 9.2. Vous devez installer ce paquetage pour pouvoir auditer les événements eDirectory à l'aide de Novell Audit.

Utilisez les informations suivantes pour installer, configurer ou désinstaller Novell Audit sur les serveurs Linux et Windows :

- « Plates-formes prises en charge » page 619
- « Conditions préalables » page 620
- « Installation des paquetages Novell Audit » page 620
- « Installation du plug-in Novell Audit iManager » page 621
- « Configuration de Novell Audit Platform Agent » page 621
- « Configuration de Novell Audit pour eDirectory » page 622
- « Chargement du module d'audit » page 623
- « Comprendre la création de rapports d'événements eDirectory » page 624
- « Comprendre les types d'événements eDirectory » page 624
- « Comprendre le filtrage des événements d'audit eDirectory » page 626
- « Surveillance des événements eDirectory avec Sentinel » page 627
- « Désinstallation des paquetages Novell Audit » page 629

Plates-formes prises en charge

Pour en savoir plus sur les plates-formes prises en charge et obtenir les instructions d'installation, reportez-vous au *Guide d'installation de NetIQ eDirectory*.

Conditions préalables

- ❒ L'audit eDirectory 9.2 nécessite au minimum la version 2.0.2.80 de Novell Audit Platform Agent.
- ❒ L'installation et l'utilisation du plug-in Novell Audit pour iManager nécessitent iManager 3.0 ou version ultérieure. Pour plus d'informations, consultez la page de documentation iManager.

Installation des paquetages Novell Audit

- « Linux » page 620
- « Windows » page 621

Linux

Installation d'eDirectory Instrumentation en tant qu'utilisateur root

Si le fichier de configuration d'Audit Platform Agent (`logevent.conf`) existe déjà dans le répertoire `/etc`, sauvegardez le fichier avant d'installer les paquetages d'audit car le nouveau paquetage écrase la configuration existante.

Si le module Audit est déjà chargé, déchargez le module `auditds` en utilisant la commande `ndstrace -c "unload auditds"`.

Pour le paquetage d'audit 64 bits :

1. Installez `novell-AUDTplatformagent-2.0.2-80.x86_64.rpm` à partir du répertoire de configuration de la version extraite d'eDirectory destinée à la plate-forme Linux.

   ```
   #rpm -ivh /root/eDirectory/setup/novell-AUDTplatformagent-2.0.2-80.x86_64.rpm
   ```

2. Installez `novell-AUDTedirinst-9.2-`*`xx`*`.x86_64.rpm` à partir du répertoire de configuration de la version extraite d'eDirectory destinée à la plate-forme Linux.

   REMARQUE : en cas de mise à niveau du serveur eDirectory, `novell-AUDTedirinst-9.2-xx.x86_64.rpm` est automatiquement mis à niveau s'il est déjà installé.

   ```
   #rpm -ivh <eDirectory build extracted folder>/eDirectory/setup/novell-
   AUDTedirinst-9.2-xx.x86_64.rpm
   ```

Exécutez `ndstrace -c "load auditds"` pour charger le module `auditds`.

Installation d'eDirectory Instrumentation en tant qu'utilisateur non-root

Pour le paquetage d'audit 64 bits :

1. Installez Platform Agent (PA) en tant qu'utilisateur non-root. Pour installer PA, rendez-vous sur le site Web des téléchargements NetIQ et le Novell Audit Platform Agent Guide (Guide de Novell Audit Platform Agent [Sentinel Plug-Ins 2011.1r3]).
2. Arrêtez le serveur eDirectory.
3. Extrayez le RPM eDirectory Instrumentation à l'aide de la commande suivante.:

   ```
   #rpm2cpio novell-AUDTedirinst-9.2-xx.x86_64.rpm | cpio -div
   ```

4. Copiez les fichiers extraits pour l'utilisateur non-root installé dans le répertoire `lib64` à l'aide de la commande suivante :

```
cp -r ./opt/novell/eDirectory/lib64/* <eDirectory build extracted folder>/
eDirectory/opt/novell/eDirectory/lib64/
```

5 Redémarrez le serveur eDirectory.

6 Exécutez `ndstrace -c "load auditds"` pour charger le module `auditds`.

Windows

Si le fichier de configuration d'Audit Platform Agent (`logevent.cfg`) existe déjà dans le répertoire `C:\WINDOWS`, sauvegardez le fichier avant d'installer les outils car le nouveau paquetage écrase la configuration existante.

Pour une installation 64 bits des paquetages d'audit et d'Audit Platform Agent, exécutez le fichier `Novell_Audit_PlatformAgent_Win64.exe` à partir du répertoire `<DossierProgrammeInstallation>/windows/x64/auditds/`

REMARQUE

- Si vous mettez à niveau un serveur eDirectory sur lequel est installé eDirectory Instrumentation, les fichiers eDirectory Instrumentation sont automatiquement mis à niveau. Si vous utilisez actuellement eDirectory 9.0 SP2 ou une version antérieure, vous devez mettre les fichiers d'instrumentation manuellement avant de mettre à niveau votre serveur eDirectory.
- Si vous mettez à niveau le serveur eDirectory en tant qu'utilisateur non-root, vous devez mettre les fichiers d'instrumentation manuellement avant de mettre à niveau votre serveur eDirectory.

Installation du plug-in Novell Audit iManager

Pour configurer l'audit des événements eDirectory à l'aide de Novell Audit Platform Agent, vous devez commencer par installer le plug-in Novell Audit pour iManager.

L'installation et l'utilisation du plug-in Novell Audit iManager requiert iManager 3.0 ou version ultérieure. Consultez le *Guide d'installation d'iManager* pour connaître les exigences d'installation et les instructions relatives au téléchargement d'iManager.

Le plug-in Novell Audit pour iManager est fourni avec les plug-ins d'eDirectory 9.2, qui peuvent être téléchargés à partir du site de téléchargement (https://download.novell.com/Download?buildid=G_8Eymx0QtI~).

Les instructions d'installation sont disponibles sur la page de téléchargement des plug-ins eDirectory 9.2 pour iManager 3.2 (https://download.novell.com/Download?buildid=G_8Eymx0QtI~).

Configuration de Novell Audit Platform Agent

Si Audit Platform Agent n'est pas déjà configuré, modifiez le fichier de configuration de Platform Agent pour définir l'adresse hôte du serveur d'audit dans `LogHost`. Par défaut, le programme d'installation place le fichier de configuration dans le répertoire suivant :

- Linux : `/etc/logevent.conf`
- Windows : *`répertoire_Windows`*`\logevent.cfg`

Par exemple, modifiez l'attribut `LogHost` comme suit :

```
LogHost=192.168.1.8
```

Pour plus d'informations, consultez la section « Configuration d'Audit Platform Agent » du *Guide d'administration de Novell Audit 2.0.*

Configuration de Novell Audit pour eDirectory

Pour configurer l'audit des événements eDirectory avec Novell Audit Platform Agent à l'aide d'iManager, sélectionnez les types d'événements eDirectory que vous souhaitez auditer.

1. Connectez-vous à la iManager en utilisant l'URL suivante :

   `https://ip_address_or_DNS/nps/`

   où *`adresse_ip_ou_DNS`* représente l'adresse IP ou le nom DNS de votre serveur iManager. Par exemple :

   `https://111.111.1.1/nps/`

2. Sous **Rôles et tâches**, sélectionnez **Audit eDirectory > Configuration de l'audit**.
3. Parcourez et sélectionnez l'objet Serveur NCP qui correspond au serveur eDirectory à partir duquel vous souhaitez collecter les événements. Cliquez sur **OK**.
4. Cliquez sur l'onglet **Novell Audit** pour afficher la page Paramètres des outils eDirectory.
5. Si vous ne voulez pas que eDirectory envoie des événements répliqués à une autre réplique dans l'anneau de répliques, sélectionnez **Ne pas envoyer d'événements répliqués**.

   Vous pouvez utiliser cette option pour filtrer le bruit des événements inutiles et réduire la taille du journal.
6. Si vous désirez activer la création de rapports pré-événements à insertion automatique, sélectionnez **Enregistrer les événements avec insertion automatique**.

   Notez que si vous sélectionnez cette option, les performances d'eDirectory peuvent en pâtir.
7. Sélectionnez les types d'événements que vous souhaitez auditer.
8. Si vous souhaitez filtrer des événements sur une ou plusieurs classes d'objet spécifiques, procédez comme suit.

   8a Cliquez sur l'un des objets suivants comportant un lien hypertexte :

   - **Objets** > **Créer**
   - **Objets** > **Supprimer**
   - **Attributs** > **Ajouter valeur**
   - **Attributs** > **Supprimer valeur**
   - **LDAP** > **Ajout LDAP**
   - **LDAP** > **Modification LDAP**
   - **LDAP** > **Suppression LDAP**
   - **LDAP** > **Modification DN LDAP**

   8b Dans la liste **Classes d'objet disponibles**, sélectionnez les classes d'objet avec lesquelles vous souhaitez auditer les événements et cliquez sur la flèche de droite.

   8c Cliquez sur **OK**, puis à nouveau sur **OK**.
9. Si vous souhaitez filtrer des événements pour un ou plusieurs attributs, procédez comme suit :

   9a Cliquez sur l'un des objets suivants comportant un lien hypertexte :

   - **Attributs** > **Ajouter valeur**
   - **Attributs** > **Supprimer valeur**

9b Dans la liste **Attributs disponibles**, sélectionnez les attributs avec lesquels vous souhaitez auditer les événements et cliquez sur la flèche de droite.

9c Cliquez sur **OK**, puis à nouveau sur **OK**.

REMARQUE : eDirectory évalue les événements individuellement par rapport à l'ensemble des filtres. Par conséquent, si un événement correspond à un filtre mais pas un autre, eDirectory envoie quand même l'événement au client. Pour plus d'informations sur le filtrage des événements, reportez-vous à la « Comprendre le filtrage des événements d'audit eDirectory » page 626.

---

10 Cliquez sur **Appliquer**, puis sur **OK**.

Les modifications apportées à votre configuration d'audit prennent effet dans les trois minutes. Si vous souhaitez les appliquer immédiatement, vous pouvez aussi décharger puis recharger le module Audit. Pour plus d'informations sur le chargement du module d'audit, consultez la « Chargement et déchargement des modules » page 640

REMARQUE : veuillez vérifier les attributs **Ajouter une valeur** et **Supprimer la valeur** pour générer les événements de métadonnées.

Chargement du module d'audit

Pour charger ou décharger le module d'audit, suivez la procédure adaptée à votre plate-forme :

- « Linux » page 623
- « Windows » page 623

Linux

1 Si le module d'audit n'est pas encore chargé, exécutez la commande ci-dessous pour le charger :

```
ndstrace -c "load auditds"
```

2 Pour décharger le module d'audit, exécutez la commande suivante :

```
ndstrace -c "unload auditds"
```

3 Pour charger automatiquement les modules d'audit au démarrage d'eDirectory, modifiez le fichier `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` en y ajoutant la ligne suivante :

```
auditds     auto     #eDirectory instrumentation
```

Windows

1 Chargez le module d'audit.

1a Cliquez sur **Démarrer > Panneau de configuration > Novell eDirectory Services**.

1b Sélectionnez **nauditds** sur l'onglet Services, puis cliquez sur **Démarrer**.

2 Déchargez le module d'audit.

2a Cliquez sur **Démarrer > Panneau de configuration > Novell eDirectory Services**.

2b Sélectionnez **nauditds** sur l'onglet Services, puis cliquez sur **Arrêter**.

3 Pour charger automatiquement le module d'audit au démarrage d'eDirectory, procédez comme suit :

   3a Cliquez sur **Démarrer > Panneau de configuration > Novell eDirectory Services**.

   3b Sélectionnez **nauditds** sur l'onglet **Services**, puis cliquez sur **Démarrer**.

   3c Sélectionnez **Automatique**, puis cliquez sur **OK**.

4 Pour désactiver le chargement automatique du module d'audit au démarrage d'eDirectory, procédez comme suit :

   4a Cliquez sur **Démarrer > Panneau de configuration > Novell eDirectory Services**.

   4b Sélectionnez **nauditds** sur l'onglet **Services**, puis cliquez sur **Démarrer**.

   4c Décochez la case **Automatique**, puis cliquez sur **OK**.

Comprendre la création de rapports d'événements eDirectory

eDirectory utilise deux systèmes de création de rapports d'événements différents pour consigner les événements, *journal* et *insertion automatique*. Par défaut, eDirectory consigne les événements à l'aide de la création de rapports d'événements sous forme de journal, mais vous pouvez activer celle à insertion automatique dans iManager. Pour plus d'informations sur l'activation de la création de rapports d'événements à insertion automatique, consultez la « Configuration de Novell Audit pour eDirectory » page 622

Journal : Ce système de création de rapports fournit une création de rapports postévénements synchrone. Une fois cette option activée, quand un événement est généré, eDirectory ajoute l'événement à la file d'attente de traitement des événements dans les journaux. eDirectory utilise alors un thread distinct pour traiter les événements dans la file d'attente et envoie ces événements au client d'audit.

Insertion automatique : Ce système de création de rapports fournit une création de rapports pré-événements synchrone. Une fois cette option activée, quand un événement est généré, eDirectory utilise le même thread pour envoyer l'événement directement au client. Notez que l'activation de la création de rapports d'événements à insertion automatique peut affecter les performances.

Comprendre les types d'événements eDirectory

Vous pouvez configurer eDirectory de sorte à consigner les événements dans les catégories suivantes :

- Métadonnées
- Objets
- Attributs
- Schéma
- Connexions
- Agent
- Divers
- Bindery
- Réplique
- Partition
- LDAP

Nous recommandons d’auditer l’ensemble par défaut de types d’événements suivant :

Catégorie	Type d'événement
Métadonnées	Tous les types d’événement
Objets	◆ Ajouter une propriété ◆ Autoriser la connexion ◆ Modifier le mot de passe ◆ Changer les équivalents de sécurité ◆ Créer ◆ Supprimer ◆ Supprimer la propriété ◆ Connexion ◆ Déconnexion ◆ Modifier RDN ◆ Déplacer (Destination) ◆ Déplacer (Source) ◆ Retirer ◆ Renommer ◆ Restauration ◆ Rechercher ◆ Vérifier le mot de passe
Attributs	Tous les types d’événement
Agent	◆ Rechargement de DS ◆ Fermeture de l'agent local ◆ Ouverture de l'agent local ◆ Chargement de NLM
Divers	◆ Clés de CA générées ◆ Clé publique recertifiée

Catégorie	Type d'événement
LDAP	◆ Liaison LDAP ◆ Modification LDAP ◆ Modification de mot de passe LDAP ◆ Ajout de réponse LDAP ◆ Annulation de la liaison LDAP ◆ Suppression LDAP ◆ Modification de DN LDAP ◆ Modification de réponse LDAP ◆ Recherche LDAP ◆ Liaison de réponse LDAP ◆ Suppression de réponse LDAP ◆ Ajout LDAP ◆ Recherche de réponse LDAP ◆ Modification de réponse DN LDAP

Comprendre le filtrage des événements d'audit eDirectory

Vous pouvez également filtrer les événements pour un(e) ou plusieurs classes ou attributs d'objet spécifiques, selon le type d'événement. eDirectory évalue tous les événements générés par rapport aux filtres configurés sur le serveur eDirectory et envoie *uniquement* les événements correspondants à ces filtres via le client d'audit.

Vous pouvez utiliser plusieurs filtres pour filtrer les événements eDirectory séparément. Par exemple, si vous configurez le filtrage sur une classe d'objet spécifique et sur un ou des attributs, eDirectory envoie tout événement correspondant à l'*un* de ces filtres au client. Vous ne pouvez pas configurer le filtrage de sorte que eDirectory n'envoie que les événements d'une certaine classe d'objet *et* certains attributs au client. Vous pouvez sélectionner plusieurs classes d'objet ou attributs pour lesquels vous souhaitez filtrer les événements eDirectory.

REMARQUE : Vous ne pouvez filtrer qu'un maximum combiné de 256 classes d'objet et attributs.

Cliquez sur l'un des types d'événement suivants comportant un lien hypertexte pour sélectionner un(e) ou plusieurs classes d'objet ou attributs à filtrer pour ce type d'événement :

Catégorie	Type d'événement	Type de filtrage
Objets	◆ Créer ◆ Supprimer	Classe d'objet
Attributs	◆ Ajouter valeur ◆ Supprimer la valeur	Classe d'objet ou attribut
LDAP	◆ Modification LDAP ◆ Suppression LDAP ◆ Modification de DN LDAP ◆ Ajout LDAP	Classe d'objet

Par exemple, si vous souhaitez être informé dès qu'une personne crée un compte utilisateur dans eDirectory, vous pouvez créer un filtre avec iManager afin de chercher uniquement les événements Créer un objet qui créent un objet Utilisateur.

Dans iManager, accédez à **Rôles et tâches > Audit eDirectory > Configuration de l'audit**, sélectionnez le serveur NCP à surveiller, puis cliquez sur l'onglet **Novell Audit**. Dans la liste Objets, cliquez sur le lien hypertexte **Créer**. Dans la liste **Classes d'objet disponibles**, sélectionnez **Utilisateur**, puis cliquez sur la flèche de droite pour déplacer **Utilisateur** vers la liste **Classes d'objet sélectionnées**, puis cliquez sur **OK**.

Une fois le filtre configuré, eDirectory vérifie tous les événements générés pour détecter tout événement de création par un utilisateur et les envoyer au client. Si vous ne sélectionnez pas d'autres types d'événement ou configurez un filtrage pour d'autres classes d'objet ou attributs, eDirectory audite *uniquement* les événements de création par un utilisateur.

Notez que les filtres de catégorie Objet et LDAP vous permettent uniquement de filtrer selon des classes d'objet, alors que les filtres de catégorie Attribut vous permettent de filtrer selon des classes d'objet et des attributs.

Si vous sélectionnez l'un des types d'événement ci-dessus mais n'indiquez pas de classe d'objet ou d'attribut avec lequel filtrer, eDirectory envoie tous les événements de ce type d'événement au client.

Surveillance des événements eDirectory avec Sentinel

NetIQ Sentinel fournit un collecteur pour collecter et auditer les événements eDirectory. Pour surveiller des types d'événements eDirectory spécifiques dans Sentinel, certains paramètres d'audit d'eDirectory doivent être configurés correctement.

Pour des informations détaillées sur la configuration des paramètres d'audit, consultez la « Configuration de Novell Audit pour eDirectory » page 622.

Pour plus d'informations sur la configuration de Sentinel pour collecter des événements eDirectory, consultez le *Guide du collecteur Sentinel pour eDirectory de NetIQ*, situé sur le site de plug-ins Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Audit des événements Créer un objet

Lors de la création d'un objet qui sera utilisé comme compte, eDirectory crée d'abord un objet générique, puis modifie la classe d'objet en type d'utilisateur avec un événement Ajouter valeur. Si vous souhaitez que Sentinel collecte correctement l'événement, vous devez activer l'audit des événements Créer un objet dans iManager. Si vous n'activez pas l'audit d'événement Ajouter valeur, le collecteur Sentinel ne peut pas analyser les événements Créer un objet et génèrera un événement « Erreur de configuration » dans Sentinel.

Pour activer l'audit des événement Créer un objet, lancez iManager et accédez à la fenêtre **Audit eDirectory > Configuration de l'audit > Novell Audit**. Sélectionnez **Objets > Créer** et **Attributs > Ajouter valeur**.

Audit d'événements LDAP

eDirectory considère chaque requête LDAP comme étant une transaction et génère des événements dès qu'une requête est initiée, qu'une réponse est reçue et que la transaction est terminée.

Dans Sentinel, chaque paire de requête-réponse est toutefois traitée comme un seul événement. Afin d'auditer un type d'événement LDAP dans eDirectory à l'aide de Sentinel, vous devez activer l'audit prévu pour l'événement de requête et l'événement de réponse. Par exemple, pour auditer une requête de liaison LDAP, vous devez configurer l'audit des événements Liaison LDAP et Réponse de liaison LDAP dans iManager.

Audit des événements Échec de connexion

Si vous voulez surveiller les événements d'échec de connexion dans eDirectory, vous devez utiliser iManager afin d'activer l'audit sur l'événement Ajouter valeur sur le serveur eDirectory. Vous devez également activer la détection des intrus sur le(s) conteneur(s) eDirectory dans le(s)quel(s) vous voulez auditer les événements d'échec de connexion.

IMPORTANT : Vous devez activer l'audit des événements Détection des intrus et Ajouter valeur sur chaque serveur comportant une réplique du conteneur à surveiller.

Utilisez la procédure suivante pour activer la détection des intrus sur un conteneur :

1. Connectez-vous à iManager.
2. Sous **Rôles et tâches**, sélectionnez **Administration des répertoires > Modifier objet**.
3. Naviguez et sélectionnez le conteneur eDirectory à auditer. Cliquez sur **OK**.
4. Sur l'onglet Général, cliquez sur **Détection des intrus**.
5. Sélectionnez **Détecter les intrus**.
6. Cliquez sur **OK**.

REMARQUE

- Vous n'avez pas besoin de configurer un autre paramètre associé à la détection des intrus ou d'activer le paramètre **Verrouiller compte après détection**.
- Pour surveiller les événements d'échec de connexion pour les connexions par le biais de NMAS, reportez-vous à **Finish Login Status** (État de connexion Terminé) dans le collecteur NMAS. Pour plus d'informations, reportez-vous au « Audit des événements NMAS » page 700.

Désinstallation des paquetages Novell Audit

Les sections suivantes expliquent comment désinstaller les paquetages Novell Audit :

- « Désinstallation des paquetages d'audit sur Linux » page 629
- « Désinstallation des paquetages d'audit sur Windows » page 629

Désinstallation des paquetages d'audit sur Linux

Pour désinstaller les paquetages d'audit sur Linux :

1. Déchargez le module d'audit à l'aide de la commande `ndstrace -c unload auditds`.
2. Désinstallez le fichier `novell-AUDTedirinst-9.2.0-`*`xx`*.rpm.

   ```
   #rpm -e --nodeps novell-AUDTedirinst-9.2.0-xx
   ```

3. Désactivez le chargement automatique des modules d'audit au démarrage eDirectory en modifiant le fichier `/etc/opt/novell/eDirectory/conf/ndsmodules.conf` et en supprimant la ligne correspondante à auditds (si elle existe). La ligne correspondant à auditds est comme suit :

   ```
   auditds     auto     #eDirectory Instrumentation
   ```

REMARQUE : Si aucun autre audit n'est installé, alors désinstallez Audit Platform Agent `novell-AUDTplatformagent-2.0.2-80` en utilisant la commande `#rpm -e novell-AUDTplatformagent-2.0.2-80.`

Désinstallation des paquetages d'audit sur Windows

Pour désinstaller les paquetages d'audit sur Windows :

1. Déchargez le module d'audit comme suit :
   - **1a** Accédez à **Démarrer > Panneau de configuration > Novell eDirectory Services**.
   - **1b** Sélectionnez **Services**.
   - **1c** Cliquez sur `nauditds.dlm`, puis cliquez sur **Arrêter**.
2. Supprimez `nauditds.dlm` du répertoire `C:\Novell\NDS`.
3. Supprimez le fichier `ediraudit.sch` du répertoire `C:\Novell\NDS`.

REMARQUE : si aucun autre outil n'est installé, désinstallez Audit Platform Agent en supprimant le fichier `logevent.dll` de l'emplacement `C:\Novell\NDS`.

Audit avec XDAS

La spécification XDAS fournit une classification standardisée pour les événements d'audit. Elle définit un ensemble d'événements génériques à un niveau système distribué global. XDAS offre un format d'enregistrement d'audit portable courant pour faciliter la fusion et l'analyse des informations d'audit provenant de plusieurs composants au niveau du système distribué. Les événements XDAS sont encapsulés dans un système de notation hiérarchique qui permet d'étendre l'ensemble d'identificateurs d'événements standard ou existants. La taxonomie définit un ensemble de champs,

les plus importants étant Observer (Observateur), Initiator (Initiateur) et Target (Cible). Les événements XDAS vous aident à comprendre facilement les parcours d'audit d'applications hétérogènes.

IMPORTANT : la prise en charge de l'audit avec XDAS a été abandonnée dans eDirectory 9.2 et les versions ultérieures. Si vous installez eDirectory 9.2 pour la première fois, l'option d'audit avec XDAS n'est plus disponible. Si vous effectuez une mise à niveau d'eDirectory à partir d'une version antérieure, vous pouvez encore utiliser XDAS, mais il est recommandé de procéder à une migration vers l'audit CEF. Si vous décidez d'utiliser XDAS sur les serveurs 9.2 que vous venez d'ajouter, vous devez copier le fichier rpm XDAS de l'ancienne version d'eDirectory et configurer les nouveaux serveurs. Veillez à copier le fichier `xdasconfig.properties` du dossier `conf` de l'ancienne version d'eDirectory vers la version la plus récente.

La configuration d'eDirectory pour qu'il utilise XDAS offre les avantages suivants :

- fournit des services d'audit sécurisés pour un système distribué ;
- définit un ensemble d'événements génériques au niveau d'un système distribué global ;
- définit un format d'enregistrement d'audit portable commun, qui facilite la fusion et l'analyse des informations d'audit provenant de plusieurs composants d'un système distribué ;
- définit un format commun pour les événements d'audit que les applications d'analyse peuvent utiliser ;
- enregistre le suivi d'audit XDAS ;
- configure des critères de présélection d'événements et des actions d'organisation des événements ;
- fournit un format d'audit commun, indépendamment de la plate-forme sur laquelle le service XDAS est exécuté ;
- prend en charge des environnements hétérogènes, sans avoir à remanier le système d'exploitation actuel ni les implémentations de service d'audit spécifiques des applications ;
- prend en charge la séparation adéquate des tâches pour les utilisateurs ;
- protège le journal d'audit en le rendant accessible uniquement aux principaux remplissant des rôles d'administration ou de sécurité bien déterminés ;
- met éventuellement en cache les événements d'audit localement sur l'agent en cas d'interruption de la communication entre l'agent et le serveur d'audit, et renvoie les événements une fois la communication rétablie.

Configuration de XDAS

Le paquetage de téléchargement du kit d'installation d'eDirectory inclut un client XDAS pour Linux et un autre pour Windows. Le programme d'installation d'eDirectory installe les paquetages XDAS sur votre système d'exploitation. Le paquetage XDAS contient les fichiers suivants :

- Linux
  - `novell-edirectory-xdaslog`
  - `novell-edirectory-xdaslog-conf`
  - `novell-edirectory-xdasinstrument`
- Windows
  - `xdasauditds.dlm`
  - `xdaslog.dll`

REMARQUE : à partir d'OES 11 SP2, les RPM XDAS sont fournis avec Open Enterprise Server.

Configuration système requise

L'installation et l'utilisation du plug-in NetIQ Audit pour iManager requièrent iManager 3.0 ou version ultérieure. Pour en savoir plus sur la configuration requise et obtenir les instructions de téléchargement, reportez-vous à la page du produit NetIQ iManager.

Installation ou mise à niveau du plug-in iManager pour XDAS

Le plug-in iManager pour XDAS est fourni avec les plug-ins eDirectory. Ces derniers peuvent également être téléchargés à partir du site de téléchargement NetIQ.

Procédez comme suit pour mettre à niveau le plug-in vers la version la plus récente.

1. Ouvrez iManager à partir d'un navigateur Web, à l'aide de l'URL suivante :

   `https://ip_address_or_DNS/nps/iManager.html`

   où *adresse_ip_ou_DNS* représente l'adresse IP ou le nom DNS de votre serveur iManager.

   Par exemple :

   `http://111.111.1.1/nps/iManager.html`

2. Connectez-vous à iManager à l'aide de votre nom d'utilisateur et de votre mot de passe.

   Si vous souhaitez accéder à toutes les fonctions de NetIQ iManager, vous devez vous connecter à l'arborescence en tant qu'administrateur. Seul un administrateur dispose d'un accès complet à toutes les fonctionnalités. S'il n'est pas administrateur, l'utilisateur peut uniquement accéder aux rôles pour lesquels des droits lui sont assignés.

   Pour plus d'informations, reportez-vous au Guide d'administration de NetIQ iManager.

3. Sélectionnez **Rôles et tâches** > **Configuration de l'audit**

   iManager affiche un message d'alerte concernant les nouvelles modifications XDAS.

4. Cliquez sur **OK**.

   Pendant la mise à niveau, les nouveaux fichiers iManager sont installés et la configuration est modifiée. Une fois la mise à niveau terminée, un message indiquant si l'installation a réussi ou échoué s'affiche.

Configuration du fichier de propriétés XDAS

Un exemple de fichier de propriétés (`xdasconfig.properties.template`) est inclus dans le répertoire `configdir` (`n4u.server.configdir`) sur le support d'eDirectory.

Le Tableau 23-1 indique l'emplacement par défaut du fichier `xdasconfig.properties` sur les systèmes d'exploitation Linux et Windows.

Tableau 23-1 Fichier de configuration de XDAS

Système d'exploitation	Emplacement du fichier de propriétés
Linux	`/etc/opt/novell/eDirectory/conf/xdasconfig.properties` Pour les installations non-root, le fichier de propriétés XDAS se trouve dans le répertoire `conf`.
Windows	`<Install Path>/novell/nds/xdasconfig` Le fichier de propriétés se trouve généralement dans le répertoire d'installation d'eDirectory.

Si vous configurez le fichier de propriétés, puis mettez à niveau votre environnement vers eDirectory 9.2, le programme d'installation ne remplace pas le fichier de propriétés. Le cas échéant, le processus de mise à niveau met à jour le fichier (`xdasconfig.properties.template`) de manière à conserver la personnalisation.

Vous pouvez configurer XDAS après l'installation d'iManager. Les paramètres de configuration de XDAS sont stockés dans un simple fichier de configuration au format texte (`xdasconfig.properties`). Vous pouvez personnaliser le fichier en fonction de vos besoins.

Le fichier de propriétés XDAS contient les informations suivantes :

Linux

```
# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=UDP

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=no

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory
```

```
# Cache File Size
# Cache File Size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c : %p%m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/xdas-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c : %p%m%n
```

Windows

```
# Brief description for appenders and their options are provided.
# For detailed decriptions refer to log4cxx documentation.

# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL).
#log4j.appender.S.Protocol=UDP

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=C:\\Novell\\mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=C:\\NetIQ\\eDirectory
```

```
# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %p%m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
# File path should be given with double backslash.
#log4j.appender.R.File=C:\\xdas-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c : %p%m%n
```

Avant d'examiner le contenu du fichier `xdasconfig.properties`, NetIQ recommande de passer en revue les points suivants :

- Les lettres S et R correspondent respectivement à l'appender Syslog et à l'appender RollingFile.
- Les entrées ne respectent pas la casse.
- Les entrées peuvent apparaître dans n'importe quel ordre.
- Les lignes vides dans le fichier sont valides.
- Toute ligne commençant par un signe dièse (#) est commentée.

Le tableau ci-dessous fournit des informations à propos des paramètres du fichier `xdasconfig.properties`.

IMPORTANT : vous devez redémarrer eDirectory après avoir modifié la configuration.

Valeur	Description
log4j.rootLogger=**debug, S, R**	Définit le niveau de l'enregistreur racine sur Débogage et y associe un appender nommé R ou S, S correspondant à Syslog et R à Rolling File.
log4j.appender.S=**org.apache.log4j.net.SyslogAppender**	Indique que l'appender S doit être un appender Syslog.
log4j.appender.S.Host=**localhost**	Indique à quel emplacement du serveur Syslog les événements XDAS sont consignés. Par exemple : log4j.appender.S.Host=192.168.0.1

Valeur	Description
log4j.appender.S.Port=**port**	Port au niveau duquel XDAS se connecte au serveur Syslog. Le numéro de port peut être compris entre 1 et 65535. Si vous spécifiez une valeur non valide, le numéro de port est défini par défaut sur 514. En cas d'échec de la connexion entre XDAS et le serveur Syslog, Identity Manager ne peut pas consigner les événements tant que la connexion n'a pas été rétablie.
log4j.appender.S.Protocol=UDP	Indique le protocole à utiliser. Par exemple : UDP, TCP ou SSL.
log4j.appender.S.SSLCertFile=**/etc/opt/novell/mycert.pem**	Spécifie le fichier de certificat SSL pour la connexion SSL. Utilisez deux barres obliques inverses pour spécifier le chemin d'accès au fichier. Ce paramètre est facultatif.
log4j.appender.S.Threshold=**INFO**	Spécifie le niveau de consignation minimal autorisé dans l'appender Syslog. Actuellement, le niveau de consignation INFO est pris en charge.
log4j.appender.S.Facility=**USER**	Indique le type d'installation. L'installation est utilisée pour tenter de classer le message. Actuellement, l'installation USER est prise en charge. Ces valeurs peuvent être spécifiées en majuscules ou en minuscules.
log4j.appender.S.layout=**org.apache.log4j.PatternLayout**	Paramètre d'agencement de l'appender Syslog.
log4j.appender.S.layout.ConversionPattern**=%c : %p%m%n**	Paramètre d'agencement de l'appender Syslog. Pour plus d'informations sur les schémas de conversion et leur description, consultez le site logging.apache.org.
log4j.appender.R=**org.apache.log4j.RollingFileAppender**	Indique que l'appender R doit être un appender RollingFile.
log4j.appender.R.File=**/var/opt/novell/eDirectory/log/xdas-events.log**	Emplacement du fichier journal pour l'appender RollingFile.
log4j.appender.R.MaxFileSize=**100MB**	Taille maximale, en Mo, du fichier journal pour l'appender RollingFile. Définissez cette valeur sur la taille maximale autorisée par le client.
log4j.appender.R.MaxBackupIndex=**10**	Spécifiez le nombre maximal de fichiers de sauvegarde pour l'appender RollingFile. Le nombre maximal de fichiers de sauvegarde peut être 10. Une valeur 0 signifie qu'aucun fichier de sauvegarde n'est présent.
log4j.appender.R.layout=**org.apache.log4j.PatternLayout**	Paramètre d'agencement de l'appender RollingFile.

Valeur	Description
log4j.appender.R.layout.ConversionPattern=**%d{MMM dd HH:mm:ss} %c : %p%m%n**	Paramètre d'agencement de l'appender RollingFile. Pour des modèles de format de date simples, reportez-vous au Tableau 23-2. Pour plus d'informations sur les schémas de conversion et leur description, consultez le site logging.apache.org.

Le Tableau 23-2 donne des exemples de modèles de date et d'heure interprétés aux États-Unis. Les date et heure en question sont le 04/07/2012, 12 h 8 min 56 s, heure du Pacifique aux États-Unis.

Tableau 23-2 *Exemples de modèles de date et d'heure*

Modèle de date et d'heure	Résultat
"aaaa.MM.jj G 'à' HH:mm:ss z"	2012.07.04 AD at 12:08:56 PDT (04.07.2012 ap. J-C à 12:08:56 HAP)
"EEE, MMM j, "aa"	Wed, Jul 4, '01 (Mer, 4 juil. 2001)
"h:mm a"	12:08 PM (12:08)
"hh 'heures' a, zzzz"	12 o'clock PM, Pacific Daylight Time (12 heures, heure avancée du Pacifique)
"K:mm a, z"	12:08 PM, PDT (12:08, HAP)
"aaaaa.MMMMM.jj GGG hh:mm aaa"	02012.July.24 AD 12:08 PM (02012.Juillet.24 ap. J-C 12:08)
"EEE, j MMM aaaa HH:mm:ss Z"	Wed, 24 Jul 2012 12:08:56 -0700 (Mer, 24 juil. 2012 12:08:56 -0700)
"aaMMjjHHmmssZ"	120724120856-0700
"aaaa-MM-jj'T'HH:mm:ss.SSSZ"	2012-07-04T12:08:56.235-0700 (2012-07-04T12:08:56.235-0700)

Activation de l'appender Syslog

Si vous souhaitez centraliser les messages d'audit à un seul emplacement, vous pouvez utiliser l'appender Syslog. Par ailleurs, un serveur Syslog offre une meilleure prise en charge des sauvegardes en cas de sinistre.

Pour activer l'appender Syslog, apportez les modifications suivantes dans le fichier `xdasxconfig.properties` :

1. Remplacez la valeur de l'entrée ci-dessous par S pour joindre un appender Syslog :

   ```
   log4j.rootLogger=debug, S
   ```

2. Supprimez les marques de commentaire des entrées suivantes :

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   log4j.appender.S.Host=localhost
   log4j.appender.S.Port=port
   log4j.appender.S.Protocol=UDP
   ```

```
log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

#log4j.appender.S.Threshold=INFO

#log4j.appender.S.Facility=USER

#log4j.appender.S.layout=org.apache.log4j.PatternLayout

#log4j.appender.S.layout.ConversionPattern=%c : %p%m%n
```

3 Connectez-vous à iManager et modifiez les événements de journal. Pour plus d'informations sur la configuration des événements XDAS, reportez-vous à la section « Configuration des événements XDAS pour l'audit » page 638.

REMARQUE : le caching XDAS qui utilise le protocole `UDP` pour `SyslogAppender` ne fonctionne pas.

Génération d'un certificat pour la connexion SSL Syslog

Pour générer un certificat pour la connexion Syslog :

1. Créez le certificat à l'aide de la commande OpenSSL suivante :

   ```
   openssl s_client -host LOG_SERVER  -port 1443 -showcerts
   ```

2. Indiquez l'emplacement du fichier de certificat que vous avez créé dans le fichier `/etc/opt/novell/eDirectory/conf/xdasconfig.properties`.

Activation de l'appender RollingFile

Si la solution d'audit est limitée à un seul serveur, il est préférable d'opter pour l'appender File. Le nombre de composants à configurer étant limité, cette solution est également facile à mettre en oeuvre et plus adaptée aux démonstrations.

Pour activer l'appender RollingFile, apportez les modifications suivantes dans le fichier `xdasconfig.properties` :

1 Remplacez la valeur de l'entrée ci-dessous par R pour joindre l'appender RollingFile :

```
log4j.rootLogger=debug, R
```

2 Supprimez les marques de commentaire des entrées suivantes :

```
log4j.appender.R=org.apache.log4j.RollingFileAppender

log4j.appender.R.File=/var/opt/novell/eDirectory/log/xdas-events.log

log4j.appender.R.MaxFileSize=100MB

log4j.appender.R.MaxBackupIndex=10

log4j.appender.R.layout=org.apache.log4j.PatternLayout

log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c : %p%m%n
```

3 Sélectionnez l'événement souhaité dans iManager.

Pour plus d'informations sur la configuration des événements XDAS, reportez-vous à la section « Configuration des événements XDAS pour l'audit » page 638.

Configuration de XDAS pour l'audit

- « Utilisation du plug-in iManager pour la configuration de XDAS » page 638
- « Configuration des événements XDAS pour l'audit » page 638

Utilisation du plug-in iManager pour la configuration de XDAS

1. Ouvrez iManager à partir d'un navigateur Web, à l'aide de l'URL suivante :

   `https://ip_address_or_DNS/nps/iManager.html`

   où *adresse_ip_ou_DNS* représente l'adresse IP ou le nom DNS de votre serveur iManager.

   Par exemple :

   `http://111.111.1.1/nps/iManager.html`

2. Connectez-vous en entrant votre nom d'utilisateur et votre mot de passe.

   Si vous souhaitez accéder à toutes les fonctions de NetIQ iManager, vous devez vous connecter à l'arborescence en tant qu'administrateur. Seul un administrateur dispose d'un accès complet à toutes les fonctionnalités. S'il n'est pas administrateur, l'utilisateur peut uniquement accéder aux rôles pour lesquels des droits lui sont assignés.

   Pour plus d'informations, reportez-vous au *Guide d'administration de NetIQ iManager*.

3. Sélectionnez **Rôles et tâches** > **Configuration de l'audit**.
4. Spécifiez le nom de votre serveur eDirectory dans **Serveur NCP**, puis cliquez sur l'icône **Sélecteur d'objet** pour rechercher le serveur eDirectory.
5. Cliquez sur **OK**.

   La page XDAS Audit (Audit XDAS) s'affiche. Passez à la « Configuration de XDAS » page 630.

Configuration des événements XDAS pour l'audit

1. Connectez-vous à iManager à l'aide de votre nom d'utilisateur et de votre mot de passe.
2. Sélectionnez **Rôles et tâches** > **Configuration de l'audit**.
3. Sélectionnez l'onglet **XDAS**.
4. Configurez les événements XDAS.
   - **Configuration des événements de base :** spécifiez des valeurs pour les options ci-dessous, en fonction des événements requis pour votre environnement :

REMARQUE : par défaut, les catégories d'événements individuelles sous la section Configuration des événements de base sont réduites. Vous pouvez agrandir chaque catégorie pour sélectionner des événements individuels.

Options	Description
Événements de gestion de compte	Sélectionnez les événements de gestion de compte pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour créer, supprimer, activer, désactiver et également interroger et modifier des comptes.
Événements de gestion des approbations	Sélectionnez les événements de gestion des approbations pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour créer, supprimer, interroger et modifier des approbations.
Événements de données de compte	Sélectionnez les événements de données de compte pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour créer et supprimer des éléments de données ainsi que pour modifier et interroger des attributs d'éléments de données.
Événements de sécurité	Sélectionnez les événements de sécurité de compte pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour accorder ou révoquer l'accès, la connexion, la modification de mot de passe et la requête. Cet ensemble d'événements aide également à détecter les tentatives d'intrusion sur le système eDirectory.

- **Avancé :** spécifiez des valeurs pour les options ci-dessous, en fonction des événements requis pour votre environnement :
  - **Global :** vous pouvez sélectionner ou désélectionner les paramètres globaux pour les entrées en double.
    - **Ne pas envoyer d'événement répliqué :** sélectionnez cette option pour ne plus recevoir les événements en double en raison de la réplication à partir d'autres serveurs.
  - **Consigner les valeurs de l'événement :** les événements sont consignés dans un fichier texte. Les valeurs d'événements de plus de 768 octets sont considérées comme de « grandes valeurs ». Vous pouvez consigner des événements de n'importe quelle taille.
    - **Consigner de grandes valeurs :** sélectionnez cette option pour consigner les événements dont la taille est supérieure à 768 octets.
    - **Ne pas consigner de grandes valeurs :** sélectionnez cette option pour consigner les événements dont la taille est inférieure à 768 octets.

    REMARQUE : Si l'événement est plus volumineux, sa valeur est tronquée et enregistrée dans le fichier journal.
- **Configuration des événements avancés :** spécifiez des valeurs pour les options ci-dessous, en fonction des événements requis pour votre environnement :

Options	Description
Événements de gestion de service ou d'application	Sélectionnez les événements de gestion de service ou d'application pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour activer, désactiver, appeler et arrêter des services.
Événements opérationnels	Sélectionnez les événements de gestion opérationnels pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour démarrer et arrêtez le système, sauvegarder et restaurer un espace de stockage des données, auditer des opérations internes et modifier des contextes de processus.

Pour plus d'informations sur les événements internes eDirectory assignés aux événements XDAS correspondants, reportez-vous à la section « Assignation d'événements eDirectory à des événements XDAS » page 895.

REMARQUE : une fois l'événement sélectionné, l'application des modifications de configuration sur le serveur NCP peut prendre jusqu'à 3 minutes. Si vous voulez que les modifications apportées à la configuration soient immédiatement prises en compte sur le serveur NCP, vous pouvez décharger et charger le module `xdasauditds`.

Chargement et déchargement des modules

Une fois les événements XDAS configurés, exécutez les commandes ci-dessous pour charger et décharger les modules XDAS :

Pour charger automatiquement le module xdasauditds à chaque démarrage du serveur ndsd :

- **Linux**

  Ajoutez `xdasauditds` au fichier `/etc/opt/novell/eDirectory/conf/ndsmodules.conf`.

- **Windows**

  Exécutez le fichier `ndscons.exe`, sélectionnez `xdasauditds` dans la liste des modules disponibles, cliquez sur **Démarrage**, puis définissez l'option Type de démarrage sur **Automatique**.

Pour charger et décharger manuellement le module `xdasauditds` :

- **Linux**

  Pour charger le module, exécutez `ndstrace -c "load xdasauditds"`.

  Pour décharger le module, exécutez `ndstrace -c "unload xdasauditds"`.

- **Windows**

  Pour charger le module, exécutez le fichier `ndscons.exe`, sélectionnez **xdasauditds** dans la liste des modules disponibles, puis cliquez sur **Démarrer**.

  Pour décharger le module, exécutez le fichier `ndscons.exe`, sélectionnez **xdasauditds** dans la liste des modules disponibles, puis cliquez sur **Arrêter**.

Si vous avez installé NMAS et activé l'audit de NMAS, le serveur NMAS charge automatiquement la bibliothèque XDAS.

Activation du caching des événements XDAS

eDirectory 9.2 vous permet de stocker éventuellement en local, les événements XDAS sur l'agent dans un cache de l'appender Syslog. Lorsque les événements sont mis en cache, si l'agent ne peut pas communiquer avec le serveur d'audit, les événements d'audit générés sont conservés, ce qui permet d'éviter toute perte des données d'audit. Une fois la communication rétablie entre l'ordinateur de l'agent et le serveur d'audit, l'agent tente de renvoyer les événements mis en cache.

Le caching des événements XDAS est désactivé par défaut. Pour activer le caching des événements, procédez comme suit :

1. Sur l'ordinateur de l'agent, accédez à l'emplacement du fichier de propriétés XDAS. Par défaut, le fichier xdasconfig.properties se trouve dans `/etc/opt/novell/eDirectory/conf/xdasconfig.properties`. Pour les installations non-root, le fichier de propriétés XDAS se trouve par défaut dans le répertoire `conf`.
2. Utilisez un éditeur de texte pour ouvrir le fichier `xdasconfig.properties`.
3. Dans le fichier de propriétés, accédez à la propriété `log4j.appender.S.CacheEnabled` et définissez sa valeur sur `yes`.
4. (Conditionnel) Si vous souhaitez mettre en cache les événements dans un répertoire spécifique, définissez la valeur de la propriété `log4j.appender.S.CacheDir` sur le chemin de répertoire. Si vous spécifiez un répertoire, assurez-vous que son chemin est un emplacement valide sur le serveur. Si la propriété `log4j.appender.S.CacheDir` n'est pas définie, les journaux de l'appender Syslog mettent en cache les événements dans le répertoire `dib` de cette instance.
5. (Conditionnel) Si vous souhaitez spécifier une taille de fichier personnalisée pour le cache, modifiez la valeur de la propriété `log4j.appender.S.CacheMaxFileSize`. La valeur par défaut est 500 Mo. La valeur minimale est 50 Mo et la valeur maximale, 4 Go.
6. Enregistrez, puis fermez le fichier `xdasconfig.properties`.

Utilisation de collecteurs d'événements XDAS

Pour plus d'informations sur l'utilisation de collecteurs d'événements XDAS, consultez la page des plug-ins Sentinel .

Présentation du filtrage des événements d'audit XDAS

À l'aide de filtres et de notifications d'événement, XDAS est capable de signaler la survenue ou la non-survenue d'un type d'événement spécifique. Vous pouvez également filtrer les événements pour un(e) ou plusieurs classes ou attributs d'objet spécifiques, selon le type d'événement. XDAS évalue tous les événements générés en fonction des filtres configurés sur le serveur eDirectory et ne consigne que les événements qui correspondent à ces filtres.

Vous pouvez configurer des filtres et des notifications d'événement pour les comptes, les approbations, de même que les éléments de données XDAS. Dans le cas des approbations et des comptes XDAS, Toute classe d'objet sélectionnée sera assignée à leurs catégories d'événement respectives. Par exemple, si vous sélectionnez la classe **Utilisateur** à partir du filtrage de comptes, cette classe est automatiquement assignée à la catégorie Événements de gestion des comptes. Par défaut, une classe d'objet qui n'est assignée à aucun compte ou aucune approbation sera assignée à la catégorie Événements de gestion des éléments de données.

Cette section fournit les informations dont vous avez besoin pour configurer des filtres et des notifications pour votre système.

Filtrage des événements de gestion des comptes XDAS

Vous pouvez configurer le filtrage des comptes de manière à ne rechercher qu'un ou plusieurs types d'événements spécifiques. Par exemple, si vous souhaitez être averti lorsqu'une personne crée un compte utilisateur dans eDirectory, vous pouvez créer un filtre de sélection de la classe d'objet Utilisateur pour consigner les événements dans le cadre de la création d'un nouvel objet Utilisateur.

Pour configurer le filtrage des comptes, cliquez sur le lien Événements de gestion de compte, sélectionnez la classe, puis cliquez sur **OK** pour quitter l'application.

Pour configurer des filtres pour les événements de gestion des comptes :

1. Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.

   Par défaut, l'onglet **Événements XDAS** est sélectionné.
3. Cliquez sur **Événements de gestion de compte**.

   La fenêtre Filtrage de la configuration des comptes XDAS s'affiche.
4. Dans la liste **Classes disponibles**, sélectionnez Utilisateur, choisissez une classe d'objet, puis cliquez sur la flèche droite pour déplacer la classe d'objet dans la liste **Classes sélectionnées**, puis cliquez sur **OK**. Par défaut, les classes d'objet **Personne organisationnelle**, **Personne,** et **Utilisateur** sont sélectionnées.
5. Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs pour les classes d'objet sélectionnées. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

   Le filtre pour les événements de gestion des comptes est configuré.

À l'aide du filtre configuré, le module d'audit XDAS contrôle tous les événements générés pour les classes d'objet et les attributs sélectionnés et consigne ces événements.

Filtrage des événements de gestion des approbations XDAS

Cliquez sur le lien **Événements de gestion des approbations** pour configurer le filtrage des événements de gestion des approbations. Par exemple, si vous souhaitez être averti lorsqu'une personne crée une nouvelle approbation dans eDirectory, vous pouvez créer un filtre de sélection de la classe d'objet Groupe pour consigner les événements dans le cadre de la création d'une nouvelle approbation.

Pour configurer le filtrage des événements de gestion des approbations :

1. Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.

   Par défaut, l'onglet **Événements XDAS** est sélectionné.
3. Cliquez sur **Événements de gestion des approbations**.

   La fenêtre **Configuration du filtrage de l'approbation XDAS** s'affiche.
4. Dans la liste **Classes disponibles**, sélectionnez les classes d'objet pour lesquelles vous souhaitez collecter des événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes sélectionnées.** Par défaut, les classes d'objet **dynamicGroup**, **dynamicGroupAux**, **Groupe**, **Groupe LDAP** et **Rôle organisationnel** sont sélectionnées.
5. Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs pour les classes d'objet sélectionnées. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

REMARQUE : si vous sélectionnez une classe d'objet, tous les événements d'approbation pour tous les attributs de cette classe d'objet sont sélectionnés. Dans ce cas, vous obtiendrez tous les événements de gestion d'approbation pour l'ensemble des attributs sélectionnés dans les classes d'objet sélectionnées.

6 Cliquez sur **OK**.

Lorsque le filtre est configuré, le module d'audit XDAS contrôle tous les événements générés pour les classes d'objet et les attributs sélectionnés et consigne ces événements.

Filtrage des événements de gestion des éléments de données XDAS

Cliquez sur le lien **Événements de gestion des éléments de données** pour configurer le filtrage des éléments de données XDAS. Vous pouvez configurer les éléments de données XDAS pour les objets pour lesquels vous souhaitez collecter des événements XDAS. Vous pouvez sélectionner des classes d'objet et leur définir des attributs.

Pour configurer le filtrage des événements de gestion des éléments de données :

1 Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.

2 Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.

Par défaut, l'onglet **Événements XDAS** est sélectionné.

3 Cliquez sur **Événements de gestion des éléments de données**.

La fenêtre Configuration du filtrage de l'élément de données XDAS s'affiche.

4 Dans la liste **Classes disponibles**, sélectionnez les classes d'objet pour lesquelles vous souhaitez collecter des événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes sélectionnées.** Par défaut, toute classe d'objet qui n'est assignée à aucun compte ou approbation, sera assignée à la catégorie d'événements de gestion des éléments de données par défaut.

REMARQUE : si aucune classe d'objet n'est sélectionnée, les événements pour toutes les classes d'objet disponibles seront générés.

5 Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs pour les classes d'objet sélectionnées. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

6 Cliquez sur **OK**.

À l'aide du filtre configuré, le module d'audit XDAS vérifie les événements générés pour toutes les classes d'objet et tous les attributs sélectionnés et consigne ces événements.

Filtrage des événements eDirectory à l'aide du filtre d'exclusion

Cliquez sur le lien **Filtre d'exclusion** afin de configurer le filtrage pour les classes d'objet et les attributs pour lesquels vous ne souhaitez pas générer d'événement. Vous pouvez sélectionner des classes d'objet et leur définir des attributs.

Pour configurer le filtrage des événements eDirectory indésirables :

1 Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.

2 Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.

Par défaut, l'onglet **Événements XDAS** est sélectionné.

3 Cliquez sur **Filtre d'exclusion**.

La fenêtre Filtrage des exclusions XDAS s'affiche.

4 Dans la liste **Classes disponibles**, sélectionnez les classes d'objet pour lesquelles vous ne souhaitez pas collecter d'événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes sélectionnées**.

5 Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs pour les classes d'objet sélectionnées. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

6 Cliquez sur **OK**.

À l'aide du filtre configuré, le module d'audit XDAS arrête de générer des événements pour toutes les classes d'objet et les attributs sélectionnés.

Schéma XDAS

Le schéma XDAS est défini comme suit :

Schéma XDAS JSON

```
{
    "id":"XDAS",
    "title":"XDAS Version 2 JSON Schema",
    "description":"A JSON representation of an XDAS event record.",
    "type":"objectr",
    "properties":{
      "Source":{
        "description":"The original source of the event, if applicable.",
        "type":"string",
        "optional":true
      },
      "Observer":{
        "description":"The recorder (ie., the XDAS service) of the event.",
        "type":"object",
        "optional":false,
        "properties":{
          "Account":{"$ref":"account"},
          "Entity":{"$ref":"entity"}
        }
      },
      "Initiator":{
        "description":"The authenticated entity or access  that causes an event.",
        "type":"object",
        "optional":false,
        "properties":{
          "Account":{"$ref":"account","optional":true},
          "Entity":{"$ref":"entity"},
          "Assertions":{
            "description":"Attribute/value assertions about an identity.",
            "type":"object",
            "optional":true
          }
        }
      },
      "Target":{
        "description":"The target object, account, data item, etc of the event.",
        "type":"object",
        "optional":true,
        "properties":{
```

```
          "Account":{"$ref":"account"},
          "Entity":{"$ref":"entity"},
          "Data":{
            "description":"A set attribute/value pairs describing the target
object.",        *
            "type":"object",
            "optional":true
          }
        }
      },
      "Action":{
        "description":"The action describes the event in a uniform manner.",
        "type":"object",
        "optional":false,
        "properties":{
          "Event":{
            "description":"The event identifier in standard XDAS taxonomy.",
            "type":"object",
            "optional":false,
            "properties":{
              "Id":{
                "description":"The XDAS taxonomy event identifier.",
                "type":"string",
                "optional":false,
                "pattern":"/^[0-9]+(\.[0-9]+)*$/"
              },
              "Name":{
                "description":"A short descriptive name for the specific event.",
eg. a new replica is added
                "type":"string",
                "optional":true
              },
      "CorrelationID":{
          "description":"Correlation ID, source#uniqueID#connID",
                 "type":"string",
                 "optional":true
      }
     },
     "SubEvent":{
      "type":object
      "description": "Describes the actual domain specific event that has
occured.",
      "optional":true,
      "properties":{
        "Name"":{
                    "description":"A short descriptive name for this event.",
                    "type":"string",
                    "optional":true
                  },
      }
            }
          }
          "Log":{
            "description":"Client-specified logging attributes.",
            "optional":true,
            "properties":{
              "Severity":{"type":"integer", "optional":true},
              "Priority":{"type":"integer", "optional":true},
              "Facility":{"type":"integer", "optional":true}
            }
```

```
            }
            "Outcome":{
              "description":"The XDAS taxonomy outcome identifier.",
              "type":"string",
              "optional":false,
              "pattern":"/^[0-9]+(\.[0-9]+)*$/"
            }
            "Time":{
              "description":"The time the event occurred.",
              "type":"object",
              "optional":false,
              "properties":{
                "Offset":{
                  "description":"Seconds since Jan 1, 1970.",
                  "type":"integer"
                },
                "Sequence":{
                  "description":"Milliseconds since last integral second.",
                  "type":"integer",
                  "optional":true
                },
                "Tolerance":{
                  "description":"A tolerance value in milliseconds.",
                  "type":"integer",
                  "optional":true
                },
                "Certainty":{
                  "description":"Percentage certainty of tolerance.",
                  "type":"integer",
                  "optional":true,
                  "minimum":0,
                  "maximum":100,
                  "default":100,
                },
                "Source":{
                  "description":"The time source (eg., ntp://time.nist.gov).",
                  "type":"string",
                  "optional":true
                },
                "Zone":{
                  "description":"A valid timezone symbol (eg., MST/MDT).",
                  "type":"string",
                  "optional":true
                }
              }
      "ExtendedOutcome":{
            "description":"The XDAS taxonomy outcome identifier.",
            "type":"string",
            "optional":false,
            "pattern":"/^[0-9]+(\.[0-9]+)*$/"
           }
        }
      }
    }
  },
  {
    "id":"account",
    "description":"A representation of an XDAS account.",
    "type":"object",
    "properties":{
```

```
      "Domain":{
       "description":"A (URL) reference to the authority managing this account.",
/* lets take it as the partition?
        "type":"string"
      },
      "Name":{
        "description":"A human-readable account name.",        - DN
        "type":"string",
        "optional":true
      },
      "Id":{
        "description":"A machine-readable unique account identifier value.",  -
EntryID
        "type":"integer"
      }
    }
  },
  {
    "id":"entity",                     - Server details for Target, client address
details for the initiator
    "description":"A representation of an addressable entity.",
    "type":"object",
    "properties":{
      "SysAddr":{"type":"string","optional":true},
      "SysName":{"type":"string","optional":true},
      "SvcName":{"type":"string","optional":true},
      "SvcComp":{"type":"string","optional":true},
    }
  }
```

Définitions des champs XDAS

Les champs inclus dans le schéma sont les champs XDAS définis spécifiquement pour les événements d'audit. Certains ou l'ensemble de ces champs peuvent également être pertinents pour d'autres types d'événement, mais des informations de ce type sont requises pour les services d'audit. Le format d'enregistrement JSON XDAS est un format ouvert. Cela signifie que d'autres champs peuvent être ajoutés à n'importe quel endroit de l'enregistrement, du moment qu'ils ne sont pas en conflit avec les valeurs de champ définies pour l'audit par la norme XDAS. Autrement dit, en présence d'un certain type de données de corrélation, telles qu'un identificateur de workflow ou un identificateur de session, qui peuvent servir de points de données de corrélation entre des événements au sein d'un workflow ou d'une session cliente, vous pouvez ajouter ces champs. Choisissez simplement un nom non conflictuel pour votre champ.

Tableau 23-3 *Définitions des champs XDAS*

Champ XDAS	Description
Source (facultatif)	La source d'un événement identifie le service d'événements d'un autre système à partir duquel cet événement a été initialement défini et converti en événement XDAS. Dans la mesure où de nombreux événements sont générés directement par les clients XDAS, le champ Source est facultatif.

Champ XDAS	Description
Initiator	L'initiateur d'un événement est l'entité authentifiée qui a initialement déclenché la création de l'événement. Notez qu'un initiateur ne doit pas être identifié. Si l'entité ne peut pas être identifiée (il se peut qu'une entité tente de se connecter, entraînant la génération d'un événement de connexion par un observateur), il convient de spécifier autant d'informations que possible à propos de l'origine de l'événement. REMARQUE : dans le cas particulier d'un événement de connexion, l'identité authentifiée de l'initiateur reste inconnue jusqu'à ce que la tentative de connexion ait réussi. C'est pourquoi un événement d'échec de connexion ne permet pas d'identifier l'identité du compte cible comme l'identité de l'initiateur. Un initiateur est défini par un compte et une entité (décrits ci-dessous), ainsi que par un ensemble d'assertions facultatif. Ces assertions décrivent les attributs de l'identité de l'initiateur sous la forme d'un ensemble de paires nom/valeur. Certains initiateurs ne sont pas associés à un compte spécifique, mais seulement à un ensemble d'assertions (SAML2, par exemple) qui décrivent les droits de l'intervenant. Aucun schéma n'est défini pour ces assertions, car elles varient d'une classe à l'autre et parfois même d'un objet à l'autre.
Action	L'action correspond à l'événement enregistré. Ce champ indique l'identificateur d'événement XDAS ainsi qu'un code de résultat (réussite ou classe d'échec), et affiche le plus précisément possible l'heure à laquelle l'événement s'est produit.
Event	Le champ Event est le champ clé pour les événements XDAS. Il encapsule un identificateur taxonomique ainsi qu'un court descriptif pour favoriser la lisibilité.
Id	Le code ID d'événement représente l'identificateur de l'événement, défini par la taxinomie standard des événements XDAS, et les extensions définies par le produit Novell CSS.
Name	Le nom de l'événement est une représentation lisible de l'identificateur d'événement. Le nom de l'événement est facultatif, mais recommandé pour une meilleure lisibilité.
Data	Les données d'événement fournissent des informations descriptives supplémentaires à propos de l'événement.
Log	Le champ Log contient des valeurs de niveau de consignation de type syslog standard, exprimées sous la forme d'identificateurs numériques pour les éléments Severity et Facility. Le champ Log et tous les sous-champs qu'il contient sont facultatifs. Ces valeurs ne doivent être utilisées qu'en cas d'absolue nécessité, car elles représentent généralement l'avis personnel de l'instrumenteur. Il est préférable de laisser les ingénieurs ou les logiciels d'analyse déterminer ces valeurs une fois les données d'événement collectées.
Outcome	Pour plus d'informations sur les codes de résultat, reportez-vous à la section « Codes de résultat » page 650.
Time	L'heure de l'événement est l'heure enregistrée par l'observateur au moment où l'événement a été transmis au service d'événements. Les valeurs d'heure sont collectées par la bibliothèque auxiliaire du client XDAS. Il est donc inutile de s'inquiéter à propos des valeurs stockées dans ce champ, dans la mesure où la bibliothèque auxiliaire tente d'être aussi précise que possible lorsqu'elle génère les informations d'heure.
Offset	Le champ Offset (Décalage) contient une valeur qui représente le nombre de secondes écoulées depuis le 1er janvier 1970 à minuit, autrement dit l'epoch Linux.

Champ XDAS	Description
Sequence	Le champ Sequence (Séquence) contient une valeur numérique unique qui distingue cet événement d'un autre événement qui a pu être enregistré au cours de la même seconde. Globalement, cette valeur doit être considérée comme une valeur numérique à croissance monolithique qui commence à zéro et continue jusqu'à ce qu'elle atteigne la limite de la seconde suivante, puis recommence à zéro.
Tolerance	Ce champ contient une valeur comprise entre 0 et 100, qui indique la tolérance de l'horloge utilisée pour enregistrer l'heure en termes de décalage. La valeur 0 indique que l'horloge est très précise. La valeur 100 indique qu'il ne faut pas se fier à l'horloge.
Certainty	Ce champ contient une valeur comprise entre 0 et 100, qui correspond au pourcentage de fiabilité de la valeur du champ Tolerance. La valeur 0 signifie qu'il n'existe aucune certitude quant à la tolérance et qu'il ne faut donc en aucun cas s'y fier. La valeur 100 indique que la valeur de tolérance est très précise.
Source	Ce champ spécifie la source de temps du système de l'observateur. Il peut s'agir de l'URL d'un serveur de temps ou simplement d'une source de temps locale, comme une horloge matérielle.
Zone	Ce champ contient la nouvelle chaîne de fuseau horaire représentant le fuseau horaire de cette horloge.
Target (facultatif)	La cible d'un événement est la ressource protégée ou le compte sur lequel l'initiateur tente d'agir, entraînant de ce fait la génération d'un événement. Une cible est définie par un compte et une entité (décrits ci-dessous), ainsi que par un objet Données facultatif et non spécifié. L'objet Données est un ensemble de paires nom/valeur qui décrivent les attributs spécifiques de la classe de l'intervenant. Le schéma ne définit pas les champs réels, car les différentes classes comportent un ensemble unique d'attributs de données (le cas échéant).
Observer	L'observateur d'un événement est l'identité authentifiée d'une entité (service) qui surveille le système et génère des événements en fonction des actions de l'initiateur. Un observateur est défini par un compte et une entité (décrits ci-dessous).
Referenced Classes	Les champs Observer (Observateur), Initiator (Initiateur) et Target (Cible) contiennent des références aux classes de compte et d'entité définies séparément dans le schéma. Ces autres classes identifient les attributs clés des trois principaux intervenants au sein d'un événement d'audit.
Account Class	La classe de compte représente l'identité de l'intervenant. Cette identité est relative à un domaine d'authentification. Un nom et un ID de compte sont fournis, mais seul l'ID est vraiment nécessaire. Le nom est juste spécifié à des fins de lisibilité.
Account Domain	Le domaine de compte définit l'autorité d'authentification de l'intervenant. Sans autorité d'authentification, les identificateurs de compte sont peu pertinents.
Account Name	Ce champ facultatif favorise la lisibilité.
Account Id	Ce champ contient l'identificateur unique du compte au sein du domaine d'authentification.
Entity Class	Ce champ décrit l'emplacement de l'intervenant. Cet emplacement est défini par une adresse (réseau IP) et un nom (d'hôte/de domaine) de noeud d'extrémité d'accès système. D'autres champs sont disponibles pour décrire les noms de service et de composant au sein du logiciel qui gère les noeuds d'extrémité susmentionnés.

Champ XDAS	Description
Entity SysAddr	Adresse IP décrivant le noeud d'extrémité d'accès de l'intervenant logiciel. Cette adresse est affichée au format adresse IP:port. Par exemple : ◆ IPv4 : 194.99.188.103:34564 ◆ IPv6 : [2015::15]:43333 Notez que l'adresse IP d'événement interne se présente comme suit : 0.0.0.0:0.
Entity SysName	Nom de domaine ou d'hôte décrivant le noeud d'extrémité d'accès de l'intervenant logiciel.
Entity SvcName	Nom apportant un complément d'information à propos du service qui gère le noeud d'extrémité susmentionné.
Entity SvcComp	Nom de composant de service décrivant le composant au sein du service susmentionné.

Codes de résultat

Le code de résultat est une valeur numérique hiérarchique comparable au code d'événement. Il indique si l'opération a réussi ou échoué et pour quelle raison. La hiérarchie de réussite est encapsulée par le sous-arc 0.x. Les classes d'échec sont représentées par la hiérarchie 1.x. Les codes de refus sont représentés par la hiérarchie 2.x.

Exemple d'événement

Vous trouverez ci-dessous un exemple d'événement :


```
Mar 16 21:46:40 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "164.99.179.142","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" :
"164.99.179.142:43230"}},"Target" : {"Data" : {"ClassName" : "Tree Root","Name" :
"TREEUPGRADE","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.2","Name" :
"QUERY_DATA_ITEM_ATTRIBUTE","CorrelationID" : "eDirectory#5#","SubEvent" :
"DSE_LIST_PARTITIONS"},"Time" : {"Offset" : 1489681000},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Événements XDAS

Pour plus d'informations sur les événements XDAS, reportez-vous à l'Annexe H, « Assignation d'événements eDirectory à des événements XDAS », page 895.

Dépannage des problèmes liés à XDAS

Pour plus d'informations sur la résolution des problèmes d'installation et de configuration, reportez-vous à la « Dépannage des problèmes liés à XDAS » page 949.

Audit à l'aide de CEF

Le format CEF (Common Event Format) fournit un format d'événement standard afin de faciliter la fusion et l'analyse des informations d'audit à partir de plusieurs composants au niveau du système distribué. Le format CEF utilise le format de message Syslog comme mécanisme de transport.

CEF est un format texte extensible conçu pour prendre en charge plusieurs types de périphériques, tels que les périphériques sur site et les services basés sur le cloud. Les événements CEF facilitent la compréhension des suivis d'audit d'applications hétérogènes.

La configuration d'eDirectory pour utiliser CEF offre les avantages suivants :

- fournit des services d'audit uniformes et sécurisés pour un système distribué ;
- CEF utilise un format de message standard qui simplifie la gestion des logs.
- Le nouveau format d'événement s'intègre à Sentinel de manière transparente.

REMARQUE : si vous utilisez eDirectory 9.1 avec Identity Manager 4.7, vous pouvez activer le module d'audit CEF ou XDAS. Si vous mettez à niveau Identity Manager à partir d'une version antérieure à 4.7, désactivez le module d'audit XDAS pour utiliser CEF avec eDirectory.

La section suivante explique comment configurer CEF avec eDirectory :

- « Configuration de CEF » page 651

Configuration de CEF

Le paquetage de téléchargement du kit d'installation d'eDirectory inclut un client CEF pour Linux et un autre pour Windows. Le programme d'installation d'eDirectory installe les paquetages CEF sur votre système d'exploitation. Le paquetage CEF contient les fichiers suivants :

- Linux
  - `novell-edirectory-xdaslog`
  - `novell-edirectory-xdaslog-conf`
  - `novell-edirectory-cefinstrument-9.2.0-0.x86_64.rpm`
- Windows
  - `cefauditds.dlm`
  - `xdaslog.dll`

Cette section contient les informations suivantes :

- « Configuration système requise » page 652
- « Installation du plug-in iManager pour CEF » page 652
- « Configuration du fichier de propriétés CEF » page 652
- « Configuration de CEF pour l'audit » page 658
- « Chargement et déchargement des modules » page 660
- « Activation du caching des événements CEF » page 661
- « Présentation des types d'événements CEF » page 661
- « Utilisation de collecteurs pour les événements CEF » page 663
- « Présentation du filtrage des événements d'audit CEF » page 664

- « Schéma d'implémentation CEF » page 665
- « Événements CEF » page 670

Configuration système requise

L'installation et l'utilisation du plug-in NetIQ Audit pour iManager requièrent iManager 3.1 ou version ultérieure. Pour en savoir plus sur la configuration requise et obtenir les instructions de téléchargement, reportez-vous à la page du produit NetIQ iManager.

Installation du plug-in iManager pour CEF

Le plug-in iManager pour CEF est fourni avec les plug-ins eDirectory 9.2. Ces derniers peuvent également être téléchargés à partir du site de téléchargement NetIQ.

Pour installer le plug-in iManager :

1. Ouvrez iManager à partir d'un navigateur Web, à l'aide de l'URL suivante :

   `https://ip_address_or_DNS/nps/iManager.html`

   où *adresse_ip_ou_DNS* représente l'adresse IP ou le nom DNS de votre serveur iManager.

   Par exemple :

   `http://111.111.1.1/nps/iManager.html`

2. Connectez-vous à iManager à l'aide de votre nom d'utilisateur et de votre mot de passe.

   Si vous souhaitez accéder à toutes les fonctions de NetIQ iManager, vous devez vous connecter à l'arborescence en tant qu'administrateur. Seul un administrateur dispose d'un accès complet à toutes les fonctionnalités. S'il n'est pas administrateur, l'utilisateur peut uniquement accéder aux rôles pour lesquels des droits lui sont assignés.

   Pour plus d'informations, reportez-vous au Guide d'administration de NetIQ iManager.

Configuration du fichier de propriétés CEF

Un exemple de fichier de propriétés (`auditlogconfig.properties.template`) est inclus dans le répertoire `configdir` (`n4u.server.configdir`) sur le support d'eDirectory.

Le Tableau 23-1 indique l'emplacement par défaut du fichier `auditlogconfig.properties` sur les systèmes d'exploitation Linux et Windows.

Tableau 23-4 *Fichier de configuration CEF*

Système d'exploitation	Emplacement du fichier de propriétés
Linux	`/etc/opt/novell/eDirectory/conf/auditlogconfig.properties` Pour les installations non-root, le fichier de propriétés CEF se trouve dans le répertoire `conf`.
Windows	`<Install Path>/novell/nds/auditlogconfig.properties` Le fichier de propriétés se trouve généralement dans le répertoire d'installation d'eDirectory.

Si vous configurez le fichier de propriétés, puis mettez à niveau votre environnement eDirectory 9.2 vers une version plus récente, le programme d'installation ne remplace pas le fichier de propriétés. Le cas échéant, le processus de mise à niveau met à jour le fichier (`auditlogconfig.properties`) de manière à conserver la personnalisation.

Vous pouvez configurer CEF après l'installation d'iManager. Les paramètres de configuration de CEF sont stockés dans un simple fichier de configuration au format texte (`auditlogconfig.properties`). Vous pouvez personnaliser le fichier en fonction de vos besoins.

Le fichier de propriétés CEF (auditlogconfig.properties) contient les informations suivantes :

Linux

```
# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL)
#log4j.appender.S.Protocol=TCP

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=no

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=/var/opt/novell/eDirectory

# Cache File Size
# Cache File Size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender

# Log file for appender R.
#log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB
```

```
# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
```

Windows

```
# Brief description for appenders and their options are provided.
# For detailed decriptions refer to log4cxx documentation.

# Set the level of the root logger to DEBUG and attach appenders.
#log4j.rootLogger=debug, S, R

# Defines appender S to be a SyslogAppender.
#log4j.appender.S=org.apache.log4j.net.SyslogAppender

# Defines location of Syslog server.
#log4j.appender.S.Host=localhost
#log4j.appender.S.Port=port

# Specify protocol to be used (UDP/TCP/SSL).
#log4j.appender.S.Protocol=SSL

# Specify SSL certificate file for SSL connection.
# File path should be given with double backslash.
#log4j.appender.S.SSLCertFile=C:\\Novell\\mycert.pem

# Minimum log-level allowed in syslog.
#log4j.appender.S.Threshold=INFO

# Defines the type of facility.
#log4j.appender.S.Facility=USER

# Defines caching for SyslogAppender.
# Inputs should be yes/no
#log4j.appender.S.CacheEnabled=yes

# Cache location directory
# Directory should be available for creating cache files
#log4j.appender.S.CacheDir=C:\\NetIQ\\eDirectory

# Cache File Size
# Cache File size should be in the range of 50MB to 4000MB
#log4j.appender.S.CacheMaxFileSize=500MB

# Layout definition for appender Syslog S.
#log4j.appender.S.layout=org.apache.log4j.PatternLayout
#log4j.appender.S.layout.ConversionPattern=%c: %m%n

# Defines appender R to be a Rolling File Appender.
#log4j.appender.R=org.apache.log4j.RollingFileAppender
```

```
# Log file for appender R.
# File path should be given with double backslash.
#log4j.appender.R.File=C:\\cef-events.log

# Max size of log file for appender R.
#log4j.appender.R.MaxFileSize=100MB

# Set the maximum number of backup files to keep for appender R.
# Max can be 13. If set to zero, then there will be no backup files.
#log4j.appender.R.MaxBackupIndex=10

# Layout definition for appender Rolling log file R.
#log4j.appender.R.layout=org.apache.log4j.PatternLayout
#log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
```

Avant d'examiner le contenu du fichier `auditlogconfig.properties`, NetIQ recommande de passer en revue les considérations suivantes :

- Les lettres S et R correspondent respectivement à l'appender Syslog et à l'appender RollingFile.
- Les entrées ne respectent pas la casse.
- Les entrées peuvent apparaître dans n'importe quel ordre.
- Les lignes vides dans le fichier sont valides.
- Toute ligne commençant par un signe dièse (#) est commentée.

Le tableau ci-dessous fournit des informations à propos des paramètres du fichier `auditlogconfig.properties` :

IMPORTANT : vous devez redémarrer eDirectory après avoir modifié la configuration.

Valeur	Description
log4j.rootLogger=**debug, S, R**	Définit le niveau de l'enregistreur racine sur Débogage et y associe un appender nommé R ou S, S correspondant à Syslog et R à Rolling File.
log4j.appender.S=**org.apache.log4j.net.SyslogAppender**	Indique que l'appender S doit être un appender Syslog.
log4j.appender.S.Host=**localhost**	Indique à quel emplacement du serveur Syslog les événements CEF sont consignés. Par exemple : log4j.appender.S.Host=192.168.0.1
log4j.appender.S.Port=**port**	Port sur lequel CEF se connecte au serveur Syslog. Le numéro de port peut être compris entre 1 et 65535. Si vous spécifiez une valeur non valide, le numéro de port est défini par défaut sur 514. En cas d'échec de la connexion entre CEF et le serveur Syslog, Identity Manager ne peut pas consigner les événements tant que la connexion n'a pas été restaurée.
log4j.appender.S.Protocol=TCP	Indique le protocole à utiliser. Par exemple : UDP, TCP ou SSL.

Valeur	Description
log4j.appender.S.SSLCertFile=**/etc/opt/novell/mycert.pem**	Spécifie le fichier de certificat SSL pour la connexion SSL. Utilisez deux barres obliques inverses pour spécifier le chemin d'accès au fichier. Ce paramètre est facultatif.
log4j.appender.S.Threshold=**INFO**	Spécifie le niveau de consignation minimal autorisé dans l'appender Syslog. Actuellement, le niveau de consignation INFO est pris en charge.
log4j.appender.S.Facility=**USER**	Indique le type d'installation. L'installation est utilisée pour tenter de classer le message. Actuellement, l'installation USER est prise en charge. Ces valeurs peuvent être spécifiées en majuscules ou en minuscules.
log4j.appender.S.layout=**org.apache.log4j.PatternLayout**	Paramètre d'agencement de l'appender Syslog.
log4j.appender.S.layout.ConversionPattern**=%c : %p%m%n**	Paramètre d'agencement de l'appender Syslog. Pour plus d'informations sur les schémas de conversion et leur description, consultez le site logging.apache.org.
log4j.appender.R=**org.apache.log4j.RollingFileAppender**	Indique que l'appender R doit être un appender RollingFile.
log4j.appender.R.File=**/var/opt/novell/eDirectory/log/cef-events.log**	Emplacement du fichier journal pour l'appender RollingFile.
log4j.appender.R.MaxFileSize=**100MB**	Taille maximale, en Mo, du fichier journal pour l'appender RollingFile. Définissez cette valeur sur la taille maximale autorisée par le client.
log4j.appender.R.MaxBackupIndex=**10**	Spécifiez le nombre maximal de fichiers de sauvegarde pour l'appender RollingFile. Le nombre maximal de fichiers de sauvegarde peut être 10. Une valeur 0 signifie qu'aucun fichier de sauvegarde n'est présent.
log4j.appender.R.layout=**org.apache.log4j.PatternLayout**	Paramètre d'agencement de l'appender RollingFile.
log4j.appender.R.layout.ConversionPattern=**%d{MMM dd HH:mm:ss} %c : %p%m%n**	Paramètre d'agencement de l'appender RollingFile. Pour des modèles de format de date simples, reportez-vous au Tableau 23-2. Pour plus d'informations sur les schémas de conversion et leur description, consultez le site logging.apache.org.

Le Tableau 23-2 donne des exemples de modèles de date et d'heure interprétés aux États-Unis. Les date et heure en question sont le 04/07/2012, 12 h 8 min 56 s, heure du Pacifique aux États-Unis.

Tableau 23-5 Exemples de modèles de date et d'heure

Modèle de date et d'heure	Résultat
"aaaa.MM.jj G 'à' HH:mm:ss z"	2012.07.04 AD at 12:08:56 PDT (04.07.2012 ap. J-C à 12:08:56 HAP)
"EEE, MMM j, "aa"	Wed, Jul 4, '01 (Mer, 4 juil. 2001)
"h:mm a"	12:08 PM (12:08)
"hh 'heures' a, zzzz"	12 o'clock PM, Pacific Daylight Time (12 heures, heure avancée du Pacifique)
"K:mm a, z"	12:08 PM, PDT (12:08, HAP)
"aaaaa.MMMMM.jj GGG hh:mm aaa"	02012.July.24 AD 12:08 PM (02012.Juillet.24 ap. J-C 12:08)
"EEE, j MMM aaaa HH:mm:ss Z"	Wed, 24 Jul 2012 12:08:56 -0700 (Mer, 24 juil. 2012 12:08:56 -0700)
"aaMMjjHHmmssZ"	120724120856-0700
"aaaa-MM-jj'T'HH:mm:ss.SSSZ"	2012-07-04T12:08:56.235-0700 (2012-07-04T12:08:56.235-0700)

Activation de l'appender Syslog

Vous pouvez utiliser l'appender Syslog pour afficher les événements en temps réel. Par ailleurs, un serveur Syslog offre une meilleure prise en charge des sauvegardes en cas de sinistre.

Pour activer l'appender Syslog, apportez les modifications suivantes au fichier `auditlogconfig.properties` :

1. Remplacez la valeur de l'entrée ci-dessous par S pour joindre un appender Syslog :

   ```
   log4j.rootLogger=debug, S
   ```

2. Supprimez les marques de commentaire des entrées suivantes :

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   log4j.appender.S.Host=localhost
   log4j.appender.S.Port=port
   log4j.appender.S.Protocol=SSL
   log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
   #log4j.appender.S.Threshold=INFO
   #log4j.appender.S.Facility=USER
   #log4j.appender.S.layout=org.apache.log4j.PatternLayout
   #log4j.appender.S.layout.ConversionPattern=%c: %m%n
   ```

3. Connectez-vous à iManager et modifiez les événements de journal. Pour plus d'informations sur la configuration des événements CEF, reportez-vous à la section « Configuration des événements CEF pour l'audit » page 659.

REMARQUE : le caching CEF qui utilise le protocole `UDP` pour `SyslogAppender` ne fonctionne pas.

Génération d'un certificat pour la connexion SSL Syslog

Pour générer un certificat pour la connexion Syslog :

1. Créez le certificat à l'aide de la commande OpenSSL suivante :

   ```
   openssl s_client -host LOG_SERVER  -port 1443 -showcerts
   ```

2. Indiquez l'emplacement du fichier de certificat que vous avez créé dans le fichier `/etc/opt/novell/eDirectory/conf/auditlogconfig.properties`.

Activation de l'appender RollingFile

Si la solution d'audit est limitée à un seul serveur, il est préférable d'opter pour cet appender de fichier. L'appender Fichier propagé est plus fiable que l'appender Syslog, car il peut stocker les événements sur votre système de fichiers local et empêche la parte d'événements. Le nombre de composants à configurer étant limité, cette solution est également facile à mettre en oeuvre et plus adaptée aux démonstrations.

REMARQUE : si vous utilisez le connecteur de fichiers pour CEF, assurez-vous que le modèle de conversion pour l'appender Fichier propagé soit similaire à celui de l'appender Syslog comme indiqué ci-dessous :

```
log4j.appender.R.layout.ConversionPattern=%c: %m%n
```

Pour activer l'appender RollingFile, apportez les modifications suivantes au fichier `auditlogconfig.properties` :

1. Remplacez la valeur de l'entrée ci-dessous par R pour joindre l'appender RollingFile :

   ```
   log4j.rootLogger=debug, R
   ```

2. Supprimez les marques de commentaire des entrées suivantes :

   ```
   log4j.appender.R=org.apache.log4j.RollingFileAppender
   log4j.appender.R.File=/var/opt/novell/eDirectory/log/cef-events.log
   log4j.appender.R.MaxFileSize=100MB
   log4j.appender.R.MaxBackupIndex=10
   log4j.appender.R.layout=org.apache.log4j.PatternLayout
   log4j.appender.R.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %c %m%n
   ```

3. Sélectionnez l'événement souhaité dans iManager.

   Pour plus d'informations sur la configuration des événements CEF, reportez-vous à la section « Configuration des événements CEF pour l'audit » page 659.

Configuration de CEF pour l'audit

- « Utilisation du plug-in iManager pour la configuration de CEF » page 659
- « Configuration des événements CEF pour l'audit » page 659

Utilisation du plug-in iManager pour la configuration de CEF

1 Ouvrez iManager à partir d'un navigateur Web, à l'aide de l'URL suivante :

   `https://ip_address_or_DNS/nps/iManager.html`

   où *adresse_ip_ou_DNS* représente l'adresse IP ou le nom DNS de votre serveur iManager.

   Par exemple :

   `http://111.111.1.1/nps/iManager.html`

2 Connectez-vous en entrant votre nom d'utilisateur et votre mot de passe.

   Si vous souhaitez accéder à toutes les fonctions de NetIQ iManager, vous devez vous connecter à l'arborescence en tant qu'administrateur. Seul un administrateur dispose d'un accès complet à toutes les fonctionnalités. S'il n'est pas administrateur, l'utilisateur peut uniquement accéder aux rôles pour lesquels des droits lui sont assignés.

   Pour plus d'informations, reportez-vous au *Guide d'administration de NetIQ iManager*.

3 Sélectionnez **Rôles et tâches** > **Configuration de l'audit**.

4 Spécifiez le nom de votre serveur eDirectory dans **Serveur NCP**, puis cliquez sur l'icône **Sélecteur d'objet** pour rechercher le serveur eDirectory.

5 Cliquez sur **OK**.

   La page CEF Audit (Audit CEF) s'affiche. Passez à la « Configuration de CEF » page 651.

Configuration des événements CEF pour l'audit

1 Connectez-vous à iManager à l'aide de votre nom d'utilisateur et de votre mot de passe.

2 Sélectionnez **Rôles et tâches** > **Audit eDirectory** > **Configuration de l'audit**.

3 Sélectionnez l'onglet **CEF**.

4 Configurez les événements CEF.

   - **Global :** vous pouvez sélectionner ou désélectionner les paramètres globaux pour les entrées en double.
     - **Ne pas envoyer d'événement répliqué :** sélectionnez cette option pour ne plus recevoir les événements en double en raison de la réplication à partir d'autres serveurs.
   - **Consigner les valeurs de l'événement :** les événements sont consignés dans un fichier texte. Les valeurs d'événements de plus de 768 octets sont considérées comme de « grandes valeurs ». Vous pouvez consigner des événements de n'importe quelle taille.
     - **Consigner de grandes valeurs :** sélectionnez cette option pour consigner les événements dont la taille est supérieure à 768 octets.
     - **Ne pas consigner de grandes valeurs :** sélectionnez cette option pour consigner les événements dont la taille est inférieure à 768 octets.
     - **Consigner les valeurs d'attribut :** sélectionnez cette option pour afficher les valeurs d'attribut. Cette option s'applique uniquement aux événements **Ajouter une valeur** et **Supprimer la valeur**.
     - **Ne pas consigner les valeurs d'attribut :** Sélectionnez cette option pour supprimer les valeurs d'attribut. Cette option s'applique uniquement aux événements **Ajouter une valeur** et **Supprimer la valeur**. Par défaut, cette option est sélectionnée.
     - **Consigner les valeurs d'attributs chiffrés :** sélectionnez cette option pour afficher les valeurs d'attributs chiffrés. Cette option s'applique uniquement aux événements **Ajouter une valeur** et **Supprimer la valeur**.

- **Ne pas consigner les valeurs d'attributs chiffrés :** sélectionnez cette option pour supprimer les valeurs d'attributs chiffrés. Cette option s'applique uniquement aux événements **Ajouter une valeur** et **Supprimer la valeur**. Par défaut, cette option est sélectionnée.

REMARQUE : Si l'événement est plus volumineux, sa valeur est tronquée et enregistrée dans le fichier journal.

- **Configuration des événements de base :** spécifiez des valeurs pour les options ci-dessous, en fonction des événements requis pour votre environnement :

REMARQUE : par défaut, les catégories d'événements individuelles sous la section Configuration des événements de base sont réduites. Vous pouvez agrandir chaque catégorie pour sélectionner des événements individuels.

Options	Description
Événements de sécurité	Sélectionnez les événements de sécurité pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour ajouter ou supprimer un membre, pour détecter un intrus, pour changer de mot de passe, pour authentifier des utilisateurs, etc.
Événements d'objets	Sélectionnez les événements d'objets pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour créer, supprimer, renommer, déplacer et rechercher des objets.
Événements d'attributs	Sélectionnez les événements d'attributs pour lesquels vous souhaitez consigner des événements. Vous pouvez consigner des événements pour lire et supprimer des attributs et pour ajouter, supprimer et comparer des valeurs d'attributs.
Événements LDAP	Sélectionnez les événements LDAP pour lesquels vous souhaitez consigner des événements.

Pour plus d'informations sur les événements internes eDirectory assignés aux événements CEF correspondants, reportez-vous à la section « Assignation d'événements eDirectory à des événements CEF » page 933.

REMARQUE : une fois la configuration d'événement modifiée, l'application des modifications de configuration sur le serveur NCP peut prendre jusqu'à 3 minutes. Si vous voulez que les modifications apportées à la configuration soient immédiatement prises en compte sur le serveur NCP, vous devez décharger et charger le module `cefauditds`.

Chargement et déchargement des modules

Une fois les événements CEF configurés, exécutez les commandes ci-dessous pour charger et décharger les modules CEF :

Pour charger automatiquement le module `cefauditds` à chaque démarrage du serveur `ndsd` :

- **Linux**

  Ajoutez `cefauditds` au fichier `/etc/opt/novell/eDirectory/conf/ndsmodules.conf`.

- **Windows**

  Exécutez le fichier `ndscons.exe`, sélectionnez `cefauditds` dans la liste des modules disponibles, cliquez sur **Démarrage**, puis définissez l'option Type de démarrage sur **Automatique**.

Pour charger et décharger manuellement le module `cefauditds` :

- **Linux**

  Pour charger le module, exécutez `ndstrace -c "load cefauditds"`.

  Pour décharger le module, exécutez `ndstrace -c "unload cefauditds"`.

- **Windows**

  Pour charger le module, exécutez le fichier `ndscons.exe`, sélectionnez **cefauditds** dans la liste des modules disponibles, puis cliquez sur **Démarrer**.

  Pour décharger le module, exécutez le fichier `ndscons.exe`, sélectionnez **cefauditds** dans la liste des modules disponibles, puis cliquez sur **Arrêter**.

Activation du caching des événements CEF

eDirectory 9.2 vous permet en option de stocker en local des événements CEF sur l'agent dans un cache de l'appender Syslog. Lorsque les événements sont mis en cache, si l'agent ne peut pas communiquer avec le serveur d'audit, les événements d'audit générés sont conservés, ce qui permet d'éviter toute perte des données d'audit. Une fois la communication rétablie entre l'ordinateur de l'agent et le serveur d'audit, l'agent tente de renvoyer les événements mis en cache.

Le caching des événements CEF est désactivé par défaut. Pour activer le caching des événements, procédez comme suit :

1. Sur l'ordinateur de l'agent, accédez à l'emplacement du fichier de propriétés CEF. Par défaut, le fichier `auditlogconfig.properties` se trouve à l'emplacement `/etc/opt/novell/eDirectory/conf/auditlogconfig.properties`. Pour les installations non-root, le fichier de propriétés CEF se trouve par défaut dans le répertoire `conf`.
2. Utilisez un éditeur de texte pour ouvrir le fichier `auditlogconfig.properties`.
3. Dans le fichier de propriétés, accédez à la propriété `log4j.appender.S.CacheEnabled` et définissez sa valeur sur `yes`.
4. (Conditionnel) Si vous souhaitez mettre en cache les événements dans un répertoire spécifique, définissez la valeur de la propriété `log4j.appender.S.CacheDir` sur le chemin de répertoire. Si vous spécifiez un répertoire, assurez-vous que son chemin est un emplacement valide sur le serveur. Si la propriété `log4j.appender.S.CacheDir` n'est pas définie, les journaux de l'appender Syslog mettent en cache les événements dans le répertoire `dib` de cette instance.
5. (Conditionnel) Si vous souhaitez spécifier une taille de fichier personnalisée pour le cache, modifiez la valeur de la propriété `log4j.appender.S.CacheMaxFileSize`. La valeur par défaut est 500 Mo. La valeur minimale est 50 Mo et la valeur maximale, 4 Go.
6. Enregistrez, puis fermez le fichier `auditlogconfig.properties`.

Présentation des types d'événements CEF

Vous pouvez configurer CEF de sorte à consigner les événements dans les catégories suivantes :

- Sécurité
- Objets

- Attributs
- LDAP

Vous pouvez auditer les ensembles de types d'événement par défaut suivants :

Catégorie	Type d'événement
Sécurité	◆ ACL modifiée ◆ Ajout d'un membre ◆ Suppression d'un membre ◆ Intrusion détectée ◆ Connexion désactivée ◆ Connexion activée ◆ Connexion ◆ Modification des équivalents de sécurité ◆ Configuration de l'audit ◆ Modification du mot de passe ◆ Déverrouillage du compte ◆ Déconnexion ◆ Connexion ◆ Emprunt d'identité ◆ Authentification ◆ Vérification du mot de passe ◆ Modification de la configuration de la connexion ◆ Référence de la requête
Objets	◆ Créer un objet ◆ Supprimer l'objet ◆ Renommer l'objet ◆ Déplacer l'objet ◆ DSU lu ◆ Rechercher
Attributs	◆ Lire l'attribut ◆ Supprimer l'attribut ◆ Ajouter une valeur ◆ Supprimer la valeur ◆ Comparer la valeur de l'attribut

Catégorie	Type d'événement
LDAP	◆ Liaison LDAP ◆ Réponse de la liaison LDAP ◆ Annulation de la liaison LDAP ◆ Connexion LDAP ◆ Recherche LDAP ◆ Réponse de la recherche LDAP ◆ Réponse de l'entrée de recherche LDAP ◆ Ajout LDAP ◆ Réponse de l'ajout LDAP ◆ Comparaison LDAP ◆ Réponse de la comparaison LDAP ◆ Modification LDAP ◆ Réponse de la modification LDAP ◆ Suppression LDAP ◆ Suppression de réponse LDAP ◆ Modification de DN LDAP ◆ Réponse de la modification du DN LDAP ◆ Abandon LDAP ◆ Opération étendue LDAP ◆ Opération étendue du système LDAP ◆ Réponse de l'opération étendue LDAP ◆ Modification de la configuration du serveur LDAP ◆ Opération LDAP inconnue ◆ Modification de mot de passe LDAP

Utilisation de collecteurs pour les événements CEF

Pour plus d'informations sur l'utilisation de collecteurs d'événements CEF, reportez-vous à la documentation du collecteur eDirectory sur la page des plug-ins Sentinel.

Présentation du filtrage des événements d'audit CEF

À l'aide de filtres et de notifications d'événement, CEF est capable de signaler la survenue ou la non-survenue d'un type d'événement spécifique. Vous pouvez également filtrer les événements pour un(e) ou plusieurs classes ou attributs d'objet spécifiques, selon le type d'événement. CEF évalue tous les événements générés en fonction des filtres configurés sur le serveur eDirectory et ne consigne que les événements qui correspondent à ces filtres.

Cette section fournit les informations nécessaires pour configurer les filtres et les notifications du système.

- « Filtrage des événements d'objet CEF » page 664
- « Filtrage des événements d'attribut CEF » page 664
- « Filtrage des événements eDirectory à l'aide du filtre d'exclusion » page 665

Filtrage des événements d'objet CEF

Vous pouvez configurer le filtrage des objets de manière à ne rechercher qu'un seul événement ou un type d'événements spécifique. Par exemple, si vous souhaitez être averti lorsqu'une personne crée un compte utilisateur dans eDirectory, vous pouvez créer un filtre de sélection de la classe d'objet Utilisateur pour consigner les événements dans le cadre de la création d'un nouvel objet Utilisateur.

Pour configurer le filtrage des comptes, cliquez sur le lien Événements d'objets, sélectionnez la classe, puis cliquez sur **OK** pour quitter l'application.

Pour configurer des filtres pour les événements de gestion des comptes :

1. Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.
3. Cliquez sur **Événements d'objets**.

   La fenêtre Configuration du filtrage des objets CEF s'affiche.
4. Dans la liste **Classes disponibles**, sélectionnez Utilisateur, choisissez une classe d'objet, puis cliquez sur la flèche droite pour déplacer la classe d'objet dans la liste **Classes sélectionnées**, puis cliquez sur **OK**. Par défaut, la classe d'objet **Ordinateur** est sélectionnée.

À l'aide du filtre configuré, le module d'audit CEF contrôle tous les événements générés pour les classes d'objet et les attributs sélectionnés et consigne ces événements.

Filtrage des événements d'attribut CEF

Cliquez sur le lien **Événements d'attributs** pour configurer le filtrage des événements d'attributs. Par exemple, si vous souhaitez être averti lorsqu'une personne ajoute une nouvelle valeur d'attribut dans eDirectory, vous pouvez créer un filtre pour consigner des événements en cas d'ajout d'une nouvelle valeur.

Pour configurer le filtrage des événements de gestion des approbations :

1. Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.
2. Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.
3. Cliquez sur **Événements d'attributs**.

   La fenêtre **Attribute Filtering** (Filtrage des attributs) s'affiche.

4 Dans la liste **Classes disponibles**, sélectionnez les classes d'objet pour lesquelles vous souhaitez collecter des événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes sélectionnées.** Par défaut, les classes d'objet **dynamicGroup**, **dynamicGroupAux**, **Groupe**, **Groupe LDAP** et **Rôle organisationnel** sont sélectionnées.

5 Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs pour les classes d'objet sélectionnées. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

REMARQUE : si vous sélectionnez une classe d'objet, tous les événements d'attributs pour tous les attributs de cette classe d'objet sont sélectionnés. Dans ce cas, vous obtiendrez tous les événements d'attributs pour l'ensemble des attributs sélectionnés dans les classes d'objet sélectionnées.

---

6 Cliquez sur **OK**.

Lorsque le filtre est configuré, le module d'audit CEF contrôle tous les événements générés pour les classes d'objet et les attributs sélectionnés et consigne ces événements.

Filtrage des événements eDirectory à l'aide du filtre d'exclusion

Cliquez sur le lien **Filtre d'exclusion** afin de configurer le filtrage des classes d'objet et des attributs pour lesquels vous ne souhaitez pas générer d'événement. Vous pouvez sélectionner des classes d'objet et des attributs.

Pour configurer le filtrage des événements eDirectory indésirables :

1 Dans iManager, accédez à **Rôles et tâches** > **Audit** > **Configuration de l'audit**.

2 Sélectionnez le serveur NCP à surveiller, puis cliquez sur **OK**.

3 Cliquez sur **Filtre d'exclusion**.

La fenêtre Filtrage des exclusions CEF s'affiche.

4 Dans la liste **Classes disponibles**, sélectionnez les classes d'objet pour lesquelles vous ne souhaitez pas collecter d'événements, puis cliquez sur la flèche droite pour les déplacer dans la liste **Classes sélectionnées**.

5 Dans la liste **Attributs disponibles**, sélectionnez le nombre souhaité d'attributs. Sélectionnez l'attribut, puis cliquez sur la flèche droite pour l'ajouter à la liste des attributs sélectionnés.

6 Cliquez sur **OK**.

À l'aide du filtre configuré, le module d'audit CEF arrête de générer des événements pour toutes les classes d'objet et les attributs sélectionnés.

Schéma d'implémentation CEF

Ce document définit le protocole CEF et fournit des informations sur la méthode à utiliser pour implémenter la norme. Il décrit en détail l'en-tête et les extensions prédéfinies utilisés dans le cadre de la norme.

Utilisation de CEF avec Syslog

CEF utilise Syslog comme mécanisme de transport. Il utilise le format suivant, constitué d'un préfixe Syslog, d'un en-tête et d'une extension, comme indiqué ci-dessous :

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
```

La partie `CEF:Version` du message est un en-tête obligatoire. Le reste du message est mis en forme à l'aide de champs séparés par une barre verticale (« | »). Tous les autres champs doivent être présents et sont définis dans la section « Définitions des champs CEF » page 666.

La partie prévue pour étendre le message est une marque de réservation pour des champs supplémentaires, mais n'est pas obligatoire. Tout autre champ supplémentaire est consigné en tant que paire clé-valeur. Pour plus d'informations, reportez-vous au « Définitions des champs CEF » page 666.

Définitions des champs CEF

Les champs inclus dans le schéma sont les champs CEF définis spécifiquement pour les événements d'audit. Certains ou l'ensemble de ces champs peuvent également être pertinents pour d'autres types d'événement, mais des informations de ce type sont requises pour les services d'audit.

Tableau 23-6 *Définitions des champs CEF*

Champ CEF	Description
Device Product (Périphérique-produit)	Device Product est une chaîne qui identifie de manière unique le périphérique à l'origine de l'envoi. Deux produits ne peuvent pas avoir la même paire périphérique-produit. L'administrateur doit veiller à assigner un nom unique à chaque paire périphérique-produit.
Device Version (Périphérique-version)	Device Version est une chaîne qui identifie de manière unique le périphérique à l'origine de l'envoi. Deux produits ne peuvent pas avoir la même paire périphérique-version. L'administrateur doit veiller à assigner un nom unique à chaque paire périphérique-version.
Device Vendor (Périphérique-fournisseur)	Device Vendor est une chaîne qui identifie de manière unique le périphérique à l'origine de l'envoi. Deux produits ne peuvent pas avoir la même paire périphérique-fournisseur. L'administrateur doit veiller à assigner un nom unique à chaque paire périphérique-fournisseur.
Device Event Class ID (ID de classe d'événement du périphérique)	Device Event Class ID est un identificateur unique par type d'événement. Il peut s'agir d'une chaîne ou d'un nombre entier. Device Event Class ID identifie le type d'événement signalé. Dans la sphère des systèmes de détection d'intrus (intrusion detection system - IDS), chaque signature ou règle qui détecte certaines activités a un identificateur unique de classe d'événement du périphérique qui lui est assigné. Cette exigence est valable pour d'autres types de périphériques également, et aide les moteurs de corrélation à traiter les événements. Cet identifiant est également connu sous l'appellation ID de signature.
Severity (Gravité)	Il s'agit d'une chaîne ou d'un nombre entier qui reflète l'importance de l'événement. Les valeurs de chaîne valides sont : **Unknown** (Inconnue), **Low** (Faible), **Medium** (Moyenne), **High** (Élevée) et **Very-High** (Très élevée). Les valeurs de nombre entier valides sont 0 à 3 = faible, 4 à 6 = moyenne, 7 et 8 = élevée et 9 et 10 = très élevée.
Version	Il s'agit d'un nombre entier qui identifie la version du format CEF. Les consommateurs d'événements utilisent ces informations pour déterminer ce que représentent les champs suivants. La version actuelle de CEF est 0.
Device Address (Adresse du périphérique)	Identifie l'adresse du périphérique à laquelle fait référence un événement dans un réseau IP. Le format est une adresse IPv4.
c6a1	Un des quatre champs d'adresse IPV6 disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire.

Champ CEF	Description
dvchost	Le format doit être un nom de domaine complet associé au nœud de périphérique, le cas échéant. Par exemple, `hôte.domaine.com` ou `hôte`.
rt	Heure de réception de l'événement associé à l'activité. Le format est MMM JJ aaaa hh:mm:ss ou millisecondes à partir de l'époque concernée.
dtz	Fuseau horaire du périphérique générant l'événement.
sourceServiceName	Service responsable de la génération de cet événement.
sproc	Nom du processus source de l'événement.
src	Identifie la source à laquelle un événement fait référence dans un réseau IP. Le format est une adresse IPv4. Par exemple, `192.168.10.1`.
spt	Il s'agit du numéro de port source. Les numéros de port valides sont compris entre 0 et 65 535.
shost	Identifie la source à laquelle un événement fait référence dans un réseau IP. Le format doit être un nom de domaine complet associé au nœud de la source, le cas échéant. Par exemple, `hôte.domaine.com` ou `hôte`.
suser	Identifie l'utilisateur source à l'aide d'un nom. Les adresses électroniques sont également assignées aux champs UserName. L'expéditeur est un candidat à placer dans `sourceUserName`.
dst	Identifie l'adresse de destination à laquelle fait référence un événement dans un réseau IP. Le format est une adresse IPv4. Par exemple, `192.168.10.1`.
duser	Identifie l'utilisateur de destination par son nom. Il s'agit de l'utilisateur associé à la destination de l'événement. Les adresses électroniques sont souvent assignées dans les champs UserName. Le destinataire est un candidat à placer dans `destinationUserName`.
cn1	Un des trois champs de nombre disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomNumber1`.
cn2	Un des trois champs de nombre disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomNumber2`.
cn3	Un des trois champs de nombre disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomNumber3`.
cn1Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomNumber1Label.`
cn2Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomNumber2Label`.

Champ CEF	Description
cn3Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomNumber3Label`
cs1	Une des six chaînes disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomString1`.
cs2	Une des six chaînes disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomString2`.
cs3	Une des six chaînes disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomString3`.
cs4	Une des six chaînes disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomString4`.
cs5	Une des six chaînes disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomString5`.
cs6	Une des six chaînes disponibles pour affecter des champs qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Également appelé `deviceCustomString6`.
cs1Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomString1Label`.
cs2Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomString2Label`.
cs3Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomString3Label`.
cs4Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomString4Label`.
cs5Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomString5Label`.

Champ CEF	Description
cs6Label	Tous les champs personnalisables comportent un champ d'étiquette pouvant accueillir une description du champ proprement dit. Chacun des champs est une chaîne qui décrit l'utilité de ce champ. Également appelé `deviceCustomString6Label`.
flexString1	Un des deux champs de chaîne disponibles pour affecter des données de chaîne qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
flexString2	Un des deux champs de chaîne disponibles pour affecter des données de chaîne qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
flexString1Label	Un des deux champs de chaîne disponibles pour affecter des données de chaîne qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
flexString2Label	Un des deux champs de chaîne disponibles pour affecter des données de chaîne qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
flexNumber1	Un des deux champs de nombre disponibles pour affecter des données longues qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
flexNumber2	Un des deux champs de nombre disponibles pour affecter des données longues qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
flexNumber1Label	Un des deux champs de nombre disponibles pour affecter des données longues qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.

Champ CEF	Description
flexNumber2Label	Un des deux champs de nombre disponibles pour affecter des données longues qui ne s'appliquent à aucun autre champ dans ce dictionnaire. À utiliser avec modération. Recherchez si possible un champ plus spécifique fourni par le dictionnaire. Ces champs sont généralement réservés à une utilisation par le client et ne doivent pas être définis par les fournisseurs, à moins que ce ne soit vraiment nécessaire.
cat	Représente la catégorie assignée par le périphérique d'origine. Les périphériques utilisent souvent leur propre schéma de catégorisation pour classer les événements. Également appelé `deviceEventCategory`. Par exemple, `/Monitor/Disk/Read`.
reason (motif)	Motif pour lequel un événement d'audit a été généré. Par exemple `Bad password` (mot de passe erroné) ou `Unknown User` (utilisateur inconnu). Il peut également s'agir d'un message d'erreur ou d'un code de renvoi.
outcome (résultat)	Affiche le résultat, généralement sous la forme de `success` (réussite) ou `failure` (échec). Également appelé `eventOutcome`.

Exemple d'événement

Vous trouverez ci-dessous un exemple d'événement :

```
Oct 31 16:29:37 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035D|AUTHENTICATE|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 31 2017 16:29:37 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=CN\=admin,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User cs3Label=Tree
Name cs3=TEST-CEF-AGN cs4Label=Correlation ID cs4=eDirectory#16# cs6Label=Server
Name cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_AUTHENTICATE flexNumber2Label=Grouping flexNumber2=309
cat=Security reason=0 outcome=Success
```

Événements CEF

Pour plus d'informations sur les événements XDAS, reportez-vous à l'Annexe I, « Assignation d'événements eDirectory à des événements CEF », page 933.

Caching des événements de journal

eDirectory dispose d'un système qui permet aux consommateurs d'événements de s'inscrire à des événements et de les consommer lorsqu'ils surviennent. Un gestionnaire d'événements peut être inscrit en tant qu'employé, que système en ligne ou que journal. La file d'attente des événements de journal est censée répertorier les événements dans l'ordre où ils se produisent. Avec le système d'événements de journal actuel, la file d'attente des événements de journal est conservée en mémoire. Si les consommateurs des événements sont lents, ou si la fréquence à laquelle les événements se produisent est supérieure au rythme auquel ils peuvent être traités, la file d'attente de journal commence à s'allonger, entraînant la croissance de la mémoire du processus ndsd.

Le système des événements de journal est modifié pour vous permettre d'utiliser une combinaison de mémoire et de disque afin de gérer les événements figurant dans une file d'attente. La forte augmentation en mémoire du processus ndsd est ainsi réduite.

Dans certains cas, les événements peuvent causer une croissance de la mémoire, par exemple lorsque *ndstrace* ou *l'audit* est activé. Vous pouvez contrôler la croissance de la mémoire en activant le caching du système d'événements.

Configuration du caching du système d'événements

Vous devez définir les variables d'environnement ci-dessous pour le caching du système d'événements :

- NDSD_EVENT_DISK_CACHE

  Cette variable contrôle l'utilisation du nouveau système d'événements. Par défaut, le nouveau système d'événements est désactivé. Pour l'activer, exportez cette variable avec une valeur *true* ou *1*.

- (Facultatif) NDSD_EVENT_DISK_CACHE_DIR

  Cette variable spécifie l'emplacement temporaire auquel les fichiers d'événements sont créés. S'il n'existe pas encore, le sous-répertoire `cdir` est créé sous le répertoire spécifié. Au démarrage, tous les fichiers contenus dans le sous-répertoire sont nettoyés. Nous vous recommandons de configurer le répertoire de caching dans une autre partition de disque que celle de DIB.

  Sous Linux, si `NDSD_EVENT_DISK_CACHE_DIR` n'est pas spécifié ou que le répertoire indiqué n'est pas accessible, ndsd utilise `vardir` comme répertoire de caching. Par défaut, la valeur de `vardir est /var/opt/novell/eDirectory/data/`.

  Sous Windows, si cette variable n'est pas spécifiée ou que le répertoire indiqué n'est pas accessible, dhost utilise le répertoire `DIBFiles`.

REMARQUE : assurez-vous que répertoire de caching comporte suffisamment d'espace disque disponible, car ndsd/dhost peut rapidement consommer plusieurs Go d'espace disque.

Audit LDAP

L'audit est l'une des principales fonctionnalités qui intéresseront l'administrateur pour l'évaluation d'un annuaire. Le mécanisme d'événements eDirectory facilite l'audit eDirectory. Étant donné que les applications adoptent largement le protocole LDAP pour accéder aux répertoires, il est désormais essentiel que les opérations LDAP soient auditées.

Ce chapitre comprend les sections suivantes :

- « Nécessité d'un audit LDAP » page 671
- « Utilisation de l'audit LDAP » page 672
- « Pour plus d'informations » page 672

Nécessité d'un audit LDAP

L'absence de ce mécanisme d'événement sur le serveur LDAP eDirectory existant était particulièrement notable, car les informations LDAP fournies n'étaient pas suffisantes. Le système d'événements NDS produisait des événements pour toutes les opérations eDirectory, mais la plupart de ces informations étaient insuffisantes ou inadaptées pour qu'une application puisse auditer le serveur LDAP. Les informations concernant le protocole et la liaison, l'adresse réseau, les méthodes et types d'authentification, la recherche et les transactions LDAP, etc., sont essentielles à l'audit d'un

serveur LDAP, mais elles n'étaient pas disponibles avec les événements NDS. Pour les développeurs d'applications, il était compliqué d'écrire dans des applications d'audit LDAP en fonction de ces événements.

LDAP est une interface importante d'eDirectory. eDirectory inclut un sous-système d'événements LDAP qui permet aux applications d'auditer le serveur LDAP eDirectory. Ce sous-système génère des événements LDAP spécifiques, avec toutes les informations pertinentes, pour qu'une application puisse auditer un serveur LDAP. Il s'intitule « audit LDAP ».

Utilisation de l'audit LDAP

L'audit LDAP permet aux applications de surveiller/auditer les opérations LDAP, notamment l'ajout, la modification et la recherche, et extrait du serveur LDAP des informations utiles telles que les informations de connexion, l'IP du client auquel le serveur était connecté au moment de l'opération LDAP, l'ID du message, le code de résultat de l'opération, etc.

L'audit LDAP peut être exercé par le biais de LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html), qui fournissent l'interface côté client de cette fonctionnalité par l'intermédiaire de nouveaux événements et structures LDAP.

Pour plus d'informations

Pour plus d'informations sur les événements d'audit LDAP, reportez-vous à la documentation suivante :

- NDK : outils LDAP (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html) dans la documentation LDAP Libraries for C.
- Pour plus d'informations sur les outils LDAP, reportez-vous à la documentation LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html).

24 Présentation de l'infrastructure d'authentification d'eDirectory

Cette section présente le fonctionnement de NMAS, un composant qui est automatiquement installé avec eDirectory. Pour en savoir plus sur les plates-formes prises en charge et obtenir les instructions d'installation, reportez-vous au *Guide d'installation de NetIQ eDirectory*.

- « Fonctionnalités de NMAS » page 673
- « Logiciel NMAS » page 677
- « Gestion des méthodes et des séquences de connexion et de post-connexion » page 679
- « Connexion au réseau à l'aide de NMAS » page 686
- « Historique des mots de passe NetIQ » page 688
- « Connexion basée sur HOTP NMAS » page 689
- « Autres tâches d'administration » page 694
- « Considérations relatives à la sécurité » page 701

Fonctionnalités de NMAS

NMAS a été conçu pour vous aider à protéger les informations résidant sur votre réseau. Outre l'outil de gestion des mots de passe, NMAS inclut plusieurs méthodes d'authentification pour les réseaux NetIQ eDirectory. De cette manière, vous pouvez vous assurer que les individus qui tentent d'accéder à vos ressources réseau sont bien qui ils prétendent être.

Concernant les périphériques d'authentification, NMAS fait appel à trois phases d'opération au cours d'une session utilisateur sur un poste de travail. Ces trois phases sont les suivantes :

1. Phase d'identification de l'utilisateur (qui êtes-vous ?)
2. Phase d'authentification (connexion) (prouvez que vous êtes bien la personne que vous prétendez être)
3. Phase de détection de retrait de périphérique (vous êtes toujours là ?)

Ces trois phases sont totalement indépendantes les unes des autres. Des périphériques d'authentification peuvent être utilisés à chaque phase, mais le même périphérique ne doit pas nécessairement être utilisé à chaque fois.

Phase d'identification de l'utilisateur

Il s'agit du processus de collecte du nom d'utilisateur. Au cours de cette phase, le nom de l'arborescence, le contexte de l'utilisateur, le nom du serveur et le nom de la séquence NMAS à utiliser lors de la phase d'authentification sont également collectés. Ces informations d'authentification peuvent être obtenues à partir d'un périphérique d'authentification, ou spécifiées manuellement par l'utilisateur.

Phase d'authentification (connexion)

- « Authentification par mot de passe » page 674
- « Authentification par périphérique physique » page 675
- « Authentification biométrique » page 675

Pour la connexion au réseau, NMAS utilise trois approches différentes appelées **facteurs d'authentification**. Ces facteurs d'authentification décrivent différents éléments ou qualités qu'un utilisateur peut utiliser pour s'authentifier auprès du réseau :

- Authentification par mot de passe (quelque chose que vous connaissez)
- Authentification par périphérique physique (quelque chose que vous possédez)
- Authentification biométrique (quelque chose qui vous caractérise)

Pour plus d'informations sur ces facteurs d'authentification, reportez-vous à la « Méthodes et séquences de connexion et de post-connexion » page 676.

Authentification par mot de passe

Les mots de passe (quelque chose que vous connaissez) font partie des principaux moyens d'authentification auprès d'un réseau. NMAS propose plusieurs options d'authentification par mot de passe :

- **Méthode de connexion NDS :** stocké dans un format haché irréversible, le mot de passe NDS ne peut être utilisé que par le système NDS. Cette option utilise le mot de passe universel, s'il est activé et défini.
- **Méthode de connexion SCRAM :** la méthode d'authentification SCRAM (Salted Challenge Response Authentication Mechanism) utilise le hachage de mots de passe PBKDF2 pour authentifier les utilisateurs lorsqu'ils tentent de se connecter aux serveurs eDirectory (RFC 5802). Pour plus d'informations, reportez-vous à la section « Présentation du stockage de mots de passe non réversibles » page 786.

  REMARQUE : lors de la création d'une arborescence eDirectory 9.2, la méthode SCRAM est automatiquement installée. En cas de mise à niveau d'une version antérieure de l'arborescence eDirectory vers la version 9.2, vous devez installer manuellement la méthode SCRAM. Pour plus d'informations, reportez-vous à la section « Procédures d'installation d'une méthode de connexion » page 680.

- **Mot de passe simple :** le mot de passe simple permet aux administrateurs d'importer des utilisateurs et des mots de passe (en texte clair et au format haché) à partir d'annuaires LDAP étrangers. Cette option utilise le mot de passe universel, s'il est activé et défini.
- **Digest-MD5 SASL :** cette option fournit le mécanisme DIGEST-MD5 SASL, conforme à la convention IETF, qui valide un mot de passe haché par l'algorithme MD5 servant à établir une liaison SASL LDAP. Cette option utilise le mot de passe universel, s'il est activé et défini.
- **Réponse de stimulations :** cette option permet à l'utilisateur de prouver son identité en répondant à une ou plusieurs questions de vérification d'identité préconfigurées.

Le mot de passe universel est un moyen de simplifier l'intégration et la gestion des différents systèmes de mot de passe et d'authentification dans un réseau cohérent. Pour plus d'informations sur le mot de passe universel, reportez-vous au Chapitre 26, « Gestion des mots de passe », page 783.

Authentification par périphérique physique

Les développeurs de NetIQ et de solutions d'authentification tierces ont écrit, pour NMAS, des modules d'authentification pour plusieurs types de périphériques physiques (quelque chose que vous possédez).

REMARQUE : NMAS utilise ce terme pour faire référence à toutes les méthodes d'authentification par périphérique physique (cartes à puce avec certificats, périphériques de génération de mots de passe à usage unique, cartes de proximité, etc.).

- **Carte à puce :** une carte à puce est une carte en plastique de la taille d'une carte de crédit, ou un périphérique USB intégrant une puce programmable capable de stocker des données et d'exécuter des opérations de chiffrement. NMAS permet d'utiliser une carte à puce pour vérifier une identité lors de l'authentification auprès d'eDirectory.

  Pour les cartes à puce, NetIQ propose la méthode de connexion NetIQ Enhanced Smart Card, laquelle est fournie avec Identity Assurance Client. Pour plus d'informations, reportez-vous au *NetIQ Enhanced Smart Card Method 3.0 Installation and Administration Guide* (Guide d'installation et d'administration de NetIQ Enhanced Smart Card Method 3.0).
- **Périphérique de génération de mots de passe à unique (OTP) :** un périphérique OTP est un périphérique matériel de poche qui génère des mots de passe à usage unique pour authentifier son propriétaire.
- **Carte de proximité :** une carte de proximité est une carte portée par une personne. Cette technologie verrouille et déverrouille le poste de travail d'une personne en fonction de la proximité de la carte par rapport au poste de travail.

  NetIQ propose la méthode de connexion pcProx, laquelle prend en charge les cartes de proximité RFID. Cette méthode de connexion est fournie avec la solution NetIQ SecureLogin. Pour plus d'informations, reportez-vous à la documentation *NMAS Login Method and Login ID Snap-In for pcProx* (Méthode de connexion NMAS et snap-in d'ID de connexion pour pcProx).

Authentification biométrique

La *biométrie* désigne la science et la technologie qui s'intéressent à la mesure et à l'analyse statistique des caractéristiques du corps humain (quelque chose qui vous caractérise). Des sociétés tierces proposent des méthodes biométriques à utiliser avec NMAS.

L'authentification biométrique requiert des lecteurs ou scanneurs, un logiciel de conversion des informations scannées au format numérique, ainsi qu'une base de données ou un répertoire pour stocker les données biométriques à comparer avec les informations entrées.

Lors de la conversion des données biométriques entrées, le logiciel identifie des points de données spécifiques comme des points de correspondance. Ces derniers sont traités à l'aide d'un algorithme afin de créer une valeur qui peut être comparée aux données biométriques scannées lorsqu'un utilisateur tente d'accéder à un système.

Les méthodes d'authentification biométrique incluent notamment la reconnaissance faciale, rétinienne, vocale, des empreintes digitales et de l'iris, mais aussi l'authentification par l'écriture manuscrite et la dynamique de frappe.

Phase de détection de retrait de périphérique

La session de l'utilisateur entre dans cette phase une fois la phase de connexion terminée. Deux méthodes sont disponibles :

- La méthode Secure Workstation est fournie avec NetIQ SecureLogin. La session de l'utilisateur peut être arrêtée lors du retrait d'un périphérique d'authentification (par exemple, une carte à puce). Ce périphérique n'est nécessaire dans aucune des autres phases.

  Pour plus d'informations sur la méthode Secure Workstation, reportez-vous au *NetIQ SecureLogin 7.0 SP3 Administration Guide* (Guide d'administration de NetIQ SecureLogin 7.0 SP3).
- La méthode de connexion NetIQ Enhanced Smart Card repose également sur la détection du retrait d'une carte à puce. Pour plus d'informations sur cette méthode de connexion, reportez-vous au *NetIQ Enhanced Smart Card Method Installation Guide* (Guide d'installation de NetIQ Enhanced Smart Card Method).

Méthodes et séquences de connexion et de post-connexion

Une **méthode de connexion** est une implémentation spécifique d'un facteur d'authentification. NMAS permet de choisir entre plusieurs méthodes de connexion sur la base des trois facteurs de connexion (mot de passe, périphérique physique et authentification biométrique).

Une *méthode de post-connexion* est un processus de sécurité qui s'exécute après qu'un utilisateur s'est authentifié auprès de NetIQ eDirectory. Un exemple de méthode de post-connexion est la méthode NetIQ Secure Workstation (fournie avec NetIQ SecureLogin), laquelle oblige l'utilisateur à fournir des références pour accéder à l'ordinateur une fois que le poste de travail est verrouillé.

Le logiciel NMAS prend en charge un certain nombre de méthodes de connexion et de post-connexion développées par NetIQ et d'autres fournisseurs de solutions d'authentification. Selon la méthode de connexion utilisée, du matériel supplémentaire peut s'avérer nécessaire. Pour plus d'informations, reportez-vous à la documentation de la solution tierce.

Après avoir fait votre choix et installé une méthode, vous devez l'assigner à une séquence de connexion pour qu'elle puisse être utilisée. Une *séquence de connexion* est un ensemble ordonné d'une ou de plusieurs méthodes. Les utilisateurs se connectent au réseau en utilisant ces séquences de connexion prédéfinies. Si la séquence de connexion contient plusieurs méthodes, celles-ci sont présentées à l'utilisateur dans l'ordre spécifié. Les méthodes de connexion sont présentées en premier, suivies des méthodes de post-connexion.

NMAS prend en charge les séquences de connexion And (Et) et Or (Ou). Une séquence And requiert que toutes les méthodes de connexion contenues dans la séquence soient exécutées correctement. Une séquence Or nécessite uniquement qu'une des méthodes de connexion contenues dans la séquence soit exécutée correctement. Ainsi, permettre aux utilisateurs d'utiliser la même séquence de connexion pour se connecter à des postes de travail avec des périphériques d'authentification différents est un exemple de séquence d'utilisation Or.

Caching des objets Sécurité

Créé au niveau de la partition racine lors de l'installation du premier serveur dans l'arborescence, le conteneur Sécurité contient des informations telles que des données générales, des règles de sécurité et des clés.

Après l'introduction du mot de passe universel, chaque fois qu'un utilisateur se connectait à eDirectory via NMAS®, NMAS accédait aux informations du conteneur Sécurité pour authentifier la connexion. Si la partition renfermant le conteneur Sécurité n'était pas présente au niveau local, NMAS accédait au serveur qui contenait cette partition. Cela affectait les performances de l'authentification NMAS. C'était encore pire lorsqu'il fallait accéder au serveur qui contenait la partition disposant du conteneur Sécurité par le biais de liaisons WAN.

Pour y remédier, les données du conteneur de sécurité sont mises en cache sur le serveur local. Ainsi, NMAS ne doit pas accéder au conteneur Sécurité situé sur une autre machine chaque fois qu'un utilisateur se connecte ; il peut facilement le faire au niveau local, ce qui améliore les performances. L'ajout au serveur local de la partition disposant du conteneur Sécurité augmente les performances, mais n'est pas toujours possible si les serveurs sont trop nombreux.

Si les données du conteneur Sécurité changent sur le serveur qui contient la partition renfermant le conteneur Sécurité, le cache local est rafraîchi par un processus en arrière-plan appelé « liaison en amont ». Par défaut, une liaison en amont est exécutée toutes les treize heures pour extraire les données modifiées du serveur distant. Dans ce cas, les données doivent être synchronisées immédiatement et vous pouvez planifier un processus de liaison en amont sur le serveur local par l'intermédiaire d'iMonitor, ndstrace sous Linux ou ndscons sous Windows. Pour plus d'informations, consultez l'aide en ligne d'iMonitor ou la page du manuel ndstrace.

La fonction de caching des objets Sécurité est activée par défaut. Si vous ne souhaitez pas que le processus de liaison en amont mette des données en cache, retirez `CachedAttrsOnExtRef` de l'objet Serveur NCP.

Logiciel NMAS

Le logiciel NMAS est fourni avec NetIQ eDirectory. Son image inclut les éléments suivants :

- Logiciel serveur NMAS
- Logiciel de méthodes de connexion
- Prise en charge de plusieurs méthodes de connexion par séquence de connexion
- Prise en charge de l'authentification progressive
- Mot de passe universel

Le logiciel client NMAS est fourni avec le client NetIQ pour Windows et NetIQ SecureLogin.

- « Installation des logiciels serveur et client » page 678
- « Logiciel de méthodes de connexion et partenaires » page 678
- « Mot de passe universel » page 679
- « Gestion à l'aide » page 679

Installation des logiciels serveur et client

Par défaut, le logiciel serveur NMAS est installé avec eDirectory. Le logiciel client NMAS doit, quant à lui, être installé sur chaque poste de travail client qui accèdera au réseau en utilisant les méthodes de connexion NMAS. Une fois l'installation terminée, vous pouvez gérer NMAS à l'aide d'iManager.

Le logiciel client NMAS est désormais fourni avec le client NetIQ. Pour plus d'informations, reportez-vous à la documentation du client NetIQ pour Windows.

Pendant l'installation, NMAS étend le schéma eDirectory et crée de nouveaux objets dans le conteneur Security (Sécurité) au sein de l'arborescence eDirectory. Ces nouveaux objets sont les conteneurs Authorized Login Methods (Méthodes de connexion autorisées) et Authorized Post-Login Methods (Méthodes de post-connexion autorisées), ainsi que les objets Security Policy (Stratégie de sécurité) et Login Policy (Stratégie de connexion). Toutes les méthodes de connexion sont stockées et gérées dans le conteneur Authorized Login Methods (Méthodes de connexion autorisées). Toutes les méthodes de post-connexion sont stockées et gérées dans le conteneur Authorized Post-Login Methods (Méthodes de post-connexion autorisées).

Logiciel de méthodes de connexion et partenaires

- « Logiciel et partenaires » page 678
- « Installation d'une méthode de connexion » page 678

Logiciel et partenaires

Plusieurs méthodes de connexion actuellement prises en charge sont disponibles sur l'image du logiciel NMAS.

Le logiciel NMAS inclut la prise en charge d'un certain nombre de méthodes de connexion développées par des fournisseurs de solutions d'authentification tierces. Pour obtenir la liste des partenaires de NetIQ, visitez le site Web des partenaires de NetIQ.

Chaque partenaire qui développe des méthodes de connexion pour NMAS propose des solutions d'authentification réseau disposant de caractéristiques et de fonctionnalités uniques. Par conséquent, les propriétés de sécurité varient d'une méthode de connexion à l'autre.

NetIQ n'a pas évalué les méthodologies de sécurité utilisées par ces solutions tierces. Dès lors, même si ces solutions peuvent arborer les logos NetIQ Yes, Tested & Approved ou NetIQ Directory Enabled, notez que ces derniers concernent uniquement l'interopérabilité générale du produit.

Nous vous conseillons d'examiner scrupuleusement les fonctionnalités de chacune des solutions tierces afin de déterminer laquelle est la plus à même de répondre à vos besoins en matière de sécurité. Notez également que certaines méthodes de connexion requièrent du matériel et des logiciels supplémentaires qui ne sont pas fournis avec NMAS.

Installation d'une méthode de connexion

Les méthodes de connexion NMAS (logiciel serveur, plug-ins et snap-ins) peuvent être installés à l'aide des éléments suivants :

- utilitaire `nmasinst` (disponible sur toutes les plates-formes eDirectory), qui requiert l'installation d'eDirectory ;
- plug-in iManager.

Pour plus d'informations sur l'installation d'une méthode de connexion, reportez-vous à la « Procédures d'installation d'une méthode de connexion » page 680.

Mot de passe universel

Le mot de passe universel est un moyen de simplifier l'intégration et la gestion des différents systèmes de mot de passe et d'authentification dans un réseau cohérent. Il permet d'utiliser un seul mot de passe pour tous les accès à eDirectory, d'utiliser des caractères étendus dans les mots de passe, d'appliquer des stratégies de mot de passe avancées et de synchroniser les mots de passe entre eDirectory et d'autres systèmes.

Pour plus d'informations sur le mot de passe universel, reportez-vous au Chapitre 26, « Gestion des mots de passe », page 783.

Gestion à l'aide

Vous pouvez gérer NMAS à l'aide de NetIQ iManager, un utilitaire Web de gestion d'eDirectory. iManager inclut des pages de propriétés spécifiques qui permettent de gérer les méthodes de connexion, les séquences de connexion, le processus d'inscription et l'authentification progressive.

Par défaut, NMAS installe la méthode de connexion standard, à savoir par mot de passe NDS. Vous pouvez toutefois installer d'autres méthodes de connexion à l'aide d'iManager et d'un assistant exécutable à partir du conteneur Authorized Login Methods (Méthodes de connexion autorisées) au moyen de l'option Create New Object (Créer un objet). Vous pouvez également installer des méthodes de post-connexion en exécutant un assistant à partir du conteneur Authorized Post-Login Methods (Méthodes de post-connexion autorisées) à l'aide de l'option Create New Object (Créer un objet).

Pour plus d'informations sur l'installation des méthodes de connexion, reportez-vous à la « Procédures d'installation d'une méthode de connexion » page 680.

Gestion des méthodes et des séquences de connexion et de post-connexion

Cette section explique comment installer et configurer des méthodes et des séquences de connexion et de post-connexion pour NMAS.

NMAS permet de choisir entre plusieurs méthodes de connexion sur la base des trois facteurs de connexion (mot de passe, périphérique physique et authentification biométrique).

NMAS prend en charge un certain nombre de méthodes de connexion et de post-connexion développées par NetIQ et d'autres fournisseurs de solutions d'authentification. Certaines méthodes requièrent du matériel et des logiciels supplémentaires. Assurez-vous que vous disposez du matériel et de tous les logiciels nécessaires pour les méthodes que vous comptez utiliser.

Le logiciel NMAS inclut un certain nombre de méthodes de connexion. Toutefois, d'autres méthodes de connexion sont disponibles auprès de fournisseurs tiers.

Pour obtenir la liste des partenaires d'eDirectory, visitez le site Web des partenaires de NetIQ. Certains partenaires développent des méthodes de connexion tierces.

- « Procédures d'installation d'une méthode de connexion » page 680
- « Mise à jour de méthodes de connexion et de post-connexion » page 681
- « Gestion des séquences de connexion » page 682

- « Autorisation de séquences de connexion pour les utilisateurs » page 684
- « Configuration de séquences de connexion par défaut » page 684
- « Suppression d'une méthode de connexion » page 685
- « Suppression d'une séquence de connexion » page 686

Procédures d'installation d'une méthode de connexion

Il existe trois façons d'installer une méthode de connexion à utiliser dans NetIQ eDirectory :

- À l'aide de l'utilitaire nmasinst (Linux et Windows), qui permet d'installer des méthodes de connexion dans eDirectory.
- À l'aide de NetIQ iManager (Linux et Windows), qui permet d'installer des méthodes de connexion et de post-connexion dans eDirectory.

- « Installation d'une méthode de connexion à l'aide de l'utilitaire nmasinst » page 680
- « Installation d'une méthode de connexion ou de post-connexion à l'aide de NetIQ iManager » page 681

Installation d'une méthode de connexion à l'aide de l'utilitaire nmasinst

Dans la ligne de commande de console du serveur, entrez :

```
nmasinst -addmethod admin.context treename config.txt_path [-h hostname[:port]] [-
w password|file:<nom_fichier>|env:<variable_environnement>] [-checkversion] [-d]
```

- *admin.context* : nom et contexte de l'administrateur.
- *treename* : nom de l'arborescence eDirectory dans laquelle vous installez la méthode de connexion.
- *config.txt_ path* : chemin d'accès complet ou relatif au fichier `config.txt` de la méthode de connexion. Un fichier `config.txt` est fourni avec chaque méthode de connexion.
- `[-h hostname[:port]]` : (facultatif) nom d'hôte et port du serveur. Utilisez cette option si eDirectory ne s'exécute pas sur le port par défaut. Vous pouvez également spécifier l'adresse IP. eDirectory 9.2 prend en charge les adresses IPv4 et IPv6. Par exemple :
  - **IPv4 :** `-h 127.0.0.1:8443`
  - **IPv6 :** `-h [2001:db8::6]:8443`
- `[-w password|file:<nom_fichier>|env:<variable_environnement>]` : cette option permet de spécifier le mot de passe comme suit :
  - Sur la ligne de commande. Par exemple : `-w n`
  - Via un fichier. Par exemple : `-w file:/tmp/passwd`
  - Via une variable d'environnement. Par exemple : `-w env:PASSWD`
- `[-checkversion]` : cette option signale une erreur si la version de la méthode déjà installée est identique ou ultérieure à la version en cours d'installation.
- `[-d]` : cette option permet de supprimer les méthodes pour les plates-formes non prises en charge.

Si la méthode de connexion existe déjà, nmasinst la met à jour.

Installation d'une méthode de connexion ou de post-connexion à l'aide de NetIQ iManager

1. Lancez NetIQ iManager.
2. Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.
3. Dans le menu **Rôles et tâches**, cliquez sur **NMAS**, puis sur **NMAS Login Methods** (Méthodes de connexion NMAS).
4. Cliquez sur **Nouveau**.
5. Recherchez et sélectionnez le fichier (`.zip`) de la méthode de connexion à installer, puis cliquez sur **Suivant**.
6. Suivez les instructions de l'assistant pour terminer l'installation.

Mise à jour de méthodes de connexion et de post-connexion

Lorsqu'un fournisseur de méthodes de connexion fournit une mise à jour pour une méthode de connexion ou de post-connexion, vous pouvez la mettre à jour en procédant comme suit :

- « Mise à jour d'une méthode de connexion à l'aide de l'utilitaire nmasinst » page 681
- « Mise à jour d'une méthode de connexion à l'aide » page 681

Mise à jour d'une méthode de connexion à l'aide de l'utilitaire nmasinst

Employez la même procédure que celle que vous avez utilisée pour installer une méthode de connexion à l'aide de l'utilitaire nmasinst (reportez-vous à la section « Mise à jour d'une méthode de connexion à l'aide de l'utilitaire nmasinst » page 681). Incluez le chemin du nouveau fichier `config.txt` fichier et la méthode de connexion est mise à jour.

Mise à jour d'une méthode de connexion à l'aide

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.
3. Dans le menu **Rôles et tâches**, cliquez sur **NMAS**, puis sur **NMAS Login Methods** (Méthodes de connexion NMAS).
4. Cliquez sur la méthode de connexion que vous voulez mettre à jour.
5. Sur la page de propriétés de la méthode de connexion, cliquez sur **Update Method** (Mettre à jour la méthode).
6. Suivez les instructions de l'assistant pour terminer la mise à jour.

Gestion des séquences de connexion

Lorsque vous installez une méthode de connexion, le système vous demande si vous souhaitez créer une séquence de connexion qui utilisera uniquement la méthode de connexion en cours d'installation. Si vous répondez Oui, le système crée une séquence de connexion contenant uniquement cette méthode de connexion.

Vous pouvez aussi créer et gérer manuellement des séquences de connexion. Une fois les méthodes de connexion et de post-connexion installées, vous pouvez afficher, ajouter, modifier ou supprimer des séquences de connexion à l'aide d'iManager. Des séquences de connexion ne sont pas créées lorsque vous modifiez ou mettez à jour des méthodes.

Dans NMAS, vous pouvez configurer plusieurs méthodes de connexion et de post-connexion par séquence. Pour pouvoir sélectionner une méthode de post-connexion, vous devez sélectionner au moins une méthode de connexion.

Lorsque plusieurs méthodes sont sélectionnées pour une séquence, elles sont exécutées dans leur ordre d'apparition dans la liste. Les méthodes de connexion sont exécutées en premier, suivies des méthodes de post-connexion.

Une séquence de connexion peut être de type And (ET) ou Or (OU). Une séquence And aboutit si toutes les méthodes de connexion parviennent à valider l'identité de l'utilisateur. Avec une séquence Or, il suffit qu'une seule des méthodes de connexion valide l'identité de l'utilisateur pour que la connexion aboutiisse.

Les méthodes de post-connexion ne sont exécutées que si la connexion réussit, indépendamment de la relation And/Or.

Une fois qu'une séquence est créée, vous pouvez autoriser les utilisateurs à l'utiliser pour se connecter à eDirectory.

- « Création d'une séquence de connexion à l'aide de NetIQ iManager » page 682
- « Modification d'une séquence de connexion » page 683
- « Suppression d'une séquence de connexion » page 683

Création d'une séquence de connexion à l'aide de NetIQ iManager

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.
3. Dans le menu **Rôles et tâches**, cliquez sur **NMAS**, puis sur **NMAS Login Sequences** (Séquences de connexion NMAS).
4. Cliquez sur **New** (Nouveau) et spécifiez un nom pour la nouvelle séquence de connexion.

   Toutes les méthodes disponibles sont répertoriées dans **Available Login Methods** (Méthodes de connexion disponibles) et **Available Post-Login Methods** (Méthodes de post-connexion disponibles).
5. Sélectionnez le **type de séquence** dans la liste déroulante.

   Si vous sélectionnez *And* (Et), un utilisateur doit se connecter à l'aide de chaque méthode de connexion incluse dans la séquence de connexion. Si vous sélectionnez *Or* (Ou), l'utilisateur doit se connecter en n'utilisant qu'une seule des méthodes de connexion incluses dans la séquence de connexion.
6. Utilisez les flèches horizontales pour ajouter la/les méthode(s) souhaitée(s) à la séquence.

Si vous utilisez plusieurs méthodes, utilisez les flèches verticales pour modifier l'ordre d'exécution.

Le champ **Sequence Grade** (Niveau de séquence) indique le niveau de la séquence de connexion. Pour les séquences And, le niveau de séquence représente la synthèse des niveaux des différentes méthodes de connexion. Pour les séquences Or, il s'agit de l'intersection des niveaux des méthodes.

7 Cliquez sur **Finish** (Terminer) pour enregistrer la séquence de connexion.

Modification d'une séquence de connexion

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.

3 Dans le menu **Rôles et tâches**, cliquez sur **NMAS**, puis sur **NMAS Login Sequences** (Séquences de connexion NMAS).

4 Cliquez sur le nom d'une séquence de connexion.

Le niveau et le type de séquence s'affichent, et les méthodes de connexion et de post-connexion sont répertoriées. Toutes les méthodes disponibles sont répertoriées dans les listes **Available Login Methods** (Méthodes de connexion disponibles) et **Available Post-Login Methods** (Méthodes de post-connexion disponibles).

5 Sélectionner une opération :

- Pour modifier le type de séquence, utilisez la liste déroulante située en regard du type de séquence.
- Pour ajouter ou supprimer des méthodes de connexion ou de post-connexion d'une séquence, utilisez les flèches gauche et droite.

  REMARQUE : pour pouvoir sélectionner une méthode de post-connexion, vous devez sélectionner au moins une méthode de connexion.

- Pour modifier l'ordre des méthodes de connexion incluses dans une séquence, utilisez les flèches haut et bas.
- Pour quitter sans enregistrer les modifications, cliquez sur **Cancel** (Annuler).

IMPORTANT : les séquences de connexion qui ne sont associées à aucune méthode ne sont pas enregistrées.

6 Cliquez sur **Appliquer** ou sur **OK**.

Suppression d'une séquence de connexion

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.

3 Dans le menu **Rôles et tâches**, cliquez sur **NMAS**, puis sur **NMAS Login Sequences** (Séquences de connexion NMAS).

4 Sélectionnez la séquence de connexion à supprimer, puis cliquez sur **Delete** (Supprimer).

5 Cliquez sur **Appliquer** ou sur **OK**.

Autorisation de séquences de connexion pour les utilisateurs

- « Assignation de séquences de connexion » page 684
- « Autorisation d'une séquence de connexion » page 684

Assignation de séquences de connexion

Les séquences de connexion par défaut et autorisées peuvent être assignées à un utilisateur, à un conteneur, à une racine de partition ou à l'objet Stratégie de connexion. NMAS recherche les séquences de connexion par défaut ou autorisées pour un utilisateur en tentant de lire les attributs de l'objet Utilisateur, puis du conteneur de l'objet Utilisateur, de la racine de la partition de l'objet Utilisateur et enfin de l'objet Stratégie de connexion.

Les attributs identifiés avec l'objet Utilisateur remplacent tous les attributs identifiés avec l'objet Conteneur, Racine de partition ou Stratégie de connexion. Si une séquence de connexion a été assignée à une racine de partition, cette séquence s'applique à tous les utilisateurs figurant sous cette racine de partition uniquement si une autre séquence de connexion n'a pas déjà été assignée individuellement à des utilisateurs spécifiques.

Par ailleurs, une séquence de connexion assignée à un conteneur s'applique uniquement aux utilisateurs de ce conteneur auxquels aucune séquence de connexion n'a été assignée, et non aux utilisateurs figurant dans les sous-conteneurs de ce conteneur.

Autorisation d'une séquence de connexion

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.
3. Dans le menu **Rôles et tâches** menu, cliquez sur **NMAS** > **NMAS Users** (Utilisateurs NMAS), sélectionnez l'utilisateur que vous souhaitez autoriser à utiliser les séquences de connexion, puis cliquez sur l'onglet **NMAS**.
4. Autorisez ou désautorisez une séquence de connexion pour un utilisateur en sélectionnant la séquence en question, puis en cliquant sur **Authorize** (Autoriser) ou **De-authorize** (Désautoriser).
5. Cliquez sur **Appliquer** ou sur **OK**.

Configuration de séquences de connexion par défaut

Pour définir une séquence de connexion par défaut afin que les utilisateurs ne doivent pas spécifier de séquence de connexion lorsqu'ils se connectent, procédez comme suit :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.
3. Dans le menu **Rôles et tâches** menu, cliquez sur **NMAS** > **NMAS Users** (Utilisateurs NMAS), sélectionnez l'utilisateur pour lequel vous souhaitez définir la séquence de connexion par défaut, puis cliquez sur l'onglet **NMAS**.
4. Sélectionnez une séquence de connexion autorisée, puis cliquez sur **Make Default** (Définir comme séquence de connexion par défaut).

La séquence sélectionnée devient la séquence de connexion par défaut. Si un utilisateur tente de se connecter sans utiliser une séquence de connexion, cette séquence de connexion par défaut sera utilisée.

5 Cliquez sur **Appliquer** ou sur **OK**.

REMARQUE : si un poste de travail ne parvient pas à exécuter la séquence de connexion par défaut de l'utilisateur, la méthode de connexion par mot de passe NDS est utilisée.

Pour plus d'informations sur l'assignation de séquences de connexion, reportez-vous à la section « Assignation de séquences de connexion » page 684.

Suppression d'une méthode de connexion

Les plug-ins iManager pour NMAS ne permettent pas de supprimer une méthode de connexion si cette dernière fait partie d'une séquence de connexion. Par défaut, l'installation d'une méthode de connexion crée une séquence de connexion qui contient uniquement cette méthode. Par conséquent, la plupart des méthodes sont incluses dans au moins une séquence.

REMARQUE : nmasinst ne contient pas d'option permettant de supprimer les méthodes NMAS. Cette opération doit être effectuée via iManager.

Pour supprimer une méthode de connexion, vous devez exécuter les deux procédures ci-dessous :

- « Suppression d'une méthode de connexion d'une séquence de connexion » page 685
- « Suppression de la méthode de connexion » page 686

Suppression d'une méthode de connexion d'une séquence de connexion

Pour supprimer une méthode de connexion d'une séquence de connexion à l'aide d'iManager, procédez comme suit :

1 Dans iManager, cliquez sur **NMAS**, puis sur **NMAS Login Sequences** (Séquences de connexion NMAS).

2 Pour chaque séquence figurant dans la liste **NMAS Login Sequences** (Séquences de connexion NMAS) :

   2a Cliquez sur le nom de la séquence.

   2b Vérifiez que la méthode de connexion que vous êtes sur le point de supprimer ne figure pas dans la liste **Login Methods** (Méthodes de connexion) ou **Post-Login Methods** (Méthodes de post-connexion).

   2c Si la méthode de connexion fait partie des méthodes sélectionnées, vous pouvez la retirer de la liste en la sélectionnant et en cliquant sur la flèche gauche.

Une fois la méthode de connexion supprimée de toutes les séquences de connexion, vous pouvez la supprimer. Reportez-vous à la section « Suppression de la méthode de connexion » page 686.

Suppression de la méthode de connexion

Pour supprimer la méthode de connexion à l'aide d'iManager, procédez comme suit :

1. Dans iManager, cliquez sur **NMAS**, puis sur **NMAS Login Methods** (Méthodes de connexion NMAS).
2. Sélectionnez la ou les méthodes de connexion à supprimer.
3. Cliquez sur **Supprimer**, puis sur **Oui**.

Suppression d'une séquence de connexion

1. Lancez NetIQ iManager.
2. Connectez-vous à l'arborescence eDirectory avec les références d'un administrateur ou d'un utilisateur disposant de droits d'administrateur.
3. Dans le menu **Rôles et tâches**, cliquez sur **NMAS**, puis sur **NMAS Login Sequences** (Séquences de connexion NMAS).
4. Sélectionnez la séquence de connexion à supprimer.
5. Cliquez sur **Supprimer**, puis sur **Oui**.

Connexion au réseau à l'aide de NMAS

Une fois NMAS installé, vous êtes prêt à authentifier les utilisateurs qui tentent de se connecter au réseau. Cette section décrit quelques-unes des autres caractéristiques de l'expérience de connexion que vous devriez communiquer aux utilisateurs de votre réseau.

- « Champ de mot de passe » page 686
- « Connexion avancée » page 687
- « Déverrouillage du poste de travail » page 687
- « Capture d'une trace du client NMAS » page 688
- « Affichage de l'état d'autorisation NMAS » page 688

Champ de mot de passe

Selon la manière dont le logiciel client NMAS a été installé, un champ de mot de passe peut éventuellement figurer dans la boîte de dialogue de connexion du client Novell. Si les utilisateurs utilisent un facteur de connexion biométrique ou par périphérique physique, il se peut qu'ils n'aient besoin d'aucun mot de passe pour se connecter au réseau.

Pour plus d'informations sur la façon de masquer le champ de mot de passe, reportez-vous à la documentation du client Novell pour Windows.

Connexion avancée

Les utilisateurs qui utilisent des méthodes de connexion NMAS pour se connecter au réseau peuvent personnaliser la connexion en sélectionnant une autorisation et une séquence de connexion de leur choix. Sinon, les dernières séquence de connexion et autorisation (le cas échéant) sont utilisées. Si aucune autorisation ou séquence de connexion n'a été spécifiée précédemment, les valeurs par défaut sont utilisées.

1. Lorsque la boîte de dialogue du client Novell s'affiche, cliquez sur **Avancé**.
2. Cliquez sur l'onglet **NMAS**.
3. Sélectionnez la séquence de connexion de votre choix dans la liste déroulante **Connexion** liste déroulante ou parcourez l'arborescence NetIQ eDirectory pour obtenir une liste complète et actualisée.

   Vous pouvez effectuer une recherche uniquement si vous avez spécifié une arborescence eDirectory sous l'onglet **eDirectory**.
4. Spécifiez l'autorisation de session utilisateur de votre choix, ou parcourez l'arborescence eDirectory pour obtenir une liste complète et actualisée.

   Par défaut, le champ **Clearance** (Autorisation) est désactivé. Pour activer le champ **Clearance** (Autorisation) :

   4a Cliquez avec le bouton droit de la souris sur l'icône N rouge dans la barre des tâches.

   4b Sélectionnez **Novell Client Properties** (Propriétés du client Novell) > **Location Profiles** (Profils d'emplacement).

   4c Sélectionnez le profil souhaité, cliquez sur **Properties** (Propriétés), puis sur **Properties** (Propriétés).

   4d Sous l'onglet **NMAS**, sélectionnez **Display Clearance Field** (Afficher le champ Autorisation).

   4e Cliquez trois fois sur **OK**.

   IMPORTANT : les utilisateurs peuvent avoir plusieurs autorisations de session pour chaque séquence de connexion. Assurez-vous que le champ **Clearance** (Autorisation) contient l'autorisation de session utilisateur souhaitée.

   ---
5. Cliquez sur **OK**.

Déverrouillage du poste de travail

Le processus de déverrouillage des postes de travail Windows auxquels NMAS est ajouté est différent. En temps normal, les utilisateurs peuvent activer la protection par mot de passe pour leurs postes de travail à l'aide d'un écran de veille configurable à partir de la section Affichage du panneau de configuration Windows. Pour déverrouiller un poste de travail avec NMAS, les utilisateurs doivent passer par le même processus d'authentification que celui qu'ils ont utilisé pour se connecter initialement.

Par exemple, si vous avez employé NMAS pour vous authentifier auprès du réseau et que vous avez utilisé une méthode de connexion biométrique, vous devez réutiliser la même méthode de connexion biométrique pour déverrouiller et utiliser le poste de travail.

Si vous utilisez un poste de travail Windows, vous devez le déverrouiller à l'aide de la méthode de connexion que vous avez utilisée pour vous connecter à l'arborescence. Si vous disposez de connexions à plusieurs arborescences eDirectory, vous pouvez utiliser la séquence de connexion de n'importe quelle arborescence. La valeur par défaut est la première arborescence eDirectory.

Capture d'une trace du client NMAS

La capture d'une trace du client NMAS peut aider à résoudre les problèmes d'authentification NMAS. Pour plus d'informations, reportez-vous au document TID 3331372.

Affichage de l'état d'autorisation NMAS

1. Cliquez avec le bouton droit de la souris sur l'icône N rouge dans la barre des tâches.
2. Cliquez sur **Novell Connections** (Connexions Novell).
3. Faites défiler la liste pour visualiser l'autorisation NMAS associée à chaque connexion.

Historique des mots de passe NetIQ

Auparavant, les administrateurs devaient gérer plusieurs mots de passe (mot de passe simple, mot de passe NDS, mot de passe étendu) en raison des limitations inhérentes aux mots de passe. Ils devaient également s'assurer de leur synchronisation.

- Mot de passe NDS : l'ancien mot de passe NDS est stocké dans un format haché irréversible. Ce mot de passe ne peut être utilisé que par le système NDS et ne peut pas être converti dans un autre format exploitable par un autre système.
- Mot de passe simple : à l'origine, le mot de passe simple a été implémenté pour permettre aux administrateurs d'importer des utilisateurs et des mots de passe (en texte clair et au format haché) à partir de répertoires LDAP étrangers tels qu'Active Directory* et iPlanet*.

  L'inconvénient du mot de passe simple est qu'il ne permet pas d'appliquer de stratégies de mot de passe (longueur minimale, expiration, etc.) .
- Mot de passe étendu : le mot de passe étendu (qui n'est plus pris en charge), l'ancêtre du mot de passe universel, permet d'appliquer quelques stratégies de mot de passe, mais sa conception n'est pas cohérente avec celle des autres mots de passe. Il fournit une synchronisation unidirectionnelle et remplace le mot de passe NDS ou simple.

Le mot de passe universel a été créé pour résoudre ces problèmes de mot de passe. Il offre les avantages suivants :

- Il permet d'utiliser un seul mot de passe pour tous les accès à eDirectory.
- Il permet d'utiliser des caractères étendus dans les mots de passe.
- Il permet d'appliquer des stratégies de mot de passe avancées.
- Il permet de synchroniser les mots de passe entre eDirectory et d'autres systèmes.

Le mot de passe universel est géré par Secure Password Manager, un composant du module NMAS qui simplifie la gestion des modèles d'authentification par mot de passe pour une vaste gamme de solutions développées par NetIQ, Novell et des partenaires de NetIQ. Les outils de gestion n'exposent qu'un mot de passe et ne montrent pas tout le traitement en arrière-plan qui s'exécute à des fins de compatibilité avec les versions précédentes.

Secure Password Manager et les autres composants qui gèrent ou utilisent le mot de passe universel sont installés avec eDirectory. Toutefois, le mot de passe universel n'est pas activé par défaut. Étant donné que toutes les API d'authentification et de définition de mots de passe évoluent pour prendre en charge le mot de passe universel, tous les outils de gestion existants fonctionnent automatiquement avec le mot de passe universel lorsqu'ils sont exécutés sur des clients dotés de ces nouvelles bibliothèques.

REMARQUE : le plug-in de gestion des mots de passe peut être téléchargé à partir du site Web de téléchargement.

Le client Novell prend en charge le mot de passe universel. Il continue également de prendre en charge le mot de passe NDS pour les systèmes plus anciens du réseau. Le client Novell est capable de passer automatiquement du mot de passe NDS au mot de passe universel au moment de la première connexion.

La date d'expiration du mot de passe n'est pas mise à jour lorsque le mot de passe NDS est migré vers le mot de passe universel, à moins que la règle de stratégie de mot de passe « Vérifier si les mots de passe existants respectent la stratégie de mot de passe (la vérification se fait lors de la connexion) » ne soit définie sur « true » (vrai).

Pour plus d'informations sur le déploiement et la gestion du mot de passe universel, reportez-vous au Chapitre 26, « Gestion des mots de passe », page 783.

Connexion basée sur HOTP NMAS

Les sections suivantes contiennent des informations à propos de l'algorithme HOTP de NMAS :

- « Présentation » page 689
- « Installation » page 690
- « Resynchronisation du compteur » page 692
- « Configuration » page 693
- « Problèmes connus » page 694
- « L'utilitaire nmashotpconf ne peut pas modifier la fenêtre de resynchronisation des utilisateurs » page 694

Présentation

HOTP est un algorithme de mot de passe à usage unique (OTP) basé sur HMAC. Un OTP est un mot de passe valide pour une seule session de connexion ou transaction. Les mots de passe de ce type sont plus efficaces que les mots de passe (statiques) traditionnels, car ils sont associés à un risque inférieur de menaces de sécurité. Un intrus potentiel qui enregistre un OTP qui a été utilisé pour se connecter à un service ou réaliser une transaction ne peut pas le manipuler, car il a déjà été utilisé une fois et n'est donc plus valide. Toute authentification OTP requiert un serveur et un client OTP (matériel/logiciel). Dans NMAS, l'implémentation de l'authentification par OTP est basée sur la convention RFC 4226. En règle générale, le mot de passe NDS qui était présenté séparément au serveur est désormais joint à l'OTP afin d'améliorer l'authentification par mot de passe en conservant tous les composants client et leur interface utilisateur. L'authentification auprès du serveur eDirectory s'effectue via la fonction HOTP à l'aide de la connexion LDAP.

Connexion LDAP

Conditions préalables

- Assurez-vous que la variable d'environnement `NDSD_TRY_NMASLOGIN_FIRST` est définie sur true.

  Pour plus d'informations, reportez-vous à la section « Procédure pour rendre votre mot de passe sensible à la casse » du *Guide des nouveautés de NetIQ eDirectory*.

REMARQUE : cette variable est définie par défaut avec eDirectory 9.0 ou version ultérieure.

Méthode de connexion

Un utilisateur activé pour HOTP peut exécuter une liaison LDAP en concaténant le mot de passe NDS avec la valeur HOTP.

Par exemple :

```
ldapsearch -D cn=user1,o=novell -w secret40338314 -h 164.99.91.165 -p 389 -b
"o=novell" -s sub -LLL dn
```

Connexion NCP

Un utilisateur prêt/activé pour HOTP peut effectuer une connexion NCP en concaténant le mot de passe NDS avec la valeur HOTP à l'aide d'un des utilitaires suivants :

- ndslogin

  Par exemple :

  ```
  ndslogin user1.org -h org.com -p secret40338314
  ```

- iManager
- iMonitor

REMARQUE : les plug-ins iManager qui procèdent à l'authentification LDAP échouent s'ils sont utilisés par des utilisateurs activés pour HOTP.

Installation

- « Installation des serveurs » page 690
- « Obtention et emploi de l'utilitaire nmashotpconf » page 691

Installation des serveurs

Le module serveur HOTP fait partie du composant serveur NMAS. Le module serveur valide l'OTP présenté par le client.

Les attributs suivants sont disponibles sur le serveur HOTP NMAS :

- `sasOTPCounter` (par attribut utilisateur)
- `sasOTPEnabled` (par objet Utilisateur/Conteneur parent immédiat/Racine de partition/Stratégie de connexion)
- `sasOTPDigits` (par objet Utilisateur/Conteneur parent immédiat/Racine de partition/Stratégie de connexion)
- `asOTPLookAheadWindow` (défini pour l'ensemble de l'arborescence au niveau de l'objet Stratégie de connexion)
- `sasOTPResync` (9 par attribut utilisateur)

Obtention et emploi de l'utilitaire nmashotpconf

L'utilitaire `nmashotpconf` permet de configurer les attributs OTP sur le serveur eDirectory.

REMARQUE : l'utilitaire HOTP est disponible uniquement pour les plates-formes Linux 64 bits.

Pour exécuter l'utilitaire `nmashotpconf`, procédez comme suit :

1. Procurez-vous l'utilitaire `nmashotpconf` et indiquez le répertoire dans lequel vous avez dézippé l'utilitaire `NMAS HOTP`.

   REMARQUE : l'utilitaire `nnmashotpconf` est fourni avec NMAS. Pour le télécharger, rendez-vous sur le site https://download.novell.com/Download?buildid=BfnNcVX8U_I.

   Le fichier dézippé contient les répertoires `linux` et `linux_x64` pour les machines Linux 32 et 64 bits.

   Les répertoires `linux` et `linux_x64` contiennent l'exécutable `nmashotpconf` et les fichiers `libnmasext.so`.

2. Accédez au répertoire `linux/final` sur une machine Linux 32 bits, ou au répertoire `linux_x64/final` sur une machine Linux 64 bits.

3. Téléchargez le certificat de racine approuvée et enregistrez-le en local.

   Pour plus d'informations, reportez-vous à la section « Exportation d'un certificat de racine approuvée ou d'un certificat de clé publique » page 737.

   La syntaxe se présente comme suit :

```
nmashotpconf -h <host_name> [-p <ssl_port>] -D <login_dn> [-w <password>]
 -e <trusted_cert> -t <cert_type> [-r <resync_window>] [-y
 <user_resync_window>] [-u <hotp_dn> [-o <hotp_options>] [-d digits] [-c
 <counter>] [-s <secret> -f <secret_format>]]
```

Option	Description
host_name	Nom ou adresse IP du serveur LDAP.
ssl_port	Port SSL sur le serveur LDAP. La valeur par défaut est 636.
login_dn	DN de l'utilisateur.
password	Mot de passe associé au DN utilisateur.
trusted_cert	Fichier de certificat de racine approuvée.
cert_type	Type de codage du certificat de racine approuvée. Par exemple, DER indique que le fichier est codé en der, et B64 signifie qu'il est codé en b64.
encoded file digits	Nombre de chiffres constituant la valeur HOTP. **REMARQUE :** ce paramètre s'applique à tous les utilisateurs de l'arborescence.
resync_window	Fenêtre d'anticipation de resynchronisation des compteurs.
user_resync_window	Fenêtre d'anticipation de resynchronisation des utilisateurs des compteurs.

Option	Description
hotp_dn	DN cible pour lequel vous configurez les attributs HOTP. Pour configurer l'HOTP au niveau de l'arborescence, activez/désactivez-le au niveau de l'arborescence ou configurez les **chiffres** au niveau de l'arborescence, puis spécifiez le DN au format `cn=Login Policy,cn=Security`.
hotp_options	Active ou désactive l'HOTP pour l'option **hotp_dn**. Spécifiez ENABLE pour activer l'HOTP ou DISABLE pour le désactiver.
counter	Valeur du compteur HOTP. Cette valeur doit être comprise entre 0 et 2147483647. Elle est définie via l'option **hotp_dn**.
hotp_dn secret	Secret HOTP OATH. Par exemple, la valeur du **secret** en octets bruts au format hexadécimal est 313233343536373839303132333435363738393 0. La chaîne ASCII/ASCII étendu correspondante est 12345678901234567890.
secret_format	Format du secret HOTP OATH. ◆ **STRING :** ce format est utilisé pour une chaîne ASCII/ASCII étendu. Par exemple, 12345678901234567890. ◆ **RAW :** ce format est utilisé pour les valeurs d'octets bruts au format hexadécimal. Par exemple, 313233343536373839303132333435363738393 0, la valeur hexadécimale du premier caractère étant 31, la valeur du deuxième caractère 32, et ainsi de suite.

Resynchronisation du compteur

La valeur de compteur du serveur est incrémentée uniquement en cas de réussite de l'authentification HOTP. Le compteur du client est incrémenté chaque fois que l'utilisateur demande un nouvel HOTP. Les valeurs de compteur sur le serveur et celles sur le client risquent de ne pas être synchronisées.

Pour contourner ce problème, vous devez adopter une approche anticipative à l'échelle de l'arborescence ou configurer une fenêtre de resynchronisation. Si le serveur détecte que l'HOTP reçu ne correspond pas à la valeur de compteur du serveur, le serveur peut recalculer les quelques valeurs HOTP suivantes qui se trouvent dans la fenêtre de resynchronisation et les vérifier par rapport à l'HOTP reçu. En cas de correspondance, l'authentification réussit et le compteur du serveur est défini sur la valeur de compteur correspondant à l'HOTP équivalent.

Pour que l'authentification réussisse, le compteur du serveur est défini sur la valeur de compteur suivante à laquelle l'authentification est correcte.

La valeur du paramètre de fenêtre de resynchronisation à l'échelle de l'arborescence doit être la plus faible possible pour réduire le champ des possibilités des attaquants qui tenteraient de recréer les valeurs HOTP. Si la discordance entre les compteurs du client et du serveur excède la valeur du paramètre de fenêtre de resynchronisation à l'échelle de l'arborescence, il est possible de procéder à une resynchronisation en définissant temporairement une fenêtre de resynchronisation propre à l'utilisateur sur une valeur élevée, puis en essayant d'exécuter une authentification par HOTP.

L'utilitaire nmashotpconf doit être utilisé pour configurer l'authentification par HOTP. Pour en savoir plus, reportez-vous à la section Configuration.

Configuration

Pour déployer un utilisateur eDirectory pour une authentification par HOTP, configurez votre système comme décrit ci-dessous, conformément à la convention RFC 4226.

- Activez HOTP sur l'objet Utilisateur/Conteneur/Racine de partition/Stratégie de connexion dans cet ordre de priorité.
- Définissez la clé secrète partagée HOTP et le compteur de l'utilisateur. Ensemble, ces deux paramètres déterminent la valeur HOTP.
- Configurez le nombre de chiffres des valeurs HOTP sur l'objet Utilisateur/Conteneur/Racine de partition/Stratégie de connexion. La plage de chiffres valide est comprise entre 6 et 9.
- Définissez les fenêtres de resynchronisation comme suit :
  - Définissez la fenêtre de resynchronisation à l'échelle de l'arborescence au niveau de l'objet Stratégie de connexion.
  - Définissez la fenêtre de resynchronisation propre à l'utilisateur au niveau de l'utilisateur. Cette opération doit être effectuée uniquement lorsque le client et le serveur sont désynchronisés.

Exemples :

- Pour configurer un secret et un compteur sur l'objet Utilisateur, exécutez la commande suivante :

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e   /
  var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -c 0
  -s   31323334353637383930313233343536373839 30 -f  RAW
  ```

- Pour activer l'OTP pour un objet Utilisateur, exécutez la commande suivante :

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e   /
  var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -o
  ENABLE
  ```

- Pour désactiver l'OTP, exécutez la commande suivante :

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e   /
  var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -o
  DISABLE
  ```

  De même, vous pouvez activer ou désactiver l'OTP pour un objet Conteneur/Racine de partition/Stratégie de connexion.

- Pour configurer un chiffre d'OTP pour un objet Utilisateur, exécutez la commande suivante :

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -e /var/
  opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell  -d 6
  ```

  De même, vous pouvez configurer un chiffre d'OTP pour un objet Conteneur parent/Racine de partition/Stratégie de connexion.

- Pour configurer la fenêtre de resynchronisation des utilisateurs, exécutez la commande suivante :

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -y 5 -e
  /var/opt/novell/eDirectory/data/SSCert.der  -t  DER  -u cn=user1,o=novell
  ```

- Pour configurer la fenêtre d'anticipation de resynchronisation des compteurs, exécutez la commande suivante :

  ```
  ./nmashotpconf -h 192.168.1.1 -p 636 -D cn=admin,o=novell -w novell   -r 6
  ```

REMARQUE : pour tester la configuration, vous pouvez utiliser des mots de passe HOTP générés par tout matériel ou logiciel conforme aux normes HOTP.

Problèmes connus

- « Échec de l'ajout de ndsconfig pour un administrateur activé pour HOTP » page 694
- « Échec de la connexion à une réplique en lecture seule par le biais d'un utilisateur activé pour HOTP » page 694

Échec de l'ajout de ndsconfig pour un administrateur activé pour HOTP

Pour les utilisateurs activés pour HOTP, le chiffre d'OTP est utilisé à des fins d'authentification. L'utilitaire ndsconfig utilise le même chiffre d'OTP pour les authentifications suivantes, entraînant l'échec de l'ajout de ndsconfig. De même, la mise à niveau de ndsconfig échoue également.

Pour contourner ce problème, n'activez pas HOTP pour l'utilisateur avec lequel vous ajoutez/mettez à niveau ndsconfig.

Échec de la connexion à une réplique en lecture seule par le biais d'un utilisateur activé pour HOTP

Si vous procédez à une connexion LDAP par le biais d'un utilisateur activé pour HOTP en envoyant une requête à la réplique en lecture seule, le chaînage LDAP ne s'effectue pas. La réplique en lecture seule ne transfère pas la requête au serveur sur lequel réside l'utilisateur en question. La réplique échoue et un message d'erreur de type Réplique non conforme s'affiche.

L'utilitaire nmashotpconf ne peut pas modifier la fenêtre de resynchronisation des utilisateurs

Si la valeur de la fenêtre de resynchronisation des utilisateurs est déjà définie (par exemple, sur 2) et qu'elle est modifiée à l'aide de l'utilitaire nmashotpconf, le message d'erreur suivant s'affiche :

```
ldap_modify_ext_s on HOTP DN failed: error code=19: Constraint violation
```

Cette erreur peut être due à l'utilisation d'une combinaison des options **-o** (option d'activation ou de désactivation de l'OTP), **-d** (chiffre d'OTP), **-c** (otpcouter) et **-y** (fenêtre_resynchronisation_utilisateurs) pour modifier la valeur de resynchronisation des utilisateurs.

Autres tâches d'administration

Cette section décrit d'autres tâches d'administration pour NMAS :

- « Utilisation de la commande de fréquence de rafraîchissement de stratégie » page 695
- « Utilisation de la commande LoginInfo » page 695
- « Désactivation des connexions NMAS pour LDAP » page 698
- « Appel des commandes NMAS » page 699
- « Définition du délai entre les tentatives de connexion infructueuses » page 699

- « Utilisation de DSTrace » page 699
- « Désactivation et désinstallation du client NMAS » page 700
- « Audit des événements NMAS » page 700

Utilisation de la commande de fréquence de rafraîchissement de stratégie

Vous pouvez configurer NMAS de manière à ce que la stratégie de connexion NMAS mise en cache soit rafraîchie à partir de la stratégie de connexion NMAS stockée dans le conteneur de sécurité à intervalles réguliers, et non à chaque tentative de connexion. Cette configuration est définie par serveur à l'aide de la commande de fréquence de rafraîchissement de stratégie NMAS.

REMARQUE : le serveur accède une fois au conteneur de sécurité pendant le démarrage pour mettre en cache la stratégie. En fonction des intervalles configurés, le serveur tente ensuite d'accéder au conteneur de sécurité pour rafraîchir la stratégie.

La commande de fréquence de rafraîchissement de stratégie présente la syntaxe suivante :

```
nmas RefreshRate minutes
```

minutes correspond au nombre de minutes écoulées entre chaque tentative de vérification de la nécessité de mettre à jour la stratégie de connexion NMAS mise en cache.

Pour plus d'informations sur la manière d'appeler la commande de fréquence de rafraîchissement de stratégie pour chaque plate-forme de serveur NMAS, reportez-vous à la « Appel des commandes NMAS » page 699.

Utilisation de la commande LoginInfo

Avec NMAS 3.2 ou version ultérieure, vous pouvez désactiver la mise à jour automatique de certains attributs de connexion de l'objet Utilisateur à l'aide de la commande `LoginInfo <numb>`. À un moment donné, il se peut que la mise à jour automatique de ces attributs pose problème et que vous souhaitiez effectuer cette opération manuellement. Les sections ci-dessous décrivent cette fonctionnalité de façon plus détaillée :

- « Connexion NMAS pour la liaison LDAP » page 695
- « Problèmes causés par la mise à jour automatique des attributs de connexion de l'objet Utilisateur » page 696
- « Utilisation de la commande LoginInfo pour définir à quel moment les attributs de connexion doivent être mis à jour » page 696
- « Utilisation des attributs ssasUpdateLoginInfo et sasUpdateLoginTimeInterval » page 696

Connexion NMAS pour la liaison LDAP

Dans eDirectory 9.2, la connexion NMAS est activée par défaut pour la liaison LDAP. Lorsque la connexion NMAS est activée, eDirectory met automatiquement à jour les attributs de connexion de l'objet Utilisateur une fois que l'utilisateur s'est authentifié. Vous trouverez ci-dessous une liste non exhaustive des attributs de connexion mis à jour :

- Heure de connexion

- Adresse réseau
- Heure de la dernière connexion

Pour désactiver la connexion NMAS pour la liaison LDAP, reportez-vous à la « Désactivation des connexions NMAS pour LDAP » page 698.

Problèmes causés par la mise à jour automatique des attributs de connexion de l'objet Utilisateur

La mise à jour automatique des attributs de connexion de l'objet Utilisateur peut causer les problèmes suivants :

- Utilisation intensive
- Blocage
- Timeouts du client sur les serveurs d'authentification occupés, en particulier dans les environnements LDAP

Si vous rencontrez ces problèmes, vous souhaiterez peut-être ajuster le moment auquel les attributs de connexion sont mis à jour. Pour savoir comment faire, reportez-vous à la section « Utilisation de la commande LoginInfo pour définir à quel moment les attributs de connexion doivent être mis à jour » page 696.

Utilisation de la commande LoginInfo pour définir à quel moment les attributs de connexion doivent être mis à jour

Pour définir à quel moment les attributs de connexion doivent être mis à jour, exécutez la commande `nmas LoginInfo <num>`.

Le paramètre `<num>` est défini sur l'une des valeurs suivantes :

- **0 ou désactivé :** ne mettre à jour aucun attribut de connexion.
- **1 :** mettre à jour uniquement les attributs requis pour la détection d'intrus.
- **2 :** mettre à jour tous les attributs de connexion, à l'exception des attributs de stratégie de mot de passe utilisateur inutilisés.
- **3 ou activé :** mettre à jour tous les attributs de connexion.

Pour plus d'informations sur la façon d'appeler la commande LoginInfo pour chaque plate-forme de serveur NMAS, reportez-vous à la « Appel des commandes NMAS » page 699.

Utilisation des attributs ssasUpdateLoginInfo et sasUpdateLoginTimeInterval

L'attribut `sasUpdateLoginInfo` contrôle les mises à jour des attributs `LoginInfo`.

L'attribut `sasUpdateLoginTimeInterval` contrôle, quant à lui, la mise à jour de l'attribut `Heure de connexion` d'un utilisateur à un intervalle donné.

L'attribut `sasUpdateLoginInfo` peut présenter les valeurs suivantes :

- **0 ou désactivé :** ne mettre à jour aucun attribut de connexion.
- **1 :** mettre à jour uniquement les attributs requis pour la détection d'intrus.

- **2 :** mettre à jour tous les attributs de connexion, à l'exception des attributs de stratégie de mot de passe utilisateur inutilisés.
- **3 ou activé :** mettre à jour tous les attributs de connexion.

La valeur de l'attribut `sasUpdateLoginTimeInterval` peut être comprise entre 0 et 1 440 minutes (autrement dit, un jour).

- Si la valeur est 0, les attributs `Login Time` (Heure de connexion) et `Last Login Time`(Heure de la dernière connexion) sont mis à jour lors de chaque connexion réussie.
- Si la valeur est comprise entre **1** et **1440** minutes, l'attribut `Heure de connexion` est mis à jour après l'intervalle spécifié. L'attribut Heure de la dernière connexion n'est, quant à lui, pas mis à jour.

REMARQUE : l'attribut `Login Time` (Heure de connexion) n'est pas mis à jour lors des connexions réussies suivantes pendant l'intervalle. En revanche, si une connexion échoue, puis réussit au cours de l'intervalle, l'attribut `Login Time` (Heure de connexion) est mis à jour. L'intervalle à partir de la connexion réussie est compté.

L'attribut `sasUpdateLoginTimeInterval` s'applique uniquement si la valeur de l'attribut `sasUpdateLoginInfo` est définie sur 2 ou 3.

Les attributs peuvent être spécifiés pour les objets ci-dessous, dans le même ordre de priorité (l'objet Utilisateur ayant la plus haute priorité).

- Utilisateur
- Conteneur de l'utilisateur
- Racine de la partition
- Stratégie de connexion

Si les attributs `sasUpdateLoginInfo` et `sasUpdateLoginTimeInterval` sont définis sur l'objet Stratégie de connexion, le paramètre s'applique après le cycle de rafraîchissement de stratégie suivant. Si les attributs ne sont pas définis pour l'objet Utilisateur, Conteneur, Racine de partition ou Stratégie de connexion, la valeur définie sur un serveur à l'aide de la ligne de commande est utilisée pour garantir la compatibilité avec les versions précédentes.

L'exemple ci-dessous montre comment définir les valeurs des attributs sur le serveur eDirectory :

```
#cat nmas.config (The nmas.config file must be in the same directory as the dib
directory.)
nmas LoginInfo 2
nmas UpdateLoginTimeInterval 30
```

Pour définir la valeur des attributs à la racine de la partition :

1. Pour ajouter les attributs à l'arborescence, accédez à **iManager** > **Schéma** > **Ajouter un attribut** > **Racine de l'arborescence.**
2. Utilisez la flèche pour faire passer l'attribut souhaité de la liste **Attributs facultatifs disponibles** dans la liste **Attributs facultatifs**.

Pour définir les valeurs de l'attribut à la racine de la partition, exécutez la commande `ldapmodify` et les commandes ci-dessous dans la ligne de commande ou en utilisant un fichier `ldif` :

```
dn:T=< tree name>
changetype:modify
add:sasUpdateLoginTimeInterval
sasUpdateLoginTimeInterval:35

dn:T=< tree name>
changetype:modify
add:sasUpdateLoginInfo
sasUpdateLoginInfo: 2
```

Vous pouvez modifier les valeurs de l'attribut `sasUpdateLoginInfo` ou `sasUpdateLoginTimeInterval` pour des objets Utilisateur, Conteneur et Stratégie de connexion à l'aide d'iManager ou d'un fichier `ldif`.

Exemple :

```
#cat changesasUpdateLoginInfo.ldif
dn: cn=user1,o=org
change type: modify
replace: sasUpdateLoginInfo
sasUpdateLoginInfo: 1

#cat changesasUpdateLoginTimeInterval.ldif
dn: cn=user1,o=org
changetype: modify
replace: sasUpdateLoginTimeInterval
sasUpdateLoginTimeInterval: 60
```

Ce paramètre désactive la mise à jour de l'attribut `Login Time` (Heure de connexion) de l'utilisateur 1 pendant 60 minutes à partir de la précédente mise à jour de l'attribut.

Pour spécifier les attributs `sasUpdateLoginInfo` et `sasUpdateLoginTimeInterval` à partir :

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
3. Spécifiez le nom et le contexte d'un objet Conteneur ou Stratégie de connexion, puis cliquez sur **OK**.
4. Sous l'onglet **Général**, sélectionnez **Autre**, puis sélectionnez **sasUpdateLoginTimeInterval** dans la liste **Attributs non définis**.
5. Utilisez le bouton fléché pour déplacer **sasUpdateLoginTimeInterval** de la liste **Attributs non définis** vers la liste **Attributs définis**, puis cliquez sur **Appliquer**.

Désactivation des connexions NMAS pour LDAP

Dans eDirectory 9.2, la connexion NMAS est activée par défaut. Pour désactiver la connexion NMAS, définissez le paramètre `NDSD_TRY_NMASLOGIN_FIRST` sur `false`.

Pour désactiver la connexion NMAS pour LDAP sous Windows, cliquez avec le bouton droit de la souris sur Ordinateur et sélectionnez Propriétés. Dans l'onglet Avancé, cliquez sur Variables d'environnement. Sous Variables système, ajoutez la variable et définissez la valeur sur False.

REMARQUE : vous devez ajouter toutes les variables d'environnement requises pour le service eDirectory dans le fichier `env` qui se trouve dans le répertoire `etc/opt/novell/eDirectory/conf` sur les plates-formes RHEL 7.x et SLES 12.x.

Appel des commandes NMAS

La manière d'appeler une commande NMAS varie en fonction de la plate-forme que vous exécutez. Les plates-formes suivantes sont prises en charge :

- « Windows » page 699
- « Linux » page 699

Windows

À son lancement, NMAS traite les commandes figurant dans le fichier `nmas.cfg`. Le fichier `nmas.cfg` doit se trouver dans le même répertoire que les fichiers `dib`, lesquels sont généralement enregistrés dans `c:/novell/nds/dibfiles`.

ou

Une fois NMAS démarré, procédez comme suit :

1. Dans la console Services NetIQ eDirectory, sélectionnez `nmas.dlm`.
2. Saisissez la commande dans le champ **Paramètres de démarrage**.
3. Cliquez sur **Configurer**.

Linux

À son lancement, NMAS traite les commandes figurant dans le fichier `nmas.config`. Le fichier `nmas.config` doit se trouver au même emplacement que le répertoire `dib`. Par exemple, si le chemin du répertoire `dib` est `/var/opt/novell/eDirectory/data/dib`, le chemin du fichier `nmas.config` doit être `/var/opt/novell/eDirectory/data/nmas.config`.

Définition du délai entre les tentatives de connexion infructueuses

1. Installez le plug-in NMAS dans iManager.

   Le plug-in NMAS peut être téléchargé à partir du site de téléchargement Novell.
2. Dans le menu **Rôles et tâches** d'iManager, cliquez sur **Administration de l'annuaire > Modifier un objet**.
3. Recherchez et sélectionnez l'objet Stratégie de connexion, puis cliquez sur **OK**.
4. Cliquez sur l'onglet **NMAS**, puis sur **Paramètres**.
5. Indiquez le nombre de secondes devant s'écouler avant que l'écran de connexion ne s'affiche entre chaque tentative de connexion infructueuse, puis cliquez sur **OK**.

Utilisation de DSTrace

Vous pouvez utiliser l'utilitaire DSTrace pour collecter des informations de trace à partir de NMAS.

Pour plus d'informations sur la capture d'une trace du client NMAS, reportez-vous au document TID 3331372.

Pour plus d'informations sur la capture d'une trace du serveur NMAS, reportez-vous au document TID 3815371.

Désactivation et désinstallation du client NMAS

Pour désactiver le client NMAS :

1. Sur le poste de travail, cliquez avec le bouton droit de la souris sur l'icône N rouge.
2. Cliquez sur **Novell Client Properties** (Propriétés du client Novell).
3. Cliquez sur l'onglet **Advanced Login** (Connexion avancée).
4. Dans la liste **Parameter Groups** (Groupes de paramètres), sélectionnez **NMAS Authentication** (Authentification NMAS).
5. Sous **Setting** (Paramètre), sélectionnez **Off** (Désactivé).
6. Cliquez sur **OK**.

Pour désinstaller le client NMAS, utilisez l'option Ajouter/Supprimer des programmes du Panneau de configuration Windows.

REMARQUE : même si vous désactivez ou supprimez NMAS, vous pourrez toujours modifier le mot de passe universel à partir du client Novell pour Windows.

Audit des événements NMAS

Vous pouvez auditer les événements NMAS à l'aide de deux produits :

- Serveur de consignation sécurisée NetIQ Audit

  Vous pouvez utiliser le serveur de consignation sécurisée NetIQ Audit pour installer le fichier `nmas_en.lsc`, lequel se trouve dans les répertoires suivants :

  Windows : `novell\nds`

  Linux : `/opt/novell/eDirectory/lib64/nds-schem`

  Pour plus d'informations sur l'installation et la gestion de NetIQ Audit, reportez-vous à la documentation en ligne de NetIQ Audit.
- NetIQ Sentinel

Vous devez également activer l'audit des événements NMAS à l'aide du plug-in NMAS 9.0 ou version ultérieure pour iManager. Procédez comme suit pour activer l'audit NMAS avec Platform Agent.

1. Installez le plug-in NMAS 9.0 ou version ultérieure dans iManager.

   Vous pouvez télécharger ce plug-in partir du site de téléchargement NetIQ.
2. Dans le menu **Rôles et tâches** d'iManager, cliquez sur **Administration de l'annuaire > Modifier un objet**.
3. Recherchez et sélectionnez l'objet Stratégie de connexion, puis cliquez sur **OK**.
4. Cliquez sur l'onglet **NMAS**, puis sur **Paramètres**.
5. Cochez la case en regard de l'option **Enable auditing** (Activer l'audit), puis cliquez sur **OK**.

Utilisation de certificats externes avec NetIQ Audit

Pour utiliser un certificat externe avec NMAS et NetIQ Audit, vous devez d'abord convertir le certificat en deux fichiers `.pem` portant les noms suivants :

- `nmascert.pem` : fichier contenant le certificat.
- `nmaskey.pem` : fichier contenant la clé privée.

Ces fichiers doivent être copiés dans les répertoires ci-dessous sur chaque plate-forme pour chaque serveur NMAS du système :

- Linux : `/etc`
- Windows : répertoire renvoyé par la fonction GetWindowsDirectory (généralement, `c:\windows`)

Si les fichiers `nmascert.pem` et `nmaskey.pem` existent, NMAS les transmet à l'agent de plate-forme NetIQ Audit lorsque le journal est ouvert. S'ils n'existent pas, NMAS transmet le certificat et la clé internes à l'agent de plate-forme NetIQ Audit.

Utilisation de XDAS pour l'audit des événements NMAS

Les événements NMAS peuvent être audités à l'aide de XDAS. Pour plus d'informations, reportez-vous au « Audit avec XDAS » page 629.

Considérations relatives à la sécurité

Cette section contient des informations spécifiques à propos de la sécurité offerte par NetIQ Modular Authentication Services. Elle comprend les sous-sections suivantes :

- « Méthodes de connexion développées par des partenaires » page 701
- « Stratégies de connexion » page 701
- « NMASInst » page 702
- « Mot de passe universel » page 702
- « Clé SDI » page 704

Méthodes de connexion développées par des partenaires

NetIQ n'a pas évalué les méthodologies de sécurité des méthodes de connexion développées par ses partenaires. Dès lors, même si ces solutions tierces peuvent arborer les logos NetIQ Yes, Tested & Approved ou NetIQ Directory Enabled, notez que derniers concernent uniquement l'interopérabilité générale du produit.

Stratégies de connexion

- Si des séquences de connexion autorisées/par défaut ou des autorisations approuvées/par défaut sont assignées à un conteneur qui n'est pas une racine de partition, la stratégie s'applique uniquement aux objets Utilisateur présents dans le conteneur et non à ceux qui figurent dans les sous-conteneurs.
- Si des séquences de connexion autorisées/par défaut ou des autorisations approuvées/par défaut sont assignées à un conteneur qui est une racine de partition, la stratégie s'applique à tous les utilisateurs de la partition pour lesquels ces valeurs ne sont pas assignées à l'objet Utilisateur ou à son conteneur parent.

- Si des séquences de connexion autorisées/par défaut ou des autorisations approuvées/par défaut sont assignées à une stratégie de connexion, cette dernière s'applique à tous les utilisateurs de l'arborescence pour lesquels ces valeurs ne sont pas assignées à l'objet Utilisateur, à son conteneur parent ou à sa racine de partition.
- Si des mots de passe ou autres secrets de connexion devinables, tels que des questions et réponses de vérification d'identité, sont assignés à des utilisateurs, il est recommandé d'activer la fonction de détection d'intrus afin de freiner les intrus ou de les empêcher de deviner ces secrets de connexion.
- Par défaut, un délai de 3 secondes est observé entre chaque tentative de connexion infructueuse, afin de freiner les éventuels intrus et de les empêcher de deviner les mots de passe. Bien que la longueur de ce délai soit configurable, il est conseillé d'utiliser la valeur par défaut de 3 secondes.
- Des stratégies de connexion telles que la détection des intrusions, les restrictions d'adresse réseau et les restrictions horaires sont appliquées à toutes les séquences de connexion. Par exemple, des stratégies de connexion sont appliquées lorsque la fonction de self-service de mot de passe oublié de plusieurs produits NetIQ appelle la méthode de connexion par réponse de vérification d'identité.
- Il est recommandé d'activer la fonction d'audit de NMAS™ afin de pouvoir assurer le suivi des tentatives de connexion et des modifications apportées à la configuration.
- L'utilisation de la commande de fréquence de rafraîchissement de stratégie pour vérifier si la stratégie de mot de passe mise en cache doit être rafraîchie à intervalles définis plutôt qu'à chaque connexion ralentit l'application des modifications de stratégie de connexion.
- La commande `LoginInfo` peut être utilisée pour désactiver la mise à jour des attributs de connexion lors de la connexion. Ces attributs englobent notamment les attributs de détection des intrusions. La désactivation de leur mise à jour permet d'améliorer les performances de connexion, mais peut affaiblir la sécurité du système.
- La stratégie de détection des intrusions peut être définie au niveau du conteneur direct ou de la racine de partition de l'objet Utilisateur. NMAS commence par vérifier si une stratégie de détection des intrusions est présente dans le conteneur parent. Si ce dernier ne contient aucune stratégie, NMAS vérifie dans la racine de partition.

NMASInst

Lorsque vous mettez à niveau une méthode de connexion, l'utilitaire nmasinst remplace l'ancienne version par une version plus récente, à moins que l'option `-checkversion` ne soit utilisée.

Même si nmasinst inclut une option permettant de spécifier le mot de passe dans la ligne de commande, il n'est pas recommandé de l'utiliser, car le mot de passe pourrait être endommagé. Avec eDirectory 9.0 ou version ultérieur, nmasinst vous permet de récupérer un mot de passe à partir d'un fichier ou d'une variable d'environnement.

Mot de passe universel

- Dans la mesure où le conteneur de sécurité contient des stratégies globales, faites attention où vous placez les répliques accessibles en écriture. Certains serveurs peuvent modifier les stratégies de sécurité globales spécifiées dans l'arborescence eDirectory. Pour que les utilisateurs puissent se connecter avec NMAS, les répliques des objets Utilisateur et du conteneur de sécurité doivent se trouver sur le serveur NMAS.
- Si une stratégie de mot de passe est assignée à un conteneur qui n'est pas une racine de partition, cette stratégie s'applique uniquement aux objets Utilisateur présents dans le conteneur et non à ceux qui figurent dans les sous-conteneurs.

- Si une stratégie de mot de passe est assignée à un conteneur qui est une racine de partition, cette stratégie s'applique à tous les utilisateurs de la partition pour lesquels ces valeurs ne sont pas assignées à l'objet Utilisateur ou à son conteneur parent.
- Si une stratégie de mot de passe est assignée à une stratégie de connexion, cette dernière s'applique à tous les utilisateurs de l'arborescence pour lesquels ces valeurs ne sont pas assignées à l'objet Utilisateur, à son conteneur parent ou à sa racine de partition.
- La date d'expiration du mot de passe n'est pas mise à jour lorsque le mot de passe NDS est migré vers le mot de passe universel, à moins que la règle de stratégie de mot de passe « Vérifier si les mots de passe existants respectent la stratégie de mot de passe (la vérification se fait lors de la connexion) » ne soit définie sur « true » (vrai).
- Il est possible de configurer des stratégies de mot de passe permettant à l'utilisateur ou à un administrateur de mot de passe de lire le mot de passe universel à l'aide d'extensions LDAP NMAS documentées. Sauf si votre installation spécifique le requiert, il est recommandé de ne pas activer ces options. Si les mots de passe utilisateur doivent être lisibles, il recommandé de configurer la stratégie de mot de passe de manière à ce que seuls certains utilisateurs puissent les lire.
- Il est conseillé de configurer une stratégie de synchronisation du mot de passe de distribution uniquement si vous utilisez la fonction de synchronisation de mots de passe d'Identity Manager pour synchroniser les mots de passe entre des systèmes connectés.

  Pour plus d'informations sur la synchronisation des mots de passe entre des systèmes connectés à l'aide de la fonction de synchronisation de mots de passe d'Identity Manager, reportez-vous au *NetIQ Identity Manager 4.5 Password Management Guide* (Guide de gestion des mots de passe de NetIQ Identity Manager 4.5).
- Vous devez configurer une stratégie de synchronisation du mot de passe simplement uniquement si :
  - vous disposez de serveurs qui comportent une réplique accessible en écriture des objets Utilisateur ;
  - les utilisateurs accèdent à ces serveurs à l'aide de protocoles natifs d'accès aux fichiers, tels que CIDS et AFP.
- Si des règles avancées sont activées pour une stratégie de mot de passe, les règles existantes appliquées à l'objet Utilisateur sont ignorées et mises à jour pour concorder avec les règles de stratégie de mot de passe lorsque les utilisateurs modifient leur mot de passe ou se connectent.
- Les règles d'exclusion de mots de passe (historique des mots de passe, mots de passe exclus et valeurs d'attribut interdites) ne sont pas appliquées lorsque NMAS est utilisé pour générer des mots de passe aléatoires.
- Lorsque vous sélectionnez des règles de mot de passe, vous devez trouver le juste équilibre pour que les mots de passe ne soient pas trop faciles à deviner et trop difficiles à retenir.
- Lorsqu'un administrateur spécifie que le mot de passe NDS doit être supprimé, le paramètre de hachage du mot de passe NDS est défini sur une valeur aléatoire que personne ne connaît, hormis eDirectory. Une valeur de mot de passe pourrait éventuellement être hachée sur la base de cette valeur aléatoire.
- Complexité des mots de passe XML
  - En présence de balises de règle en double, la règle la plus restrictive est utilisée (les autres sont ignorées) pour vérifier les mots de passe par rapport à la stratégie et générer des mots de passe aléatoires.

- Les attributs d'ensemble de règles `ViolationsAllowed` et `NumberOfCharactersToEvaluate` sont ignorés pour la génération de mots de passe aléatoires.
- Seule la première stratégie d'un ensemble de stratégies XML est utilisée pour la génération de mots de passe aléatoires.

Pour plus d'informations sur la sécurité du mot de passe universel, reportez-vous au Chapitre 26, « Gestion des mots de passe », page 783.

Clé SDI

Il est recommandé de faire de la clé SDI (Security Domain Infrastructure), également connu sous le nom de clé d'arborescence, une clé Triple DES (3DES). La clé SDI peut être vérifiée et mise à niveau à l'aide de l'utilitaire SDIDiag. Reportez-vous à l'étape Vérifiez que les serveurs de clés de domaine SDI exécutent NICI 3.0. du Chapitre 26, « Gestion des mots de passe », page 783.

À partir de la version 9.0 d'eDirectory, les clés d'arborescence AES 256 sont également prises en charge. Pour plus d'informations, reportez-vous à la section Création d'une clé d'arborescence AES 256 bits.

25 Présentation du serveur de certificats

NetIQ Certificate Server est automatiquement installé lors de l'installation d'eDirectory. Il propose des services de cryptographie à clé publique intégrés dans eDirectory, qui permettent de créer, d'émettre et de gérer des certificats utilisateur et de serveur. Ces services permettent de protéger les transmissions de données confidentielles sur des canaux de communication publics tels qu'Internet.

REMARQUE

- Si les concepts de cryptographie à clé publique vous sont méconnus, reportez-vous à la section « Cryptographie à clé publique - Notions » page 771.
- eDirectory 9.2 et versions ultérieures ne prennent pas en charge les algorithmes de signature MD2 et MD5 pour le chiffrement RSA.

- « Fonctionnalités de NetIQ Certificate Server » page 705
- « Composants de NetIQ Certificate Server » page 706
- « Configuration de NetIQ Certificate Server » page 713
- « Gestion de NetIQ Certificate Server » page 723
- « Cryptographie à clé publique - Notions » page 771
- « Droits sur les entrées nécessaires à la réalisation des tâches » page 778

Fonctionnalités de NetIQ Certificate Server

La cryptographie à clé publique pose de véritables défis auxquels doivent faire face les administrateurs réseau. NetIQ Certificate Server vous aide à relever ces défis grâce aux avantages suivants :

- Les services de cryptographie à clé publique sont disponibles sur le réseau.

  Vous pouvez créer une autorité de certification (CA) organisationnelle au sein de votre arborescence eDirectory, ce qui vous permet d'émettre un nombre illimité de certificats utilisateur et de serveur. Vous pouvez également utiliser les services d'une autorité de certification externe ou une combinaison des deux, selon vos besoins.
- Les coûts associés à l'obtention et à la gestion des certificats de clé publique sont contrôlés.

  Vous pouvez créer une autorité de certification organisationnelle et vous en servir pour émettre des certificats de clé publique.
- Les certificats de clé publique sont librement accessibles, tout en étant protégés contre toute altération.

  Les certificats sont stockés dans eDirectory et peuvent dès lors exploiter les fonctionnalités de réplication et de contrôle d'accès d'eDirectory.
- Les clés privées ne sont accessibles que par les routines logicielles qui les utilisent dans le cadre d'opérations de signature et de déchiffrement.

  Les clés privées sont chiffrées par Novell International Cryptography Infrastructure (NICI) et réservées aux routines logicielles qui les utilisent dans le cadre d'opérations de signature et de déchiffrement.

- Sauvegarde sécurisée des clés privées.

  Les clés privées sont chiffrées par NICI, stockées dans eDirectory et sauvegardées à l'aide d'utilitaires de sauvegarde standard.
- Les certificats sont gérés de manière centralisée à l'aide d'iManager.

  Les plug-ins iManager fournis vous permettent de gérer les certificats émis par votre autorité de certification organisationnelle ou par toute autre CA prenant en charge les requêtes de signature de certificat au format PKCS#10.
- Les utilisateurs peuvent gérer leurs propres certificats.

  Les utilisateurs peuvent utiliser iManager pour exporter des clés en vue de les utiliser dans des applications codées, sans intervention de l'administrateur système.
- Les navigateurs et les clients de messagerie les plus courants sont pris en charge.

Composants de NetIQ Certificate Server

Cette section décrit les composants de NetIQ Certificate Server.

- « NetIQ Certificate Server » page 706
- « Infrastructure cryptographique de Novell International » page 713

NetIQ Certificate Server

NetIQ Certificate Server est constitué du composant serveur PKI et d'un module de plug-ins pour iManager. iManager est l'interface d'administration de Certificate Server.

Certificate Server permet d'exécuter les tâches suivantes :

- Établir une autorité de certification organisationnelle propre à votre arborescence eDirectory et à votre organisation.
- Demander, gérer et stocker les certificats de clé publique et les clés privées qui y sont associées dans l'arborescence eDirectory.

Utilisation de clés RSA de 8192 bits dans des certificats

Certificate Server vous permet de sélectionner la taille de clé dans le cadre de toute procédure de création d'un certificat. eDirectory prend en charge les clés d'une taille allant jusqu'à 8192 bits. Si vous envisagez d'utiliser des certificats X.509 avec une clé publique RSA de 8 192 bits pour vos applications, ces dernières doivent prendre en charge ce type de clé. À défaut, vos applications risquent de ne pas fonctionner comme prévu.

IMPORTANT : l'utilisation d'un certificat X.509 avec des clés publiques RSA de 8 000 bits pour établir une connexion TLS a une incidence sur les performances des serveurs eDirectory. NetIQ déconseille de configurer les serveurs eDirectory pour qu'ils utilisent des certificats RSA avec des clés de 8 000 bits, car l'établissement d'une session TLS peut monopoliser de nombreuses ressources des serveurs et l'établissement de plusieurs sessions TLS simultanément risque de fortement ralentir le système.

Veillez à mettre à niveau tous les serveurs de votre arborescence eDirectory vers la version 9.1 avant de créer un certificat d'une autorité de certification avec une clé publique RSA de 8 192 bits.

REMARQUE : vérifiez que vous utilisez au moins eDirectory 9.1, iManager 3.1 et le plug-in PKI eDirectory 9.1 avant de configurer un certificat de serveur avec une clé publique RSA 8 192 bits.

Utilisation de certificats ECDSA

Outre les certificats RSA, Certificate Server prend également en charge l'utilisation et la gestion des certificats et des clés ECDSA (Elliptic Curve Digital Signature Algorithm).

Une paire de clés ECDSA présente une sécurité comparable et une taille nettement inférieure à celles d'une clé RSA, a une taille considérablement inférieure à la clé RSA et améliore considérablement les performances lorsqu'il est utilisé lors de l'établissement de connexions TLS. ECDSA fait appel à la cryptographie basées sur les courbes elliptiques (ECC), une technologie qui génère des clés par le biais de courbes elliptiques. La technologie ECC peut être utilisée conjointement avec la plupart des méthodes de chiffrement par clés publiques, telles que RSA et Diffie-Hellman. L'utilisation de signatures ECC avec des certificats numériques offre des avantages supplémentaires en termes de taille et de performances.

eDirectory prend en charge les certificats ECDSA avec des clés basées sur les courbes suivantes :

- P-256
- P-384
- P-521

En mode SuiteB, Certificate Server respecte la convention RFC 5759. Cette convention RFC stipule que tous les certificats et listes de révocation de certificats (CRL) doivent être signés au moyen d'ECDSA avec des clés générées à l'aide de la courbe P-256 ou P-384.

Si le certificat contient une clé basée sur la courbe P-256, la clé de l'autorité de certification signataire doit être sur la courbe P-256 ou P-384. Si le certificat contient une clé basée sur la courbe P-384, la clé de l'autorité de certification signataire doit être sur la courbe P-384. Tous les certificats et CRL doivent être hachés à l'aide de l'algorithme SHA-256 ou SHA-384, en fonction de la taille de la clé de l'autorité de certification signataire.

Une fois NetIQ Certificate Server installé, vous pouvez le gérer à l'aide d'iManager.

iManager permet d'effectuer les tâches suivantes :

- « Création d'une autorité de certification organisationnelle pour votre organisation » page 708
- « Création d'un objet Certificat de serveur pour toute application codée » page 708
- « Création d'un certificat utilisateur » page 709
- « Création d'un conteneur de racines approuvées » page 709
- « Création d'un objet Racine approuvée » page 710
- « Création de certificats pour des serveurs et des utilisateurs externes » page 710
- « Validation de certificats » page 710
- « Gestion des listes de révocation de certificats » page 711
- « Exportation de certificats et de clés privées » page 712
- « Importation de certificats et de clés privées » page 712
- « Création d'un objet Service SAS » page 712

Création d'une autorité de certification organisationnelle pour votre organisation

Pendant l'installation, vous pouvez choisir de créer une autorité de certification (CA) organisationnelle si l'arborescence eDirectory n'en comporte pas déjà une. Vous pouvez également créer ou recréer l'autorité de certification organisationnelle une fois l'installation terminée.

L'objet Autorité de certification organisationnelle contient la clé publique, la clé privée, le certificat, la chaîne de certificats et d'autres informations de configuration la concernant. Cet objet se trouve dans le conteneur de sécurité d'eDirectory.

Dès qu'un serveur est configuré pour offrir le service d'Autorité de certification, il peut le fournir à l'ensemble de l'arborescence eDirectory. Si l'arborescence comporte un certificat d'autorité de certification subordonnée et que vous mettez à niveau le serveur hébergeant la CA subordonnée vers eDirectory 9.2, aucun certificat ECDSA de CA n'est généré. L'administrateur doit importer un certificat ECDSA d'autorité de certification subordonnée portant le même nom d'objet que le certificat RSA de la CA subordonnée. Si le serveur qui agit en qualité d'autorité de certification exécute eDirectory 9.2, eDirectory crée les certificats ECDSA pour la CA organisationnelle. eDirectory crée automatiquement les certificats ECDSA pour les serveurs si l'autorité de certification organisationnelle dispose d'un certificat ECDSA.

Pour plus d'informations sur la création d'une autorité de certification organisationnelle, reportez-vous à la section « Création d’un objet Autorité de certification organisationnelle » page 725.

Création d'un objet Certificat de serveur pour toute application codée

Le programme d'installation de Certificate Server crée des objets Certificat de serveur par défaut.

- SSL CertificateDNS - *nom_serveur*
- Un certificat pour chaque adresse IP configurée sur le serveur (IP AG *xxx.xxx.xxx.xxx* - *nom_serveur*)
- Un certificat pour chaque nom DNS configuré sur le serveur (DNS AG *www.exemple.com* - *nom_serveur*)
- SSL EC CertificateDNS - *nom_serveur*
- Un certificat pour chaque adresse IP configurée sur le serveur (IP EC AG *xxx.xxx.xxx.xxx* - *nom_serveur*)
- Un certificat pour chaque nom DNS configuré sur le serveur (DNS EC AG *www.exemple.com* - *nom_serveur*)

REMARQUE : eDirectory ne crée pas automatiquement le certificat SSL CertificateIP. Le nom CertificateDNS SSL contient toutes les adresses IP répertoriées dans le champ Subject Alternative Name (Autre nom de l'objet).

Vous pouvez créer des autres objets Certificat de serveur une fois l'installation terminée.

L'objet Certificat de serveur contient la clé publique, la clé privée, le certificat et la chaîne de certificats qui active les services de sécurité SSL pour les applications serveur. Les objets Certificat de serveur peuvent être signés par l'autorité de certification organisationnelle ou par une CA externe.

Un serveur peut être associé à plusieurs objets Certificat de serveur. Toutes les applications codées exécutées sur un serveur spécifique peuvent être configurées pour utiliser n'importe lequel des objets Certificat de serveur de ce serveur. Plusieurs applications exécutées sur un serveur donné peuvent utiliser le même objet Certificat de serveur. Toutefois, un objet Certificat de serveur ne peut pas être partagé par plusieurs serveurs.

Vous ne pouvez créer des objets Certificat de serveur que dans le conteneur où se trouve le serveur. Si l'objet Serveur est déplacé, tous les objets Certificat de serveur appartenant à ce serveur doivent être déplacés aussi. Vous ne devez pas renommer les objets Certificat de serveur. Vous pouvez déterminer quels objets Certificat de serveur appartiennent à un serveur en recherchant le nom du serveur dans le nom des objets Certificat de serveur ou en consultant le champ Serveur hôte lorsque vous affichez l'objet Certificat de serveur dans iManager.

La paire de clés stockée dans l'objet Certificat de serveur est référencée par le nom que vous saisissez au moment de sa création. Le nom de la paire de clés n'est pas celui de l'objet Certificat de serveur. Lorsque vous configurez des applications codées pour qu'elles utilisent des paires de clés, vous référencez ces clés d'après le nom de la paire à laquelle elles appartiennent, et non d'après le nom de l'objet Certificat de serveur.

Si les objets Certificat de serveur par défaut sont endommagés ou non valides, utilisez l'assistant de création de certificats par défaut pour remplacer les anciens certificats par défaut. Pour plus d'informations sur la façon d'accéder à l'assistant de création de certificats par défaut, reportez-vous à la section « Création d'objets Certificat de serveur par défaut » page 735.

Par défaut, eDirectory crée des certificats ECDSA si l'autorité de certification organisationnelle dispose d'un certificat ECDSA.

Création d'un certificat utilisateur

Les utilisateurs ont accès à leurs propres certificats et clés privées, qui servent à l'authentification, au chiffrement/déchiffrement des données, à la signature numérique et à la sécurisation du courrier électronique. Ces certificats sont souvent utilisés pour l'envoi et la réception de courriers électroniques chiffrés et signés numériquement à l'aide de la norme S/MIME.

En règle générale, seul l'administrateur de l'autorité de certification dispose de droits nécessaires pour créer des certificats utilisateur. Toutefois, seul l'utilisateur dispose de droits lui permettant d'exporter ou de télécharger la clé privée à partir d'eDirectory. N'importe quel utilisateur peut exporter le certificat de clé publique de tout autre utilisateur.

Le certificat utilisateur est créé sous l'onglet **Sécurité** de la page de propriétés de l'utilisateur et signé par l'autorité de certification organisationnelle. Les clés privées et les certificats créés par d'autres autorités de certification peuvent être importés après leur création.

Plusieurs certificats peuvent être stockés sur l'objet de l'utilisateur.

Pour plus d'informations sur la création d'un certificat utilisateur, reportez-vous à la section « Création d'un certificat utilisateur » page 721.

Création d'un conteneur de racines approuvées

Les racines approuvées constituent la base de l'approbation dans le cadre de la cryptographie à clé publique. Elles sont utilisées pour valider les certificats signés par d'autres autorités de certification, et permettent d'établir des connexions SSL sécurisées, de sécuriser le courrier électronique et de procéder à l'authentification par certificat.

Un conteneur de racines approuvées est un objet eDirectory qui contient des objets Racine approuvée.

Le conteneur de racines approuvées par défaut est CN=trusted roots.CN=security.

Pour plus d'informations sur la création d'un conteneur de racines approuvées, reportez-vous à la section « Création d'un conteneur de racines approuvées » page 722.

Création d'un objet Racine approuvée

Un objet Racine approuvée est un objet eDirectory qui contient le certificat de racine approuvée authentique et valide d'une autorité de certification. Vous pouvez exporter et utiliser le certificat de racine approuvée selon vos besoins. Les applications configurées pour utiliser le certificat de racine approuvée considèrent qu'un certificat est valide s'il a été signé par l'une des autorités de certification présentes dans le conteneur de racines approuvées.

L'objet Racine approuvée doit se trouver dans un conteneur de racines approuvées.

Pour plus d'informations sur la création d'un objet Racine approuvée, reportez-vous à la section « Création d'un objet Racine approuvée » page 722.

Création de certificats pour des serveurs et des utilisateurs externes

L'administrateur de l'autorité de certification peut utiliser la CA organisationnelle afin de signer des certificats pour des utilisateurs et des serveurs externes à eDirectory. Ces certificats sont demandés par le biais d'une requête de signature de certificat PKCS#10 qui est transmise à l'administrateur de l'autorité de certification en mode hors bande.

Lorsqu'il reçoit une requête de signature de certificat, l'administrateur de l'autorité de certification peut émettre le certificat à l'aide de l'outil d'émission de certificats disponible dans iManager. Le certificat généré n'est pas stocké dans un objet au sein d'eDirectory. Il doit être renvoyé au demandeur en mode hors bande.

Validation de certificats

NetIQ Certificate Server permet de vérifier la validité de tous les certificats présents dans l'arborescence eDirectory. Le processus de validation des certificats vérifie chaque certificat de la chaîne de certificats jusqu'au certificat de racine approuvée et renvoie un état Valide ou Non valide.

- Pour vérifier la validité des certificats de l'autorité de certification organisationnelle, reportez-vous à la section « Validation des certificats de l'autorité de certification organisationnelle » page 732.
- Pour vérifier la validité des certificats d'un serveur, reportez-vous à la section « Validation d'un certificat de serveur » page 742.
- Pour vérifier la validité des certificats d'un utilisateur, reportez-vous à la section « Validation d'un certificat utilisateur » page 748.
- Pour vérifier la validité des certificats d'une racine approuvée, reportez-vous à la section « Validation d'un objet Racine approuvée » page 757.

Les certificats sont considérés comme valides s'ils répondent à un certain nombre de critères prédéfinis. Ainsi, leur période de validité ne doit pas avoir expiré, ils ne doivent pas avoir été révoqués et ils doivent avoir été signés par une autorité de certification approuvée.

Pour que les certificats utilisateur ou les certificats d'autorité de certification intermédiaire situés dans le conteneur CN=trusted roots.CN=security et signés par des CA externes puissent être validés correctement, le certificat de la CA externe doit être stocké dans un objet Racine approuvée.

Gestion des listes de révocation de certificats

Une liste de révocation de certificats est une liste qui répertorie des certificats révoqués et les raisons pour lesquelles ils ont été révoqués.

NetIQ Certificate Server fournit un système de gestion des listes de révocation de certificats. Ce système est facultatif, mais doit être implémenté si vous souhaitez être en mesure de révoquer les certificats créés par l'autorité de certification organisationnelle. Pour plus d'informations sur la gestion des listes de révocation de certificats, reportez-vous à la « Tâches relatives aux listes de révocation de certificats » page 758.

Lors de l'installation de Certificate Server, un conteneur CRL est créé si l'utilisateur dispose des droits appropriés pour le créer. Dans le cas contraire, le conteneur CRL peut être créé manuellement par un utilisateur disposant des droits nécessaires une fois l'installation terminée.

Un objet Configuration CRL peut être créé dans le conteneur CRL. Cet objet contient les informations de configuration des objets Liste de révocation de certificats disponibles dans l'arborescence eDirectory. Normalement, l'arborescence ne compte qu'un seul objet Configuration CRL. Il se peut que vous ayez besoin de plusieurs objets Configuration CRL si vous créez ou déployez une nouvelle autorité de certification organisationnelle, mais un seul objet Configuration CRL peut être utilisé pour créer de nouveaux certificats.

Un objet CRL, également connu sous le nom de point de distribution, peut être créé dans n'importe quel conteneur de l'arborescence eDirectory. Toutefois, les objets CRL NetIQ se trouvent généralement dans un conteneur CRL. Un objet CRL est créé automatiquement pour vous lorsque vous créez un objet Configuration CRL. L'objet CRL héberge un fichier CRL qui contient des informations détaillées sur la liste de révocation des certificats. Pour chaque objet CRL NetIQ, un fichier CRL est automatiquement créé et mis à jour chaque fois que le serveur en émet un nouveau. Pour les autres objets CRL, vous devez importer un fichier CRL à partir d'une autorité de certification tierce. Lorsqu'un serveur qui contient l'autorité de certification de l'organisation est mis à niveau vers eDirectory 9.2, le processus de mise à niveau crée automatiquement des points de distribution de CRL. En outre, eDirectory fournit des objets Configuration CRL distincts pour les certificats RSA et ECDSA.

Bien que la suppression d'un objet Configuration CRL soit possible, elle n'est pas recommandée. Lorsqu'un objet Configuration CRL est supprimé, le serveur s'arrête et crée les fichiers CRL. Si un fichier CRL existe déjà à l'emplacement indiqué dans l'objet CRL, la validation de certificat continue de l'utiliser jusqu'à ce qu'il arrive à expiration. Une fois arrivé à expiration, la validation de tous les certificats disposant d'un point de distribution CRL faisant référence à ce fichier CRL échoue.

Si vous supprimez un objet CRL, il sera recréé la prochaine fois que le serveur génère le fichier CRL. Si vous supprimez un objet CRL créé et importé à l'aide d'iManager, il est définitivement supprimé et tous les certificats qui y font référence sont considérés comme non valides.

La règle générale consiste à ne pas supprimer un conteneur CRL, un objet Configuration CRL, un objet CRL ni un fichier CRL tant que la date d'émission du dernier certificat qui contient un point de distribution lié n'a pas expiré.

Exportation de certificats et de clés privées

Les clés d'utilisateur, de serveur et d'autorité de certification peuvent être marquées comme exportables lors de leur création. Si une clé est exportable, elle peut être extraite et placée dans un fichier avec le certificat associé. Le fichier est écrit dans un format standard pour le secteur (PFX ou PKCS#12) lui permettant d'être transporté vers d'autres plates-formes. Il est chiffré avec un mot de passe défini par l'utilisateur afin de protéger la clé privée.

L'exportation de certificats et de clés privées peut être effectuée afin d'obtenir une copie de sauvegarde de la clé, de déplacer la clé sur un autre serveur ou de partager la clé entre les serveurs.

Pour plus d'informations sur l'exportation des clés privées et des certificats, reportez-vous à la section « Exportation d'un certificat utilisateur et de la clé privée » page 747.

Importation de certificats et de clés privées

Vous pouvez choisir d'importer une clé au lieu d'en créer une nouvelle au moment de la création d'un objet Certificat de serveur, Certificat utilisateur ou Autorité de certification. La clé et ses certificats associés doivent être au format PFX ou PKCS#12.

Vous pouvez choisir d'importer une clé au lieu d'en créer une nouvelle pour un objet Autorité de certification afin d'effectuer une récupération à la suite d'une défaillance du serveur, pour déplacer l'autorité de certification organisationnelle d'un serveur vers un autre ou pour une autorité de certification qui est subordonnée à une autre.

Vous pouvez choisir d'importer un certificat utilisateur ou un clé privée si elle a été signée par une autorité de certification tierce.

Vous pouvez choisir d'importer une clé au lieu d'en créer une nouvelle pour un objet Certificat de serveur afin d'effectuer une récupération à la suite d'une défaillance du serveur, pour déplacer la clé et le certificat vers un autre serveur ou pour partager la clé et le certificat avec un autre serveur.

Création d'un objet Service SAS

L'objet Service SAS facilite la communication entre un serveur et ses certificats. Si vous supprimez un serveur d'une arborescence eDirectory, vous devez également supprimer l'objet Service SAS qui lui est associé. Si vous souhaitez restaurer le serveur dans l'arborescence, vous devez créer l'objet Service SAS qui l'accompagne. À défaut, vous ne pouvez pas créer de nouveaux certificats de serveur.

L'objet Service SAS est automatiquement créé dans le cadre de la vérification de l'état de santé du serveur. Il n'est pas nécessaire de le créer manuellement.

Vous ne pouvez créer un nouvel objet Service SAS que si le conteneur de l'objet Serveur ne contient pas encore d'objet Service avec un nom approprié. Par exemple, pour un serveur nommé WAKE, l'objet Service SAS est appelé Service SAS – WAKE. L'utilitaire ajoute les pointeurs DS de l'objet Serveur vers l'objet SAS, et de l'objet SAS vers l'objet Serveur. Il configure également les entrées ACL correctes sur l'objet Service SAS.

Si un objet Service SAS avec un nom approprié existe déjà, vous ne pouvez pas en créer un nouveau. Les pointeurs DS de l'ancien objet Service SAS peuvent être erronés ou manquants ou les ACL peuvent se révéler incorrectes. Dans ce cas, vous pouvez supprimer l'objet Service SAS altéré et utiliser iManager pour en créer un nouveau. S'il existe des certificats de serveur qui appartiennent à ce serveur, vous devez les lier manuellement à l'objet Service SAS, en utilisant l'onglet **Autre**.

Pour plus d'informations sur la création d'un objet Service SAS, reportez-vous à la section « Création d'un objet Service SAS » page 723.

Infrastructure cryptographique de Novell International

Novell International Cryptographic Infrastructure (NICI) est l'infrastructure cryptographique sous-jacente permet à NetIQ Certificate Server, aux services NetIQ Modular Authentication Services (NMAS) ainsi qu'à d'autres applications de fournir des services de chiffrement.

NICI doit être installé sur le serveur pour permettre le bon fonctionnement de NetIQ Certificate Server. NICI n'est pas livré avec NetIQ Certificate Server. Dans la plupart des cas, NICI est fourni et installé lorsque NetIQ Certificate Server est intégré dans un autre produit, tel qu'Open Enterprise Server (OES) ou eDirectory. Si vous avez besoin d'une version plus récente de NICI, vous pouvez la télécharger à partir du site Web de téléchargement NetIQ.

Configuration de NetIQ Certificate Server

Une fois NetIQ Certificate Server installé, vous devez le configurer pour pouvoir l'utiliser sur votre réseau. Pour ce faire, effectuez les tâches suivantes :

- « Choix du type d'autorité de certification à utiliser » page 713
- « Création d’un objet Autorité de certification organisationnelle » page 714
- « Autorité de certification subordonnée » page 716
- « Restrictions associées à la création d'un objet Autorité de certification » page 719
- « Configuration de l'autorité de certification en mode SuiteB » page 719
- « Création d'un objet Certificat de serveur » page 720
- « Configuration des applications codées » page 721
- « Composants supplémentaires à configurer » page 721

Choix du type d'autorité de certification à utiliser

NetIQ Certificate Server permet de créer des certificats pour les serveurs et les utilisateurs finaux. Les certificats de serveur peuvent être signés par l'autorité de certification organisationnelle ou par une autorité de certification externe ou tierce. Les certificats utilisateur ne peuvent être signés que par l'autorité de certification organisationnelle. Vous pouvez cependant importer les certificats utilisateur signés par une autorité de certification tierce au format PKCS#12.

Au cours de la procédure de création de l'objet Certificat de serveur, vous devez indiquer le type d'autorité de certification qui signera cet objet.

L'autorité de certification organisationnelle est propre à votre organisation et utilise une clé publique spécifique pour les opérations de signature. La clé privée est générée lors de la création de l'autorité de certification organisationnelle.

Une autorité de certification tierce est gérée par un tiers en dehors de l'arborescence eDirectory. VeriSign est un exemple d'autorité de certification tierce.

Vous pouvez utiliser simultanément les deux types d'autorité de certification. L'utilisation d'un type d'autorité de certification n'exclut pas l'utilisation de l'autre.

- « Avantages de l'utilisation d'une autorité de certification organisationnelle fournie avec NetIQ Certificate Server » page 714
- « Avantages de l'utilisation d'une autorité de certification externe » page 714

Avantages de l'utilisation d'une autorité de certification organisationnelle fournie avec NetIQ Certificate Server

- **La compatibilité :** l'autorité de certification organisationnelle est compatible avec les applications NetIQ ou Novell telles que les services LDAP. Les certificats émis par l'autorité de certification organisationnelle sont conformes à la norme X.509 v3 et peuvent également être utilisés dans des applications tierces.
- **Les économies :** l'autorité de certification organisationnelle vous permet de créer gratuitement un nombre illimité de certificats de clé publique. Sachez que l'obtention d'un seul certificat de clé publique auprès d'une autorité de certification externe peut parfois être très coûteux.
- **Élément d'une solution complète et compatible :** L'autorité de certification organisationnelle vous permet d'utiliser le système cryptographique complet intégré dans eDirectory sans devoir faire appel au moindre service externe. Qui plus est, NetIQ Certificate Server est compatible avec une large gamme de produits NetIQ et Novell.
- **Attribut de certificat et contrôle du contenu :** Une autorité de certification organisationnelle est gérée par l'administrateur réseau. Ce dernier sélectionne les attributs de certificat de clé publique comme la durée de vie, la taille de la clé et l'algorithme de signature.
- **Gestion simplifiée :** l'autorité de certification organisationnelle remplit une fonction similaire aux autorités de certification externes, sans le moindre coût supplémentaire ni surcroît de complexité.

Avantages de l'utilisation d'une autorité de certification externe

- **Responsabilité :** une autorité de certification externe peut offrir une certaine protection en matière de responsabilité si, par la faute de l'autorité de certification, votre clé privée a été dévoilée ou si votre certificat de clé publique n'a pas été correctement représenté.
- **Disponibilité :** le certificat d'une autorité de certification externe peut être plus largement disponible et plus largement approuvé par les applications autres qu'eDirectory.

Création d’un objet Autorité de certification organisationnelle

Par défaut, la procédure d'installation de NetIQ Certificate Server crée l'autorité de certification organisationnelle (CA) pour vous. Vous êtes invité à spécifier le nom d'une autorité de certification organisationnelle. Lorsque vous cliquez sur **Terminer**, l'autorité de certification organisationnelle est créée avec les paramètres par défaut et placée dans le conteneur de sécurité.

Si vous souhaitez mieux contrôler la création de l'autorité de certification organisationnelle, vous pouvez la créer manuellement à l'aide d'iManager. En outre, si vous supprimez l'autorité de certification organisationnelle, vous devrez la recréer.

Au cours de la procédure de création, vous êtes invité à attribuer un nom à l'objet Autorité de certification organisationnelle et à choisir un serveur pour l'héberger (le serveur sur lequel le service de l'autorité de certification organisationnelle doit s'exécuter). Pour déterminer le serveur sur lequel le service Autorité de certification organisationnelle doit être hébergé, tenez compte des aspects suivants :

- Sélectionnez un serveur physiquement sécurisé.

  L'accès physique au serveur de l'autorité de certification est un aspect important de la sécurité du système. Si le serveur de l'autorité de certification est endommagé, tous les certificats émis par l'autorité de certification le sont également.

- Sélectionnez un serveur stable, résistant et présentant une haute disponibilité.

  Si le service de l'autorité de certification n'est pas disponible, les certificats ne peuvent pas être créés. L'installation de nouveaux serveurs s'en trouve affectée, car les certificats doivent être créés lors de l'installation.

- Sélectionnez un serveur qui exécute uniquement des logiciels que vous avez approuvés.

  L'exécution de logiciels inconnus ou douteux risque d'endommager le fonctionnement de l'autorité de certification.

- Sélectionnez un serveur qui ne sera pas supprimé de l'arborescence.

  Si le serveur est supprimé de l'arborescence, vous devez soit recréer l'objet Autorité de certification à l'aide d'une sauvegarde effectuée avant de l'avoir supprimé l'autorité de certification ou vous devez créer une nouvelle autorité de certification. Si vous créez une nouvelle autorité de certification, vous devrez peut-être remplacer les certificats serveur et utilisateur existants.

- Sélectionnez un serveur qui exécute un protocole compatible avec d'autres serveurs de votre arborescence ;

  un protocole IP par exemple.

- Utilisez un certificat ECDSA pour créer une autorité de certification pour l'organisation.

Pour créer l'objet Autorité de certification organisationnelle, procédez comme suit :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   S'il n'existe aucun objet Autorité de certification organisationnelle, la boîte de dialogue de création d'un objet Autorité de certification organisationnelle s'ouvre, de même que l'assistant correspondant qui crée l'objet. Suivez les instructions à l'écran pour créer l'objet. Pour obtenir des informations spécifiques sur la boîte de dialogue ou sur l'une des pages de l'assistant, cliquez sur Aide.

   REMARQUE : assurez-vous que le chemin d'accès au fichier CRL spécifié ici correspond au chemin d'installation d'eDirectory.

4. Une fois l'autorité de certification créée, il est recommandé d'effectuer une sauvegarde de la paire de clés publique/privée de l'autorité de certification et de la conserver en lieu sûr. Reportez-vous à la section « Sauvegarde d'une autorité de certification organisationnelle » page 728.

REMARQUE : vous ne pouvez avoir qu'un seul objet Autorité de certification organisationnelle dans votre arborescence eDirectory.

eDirectory autorise l'administrateur à indiquer une taille de clé RSA, une courbe elliptique et un certificat à utiliser lorsque les certificats de serveur par défaut sont générés. Ces paramètres peuvent être spécifiés à l'aide des trois attributs suivants sur l'objet Autorité de certification :

- **ndspkiDefaultRSAKeySize :** indiquez la taille de clé pour les certificats de serveur RSA. Vous pouvez spécifier dans ce champ un chiffrement RSA pouvant atteindre 8 192 bits.

IMPORTANT : l'utilisation d'un certificat X.509 avec des clés publiques RSA de 8 000 bits pour établir une connexion TLS a une incidence sur les performances des serveurs eDirectory. NetIQ déconseille de configurer les serveurs eDirectory pour qu'ils utilisent des certificats RSA avec des clés de 8 000 bits, car l'établissement d'une session TLS peut monopoliser de nombreuses ressources des serveurs et l'établissement de plusieurs sessions TLS simultanément risque de fortement ralentir le système.

- **ndspkiDefaultECCurve :** indiquez la courbe elliptique (EC) limite pour les certificats de serveur. Vous pouvez spécifiez l'une des courbes elliptiques suivantes :
  - P 256
  - P 384
  - P 521
- **ndspkiDefaultCertificateLife :** indiquez la durée de vie des certificats de serveur par défaut. Vous pouvez indiquer une durée de vie en années. Par exemple, si vous spécifiez 4 dans ce champ, la durée de vie du certificat de serveur est définie sur 4 ans. Certificate Server veille à ce que les certificats de serveur par défaut aient une validité minimale de 1 an et que la validité maximale ne s'étende pas au-delà de la date d'expiration de l'autorité de certification.

REMARQUE

- L'attribut `ndspkiDefaultCertificateLife` s'applique uniquement aux certificats de serveur.
- Si vous transmettez les anciennes valeurs par défaut lors de la configuration d'un nouveau serveur eDirectory, les paramètres mentionnés ci-dessus restent indéfinis.
- Les paramètres ci-dessus n'affectent pas les certificats par défaut existants. Lors de la mise à niveau du serveur eDirectory vers la version 9.2, après avoir spécifié ces paramètres sur l'autorité de certification, les certificats du serveur par défaut existants ne sont pas recréés.

Si vous indiquez ces paramètres lors de la configuration d'une nouvelle arborescence eDirectory, les certificats de l'autorité de certification organisationnelle sont également créés avec ces paramètres. Pour plus d'informations, reportez-vous au Guide d'installation de Novell eDirectory.

Autorité de certification subordonnée

NetIQ Certificate Server prend désormais en charge une autorité de certification subordonnée. Cette fonction permet à l'autorité de certification organisationnelle d'être subordonnée à une autorité de certification tierce ou à une autorité de certification dans une autre arborescence eDirectory. Votre arborescence eDirectory ne peut toutefois contenir qu'une seule autorité de certification organisationnelle.

Voici quelques raisons justifiant d'avoir une autorité de certification subordonnée à votre disposition :

- permet à l'autorité de certification organisationnelle de devenir partie intégrante d'une infrastructure PKI existante tierce ;
- permet à plusieurs arborescences de partager une même racine approuvée (ou la même ancre d'approbation) pour l'infrastructure PKI ;

- permet de renforcer la sécurité de l'autorité de certification racine en hébergeant l'autorité de certification sur un système davantage sécurisé ;
- permet de réduire les risques en faisant résider l'autorité de certification racine dans une arborescence gérée de manière plus stricte (par exemple, dans une arborescence à l'abri d'administrateurs/utilisateurs malveillants).

- « Création d'une autorité de certification subordonnée » page 717
- « Création de fichiers PKCS#12 pour une autorité de certification subordonnée » page 717

Création d'une autorité de certification subordonnée

Pour créer une autorité de certification subordonnée, vous devez d'abord supprimer l'autorité de certification organisationnelle existante (pour ce faire, reportez-vous à la section « Suppression d'une autorité de certification organisationnelle » page 732). Vous devez déjà disposer d'un fichier PKCS#12 contenant les clés publique/privée ainsi que la chaîne de certificats de l'autorité de certification subordonnée. Vous pouvez vous procurer ce fichier directement auprès d'une autorité de certification tierce ou consulter la section « Création de fichiers PKCS#12 pour une autorité de certification subordonnée » page 717 pour apprendre comment créer ce type de fichier. Pour créer l'autorité de certification subordonnée, connectez-vous à l'arborescence dans iManager et utilisez la tâche de configuration d'une autorité de certification à l'aide de la méthode de création d'une importation.

Création de fichiers PKCS#12 pour une autorité de certification subordonnée

1 Créez un objet Certificat de serveur (ou un objet Matériel clé) et une requête de signature de certificat PKCS#10 à l'aide de clés ECDSA et RSA.

   1a Lancez iManager.

   1b Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create Server Certificate** (Créer un certificat de serveur).

   1c Sélectionnez le serveur devant héberger l'autorité de certification, indiquez un surnom pour le certificat, sélectionnez la méthode de création personnalisée, puis cliquez sur **Suivant**.

   1d Sélectionnez **Autorité de certification externe**, puis cliquez sur **Suivant**.

   1e Sélectionnez l'algorithme et une taille de clé et vérifiez que l'option **Allow Private Key to Be Exported** (Autoriser l'exportation de la clé privée) est sélectionnée, puis cliquez sur **Next** (Suivant).

   IMPORTANT : si vous souhaitez utiliser des certificats RSA et ECDSA dans votre environnement eDirectory, répétez cette étape pour le certificat que vous souhaitez utiliser. NetIQ recommande d'utiliser une taille de clé de 2 048 bits pour RSA et 384 bits pour ECDSA.

   1f Cliquez sur le bouton **Modifier** à droite du champ **Nom de l'objet** et éditez le **Nom de l'objet** afin de refléter l'autorité de certification subordonnée et l'arborescence. Sélectionnez ensuite l'algorithme de signature (NetIQ recommande d'utiliser un algorithme plus puissant que SHA-1), puis cliquez sur **Suivant**.

   1g Vérifiez que le résumé est correct, puis cliquez sur **Terminer**.

   1h Cliquez sur **Save Certificate Signing Request** (Enregistrer la requête de signature de certificat), puis suivez les invites pour enregistrer la CSR dans un fichier.

2 Faites signer la CSR pour créer un certificat.

2a Si l'autorité de certification subordonnée doit faire partie d'une infrastructure à clé publique tierce, demandez à l'autorité de certification tierce de créer le certificat à partir de la CSR.

ou

Si l'autorité de certification subordonnée doit être signée par une autorité de certification dans une autre arborescence eDirectory, passez à l'Étape 2b.

REMARQUE : s'il s'agit d'un certificat ECDSA, la CSR ne peut être signée que par l'autorité de certification ECDSA.

2b Lancez iManager.

2c Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Issue Certificate** (Émettre le certificat).

2d Sélectionnez le fichier contenant la CSR, puis cliquez sur **Next** (Suivant).

2e Sélectionnez un type de clé pour l'**autorité de certification**, désélectionnez l'option **Enable Extended Key Usage** (Activer l'utilisation de clés étendues), puis cliquez sur **Next** (Suivant).

2f Sélectionnez le type d'autorité de certification du certificat, puis sélectionnez une longueur **non spécifiée** ou un **chemin d'accès spécifique**, puis cliquez sur **Next** (Suivant).

2g Vérifiez le nom de l'objet et modifiez-le si nécessaire. Spécifiez une durée de validité (une période de 5 à 10 ans est recommandée), puis cliquez sur **Next** (Suivant).

2h Sélectionnez le format du certificat, puis cliquez sur **Next** (Suivant).

2i Cliquez sur **Finish** (Terminer).

2j Cliquez sur **Download the issued certificate** (Télécharger le certificat émis), puis suivez les invites pour enregistrer le certificat.

3 Procurez-vous les certificats de l'autorité de certification.

3a Si l'autorité de certification subordonnée doit faire partie d'une infrastructure à clé publique tierce, procurez-vous les certificats auprès d'une d'autorité de certification tierce.

ou

Si le certificat de l'autorité de certification subordonnée doit être signé par une autorité de certification dans une autre arborescence eDirectory, passez à l'Étape 3b.

3b Lancez iManager.

3c Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

3d Cliquez sur l'onglet **Certificates** (Certificats), puis sélectionnez **Self-Signed Certificate** (Certificat auto-signé).

3e Cliquez sur **Exporter**.

3f N'exportez pas la clé privée et sélectionnez un format pour le certificat, puis cliquez sur **Next** (Suivant).

3g Cliquez sur **Save the Exported Certificate to a File** (Enregistrer le certificat exporté dans un fichier), puis suivez les invites pour enregistrer le certificat.

4 Importez les certificats dans l'objet Certificat de serveur (ou l'objet Matériel clé).

4a Lancez iManager.

4b Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **Server Certificates** (Certificats de serveur).

4c Sélectionnez le serveur supposé héberger l'autorité de certification.

4d Sélectionnez l'objet Certificat de serveur (ou objet Matériel clé) créé à l'Étape 1, puis cliquez sur l'option **Import** (Importer).

4e Sélectionnez les deux fichiers contenant les certificats obtenus à l'Étape 2 et l'Étape 3, puis cliquez sur **OK**.

IMPORTANT : si vous souhaitez utiliser des certificats RSA et ECDSA dans votre environnement eDirectory, répétez cette étape pour le certificat que vous souhaitez utiliser.

---

5 Exportez les clés publique/privée dans un fichier PKCS#12.

5a Reprenez à l'Étape 4e, cliquez sur **Export** (Exporter), choisissez d'inclure la clé privée, puis cliquez sur **Next** (Suivant).

5b Cliquez sur **Save the Exported Certificate to a File** (Enregistrer le certificat exporté dans un fichier), puis suivez les invites pour enregistrer le fichier PKCS#12.

5c Effectuez une copie de ce fichier et conservez-le en lieu sûr (accompagné de son mot de passe).

6 (Facultatif) Supprimez l'objet Certificat de serveur (ou l'objet Matériel clé).

7 Supprimez l'autorité de certification organisationnelle Pour plus d'informations, reportez-vous à la section « Suppression d'une autorité de certification organisationnelle » page 732.

8 Importez les certificats de l'autorité de certification subordonnée ainsi que les clés privées à partir du fichier PKCS#12. Pour plus d'informations, reportez-vous à la section « Restauration d'une autorité de certification organisationnelle » page 730.

Restrictions associées à la création d'un objet Autorité de certification

À partir de la version 9.0 d'eDirectory, les certificats RSA et CE sont pris en charge pour l'autorité de certification. Les points suivants s'appliquent à la création d'un objet Autorité de certification avec des certificats RSA et EC :

- Le nom d'objet des certificats RSA et EC doit être identique.
- Les autorités de certification RSA et EC ne doivent pas être en mode mixte. Les autorités de certification RSA et CE peuvent être des autorités de certification racine ou subordonnée. Par exemple, l'autorité de certification RSA ne peut pas être à la racine si l'autorité de certification EC est subordonnée et inversement.
- eDirectory ne vous autorise pas à importer les certificats auto-signés d'un autorité de certification générés par une application tierce en dehors d'eDirectory.

Configuration de l'autorité de certification en mode SuiteB

Avant de configurer l'autorité de certification en mode SuiteB, assurez-vous que le serveur sur lequel l'autorité de certification est hébergée contient la version 3.0 de NICI et qu'il est configuré pour exécuter une authentification EBA.

Pour configurer l'autorité de certification afin qu'elle fonctionne en mode SuiteB, procédez comme suit :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ > Configurer l'autorité de certification**.

4 Sélectionnez **Activer le mode SuiteB**.

5 Cliquez sur **OK**.

Lorsque l'autorité de certification est en mode SuiteB, NetIQ Certificate Server ne vous autorise pas à créer des certificats RSA. Pour plus d'informations sur les certificats ECDSA pris en charge, reportez-vous à la « Composants de NetIQ Certificate Server » page 706.

Si vous ajoutez un serveur avec une ancienne version d'eDirectory à une arborescence eDirectory 9.0 ou version ultérieure configurée en mode SuiteB, NetIQ Certificate Server ne crée pas les certificats pour le serveur, car il ne dispose pas de la fonctionnalité SuiteB. Pour activer la fonctionnalité SuiteB sur ces serveurs, vous devez procéder à une mise à niveau vers eDirectory 9.0 ou version ultérieure.

Création d'un objet Certificat de serveur

Les objets Certificat de serveur sont créés dans le conteneur dans lequel se trouve l'objet eDirectory du serveur. Selon vos besoins, vous pouvez créer un objet Certificat de serveur distinct pour chaque application codée sur le serveur ou vous pouvez créer un objet Certificat de serveur pour toutes les applications utilisées sur ce serveur.

REMARQUE : les expressions « objet Certificat de serveur » et « objet Matériel clé (KMO) » sont synonymes. Le nom de schéma de l'objet eDirectory est NDSPKI:Key Material.

Lorsque vous installez NetIQ Certificate Server, eDirectory crée automatiquement l'objet Certificat de serveur avec les paramètres par défaut et le place dans le conteneur hébergeant le serveur cible. Si vous devez écraser ou créer de nouveaux certificats par défaut, vous pouvez utiliser l'assistant de création de certificats par défaut. Reportez-vous à la section « Création d'objets Certificat de serveur par défaut » page 735.

Si vous souhaitez mieux contrôler la création de l'objet Certificat de serveur, vous pouvez le créer manuellement. Vous pouvez également créer des objets Certificat de serveur supplémentaires.

- « Création manuelle d'un objet Certificat de serveur » page 720
- « Conseils sur la création de certificats de serveur » page 721

Création manuelle d'un objet Certificat de serveur

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create Server Certificate** (Créer un certificat de serveur).

   La boîte de dialogue de création d'un certificat de serveur et l'Assistant qui crée cet objet apparaissent. Suivez les instructions à l'écran pour créer l'objet. Pour obtenir des informations spécifiques sur la boîte de dialogue ou sur l'une des pages de l'assistant, cliquez sur **Aide**.

Conseils sur la création de certificats de serveur

Au cours du processus de création de l'objet Certificat de serveur, vous êtes invité à attribuer un nom à la paire de clés et à sélectionner le serveur auquel elle doit être associée. L'objet Certificat de serveur est généré par NetIQ Certificate Server et son nom est basé sur le nom de la paire de clés choisie.

Si vous sélectionnez la méthode de création personnalisée, vous êtes également invité à indiquer si l'objet Certificat de serveur doit être signé par une autorité de certification de votre organisation ou par une autorité de certification externe. Pour obtenir des informations sur le type d'autorité à choisir, reportez-vous à la « Choix du type d'autorité de certification à utiliser » page 713.

Si vous décidez d'utiliser l'autorité de certification de votre organisation, le serveur auquel l'objet Certificat de serveur est associé doit pouvoir communiquer avec le serveur qui héberge l'autorité de certification organisationnelle ou doit être ce serveur proprement dit. Ces serveurs doivent exécuter le même protocole (IP).

Si vous décidez d'utiliser une autorité de certification externe pour signer le certificat, le serveur auquel est associé l'objet Certificat de serveur génère une requête de signature de certificat que vous devez soumettre à cette autorité.

Une fois que le certificat est signé et qu'il vous a été renvoyé, vous devez l'installer dans l'objet Certificat de serveur, ainsi que la racine approuvée de l'autorité de certification externe.

Après avoir créé l'objet Certificat de serveur, vous pouvez configurer vos applications de manière à ce qu'elles l'utilisent. (Reportez-vous à la « Configuration des applications codées » page 721.) Dans la configuration de l'application, les clés sont référencées en fonction du nom de la paire de clés que vous saisissez lors de la création de l'objet Certificat de serveur.

Configuration des applications codées

Après avoir configuré NetIQ Certificate Server, vous devez configurer vos applications codées individuelles afin qu'elles puissent utiliser les certificats personnalisés que vous avez créés. Les procédures de configuration sont propres à chaque application. Veillez donc à consulter la documentation relative à chacune des applications utilisées pour obtenir des instructions spécifiques.

Composants supplémentaires à configurer

NetIQ Certificate Server inclut d'autres composants qui peuvent être configurés pour offrir des fonctionnalités supplémentaires.

- « Création d'un certificat utilisateur » page 721
- « Création d'un conteneur de racines approuvées » page 722
- « Création d'un objet Racine approuvée » page 722
- « Création d'un objet Service SAS » page 723

Création d'un certificat utilisateur

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create User Certificate** (Créer un certificat utilisateur).

   Un assistant s'ouvre et vous aide à créer le certificat utilisateur. Suivez les instructions à l'écran pour créer l'objet. Pour obtenir des informations précises sur les pages de l'assistant, cliquez sur **Aide**.

Création d'un conteneur de racines approuvées

Vous pouvez créer un conteneur de racines approuvées à n'importe quel emplacement de l'arborescence eDirectory.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create Trusted Root Container** (Créer un conteneur de racines approuvées).

4 Spécifiez un nom pour le conteneur de racines approuvées.

5 Recherchez et sélectionnez le contexte pour le conteneur de racines approuvées.

6 Cliquez sur **OK**.

REMARQUE : différentes applications peuvent nécessiter que le conteneur de racines approuvées reçoive un nom spécifique et soit hébergé à un emplacement spécifique de l'arborescence eDirectory. NetIQ Certificate Server exige que le conteneur de racines approuvées soit nommé Trusted Roots (Racines approuvées) et se trouve dans le conteneur de sécurité. Les certificats de ce conteneur sont utilisés pour valider des certificats utilisateur signés par des autorités de certification externes et les certificats d'autorité de certification intermédiaires sont stockés dans des objets Racine approuvée. Les certificats de serveur et ceux des autorités de certification organisationnelle utilisent la chaîne de certificats stockée dans leurs propres objets.

Création d'un objet Racine approuvée

Un objet Racine approuvée peut uniquement résider dans un conteneur de racines approuvées.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create Trusted Root** (Créer une racine approuvée).

   L'assistant de création d'un objet Racine approuvée s'ouvre et vous aide à créer l'objet Racine approuvée. Suivez les instructions à l'écran pour créer l'objet. Pour obtenir des informations précises sur les pages de l'assistant, cliquez sur **Aide**.

REMARQUE : Un objet Racine approuvée peut stocker tout type de certificat (certificats d'autorités de certification, certificats d'autorités de certification intermédiaires ou certificats utilisateur).

Création d'un objet Service SAS

L'objet Service SAS est automatiquement créé dans le cadre de la vérification de l'état de santé du serveur. Il n'est pas nécessaire de le créer manuellement. Si vous devez le créer manuellement, utilisez la procédure suivante :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create SAS Service Object** (Créer un objet Service SAS).

   L'assistant de création d'un objet Service SAS s'ouvre et vous aide à créer l'objet Service SAS. Suivez les instructions à l'écran pour créer l'objet. Pour obtenir des informations précises sur les pages de l'assistant, cliquez sur **Aide**.

Gestion de NetIQ Certificate Server

En tant qu'administrateur système, vous devez effectuer plusieurs tâches pour gérer les services de cryptographie à clé publique fournis par NetIQ Certificate Server. iManager vous permet d'effectuer ces tâches. Cette section fournit un bref aperçu et des informations spécifiques de l'exécution de chaque tâche.

Tâches relatives à l'autorité de certification :

- « Création d’un objet Autorité de certification organisationnelle » page 725
- « Émission d'un certificat de clé publique » page 726
- « Affichage des propriétés de l'autorité de certification organisationnelle » page 726
- « Affichage des propriétés du certificat de clé publique d'une autorité de certification organisationnelle » page 727
- « Affichage des propriétés de certificat auto-signé de l'autorité de certification » page 727
- « Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle » page 728
- « Sauvegarde d'une autorité de certification organisationnelle » page 728
- « Restauration d'une autorité de certification organisationnelle » page 730
- « Déplacement de l'autorité de certification organisationnelle vers un autre serveur » page 731
- « Validation des certificats de l'autorité de certification organisationnelle » page 732
- « Suppression d'une autorité de certification organisationnelle » page 732
- « Déploiement d'une autorité de certification organisationnelle » page 733

Tâches relatives à l'objet Certificat de serveur :

- « Création d'objets Certificat de serveur » page 735
- « Création d'objets Certificat de serveur par défaut » page 735
- « Importation d'un certificat de clé publique dans un objet Certificat de serveur » page 736
- « Exportation d'un certificat de racine approuvée ou d'un certificat de clé publique » page 737
- « Suppression d'un objet Certificat de serveur » page 738

- « Affichage des propriétés d'un objet Certificat de serveur » page 738
- « Affichage des propriétés du certificat de clé publique d'un objet Certificat de serveur » page 739
- « Affichage des propriétés du certificat de racine approuvée d'un objet Certificat de serveur » page 739
- « Sauvegarde d'un objet Certificat de serveur » page 740
- « Restauration d'un objet Certificat de serveur » page 741
- « Objets Certificat de serveur et mise en grappe » page 742
- « Validation d'un certificat de serveur » page 742
- « Révocation d'un certificat de racine approuvée ou auto-signé » page 743
- « Déplacement d'un objet Certificat de serveur vers un autre serveur » page 743
- « Remplacement du matériel de codage par clé d'un objet Certificat de serveur » page 744

Tâches relatives au certificat utilisateur :

- « Création de certificats utilisateur » page 745
- « Création groupée de certificats utilisateur » page 745
- « Importation d'un certificat de clé publique dans un objet Utilisateur (avec ou sans clé privée) » page 745
- « Affichage des propriétés d'un certificat utilisateur » page 746
- « Exportation d'un certificat utilisateur » page 747
- « Exportation d'un certificat utilisateur et de la clé privée » page 747
- « Validation d'un certificat utilisateur » page 748
- « Révocation d'un certificat utilisateur » page 749
- « Suppression d'un certificat utilisateur et de la clé privée » page 749

Auto-provisioning du certificat X.509 :

- « Présentation » page 750
- « Auto-provisioning des utilisateurs » page 751
- « Auto-provisioning du serveur » page 752
- « Auto-provisioning et tâche d'émission du certificat » page 753

Utilisation des certificats eDirectory avec des applications externes :

- « Fonctionnalité de vérification de l'état de santé PKI » page 754
- « Configuration de l'objet SAS:Service pour exporter des certificats eDirectory » page 755

Tâches relatives à l'objet Racine approuvée :

- « Création d'un conteneur de racines approuvées » page 709
- « Création d'un objet Racine approuvée » page 710
- « Affichage des propriétés d'un objet Racine approuvée » page 756
- « Remplacement d'un certificat de racine approuvée » page 757
- « Validation d'un objet Racine approuvée » page 757
- « Révocation d'un certificat de racine approuvée » page 758

Tâches relatives aux listes de révocation de certificats

- « Création manuelle d'un conteneur CRL » page 759
- « Suppression d'un conteneur CRL » page 759
- « Création d'un objet Configuration CRL » page 760
- « Activation d'un objet Configuration CRL » page 760
- « Affichage et modification des propriétés d'un objet Configuration CRL » page 761
- « Suppression d'un objet Configuration CRL » page 762
- « Création d'un objet CRL » page 763
- « Exportation d'un fichier CRL » page 763
- « Remplacement d'un fichier CRL » page 764
- « Affichage des propriétés d'un objet CRL » page 765
- « Suppression d'un objet CRL » page 766

Tâches relatives à eDirectory :

- « Résolution de plusieurs conteneurs de sécurité, autorités de certification organisationnelles, conteneurs KAP et objets W0 » page 766
- « Restauration ou recréation d'un conteneur de sécurité » page 767
- « Restauration ou recréation d'objets KAP et W0 » page 767

Tâches relatives aux applications

Tâches concernant l'autorité de certification

- « Création d’un objet Autorité de certification organisationnelle » page 725
- « Émission d'un certificat de clé publique » page 726
- « Affichage des propriétés de l'autorité de certification organisationnelle » page 726
- « Affichage des propriétés du certificat de clé publique d'une autorité de certification organisationnelle » page 727
- « Affichage des propriétés de certificat auto-signé de l'autorité de certification » page 727
- « Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle » page 728
- « Sauvegarde d'une autorité de certification organisationnelle » page 728
- « Restauration d'une autorité de certification organisationnelle » page 730
- « Déplacement de l'autorité de certification organisationnelle vers un autre serveur » page 731
- « Validation des certificats de l'autorité de certification organisationnelle » page 732
- « Suppression d'une autorité de certification organisationnelle » page 732
- « Déploiement d'une autorité de certification organisationnelle » page 733

Création d’un objet Autorité de certification organisationnelle

Cette tâche est décrite à la « Création d’un objet Autorité de certification organisationnelle » page 714.

Émission d'un certificat de clé publique

Cette tâche vous permet de générer des certificats destinés aux applications codées qui ne reconnaissent pas les objets Certificat de serveur.

Votre autorité de certification organisationnelle fonctionne de la même manière qu'une autorité de certification externe. Autrement dit, elle est capable d'émettre des certificats à partir de requêtes de signature. Vous pouvez émettre des certificats à l'aide de votre autorité de certification organisationnelle lorsqu'un utilisateur envoie une requête vous invitant à signer le certificat. L'utilisateur qui demande le certificat peut se servir du certificat émis et l'importer directement dans l'application qui prend en charge la cryptographie.

Pour émettre un certificat de clé publique :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Issue Certificate** (Émettre le certificat).
4. Utilisez le bouton **Browse** (Parcourir) afin de localiser un fichier CSR, ouvrez le fichier, puis cliquez sur **Next** (Suivant).
5. Spécifiez le type de clé, son utilisation ainsi que son utilisation étendue, puis cliquez sur **Next** (Suivant).
6. Spécifiez les contraintes de base du certificat, puis cliquez sur **Next** (Suivant).
7. Spécifiez le nom de l'objet, la période de validité, les dates effectives et d'expiration ainsi que les extensions personnalisées, puis cliquez sur **Next** (Suivant).
8. Reportez-vous à la feuille de paramètres. Si elle vous convient, cliquez sur **Finish** (Terminer). Dans le cas contraire, cliquez sur **Back** (Précédent) jusqu'à ce que vous arriviez au point à modifier.

   Lorsque vous cliquez sur **Finish** (Terminer), une boîte de dialogue vous informe qu'un certificat a été créé. Vous pouvez enregistrer le certificat dans le Presse-papiers système au format Base64, ou dans un fichier au format Base64 ou encore, un fichier au format binaire DER. Vous pouvez également cliquer sur **Details** (Détails) pour afficher les détails du certificat émis.

Affichage des propriétés de l'autorité de certification organisationnelle

Outre les propriétés et les droits eDirectory que vous pouvez visualiser avec tout objet eDirectory, vous pouvez également afficher les propriétés propres à l'autorité de certification organisationnelle, notamment celles qui concernent le certificat de clé publique et le certificat auto-signé qui lui est associé.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

Les pages de propriétés de l'autorité de certification organisationnelle s'affichent, à savoir une page générale, une page dédiée à la liste de révocation et une page dédiée aux certificats.

4 Cliquez sur les onglets que vous souhaitez visualiser.

Affichage des propriétés du certificat de clé publique d'une autorité de certification organisationnelle

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

Les pages de propriétés de l'autorité de certification organisationnelle s'affichent, à savoir une page générale, une page dédiée à la liste de révocation, une page dédiée aux certificats et une page dédiée à eDirectory.

4 Cliquez sur **Certificates** (Certificats), puis cliquez sur le surnom du certificat de clé publique que vous souhaitez afficher.

5 Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.

6 Cliquez sur **Close** (Fermer).

Affichage des propriétés de certificat auto-signé de l'autorité de certification

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

Les pages de propriétés de l'autorité de certification organisationnelle s'affichent, à savoir une page générale, une page dédiée à la liste de révocation et une page dédiée aux certificats.

4 Cliquez sur **Certificates** (Certificats), puis cliquez sur le surnom du certificat auto-signé que vous souhaitez afficher.

S'il s'agit d'une autorité de certification subordonnée, il n'existe aucun certificat auto-signé.

5 Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.

6 Cliquez sur **Close** (Fermer).

Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle

Le certificat auto-signé peut être utilisé pour vérifier l'identité de l'autorité de certification organisationnelle ainsi que la validité d'un certificat signé par cette autorité.

À partir de la page de propriétés de l'autorité de certification organisationnelle, vous pouvez afficher les certificats et les propriétés associés à cet objet. À partir de la page de propriétés du certificat auto-signé, vous pouvez exporter le certificat auto-signé dans un fichier qui pourra être utilisé dans des applications codées.

Le certificat auto-signé qui réside dans l'autorité de certification organisationnelle est identique au certificat de racine approuvée d'un objet Certificat de serveur qui, lui, est signé par l'autorité de certification organisationnelle. Tout service qui reconnaît le certificat auto-signé de l'autorité de certification organisationnelle en tant que racine approuvée peut accepter un certificat utilisateur ou un certificat de serveur valide signé par cette autorité.

Cette tâche ne s'applique toutefois pas si l'autorité de certification est subordonnée.

Pour exporter le certificat auto-signé de l'autorité de certification organisationnelle :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   Les pages de propriétés de l'autorité de certification organisationnelle s'affichent, à savoir une page générale, une page dédiée à la liste de révocation, une page dédiée aux certificats et une page dédiée à eDirectory.
4. Cliquez sur **Certificates** (Certificats), puis sélectionnez le certificat auto-signé.
5. Cliquez sur **Exporter** et suivez les invites pour exporter le certificat.

   L'assistant d'exportation de certificats démarre. Vérifiez que la case **Export private key** (Exporter la clé privée) n'est pas cochée.
6. Cliquez sur **Finish** (Terminer).

Sauvegarde d'une autorité de certification organisationnelle

NetIQ vous recommande de sauvegarder la clé privée ainsi que les certificats de votre autorité de certification organisationnelle en cas d'échec irrécupérable du serveur hébergeant l'autorité de certification organisationnelle. Dans ce cas, le fichier de sauvegarde vous permettra de restaurer votre autorité de certification organisationnelle sur n'importe quel serveur de l'arborescence.

REMARQUE : la sauvegarde d'une autorité de certification organisationnelle n'est possible que pour les autorités de certification organisationnelle créées avec la version 9.0 (ou version ultérieure) de NetIQ Certificate Server. Dans les versions précédentes de NetIQ Certificate Server, la clé privée de l'autorité de certification organisationnelle était créée de manière à rendre toute exportation impossible.

Le fichier de sauvegarde contient la clé privée de l'autorité de certification, un certificat auto-signé, un certificat de clé publique et plusieurs autres certificats nécessaires à son fonctionnement. Ces informations sont stockées au format PKCS#12 (également appelé PFX).

L'autorité de certification organisationnelle doit être sauvegardée lorsqu'elle fonctionne correctement.

Pour pouvoir effectuer une sauvegarde complète de l'autorité de certification, il convient de sauvegarder la base de données CRL ainsi que la base de données de certificats émis à l'aide de la version 9.0 de NetIQ Certificate Server ou d'une version ultérieure.

Pour les autres plates-formes, ces deux bases de données se trouvent dans le même répertoire que les fichiers `DIB` eDirectory. Les valeurs par défaut de ces emplacements sont les suivantes :

- Windows : `c:\novell\nds\dibfiles`
- Linux : `/var/opt/novell/edirectory/data/dib`

Ces valeurs par défaut peuvent être modifiées lors de l'installation d'eDirectory.

Les fichiers de sauvegarde de la base de données sont `crl.db`, `crl.01` ainsi que le répertoire `crl.rfl`. Les fichiers de sauvegarde de la base de données d'émission des certificats sont `cert.db`, `cert.lck`, `cert.01` ainsi que le répertoire `cert.rfl`.

Le répertoire `dib` eDirectory doit faire partie d'un plan de sauvegarde standard et régulier.

Pour sauvegarder l'autorité de certification organisationnelle :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).
4. Cliquez sur **Certificates** (Certificats), puis sur **Self Signed Certificate** (Certificat auto-signé) ou **Public Key Certificate** (Certificat de clé publique). Les deux certificats sont inscrits dans le fichier lors de l'opération de sauvegarde.

   NetIQ recommande de sélectionner le **certificat auto-signé** pour les certificats RSA et ECDSA séparément.
5. Cliquez sur **Export** (Exporter).

   Un assistant s'ouvre et vous aide à exporter les certificats dans un fichier.
6. Choisissez d'exporter la clé privée, spécifiez un mot de passe avec 6 caractères alphanumériques ou plus à utiliser pour chiffrer le fichier PFX, puis cliquez sur **Next** (Suivant).
7. Cliquez sur le lien **Save the exported certificate to a file** (Enregistrer le certificat exporté dans un fichier), puis indiquez le nom et l'emplacement du fichier de sauvegarde.
8. Cliquez sur **Enregistrer**.
9. Cliquez sur **Close** (Fermer).

   Le fichier de sauvegarde chiffré est inscrit à l'emplacement spécifié. Il peut à présent être stocké à un emplacement sécurisé pour pouvoir être utilisé en cas d'urgence.

IMPORTANT : le fichier exporté doit être placé sur un support de sauvegarde et conservé en lieu sûr. Le mot de passe utilisé pour chiffrer le fichier doit être mis en mémoire ou stocké en lieu sûr pour veiller à ce qu'il soit disponible en cas de besoin, sans toutefois être accessible à d'autres utilisateurs.

Restauration d'une autorité de certification organisationnelle

Si l'objet Autorité de certification organisationnelle a été supprimé ou altéré, ou si le serveur hôte de l'autorité de certification organisationnelle a connu un échec irrérupérable, le bon fonctionnement de l'autorité de certification organisationnelle peut être restauré à l'aide d'un fichier de sauvegarde créé conformément aux indications de la section « Sauvegarde d'une autorité de certification organisationnelle » page 728.

REMARQUE : si vous n'avez pas pu effectuer une sauvegarde de l'autorité de certification organisationnelle, celle-ci peut toujours être récupérée si NICI 2.*x* est installé sur le serveur et qu'une sauvegarde des informations de configuration NICI a été effectuée.

Pour pouvoir effectuer une restauration complète de l'autorité de certification, il convient de restaurer la base de données CRL ainsi que la base de données de certificats émis à l'aide de la version 9.0 de NetIQ Certificate Server.

Ces deux bases de données se trouvent dans le même répertoire que les fichiers `DIB` eDirectory. Les valeurs par défaut de ces emplacements sont les suivantes :

- Windows : `c:\novell\nds\dibfiles`
- Linux : `/var/opt/novell/edirectory/data/dib`

Ces valeurs par défaut peuvent être modifiées lors de l'installation d'eDirectory.

Les fichiers de restauration de la base de données CRL sont `crl.db`, `crl.01` ainsi que le répertoire `crl.rfl`. Les fichiers de restauration de la base de données d'émission des certificats sont `cert.db`, `cert.lck`, `cert.01` ainsi que le répertoire `cert.rfl`.

Le répertoire `dib` eDirectory doit faire partie d'un plan de sauvegarde standard et régulier.

Pour restaurer l'autorité de certification organisationnelle :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. (Conditionnel) Si l'objet Autorité de certification organisationnelle existe encore, vous devez le supprimer :

   3a Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Supprimer l'objet**.

   3b Recherchez l'objet Autorité de certification organisationnelle, puis cliquez dessus.

   3c Cliquez sur **OK**.
4. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   La boîte de dialogue de création d'un objet Autorité de certification organisationnelle et l'Assistant qui crée cet objet apparaissent.
5. Dans la boîte de dialogue de création, spécifiez le serveur qui doit héberger l'autorité de certification organisationnelle et le nom de l'objet Autorité de certification organisationnelle.
6. Sélectionnez l'option **Importer**.

   Sélectionnez les certificats RSA et ECDSA. NetIQ Certificate Server exige que les deux certificats portent le même nom d'objet.

IMPORTANT : NetIQ Certificate Server ne prend pas en charge l'importation de certificats d'autorité de certification auto-signé externes. Toutefois, il vous permet d'importer les certificats d'autorité de certification subordonnée.

7 Cliquez sur **Suivant**.

8 Dans la boîte de dialogue qui s'ouvre, cliquez sur **Parcourir** et sélectionnez le nom du fichier RSA et ECDSA.

9 Entrez le mot de passe utilisé pour chiffrer le fichier une fois la sauvegarde effectuée.

10 Cliquez sur **OK**.

La clé privée et les certificats de l'autorité de certification organisationnelle ont à présent été restaurés et l'autorité de certification est totalement opérationnelle. Le fichier peut maintenant être enregistré à nouveau pour une utilisation ultérieure.

IMPORTANT : veillez à protéger votre support de sauvegarde.

Déplacement de l'autorité de certification organisationnelle vers un autre serveur

Vous pouvez déplacer votre autorité de certification organisationnelle d'un serveur vers un autre à l'aide des procédures de sauvegarde et de restauration décrites dans les sections « Sauvegarde d'une autorité de certification organisationnelle » page 728 et « Restauration d'une autorité de certification organisationnelle » page 730.

Pour pouvoir procéder au déplacement complet de l'autorité de certification, il convient de déplacer la base de données CRL ainsi que la base de données de certificats émis à l'aide de la version 3.2 ou version ultérieure de NetIQ Certificate Server.

Pour les autres plates-formes, ces deux bases de données se trouvent dans le même répertoire que les fichiers `DIB` eDirectory. Les valeurs par défaut de ces emplacements sont les suivantes :

- Windows : `c:\novell\nds\dibfiles`
- Linux : `/var/opt/novell/edirectory/data/dib`

Ces valeurs par défaut peuvent être modifiées lors de l'installation d'eDirectory.

Les fichiers à déplacer pour la base de données CRL sont `crl.db`, `crl.01` ainsi que le répertoire `crl.rfl`. Les fichiers à déplacer pour la base de données d'émission des certificats sont `cert.db`, `cert.lck`, `cert.01` ainsi que le répertoire `cert.rfl`.

1 Vérifiez que l'autorité de certification organisationnelle fonctionne.

2 Sauvegardez l'autorité de certification organisationnelle.

3 Exportez les clés de l'autorité de certification.

4 Supprimez l'objet Autorité de certification organisationnelle.

5 Arrêtez eDirectory sur les deux serveurs.

6 Copiez les fichiers `cert` et `crl` à partir de la source sur le serveur cible, y compris les journaux `rfl`.

7 Démarrez eDirectory sur les deux serveurs.

8 Recréez l'autorité de certification organisationnelle sur le serveur cible.

IMPORTANT : veillez à protéger votre support de sauvegarde.

Validation des certificats de l'autorité de certification organisationnelle

Si vous suspectez la présence d'un problème avec un certificat ou que vous pensez qu'il n'est peut-être plus valide, vous pouvez facilement le valider à l'aide d'iManager. Tous les certificats de l'arborescence eDirectory peuvent être validés, y compris ceux émis par des autorités de certification externes.

Le processus de validation des certificats comprend plusieurs vérifications des données contenues dans le certificat, ainsi que des données de la chaîne de certificats. Une chaîne de certificats est constituée d'un certificat d'autorité de certification racine et, éventuellement, de certificats d'une ou plusieurs autorités de certification intermédiaires.

Un résultat indiquant Valide signifie que tous les certificats de la chaîne se sont révélés valides. Les certificats sont considérés comme valides s'ils répondent à un certain nombre de critères prédéfinis. Ainsi, leur période de validité ne doit pas avoir expiré, ils ne doivent pas avoir été révoqués et ils doivent avoir été signés par une autorité de certification approuvée. Seuls les certificats avec une extension de point de distribution CRL ou une extension AIA OCSP sont vérifiés pour la révocation.

Un résultat indiquant Non valide signifie qu'un ou plusieurs certificats de la chaîne se sont révélés non valides ou que leur validité n'a pas pu être déterminée. Des informations supplémentaires sont fournies pour ces certificats et notamment quel certificat est considéré comme non valide et pourquoi. Cliquez sur **Aide** pour plus d'informations sur le motif.

Pour valider un certificat :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).
4. Cliquez sur **Certificates** (Certificats), puis sélectionnez le certificat de clé publique ou le certificat auto-signé.
5. Cliquez sur **Validate** (Valider).

   L'état du certificat est indiqué dans le champ **Certificate Status** (État du certificat). Si le certificat n'est pas valide, un motif est indiqué.
6. Cliquez sur **OK**.

Suppression d'une autorité de certification organisationnelle

La suppression d'un objet Autorité de certification organisationnelle ne doit être effectuée qu'en cas d'absolue nécessité ou si vous restaurez l'autorité de certification organisationnelle à partir d'une sauvegarde (reportez-vous à la section « Restauration d'une autorité de certification organisationnelle » page 730). La seule méthode sécurisée pour supprimer l'objet est de commencer par le sauvegarder pour pouvoir le restaurer par la suite.

Toutefois, il arrive parfois que l'autorité de certification organisationnelle doivent être supprimée, et non restaurée. Par exemple, lorsque vous fusionnez des arborescences, la nouvelle arborescence ne peut contenir qu'une seule autorité de certification organisationnelle ; l'autre doit être supprimée.

Ou, lorsque le serveur hébergeant l'autorité de certification organisationnelle est endommagé et irréparable et qu'aucune sauvegarde de l'autorité de certification ou de la configuration NICI n'a été effectuée, la seule option consiste à supprimer l'autorité de certification et à recommencer.

Pour supprimer l'objet Autorité de certification organisationnelle :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Sauvegardez le certificat auto-signé sans la clé privée.
4. Créez un certificat de racine approuvée à l'aide du certificat auto-signé dans le conteneur CN=trusted roots.CN=security. Pour plus d'informations, reportez-vous à la section
5. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Supprimer l'objet**.
6. Recherchez l'objet Autorité de certification organisationnelle, puis cliquez dessus.
7. Cliquez sur **OK**.

Déploiement d'une autorité de certification organisationnelle

Les deux problèmes importants qui doivent être pris en compte lors du remplacement des certificats de l'autorité de certification organisationnelle (CA) sont les suivants :

- les types de certificats gérés ;
- le motif de remplacement de l'autorité de certification.

Les objets Certificat de serveur (objets Matériel clé) contiennent un certificat de clé publique pour le serveur et le certificat de racine approuvée avec lequel a été signé le certificat de clé publique. Les certificats utilisateur sont stockés en tant qu'attributs sous l'objet Utilisateur et ne sont pas associés à la racine approuvée qui les a signés. Par conséquent, lors du remplacement du certificat de racine approuvée, les certificats de serveur restent valides, car la racine approuvée est toujours accessible. En revanche, les certificats utilisateur perdent immédiatement leur validité, sauf si le certificat de racine approuvée se trouve dans le conteneur de racines approuvées, auquel cas il pourra être localisé à des fins de validation.

L'autorité de certification peut être remplacée pour trois raisons :

- L'autorité de certification est arrivée au terme de sa durée de validité. (L'autorité de certification arrive à expiration.)
- L'autorité de certification a été endommagée.
- Vous souhaitez remplacer le certificat de l'autorité de certification pour une raison quelconque (vous souhaitez une clé plus puissante, une stratégie de sécurité l'exige, vous souhaitez une signature par une autorité de certification externe, etc.).

Si l'autorité de certification expire, les certificats signés par cette autorité de certification vont expirer eux aussi. Une fois l'autorité de certification remplacée, chacun des certificats signés doit être recréé à l'aide de la nouvelle autorité.

Si l'autorité de certification a été endommagée, son remplacement entraîne la perte de validité des certificats utilisateur signés par l'ancienne autorité. Vous pouvez facilement les remplacer en exécutant la tâche de création des certificats par défaut dans iManager. Tous les certificats créés par défaut par Certificate Server sont recréés avec la nouvelle autorité de certification. Tous les certificats

créés de manière personnalisée doivent être recréés manuellement avec la nouvelle autorité de certification. Pour plus d'informations sur la création de certificats par défaut, reportez-vous à la section « Création d'objets Certificat de serveur par défaut » page 735.

Si vous souhaitez recréer l'autorité de certification pour toute autre raison, le stockage du certificat de racine approuvée dans le conteneur de racines approuvées maintient la validité des certificats utilisateur jusqu'à ce que vous puissiez les recréer à votre convenance.

Pour remplacer le certificat de racine approuvée :

1. Sauvegardez l'autorité de certification actuelle si vous souhaitez la récupérer par la suite.
2. Exportez le certificat de racine approuvée utilisé pour créer les certificats. Dans les anciens systèmes, il s'agit très probablement du certificat auto-signé.

   Récemment, la possibilité de faire signer le certificat par une autorité de certification externe a été ajoutée. En cas de signature par une autorité de certification externe, exportez le certificat de clé publique. Tous les certificats de la chaîne doivent disposer de leur propre objet dans le conteneur de racines approuvées.

   Si l'autorité de certification n'a pas été endommagée, créez un certificat de racine approuvée dans le conteneur de racines approuvées. De cette façon, les certificats utilisateur restent valides jusqu'à leur remplacement.
3. Supprimez l'ancienne autorité de certification organisationnelle. Pour plus d'informations sur la suppression d'une autorité de certification organisationnelle, reportez-vous à la section « Suppression d'une autorité de certification organisationnelle » page 732.
4. Créez une nouvelle autorité de certification. Pour plus d'informations sur la création d'une autorité de certification organisationnelle, reportez-vous à la section « Création d'un objet Autorité de certification organisationnelle » page 725.
5. Au besoin, recréez les certificats de serveur à l'aide de la tâche de création de certificats par défaut dans iManager. Pour plus d'informations sur la création de certificats par défaut via iManager, reportez-vous à la section « Création d'objets Certificat de serveur par défaut » page 735.

   Recréez les autres certificats de serveur qui ne sont pas générés par défaut.
6. Au besoin, recréez les certificats utilisateur à l'aide de la tâche de création de certificats utilisateur dans iManager ou en affichant les propriétés de l'utilisateur, en affichant les certificats, puis cliquez sur **Nouveau**.

Tâches concernant l'objet Certificat de serveur

- « Création d'objets Certificat de serveur » page 735
- « Création d'objets Certificat de serveur par défaut » page 735
- « Importation d'un certificat de clé publique dans un objet Certificat de serveur » page 736
- « Exportation d'un certificat de racine approuvée ou d'un certificat de clé publique » page 737
- « Suppression d'un objet Certificat de serveur » page 738
- « Affichage des propriétés d'un objet Certificat de serveur » page 738
- « Affichage des propriétés du certificat de clé publique d'un objet Certificat de serveur » page 739
- « Affichage des propriétés du certificat de racine approuvée d'un objet Certificat de serveur » page 739
- « Sauvegarde d'un objet Certificat de serveur » page 740
- « Restauration d'un objet Certificat de serveur » page 741

- « Objets Certificat de serveur et mise en grappe » page 742
- « Validation d'un certificat de serveur » page 742
- « Révocation d'un certificat de racine approuvée ou auto-signé » page 743
- « Déplacement d'un objet Certificat de serveur vers un autre serveur » page 743
- « Remplacement du matériel de codage par clé d'un objet Certificat de serveur » page 744

Création d'objets Certificat de serveur

Cette tâche est décrite à la section « Création d'un objet Certificat de serveur » page 720.

Création d'objets Certificat de serveur par défaut

Le programme d'installation de Certificate Server crée des objets Certificat de serveur par défaut.

- SSL CertificateDNS - *nom_serveur*
- Un certificat pour chaque adresse IP configurée sur le serveur (IPAG *xxx.xxx.xxx.xxx* - *nom_serveur*)
- Un certificat pour chaque nom DNS configuré sur le serveur (DNSAG*www.exemple.com* - *nom_serveur*)

REMARQUE : eDirectory ne crée pas automatiquement le certificat SSL CertificateIP. Le nom DNS du certificat SSL contient toutes les adresses IP répertoriées dans le champ Subject Alternative Name (Autre nom de l'objet). Lorsque vous tentez de créer ou de réparer des certificats par défaut à l'aide du plug-in PKI iManager, le certificat SSL CertificateIP n'est pas créé ni réparé par défaut. Toutefois, l'interface de plug-in propose une case à cocher que vous pouvez sélectionner afin de remplacer le comportement par défaut et forcer la création/réparation du certificat SSL CertificateIP.

À partir de la version 9.0 d'eDirectory, les certificats ECDSA sont créés automatiquement si l'autorité de certification organisationnelle dispose d'un certificat ECDSA.

Si ces certificats sont altérés ou non valides pour une raison quelconque, ou si vous souhaitez simplement remplacer les certificats par défaut existants, vous pouvez utiliser l'assistant de création de certificats de serveur par défaut, comme indiqué dans la procédure suivante :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create Default Certificates** (Créer des certificats par défaut).
4. Recherchez et sélectionnez le ou les serveurs pour lesquels vous souhaitez créer des certificats par défaut, puis cliquez sur **Next** (Suivant).
5. Sélectionnez **Yes** (Oui) si vous souhaitez écraser les certificats de serveur par défaut existants ou sélectionnez **No** (Non) si vous souhaitez remplacer les certificats de serveur par défaut existants uniquement s'ils ne sont pas valides.
6. (Single Server only) (Un seul serveur uniquement) Si vous souhaitez utiliser l'adresse IP par défaut existante, sélectionnez cette option. Si vous souhaitez utiliser une autre adresse IP, sélectionnez cette option et spécifiez la nouvelle adresse IP.

7 (Single Server only) (Un seul serveur uniquement) Si vous souhaitez utiliser l'adresse DNS existante, sélectionnez cette option. Si vous souhaitez utiliser une autre adresse DNS, sélectionnez cette option et spécifiez la nouvelle adresse DNS.

8 Cliquez sur **Suivant**.

9 Passez en revue la page de résumé, puis cliquez sur **Finish** (Terminer).

Si vous souhaitez mieux contrôler la création de l'objet Certificat de serveur, vous pouvez le créer manuellement. Pour plus d'informations, reportez-vous à la section « Création manuelle d'un objet Certificat de serveur » page 720.

Importation d'un certificat de clé publique dans un objet Certificat de serveur

L'importation d'un certificat de clé publique est effectuée après avoir créé une requête de signature de certificat (CSR) et que l'autorité de certification (CA) vous a renvoyé un certificat de clé publique signé. Cette tâche s'applique lorsque vous avez créé un objet Certificat de serveur à l'aide de l'option personnalisée associée à l'option de signature par une autorité de certification externe.

L'autorité de certification peut renvoyer le certificat de plusieurs manières. En règle générale, l'autorité de certification renvoie un ou plusieurs fichiers contenant chacun un certificat, ou un fichier contenant plusieurs certificats. Ces fichiers peuvent être des fichiers binaires utilisant le chiffrement DER (`.der`, `.cer`, `.crt`, `.p7b`) ou peuvent être des fichiers texte codés au format Base64 (`.cer` ou `.b64`).

Si le fichier contient plusieurs certificats, il doit utiliser le format PKCS#7 pour pouvoir être importé dans un objet Certificat de serveur. En outre, le fichier doit contenir l'ensemble des certificats à importer dans l'objet (le certificat de l'autorité de certification au niveau de la racine, les certificats des autorités de certification de niveau intermédiaire et le certificat de serveur).

Si l'autorité de certification renvoie plusieurs fichiers après signature du certificat, chaque fichier contient un certificat distinct qui doit être importé dans l'objet Certificat de serveur. En présence de plus de deux fichiers (un pour l'autorité de certification à la racine, un ou plusieurs pour les autorités de certification intermédiaires et un pour le certificat de serveur), ces fichiers doivent être regroupés dans un fichier PKCS#7 afin de pouvoir être importés dans un objet Certificat de serveur.

Plusieurs méthodes permettent de créer un fichier PKCS#7. L'une d'entre elles consiste à importer tous les certificats dans Internet Explorer. Une fois importés, le certificat de serveur et tous les certificats de la chaîne peuvent être exportés au format PKCS#7 à l'aide d'Internet Explorer. Pour des informations sur cette procédure, reportez-vous à la section « Autorités de certification externes » page 970.

Certaines autorités de certification ne renvoient pas de certificat d'autorité de certification de niveau racine avec le certificat de serveur. Pour obtenir le certificat d'autorité de certification de niveau racine, contactez directement le fournisseur de l'autorité de certification ou appelez le support technique.

Pour importer les certificats dans un objet Certificat de serveur :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **Server Certificates** (Certificats de serveur).

4 Cliquez sur **Import** (Importer) en regard de l'objet Certificat de serveur que vous souhaitez modifier.

5 Recherchez et sélectionnez le fichier de données du certificat.

6 Recherchez et sélectionnez le fichier de données de la racine approuvée.

   Si tous les certificats sont contenus dans un seul fichier, laissez ce champ vide.

7 Cliquez sur **OK**.

Exportation d'un certificat de racine approuvée ou d'un certificat de clé publique

Il existe différentes raisons d'exporter un certificat dans un fichier :

- un client (tel qu'un navigateur Internet) peut l'utiliser pour vérifier la chaîne de certificats envoyée par une application codée ;
- pour fournir une copie de sauvegarde du fichier.

Vous pouvez exporter le certificat dans deux formats de fichier : codage DER (`.der`) et Base64 (`.b64`). L'extension `.crt` peut également être utilisée pour les certificats au codage DER. L'exportation peut également être effectuée dans le Presse-papiers du système au format Base64 afin que le certificat puisse être collé directement dans une application codée.

Pour exporter un certificat de clé publique ou de racine approuvée :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'utilisateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **Server Certificates** (Certificats de serveur).

4 Sélectionnez l'objet Certificat de serveur configuré pour utiliser l'application en question.

5 Cliquez sur **Exporter**.

   Un assistant s'ouvre et vous aide à exporter le certificat dans un fichier.

6 Utilisez la liste déroulante pour spécifier le certificat à exporter.

7 Choisissez de ne pas exporter la clé privée.

8 Sélectionnez un format d'exportation (binaire DER ou texte Base64), puis cliquez sur **Next** (Suivant).

9 Cliquez sur **Save the exported certificate to a file** (Enregistrer le certificat exporté dans un fichier) et enregistrez le fichier à l'emplacement de votre choix.

10 Cliquez sur **Close** (Fermer) > **Close** >**OK**.

11 Utilisez le fichier selon vos besoins.

   Par exemple, si vous souhaitez installer un certificat de racine approuvée dans un navigateur Internet Explorer, double-cliquez sur le fichier. Cette commande lance un assistant qui va accepter l'autorité de certification en tant que racine approuvée. L'acceptation de l'autorité de certification en tant que racine approuvée signifie que le navigateur accepte automatiquement les connexions SSL avec les services qui utilisent des certificats émis par cette autorité de certification.

Suppression d'un objet Certificat de serveur

Vous devez supprimer un certificat de serveur si vous pensez que la clé privée a été endommagée, si vous ne voulez plus utiliser la paire de clés ou si la racine de l'objet Certificat de serveur n'est plus approuvée.

IMPORTANT : une fois l'objet Certificat de serveur supprimé, vous ne pouvez plus le récupérer à moins d'avoir effectué une sauvegarde au préalable. Avant de supprimer cet objet, assurez-vous qu'il n'est plus nécessaire à aucune application codée. Vous pouvez recréer un objet Certificat de serveur, mais vous devez reconfigurer toutes les applications qui faisaient référence à l'ancien objet.

Pour supprimer un objet Certificat de serveur :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **Server Certificates** (Certificats de serveur).
4. Sélectionnez l'objet Certificat de serveur à supprimer.
5. Cliquez sur **OK** pour supprimer l'objet.

Affichage des propriétés d'un objet Certificat de serveur

Outre les propriétés et les droits eDirectory que vous pouvez visualiser avec tout objet NDS, vous pouvez également afficher les propriétés propres à l'objet Certificat de serveur, notamment celles qui concernent le certificat de clé publique et le certificat de racine approuvée qui lui est associé (le cas échéant).

Pour afficher les propriétés d'un objet Certificat de serveur :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **Server Certificates** (Certificats de serveur).
4. Cliquez sur le surnom de l'objet Certificat de serveur que vous souhaitez afficher.
5. Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.
6. Cliquez sur **Annuler**.

Affichage des propriétés du certificat de clé publique d'un objet Certificat de serveur

Pour afficher les propriétés du certificat de clé publique d'un objet Certificat de serveur :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'utilisateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.<change the navigation>
4. Recherchez et cliquez sur l'objet Certificat de serveur que vous souhaitez afficher.
5. Cliquez sur **OK**.
6. Cliquez sur Certificat de clé publique.
   - Si un certificat de clé publique est installé, la page de propriétés affiche le nom complet avec type de l'objet et de l'émetteur, ainsi que les dates de validité de ce certificat.
   - Si le certificat de clé publique n'a pas encore été installé, la page de propriétés vous l'indique.
7. Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.
8. Pour afficher des informations supplémentaires sur un certificat de clé publique, cliquez sur le surnom du certificat pour afficher la page Détails.

   La page Détails dispose des informations contenues dans le certificat de clé publique.
9. Cliquez sur **Fermer** > **Annuler**.

Affichage des propriétés du certificat de racine approuvée d'un objet Certificat de serveur

Pour afficher les propriétés du certificat de racine approuvée d'un objet Certificat de serveur :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet** <change navigation>.
4. Recherchez et sélectionnez l'objet Certificat de serveur que vous souhaitez afficher.
5. Cliquez sur **OK**.
6. Cliquez sur **Certificat de racine approuvée**.
   - Si un certificat de racine approuvée est installé, la page de propriétés affiche le nom complet avec type de l'objet et de l'émetteur, ainsi que les dates de validité de ce certificat.
   - Si le certificat de racine approuvée n'a pas encore été installé, la page de propriétés vous l'indique.

7 Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.

8 Pour afficher des informations supplémentaires sur un certificat de racine approuvée, cliquez sur le surnom du certificat pour afficher la page Détails.

   La page Détails dispose des informations contenues dans le certificat de racine approuvée.

9 Cliquez sur **Fermer** > **Annuler**.

Sauvegarde d'un objet Certificat de serveur

NetIQ Certificate Server permet de stocker des certificats signés par des autorités de certification tierces dans des objets Certificat de serveur. Souvent, ces certificats sont très coûteux. Malheureusement, si une erreur irrécupérable se produit sur le serveur qui héberge les certificats, l'objet Certificat de serveur devient inutilisable. Pour éviter les désagréments de ce type, vous souhaiterez peut-être sauvegarder les certificats de serveur signés par des autorités de certification externes ainsi que leurs clés privées associées. Ensuite, en cas d'échec, vous pouvez utiliser le fichier de sauvegarde pour restaurer l'objet Certificat de serveur sur n'importe quel serveur de l'arborescence.

Le fichier de sauvegarde contient la clé privée du serveur, un certificat de clé publique, un certificat de racine approuvée et tous les certificats d'autorités de certification intermédiaires. Ces informations sont stockées au format PKCS#12 (également appelé PFX).

Un objet Certificat de serveur doit être sauvegardé lorsqu'il fonctionne correctement.

Pour sauvegarder un objet Certificat de serveur :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.<change navigation>

4 Recherchez et cliquez sur l'objet Certificat de serveur que vous souhaitez sauvegarder.

5 Cliquez sur **OK**.

6 Cliquez sur l'onglet **Certificats**.

7 Cliquez sur le certificat de racine approuvée ou de clé publique. Les deux certificats sont inscrits dans le fichier lors de l'opération de sauvegarde.

8 Cliquez sur **Exporter**.

   Un assistant s'ouvre et vous aide à exporter les certificats dans un fichier.

9 À l'invite vous demandant si vous souhaitez exporter la clé privée, cliquez sur **Yes** (Oui), puis cliquez sur **Next** (Suivant).

10 Indiquez un mot de passe de 6 caractères alphanumériques ou plus à utiliser pour le chiffrement du fichier PFX.

11 Cliquez sur **Suivant**.

12 Cliquez sur **Save the exported certificate to a file** (Enregistrer le certificat exporté dans un fichier). Sélectionnez le nom et l'emplacement du fichier de sauvegarde.

13 Cliquez sur **Close** (Fermer).

Le fichier de sauvegarde chiffré est inscrit à l'emplacement spécifié. Il peut à présent être stocké à un emplacement sécurisé pour pouvoir être utilisé en cas d'urgence.

IMPORTANT : le fichier exporté doit être placé sur un support de sauvegarde et conservé en lieu sûr. Le mot de passe utilisé pour chiffrer le fichier doit être mis en mémoire ou stocké dans un coffre-fort pour veiller à ce qu'il soit disponible en cas de besoin, sans toutefois être accessible à d'autres utilisateurs.

Restauration d'un objet Certificat de serveur

Si l'objet Certificat de serveur a été supprimé ou altéré, ou si le serveur qui hébergeait l'objet Certificat de serveur a connu un échec irrécupérable, le bon fonctionnement de l'objet peut être restauré à l'aide d'un fichier de sauvegarde créé conformément aux indications de la section « Sauvegarde d'un objet Certificat de serveur » page 740.

Si vous n'avez pas pu effectuer une sauvegarde de l'objet Certificat de serveur, vous pourrez peut-être néanmoins toujours l'utiliser si NICI 2.x est installé sur le serveur et qu'une sauvegarde des informations de configuration NICI a été effectuée. Pour plus d'informations sur la procédure de sauvegarde et de restauration des fichiers de configuration NICI, reportez-vous à la section Backing Up and Restoring NICI (https://www.netiq.com/documentation/nici27x/nici_admin_guide/data/bwf6d4c.html) (Sauvegarde et restauration de NICI) du *Novell International Cryptographic Infrastructure Administration Guide* (Guide d'administration de Novell International Cryptographic Infrastructure).

Pour restaurer l'objet Certificat de serveur :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Supprimez l'ancien objet Certificat de serveur.

4 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create Server Certificate** (Créer un certificat de serveur).

L'assistant de création d'un Certificat de serveur s'ouvre et crée l'objet.

5 Dans l'assistant, spécifiez le serveur devant détenir l'objet Certificat de serveur, et indiquez le surnom du certificat du certificat de serveur. La version 2.21 ou version ultérieure de Certificate Server doit être installée et en cours d'exécution sur le serveur.

6 Sélectionnez l'option **Import** (Importer), puis cliquez sur **Next** (Suivant).

7 Recherchez et sélectionnez le fichier de sauvegarde, entrez le mot de passe du fichier, puis cliquez sur **Finish** (Terminer).

La clé privée et les certificats du serveur ont à présent été restaurés et l'objet Certificat de serveur est totalement opérationnel. Si vous le souhaitez, le fichier de sauvegarde peut rester stocké pour une utilisation ultérieure.

IMPORTANT : veillez à protéger votre support de sauvegarde.

Objets Certificat de serveur et mise en grappe

Vous pouvez configurer des objets Certificat de serveur dans un environnement en grappe pour vous assurer que vos applications codées qui utilisent des objets Certificat de serveur puissent toujours y accéder. La fonction de sauvegarde et de restauration des objets Certificat de serveur vous permet de dupliquer le matériel de codage par clé de l'objet d'un noeud de la grappe sur tous les noeuds. Ce processus de codage par clé du matériel signé par une autorité de certification externe vous permet d'économiser de l'argent en vous permettant de dupliquer le matériel de codage pour un certificat de serveur, plutôt que d'exiger du nouveau matériel de codage pour chaque noeud de la grappe.

Pour configurer le fonctionnement des certificats de serveur dans un environnement en grappe :

1. Créez un certificat de serveur sur un serveur de la grappe, à l'aide de l'autorité de certification organisationnelle ou d'une autorité de certification externe de votre choix. Reportez-vous à la « Création d'un objet Certificat de serveur » page 720.

   Lorsque vous créez des objets Certificat de serveur, la partie nom commun (CN) du nom de l'objet du certificat doit être un nom DNS ou l'adresse IP spécifique du service. À défaut, vous recevez un message d'avertissement du navigateur indiquant que le nom DNS ou l'adresse IP dans l'URL ne correspond pas à celui mentionné dans le certificat.

   Si différents services ont des adresses IP ou des noms DNS qui diffèrent, vous devez créer un certificat de serveur pour chaque service.

2. Sauvegardez le matériel de codage par clé pour cet objet Certificat de serveur et restaurez-le en créant un objet Certificat de serveur avec le même nom de paire de clés que celui que vous avez créé à l'Étape 1 sur tous les autres serveurs de la grappe.

   Reportez-vous à la section « Sauvegarde d'un objet Certificat de serveur » page 740.

Validation d'un certificat de serveur

Si vous suspectez la présence d'un problème avec un certificat ou que vous pensez qu'il n'est peut-être plus valide, vous pouvez facilement le valider à l'aide d'iManager. Tous les certificats de l'arborescence eDirectory peuvent être validés, y compris ceux émis par des autorités de certification externes.

Le processus de validation des certificats comprend plusieurs vérifications des données contenues dans le certificat, ainsi que des données de la chaîne de certificats. Une chaîne de certificats est constituée d'un certificat d'autorité de certification racine et, éventuellement, de certificats d'une ou plusieurs autorités de certification intermédiaires.

Un résultat indiquant Valide signifie que tous les certificats de la chaîne se sont révélés valides. Les certificats sont considérés comme valides s'ils répondent à un certain nombre de critères prédéfinis. Ainsi, leur période de validité ne doit pas avoir expiré, ils ne doivent pas avoir été révoqués et ils doivent avoir été signés par une autorité de certification approuvée. Seuls les certificats avec une extension de point de distribution CRL ou une extension AIA OCSP sont vérifiés pour la révocation.

Un résultat indiquant Non valide signifie qu'un ou plusieurs certificats de la chaîne se sont révélés non valides ou que leur validité n'a pas pu être déterminée. Des informations supplémentaires sont fournies pour ces certificats et notamment quel certificat est considéré comme non valide et pourquoi. Cliquez sur Aide pour plus d'informations sur le motif.

Pour valider un certificat :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **Server Certificates** (Certificats de serveur).

4 Sélectionnez l'objet Certificat de serveur à valider.

5 Cliquez sur **Validate** (Valider).

L'état du certificat est indiqué dans le champ **Certificate Status** (État du certificat). Si le certificat n'est pas valide, un motif est indiqué.

Révocation d'un certificat de racine approuvée ou auto-signé

Il est parfois nécessaire de révoquer un certificat si la clé ou l'autorité de certification est endommagée, si le certificat a été remplacé par un autre, s'il a été supprimé de la liste de révocation, s'il a cessé de fonctionner, etc.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

4 Recherchez et cliquez sur l'objet Certificat de serveur que vous souhaitez modifier.

5 Cliquez sur **OK**.

6 Cliquez sur l'onglet **Certificats**.

7 Cliquez sur **Certificat de racine approuvée** ou **Certificat auto-signé**.

8 Sélectionnez le certificat, puis cliquez sur **Révoquer**.

L'assistant de révocation du certificat démarre. Suivez les instructions à l'écran pour révoquer le certificat.

9 Cliquez sur **Finish** (Terminer).

Déplacement d'un objet Certificat de serveur vers un autre serveur

Vous pouvez déplacer un objet Certificat de serveur d'un serveur vers un autre à l'aide des procédures de sauvegarde et de restauration décrites dans les sections « Sauvegarde d'un objet Certificat de serveur » page 740 et « Restauration d'un objet Certificat de serveur » page 741.

1 Vérifiez que l'objet Certificat de serveur fonctionne.

2 Sauvegardez l'objet Certificat de serveur.

3 Restaurez l'objet Certificat de serveur sur le serveur de votre choix.

IMPORTANT : veillez à protéger votre support de sauvegarde.

Remplacement du matériel de codage par clé d'un objet Certificat de serveur

La clé privée et les certificats de l'objet Certificat de serveur peuvent être remplacés. Ils ne doivent toutefois être remplacés qu'à l'aide d'un fichier PFX généré en interne, créé au cours d'une sauvegarde d'un objet Certificat de serveur. Les fichiers PFX générés en externe peuvent aussi être utilisés s'ils contiennent la clé privée, le certificat de serveur et la chaîne de certificats entière. La clé et les certificats dans le fichier ne doivent pas forcément correspondre à ceux qui figurent dans l'objet ; les données dans le fichier écrasent la clé et les certificats de l'objet.

Le remplacement de la clé privée et des certificats de l'objet Certificat de serveur est une opération délicate. Si la clé et les certificats ne correspondent pas exactement à ceux qui figurent dans l'objet, cela revient à supprimer l'objet Certificat de serveur actuel et à en créer un nouveau. Reportez-vous à la section « Sauvegarde d'un objet Certificat de serveur » page 740 pour plus d'informations sur les conséquences de la suppression de l'objet.

Si la clé et les certificats correspondent à ceux de l'objet, le remplacement du matériel de codage par clé n'a aucun effet, si ce n'est de régénérer quelques attributs utilisés par les services d'authentification sécurisée.

Pour remplacer le matériel de codage par clé de l'objet Certificat de serveur :

1. Par mesure de précaution, sauvegardez l'objet Certificat de serveur ainsi que la clé privée. Reportez-vous à la section « Sauvegarde d'un objet Certificat de serveur » page 740.
2. Lancez iManager.
3. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
4. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
5. Recherchez et sélectionnez l'objet Certificat de serveur que vous souhaitez modifier.
6. Cliquez sur **OK**.
7. Cliquez sur l'onglet **Certificats**.
8. Cliquez sur **Certificat de racine approuvée** ou **Certificat auto-signé**.

   L'opération peut être démarrée à partir de ces deux pages. Elle remplace les deux certificats, ainsi que la clé privée et tous les autres certificats de la chaîne de certificats.
9. Sélectionnez le certificat, puis cliquez sur **Remplacer**.

   Un assistant s'ouvre et vous aide à spécifier le fichier (de sauvegarde) PFX.
10. Recherchez et sélectionnez le fichier de sauvegarde, entrez le mot de passe du fichier, puis cliquez sur **OK**.

La clé privée et les certificats du serveur ont à présent été remplacés et le certificat de serveur est totalement opérationnel. Le fichier de sauvegarde doit rester stocké pour une utilisation ultérieure.

IMPORTANT : veillez à protéger votre support de sauvegarde.

Tâches relatives au certificat utilisateur

- « Création de certificats utilisateur » page 745
- « Création groupée de certificats utilisateur » page 745

- « Importation d'un certificat de clé publique dans un objet Utilisateur (avec ou sans clé privée) » page 745
- « Affichage des propriétés d'un certificat utilisateur » page 746
- « Exportation d'un certificat utilisateur » page 747
- « Exportation d'un certificat utilisateur et de la clé privée » page 747
- « Validation d'un certificat utilisateur » page 748
- « Révocation d'un certificat utilisateur » page 749
- « Suppression d'un certificat utilisateur et de la clé privée » page 749

Création de certificats utilisateur

Cette tâche est décrite à la section « Création d'un certificat utilisateur » page 721.

Création groupée de certificats utilisateur

Cette fonction vous permet de créer des certificats utilisateur pour plusieurs utilisateurs simultanément, à l'aide d'une série d'opérations.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create User Certificate** (Créer un certificat utilisateur).

   Un assistant s'ouvre et vous aide à créer le certificat utilisateur.
4. Recherchez et sélectionnez tous les utilisateurs pour lesquels vous souhaitez créer un certificat.
5. Suivez les instructions de l'assistant pour créer le certificat pour chaque utilisateur. Pour obtenir des informations précises sur les pages de l'assistant, cliquez sur **Aide**.

Importation d'un certificat de clé publique dans un objet Utilisateur (avec ou sans clé privée)

Vous pouvez importer un certificat de clé publique dans un objet Utilisateur (par exemple, un certificat signé par une autorité de certification tierce). Ce certificat peut utiliser l'un des deux types de fichiers suivants :

- **DER :** contient un certificat de clé publique uniquement.
- **PFX ou PKCS#12 :** contient un certificat de clé publique et une clé privée.

Une fois importé, le certificat est stocké dans l'objet Utilisateur et apparaît dans la liste des certificats disponibles.

REMARQUE : lorsque vous importez un certificat PKCS#12, seules la clé publique et la clé privée sont stockées dans l'objet Utilisateur. Aucun autre certificat n'est stocké. Les autres certificats de la chaîne de certificats de l'utilisateur doivent probablement être stockés dans le conteneur CN=Trusted Roots.CN=Security (créez un nouvel objet Racine approuvée pour chaque certificat de la chaîne).

Pour importer un certificat de clé publique dans un objet Utilisateur :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).
4. Recherchez et sélectionnez un objet Utilisateur dans lequel importer le certificat de clé publique.
5. Cliquez sur **Nouveau**.
6. Indiquez un surnom pour le certificat utilisateur.

   Celui-ci doit être unique et doit vous permettre d'identifier le certificat facilement. Vous pouvez entrer jusqu'à 64 caractères dans le champ **Certificate Nickname** (Surnom du certificat).
7. Sélectionnez la méthode de création de l'importation, puis cliquez sur **Next** (Suivant).
8. Recherchez et sélectionnez le certificat à importer, puis cliquez sur **OK**.
9. (Conditionnel) Si vous importez un certificat avec une clé privée, entrez le mot de passe pour la clé privée, puis cliquez sur **Next** (Suivant).
10. Cliquez sur **Finish** (Terminer).

    Le certificat est alors stocké dans l'objet Utilisateur et s'affiche dans la liste des certificats disponibles pour cet utilisateur.

Affichage des propriétés d'un certificat utilisateur

Outre les droits et propriétés eDirectory qui peuvent être affichées avec n'importe quel objet eDirectory, vous pouvez également afficher les propriétés spécifiques du certificat utilisateur et notamment l'émetteur, l'état du certificat, l'état de la clé privée ainsi que la période de validité.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).
4. Recherchez et sélectionnez un objet Utilisateur dont vous souhaitez afficher les propriétés de certificat.
5. Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.
6. Cliquez sur le surnom du certificat pour afficher ses détails.
7. Cliquez sur **Close** (Fermer) lorsque vous avez terminé de les consulter.

Exportation d'un certificat utilisateur

Pour échanger des courriers électroniques en toute sécurité avec une autre personne, vous devez d'abord disposer du certificat de clé publique de cet utilisateur. L'une des manières de l'obtenir consiste à l'exporter à l'aide d'iManager. Ce certificat peut également être obtenu à l'aide de LDAP ou par courrier électronique.

Pour exporter votre certificat de clé publique personnel ou celui de tout autre utilisateur :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).
4. Recherchez et sélectionnez un objet Utilisateur dont vous souhaitez exporter le certificat.
5. Sélectionnez le certificat, puis cliquez sur **Export** (Exporter).

   Un assistant s'ouvre et vous aide à exporter le certificat utilisateur dans un fichier. Si vous êtes connecté sous l'identité de l'utilisateur qui détient le certificat, sélectionnez **No** (No) lorsque le système vous demande si vous souhaitez exporter la clé privée. Reportez-vous à la section « Exportation d'un certificat utilisateur et de la clé privée » page 747.
6. Si vous souhaitez exporter la clé privée, sélectionnez **Export private key** (Exporter la clé privée) et indiquez un mot de passe pour la protéger.
7. Sélectionnez un format d'exportation si vous n'exportez pas la clé privée, puis cliquez sur **Next** (Suivant).
8. Cliquez sur **Save the exported certificate to a file** (Enregistrer le certificat exporté dans un fichier) et enregistrez le fichier à l'emplacement de votre choix.
9. Cliquez sur **Close** (Fermer) > **Close**.

Exportation d'un certificat utilisateur et de la clé privée

Pour pouvoir utiliser un certificat à des fins d'échange de courriers électroniques, d'authentification ou de chiffrement sécurisés, la clé privée et le certificat doivent être disponibles dans l'application codée. Vous devez exporter le certificat utilisateur et la clé privée et les placer à un emplacement accessible par l'application afin que l'application puisse les utiliser.

Les clés privées de l'objet Utilisateur appartiennent à cet utilisateur. Seul un utilisateur connecté sous l'identité de cet utilisateur peut exporter la clé privée. Aucun autre utilisateur, pas même l'administrateur réseau, n'est autorisé à exporter la clé privée d'un autre utilisateur.

Pour exporter votre clé privée personnelle et le certificat :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'utilisateur propriétaire du certificat.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).
4. Recherchez et sélectionnez un objet Utilisateur dont vous souhaitez exporter le certificat.

5 Sélectionnez le certificat, puis cliquez sur **Export** (Exporter).

   Un assistant s'ouvre et vous aide à exporter le certificat utilisateur dans un fichier.

6 Sélectionnez **Export private key** (Exporter la clé privée), indiquez un mot de passe pour protéger la clé privée, puis cliquez sur **Next** (Suivant).

7 (Facultatif) Cliquez sur **Export the Certificate into the Browser** (Exporter le certificat dans le navigateur).

8 Cliquez sur **Close** (Fermer) > **Close**.

   Le fichier chiffré est inscrit à l'emplacement spécifié. Il peut à présent être importé dans une application codée.

IMPORTANT : le fichier exporté peut être conservé à des fins de sauvegarde. Dans ce cas, il doit être conservé en lieu sûr. Le mot de passe utilisé pour chiffrer le fichier doit être mis en mémoire ou stocké en lieu sûr pour veiller à ce qu'il soit disponible en cas de besoin, sans toutefois être accessible à d'autres utilisateurs.

Validation d'un certificat utilisateur

Si vous suspectez la présence d'un problème avec un certificat ou que vous pensez qu'il n'est peut-être plus valide, vous pouvez facilement le valider à l'aide d'iManager. Tous les certificats de l'arborescence eDirectory peuvent être validés, y compris ceux émis par des autorités de certification externes.

Le processus de validation des certificats comprend plusieurs vérifications des données contenues dans le certificat, ainsi que des données de la chaîne de certificats. Une chaîne de certificats est constituée d'un certificat d'autorité de certification racine et, éventuellement, de certificats d'une ou plusieurs autorités de certification intermédiaires.

Un résultat indiquant Valide signifie que tous les certificats de la chaîne se sont révélés valides. Les certificats sont considérés comme valides s'ils répondent à un certain nombre de critères prédéfinis. Ainsi, leur période de validité ne doit pas avoir expiré, ils ne doivent pas avoir été révoqués et ils doivent avoir été signés par une autorité de certification approuvée. Seuls les certificats avec une extension de point de distribution CRL ou une extension AIA OCSP sont vérifiés pour la révocation.

Un résultat indiquant Non valide signifie qu'un ou plusieurs certificats de la chaîne se sont révélés non valides ou que leur validité n'a pas pu être déterminée. Des informations supplémentaires sont fournies dans ce cas pour indiquer quel certificat est considéré comme non valide et pourquoi. Cliquez sur Aide pour plus d'informations sur le motif.

Pour valider un certificat :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).

4 Recherchez et sélectionnez un objet Utilisateur dont vous souhaitez valider le certificat.

5 Sélectionnez le certificat utilisateur à valider.

6 Cliquez sur **Validate** (Valider).

L'état du certificat est indiqué dans le champ **Certificate Status** (État du certificat). Si le certificat n'est pas valide, un motif est indiqué.

REMARQUE : si le certificat utilisateur a été signé par une autorité de certification tierce, pour que la validation réussisse, la chaîne de certificats doit se trouver dans le conteneur de racines approuvées du conteneur de sécurité (CN=Trusted Roots.CN=Security). En règle générale, la chaîne de certificats se compose d'une seule autorité de certification au niveau de la racine ou combine une autorité de certification intermédiaire et une autorité de certification racine. Le nom du conteneur de racines approuvées doit être Trusted Roots et chaque certificat de la chaîne doit être stocké dans son propre objet Racine approuvée. Pour obtenir des instructions sur la création d'un conteneur de racines approuvées et d'objets Racine approuvée, reportez-vous aux sections « Création d'un conteneur de racines approuvées » page 722 et « Création d'un objet Racine approuvée » page 722.

Lors de la validation de certificats utilisateur ou de certificats d'autorité de certification intermédiaires signés par des autorités de certification externes, le certificat de l'autorité de certification externe doit être stocké dans un objet Racine approuvée pour que la validation réussisse. L'objet Racine approuvée doit se trouver dans un conteneur de racines approuvées nommé Trusted Roots et doit se trouver dans le conteneur de sécurité.

Révocation d'un certificat utilisateur

Il est parfois nécessaire de révoquer un certificat si la clé ou l'autorité de certification est endommagée, si le certificat a été remplacé par un autre, s'il a été supprimé de la liste de révocation, s'il a cessé de fonctionner, etc.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).

4 Recherchez et sélectionnez un objet Utilisateur dont vous souhaitez valider le certificat.

5 Sélectionnez le certificat utilisateur à révoquer.

6 Cliquez sur **Révoquer**.

L'assistant de révocation du certificat démarre. Suivez les instructions à l'écran pour révoquer le certificat.

7 Cliquez sur **Finish** (Terminer).

Suppression d'un certificat utilisateur et de la clé privée

Si un certificat utilisateur n'est plus valide ou si vous pensez que la clé privée a été endommagée d'une quelconque façon, vous devrez peut-être supprimer le certificat utilisateur et la clé privée.

Avant de supprimer un certificat utilisateur et sa clé privée, vous devez révoquer le certificat utilisateur. Reportez-vous à la section « Révocation d'un certificat utilisateur » page 749.

Pour supprimer un certificat utilisateur et sa clé privée :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant que propriétaire du certificat ou d'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ) > **User Certificates** (Certificats utilisateur).
4. Recherchez et sélectionnez un objet Utilisateur dont vous souhaitez supprimer le certificat.
5. Sélectionnez le certificat utilisateur à supprimer.
6. Cliquez sur **Supprimer**.

Auto-provisioning du certificat X.509

Cette section décrit la fonction d'auto-provisioning X.509.

- « Présentation » page 750
- « Auto-provisioning des utilisateurs » page 751
- « Auto-provisioning du serveur » page 752
- « Auto-provisioning et tâche d'émission du certificat » page 753

Présentation

Lorsque vous créez un certificat X.509, de nombreuses informations importantes doivent être identifiées et vérifiées avant que l'autorité de certification (CA) émette le certificat. Les deux principales tâches sont les suivantes :

- La vérification de l'identité de l'objet du certificat (vérification de l'identité de la personne ou de l'objet à qui le certificat est destiné).
- La vérification de l'adéquation du nom d'objet du certificat (opération visant à vérifier que le nom d'objet est conforme à l'identité de la personne ou correspond à l'objet à qui le certificat est destiné).

Ces deux tâches peuvent durer très longtemps et sont souvent effectuées par un administrateur ou un groupe distinct.

NetIQ Certificate Server a toujours tiré parti des fonctionnalités de gestion sécurisée des identités d'eDirectory afin de réduire le temps et les efforts nécessaires à l'exécution de ces vérifications. iManager permet à un administrateur de créer des certificats utilisateur en bloc ; autrement dit, créer un certificat pour un grand nombre d'utilisateurs simultanément. L'autorité de certification vérifie que l'identité du certificat est liée au compte eDirectory, qui vérifie l'identité de l'objet du certificat. Toutefois, l'autorité de certification n'a pas vérifié l'adéquation du nom d'objet dans le certificat. De ce fait, la création de certificats avec NetIQ Certificate Server a toujours exigé que le logiciel ou la personne dispose des droits d'administrateur sur l'autorité de certification organisationnelle.

L'auto-provisioning permet à un utilisateur ou à un serveur de générer des certificats sans disposer de droits d'administrateur sur l'autorité de certification organisationnelle et sans intervention d'un administrateur ou d'un groupe chargé de l'administration, tout en préservant la sécurité de l'autorité de certification.

NetIQ Certificate Server vérifie l'identité de l'objet du certificat en vérifiant que l'identité du certificat est liée au compte eDirectory. L'autorité de certification permet vérifie également la conformité du nom de l'objet dans le certificat en le comparant aux informations dans eDirectory. L'autorité de certification organisationnelle parvient ainsi à tirer parti des fonctions sécurisées de gestion des identités d'eDirectory afin de réduire les tâches administratives tout en préservant la sécurité de l'autorité de certification.

Auto-provisioning des utilisateurs

Par le passé, la création d'un certificat utilisateur nécessitait des droits d'administrateur sur l'autorité de certification ainsi que des droits sur les attributs de l'objet Utilisateur. Grâce à l'auto-provisioning des utilisateurs, les droits d'administrateur sur l'autorité de certification ne sont pas nécessaires. Toutefois, les droits de lecture (R) et d'écriture (É) sur les attributs userCertificate, NDSPKI:UserCertificateInfo et SAS:SecretStore sont toujours nécessaires.

Si l'auteur de la requête de création du certificat dispose de droits d'administrateur sur l'autorité de certification, la création du certificat n'est pas affectée par l'activation ou non de l'auto-provisioning des utilisateurs. Si l'auteur de la requête de création du certificat ne dispose pas de droits d'administrateur sur l'autorité de certification, le nom de l'objet dans la requête est comparé avec le nom distinctif eDirectory de l'utilisateur ainsi que toutes les valeurs de l'attribut sasAllowableSubjectNames.

Si le nom d'objet correspond, l'autorité de certification vérifie que les autres noms d'objet sont conformes. Pour ce faire, l'autorité de certification vérifie qu'il n'y a pas plusieurs autres noms d'objet. Si le nom existe, il doit s'agir du type de nom de messagerie et il doit correspondre à un nom de messagerie configuré sur l'objet Utilisateur. Si toutes ces vérifications réussissent, il n'est pas nécessaire de disposer de droits d'administrateur sur l'autorité de certification pour créer le certificat.

Pour utiliser l'auto-provisioning des utilisateurs :

1. Vérifiez qu'eDirectory 9.1 et le plug-in NetIQ Certificate Server 9.1.0 ou version pour iManager sont installés.
2. Activez l'auto-provisioning des utilisateurs.
   - **2a** Lancez iManager.
   - **2b** Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant de droits d'administrateur sur l'autorité de certification organisationnelle.
   - **2c** Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ > Configure Certificate Authority** (Configurer l'autorité de certification).
   - **2d** Sélectionnez **Enable user self-provisioning** (Activer l'auto-provisioning des utilisateurs).
   - **2e** Cliquez sur **OK**.
3. Configurez les droits hérités pour les utilisateurs en activant l'objet « [ceci] » :
   - **3a** Connectez-vous à iManager en tant qu'administrateur de l'application.
   - **3b** Cliquez sur l'icône **Configurer**.
   - **3c** Cliquez sur **Serveur iManager > Configurer iManager**.
   - **3d** Cliquez sur l'onglet **Divers**.
   - **3e** Sélectionnez **Activer "[ceci]"**.
   - **3f** Cliquez sur **Enregistrer**.

     Vous devez ensuite ajouter des droits hérités.
4. Connectez-vous à iManager en tant qu'administrateur de l'autorité de certification.
5. Dans le menu **Rôles et tâches**, cliquez sur **Droits > Modifier les ayants droit**.

6 Recherchez et sélectionnez l'objet dont vous souhaitez que les droits soient hérités (par exemple, la racine de l'arborescence ou un conteneur), puis cliquez sur **OK**.

7 Cliquez sur **Ajouter un ayant droit**, sélectionnez l'objet **« [ceci] »**, puis cliquez sur **OK**.

8 Cliquez sur **Droits assignés**.

9 Cliquez sur **Ajouter une propriété**.

10 Sélectionnez **Afficher toutes les propriétés dans le schéma**.

11 Sélectionnez l'attribut `userCertificate`, puis cliquez sur **OK**.

12 Sélectionnez les droits **Lire** et **Écrire**.

13 Sélectionnez **Hériter**.

14 Répétez les étapes 6 à 10 pour les autres attributs (`NDSPKI:UserCertificateInfo` et `SAS:SecretStore`).

15 Cliquez sur **Terminé > OK**.

Auto-provisioning du serveur

Par le passé, la création d'un certificat de serveur nécessitait des droits d'administrateur sur l'autorité de certification ainsi que sur le contexte dans lequel le certificat de serveur était créé. Grâce à l'auto-provisioning du serveur, les droits d'administrateur sur l'autorité de certification ne sont pas nécessaires. Toutefois, les droits d'administrateur sur le contexte dans lequel le certificat de serveur a été créé sont en revanche toujours nécessaires.

Pour créer le certificat de serveur, vous devez disposer des droits d'administrateur sur l'autorité de certification. La création du certificat n'est pas affectée par l'activation ou non de l'auto-provisioning. Si vous ne disposez pas de droits d'administrateur sur l'autorité de certification, activez l'option **Require read rights to operate the CA** (Exiger des droits de lecture pour faire fonctionner l'autorité de certification) pour que l'autorité de certification puisse être gérée à partir de la tâche le **Configure Certificate Authority** (Configurer l'autorité de certification) dans iManager. Des droits d'administrateur sur l'autorité de certification ne sont pas nécessaires si l'une des conditions suivantes est vraie :

- Le nom de l'objet dans la requête est comparé avec le nom distinctif eDirectory du serveur et toutes les adresses IP ou DNS, telles que déterminées par une recherche SLP dans DNS ou dans eDirectory. Si le nom d'objet correspond à l'un des eux, l'autorité de certification n'exige pas de disposer de droits d'administrateur sur l'autorité de certification pour créer le certificat.
- Les composants non-CN du nom d'objet ne correspondent aux composants non-CN du nom d'objet du certificat de l'autorité de certification.
- L'autre nom d'objet n'a qu'un nom DNS/une adresse IP revérifié par l'autorité de certification par le biais de la recherche DNS inversée.

Les serveurs ne disposent pas, par défaut, de droits d'écriture sur l'attribut **NDSPKI:Private Key** de l'autorité de certification. Si l'option **Require write rights to operate the CA** (Exiger des droits d'écriture pour faire fonctionner l'autorité de certification) est activée dans la tâche **Configure Certificate Authority** (Configurer l'autorité de certification) dans iManager, vous devez accorder aux serveurs des droits d'écriture sur l'attribut **NDSPKI:Private Key** de l'autorité de certification.

REMARQUE : sachez que lorsque la vérification de l'état de santé PKI s'exécute sur un serveur pour lequel l'auto-provisioning est activé, les certificats de votre serveur peuvent être créés automatiquement (s'il n'en existe aucun) ou remplacés (s'ils ont expirés). Pour plus d'informations, reportez-vous à la « Vérification de l'état de santé PKI » page 768.

Pour utiliser l'auto-provisioning du serveur :

1. Vérifiez qu'eDirectory 9.0 et la version 3.2.2 (ou version ultérieure) du plug-in NetIQ Certificate Server pour iManager sont installés.

   eDirectory 8.8 et le plug-in NetIQ Certificate Server 3.2.2 pour iManager sont inclus avec OES 2 et installés automatiquement lorsque vous sélectionnez des composants requis par eDirectory pendant l'installation d'OES 2.

2. Activez l'auto-provisioning du serveur :

   2a. Lancez iManager.

   2b. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant de droits d'administrateur sur l'autorité de certification organisationnelle.

   2c. Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ > Configure Certificate Authority** (Configurer l'autorité de certification).

   2d. Sélectionnez **Enable server self-provisioning** (Activer l'auto-provisioning du serveur).

   2e. Cliquez sur **OK**.

Auto-provisioning et tâche d'émission du certificat

La tâche d'émission du certificat permet de créer un certificat à l'aide d'une requête de signature de certificat PKCS#10. Cette tâche permet à l'utilisateur de créer un certificat non lié à un objet eDirectory. Si l'auteur de la requête de création du certificat dispose de droits d'administrateur sur l'autorité de certification, la création du certificat n'est pas affectée Si l'auteur de la requête de création du certificat ne dispose pas de droits d'administrateur sur l'autorité de certification, la requête de certificat est traitée comme une requête d'auto-provisioning des utilisateurs, mais l'auteur ne doit pas disposer de droits sur les attributs userCertificate, NDSPKI:UserCertificateInfo et SAS:SecretStore pour l'objet. Cela est dû au fait que le certificat n'est pas stocké dans eDirectory, de sorte que les droits sur l'objet ne sont pas nécessaires.

L'auto-provisioning des utilisateurs doit être activé pour que des certificats puissent être émis sans disposer les droits d'administrateur sur l'autorité de certification. Effectuez les étapes 1 à 3 de la section « Auto-provisioning des utilisateurs » page 751.

Pour plus d'informations sur la tâche d'émission d'un certificat, reportez-vous à la section « Émission d'un certificat de clé publique » page 726.

Utilisation des certificats eDirectory avec des applications externes

Certains clients utilisent des applications non-eDirectory qui nécessitent des certificats et des clés X.509 (par exemple, Apache ou OpenSSL). La plupart de ces applications sont configurées et prêtes à l'emploi avec des certificats auto-signés (sans valeur), qui servent uniquement à offrir une solution temporaire jusqu'à ce que l'application puisse être configurée avec les clés et certificats X.509 effectifs.

Malheureusement, nombreux sont les administrateurs à ne pas remplacer ces certificats auto-signés, souvent car cette manipulation prend trop de temps ou est trop compliquée. Qui plus est, les certificats X.509 sont conçus de telle manière à expirer régulièrement, et de ce fait, leur remplacement régulier est une tâche administrative permanente.

Les sections suivantes permettent de résoudre ce problème :

- « Fonctionnalité de vérification de l'état de santé PKI » page 754
- « Configuration de l'objet SAS:Service pour exporter des certificats eDirectory » page 755

Fonctionnalité de vérification de l'état de santé PKI

Pour répondre à la demande des clients de fournir des applications non-eDirectory avec des certificats X.509, le code de vérification de l'état de santé PKI disponible dans NetIQ Certificate Server permet désormais d'exporter automatiquement des clés et les certificats X.509 vers le système de fichiers. De cette façon, les applications non-eDirectory peuvent tirer parti des certificats émanant d'eDirectory et gérés par eDirectory.

Lors de l'exécution de la vérification de l'état de santé PKI, tous les certificats existants sont automatiquement écrasés, y compris leurs clés privées. Toutefois, pour veiller à ce qu'aucun certificat et clés privées valides ne soient supprimées, la vérification de l'état de santé PKI détermine si les clés et certificats existants sont les mêmes que ceux configurés dans eDirectory. S'ils sont différents de ceux configurés dans eDirectory, la vérification de l'état de santé PKI crée une sauvegarde de ces fichiers avant de les écraser. De cette façon, les certificats obtenus auprès d'une source externe (par exemple, VeriSign *) ne sont pas supprimés.

Une fois la configuration créée pour le serveur sur l'objet SAS:Service, les clés et certificats associés au serveur spécifié sont automatiquement exportés vers le système de fichiers. Si les clés et les certificats sont remplacés ou mis à jour dans eDirectory (par exemple, si l'objet Certificat de serveur est supprimé et qu'un nouveau est créé avec le même nom), les nouvelles clés et les nouveaux certificats sont automatiquement exportés vers le système de fichiers lors de la prochaine exécution de vérification de l'état de santé PKI.

REMARQUE : le code de vérification de l'état de santé PKI disponible dans NetIQ Certificate Server s'exécute à chaque chargement/rechargement de NetIQ Certificate Server. Vous pouvez utiliser l'une des méthodes suivantes pour recharger NetIQ Certificate Server :

- Redémarrez le serveur.
- Redémarrez eDirectory.
- Déchargez et chargez le serveur PKI manuellement.
- Exécutez une réparation d'eDirectory (NDSRepair).

  NetIQ Certificate Server s'arrête pendant la réparation et se recharge une fois eDirectory réparé.

Pour plus d'informations sur la vérification de l'état de santé PKI, reportez-vous à la « Vérification de l'état de santé PKI » page 768.

Avant que la vérification de l'état de santé PKI puisse exporter automatiquement les certificats et les clés X.509 vers le système de fichiers, l'objet SAS:Service doit être configuré. En effet, la vérification de l'état de santé PKI lit la configuration de l'objet SAS:Service. Pour plus d'informations sur la configuration de l'objet SAS:Service, reportez-vous à la section « Configuration de l'objet SAS:Service pour exporter des certificats eDirectory » page 755.

Configuration de l'objet SAS:Service pour exporter des certificats eDirectory

Avant de pouvoir exporter un certificat de serveur eDirectory vers le système de fichiers, le serveur doit d'abord être configuré sur l'objet SAS:Service. Cette création de configuration peut être effectuée automatiquement ou manuellement, en fonction du serveur eDirectory que vous utilisez. Les sections suivantes décrivent ces options plus en détail :

- « Configuration manuelle de l'objet SAS:Service pour activer l'utilisation des certificats eDirectory » page 755

Configuration manuelle de l'objet SAS:Service pour activer l'utilisation des certificats eDirectory

Si vous n'utilisez pas OES 2 comme serveur eDirectory, vous devez configurer manuellement l'objet SAS:Service afin d'exporter les certificats eDirectory. Cette configuration doit spécifier le nom du certificat de serveur. Si plusieurs certificats de serveur doivent être exportés, il suffit de créer plusieurs configurations. Vous pouvez exporter le même certificat vers un autre chemin d'accès au fichier ou vous pouvez exporter un autre certificat vers un autre chemin d'accès au fichier.

REMARQUE : pour éviter les conflits de fichier, chaque configuration doit utiliser des chemins de fichier uniques. Les chemins de la clé publique et de la clé privée doivent être uniques et différents l'un de l'autre ainsi que de toute autre configuration.

Pour créer une configuration sur l'objet SAS:Service :

1. Dans iManager, dans la vue **Rôles et tâches**, cliquez sur **NetIQ Certificate Access** (Accès aux certificats NetIQ).
2. Cliquez sur **SAS Service Object** (objet Service SAS).
3. Sur la page de l'objet, cliquez sur l'icône **Parcourir** .
4. Recherchez et sélectionnez l'objet SAS:Service pour lequel vous souhaitez créer une configuration.
5. Cliquez sur l'objet SAS:Service.
6. Cliquez sur **Nouveau**.

   La fenêtre de synchronisation des certificats de serveur s'affiche.
7. Dans le champ **Certificat**, recherchez et sélectionnez le certificat que vous voulez exporter.
8. Dans le champ **Public key path** (Chemin de la clé publique), indiquez le chemin dans lequel l'application pourra trouver et utiliser le certificat. Par exemple : `C:/novell/nds/servercert.pem`.
9. Dans le champ **Private key path** (Chemin de la clé privée), indiquez le chemin dans lequel l'application pourra trouver et utiliser la clé privée du certificat. Par exemple : `C:/novell/nds/serverkey.pem`.
10. Sélectionnez le type de clé que vous allez utiliser. Si vous exécutez OpenSSL, sélectionnez PKCS#8. Si vous exécutez Apache, sélectionnez PKCS#1.
11. Cliquez sur **OK**.

    La configuration est créée. Le nom, le chemin, le chemin de la clé ainsi que le type de clé sont affichés.

Pour créer une autre configuration, répétez la procédure de l'Étape 6 à l'Étape 11.

Si vous utilisez un serveur OES comme serveur pour eDirectory, vous pouvez ensuite configurer automatiquement le serveur afin de créer une configuration sur l'objet SAS:Service.

REMARQUE : si l'utilisation des certificats eDirectory est activée pendant l'installation d'OES 2 (valeur par défaut), le code d'installation crée une configuration pour l'objet SSL CertificateDNS et les certificats et les clés sont exportés vers les fichiers suivants :

fichier de clé - `/etc/ssl/servercerts/serverkey.pem`

fichier de certificat - `/etc/ssl/servercerts/servercert.pem`

Tâches relatives à l'objet Racine approuvée

- « Création d'un conteneur de racines approuvées » page 756
- « Création d'un objet Racine approuvée » page 756
- « Affichage des propriétés d'un objet Racine approuvée » page 756
- « Remplacement d'un certificat de racine approuvée » page 757
- « Validation d'un objet Racine approuvée » page 757
- « Révocation d'un certificat de racine approuvée » page 758

Création d'un conteneur de racines approuvées

Cette tâche est décrite à la section « Création d'un conteneur de racines approuvées » page 722.

Création d'un objet Racine approuvée

Cette tâche est décrite à la section « Création d'un objet Racine approuvée » page 722.

Affichage des propriétés d'un objet Racine approuvée

Outre les droits et propriétés eDirectory qui peuvent être affichés avec n'importe quel objet eDirectory, vous pouvez également afficher les propriétés spécifiques de l'objet Racine approuvée et notamment l'émetteur, l'état du certificat ainsi que la période de validité.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
4. Recherchez et cliquez sur l'objet Racine approuvée que vous souhaitez afficher.
5. Cliquez sur **OK**.
6. Pour afficher la chaîne de certificats, cliquez sur le signe plus (+) en regard du surnom du certificat pour développer la vue.
7. Cliquez sur le surnom du certificat pour afficher ses détails.
8. Cliquez sur **Annuler**.

Remplacement d'un certificat de racine approuvée

Cette tâche vous permet de remplacer un certificat de racine approuvée stocké dans l'objet Racine approuvée. Elle doit être effectuée si le certificat de racine approuvée est arrivé à expiration.

Vous pouvez remplacer un certificat de racine approuvée à partir de la page de propriétés de l'objet Racine approuvée.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
4. Recherchez et cliquez sur l'objet Racine approuvée que vous souhaitez remplacer.
5. Cliquez sur **OK**.
6. Sélectionnez le certificat, puis cliquez sur **Remplacer**.
7. Recherchez et sélectionnez le nouveau certificat de racine approuvée.
8. Cliquez sur **OK**.

Validation d'un objet Racine approuvée

Si vous suspectez la présence d'un problème avec un certificat ou que vous pensez qu'il n'est peut-être plus valide, vous pouvez facilement le valider à l'aide d'iManager. Tous les certificats de l'arborescence eDirectory peuvent être validés, y compris ceux émis par des autorités de certification externes.

Le processus de validation des certificats comprend plusieurs vérifications des données contenues dans le certificat, ainsi que des données de la chaîne de certificats. Une chaîne de certificats est constituée d'un certificat d'autorité de certification racine et, éventuellement, de certificats d'une ou plusieurs autorités de certification intermédiaires.

Un résultat indiquant Valide signifie que tous les certificats de la chaîne se sont révélés valides. Les certificats sont considérés comme valides s'ils répondent à un certain nombre de critères prédéfinis. Ainsi, leur période de validité ne doit pas avoir expiré, ils ne doivent pas avoir été révoqués et ils doivent avoir été signés par une autorité de certification approuvée. Seuls les certificats avec une extension de point de distribution CRL ou une extension AIA OCSP sont vérifiés pour la révocation.

Un résultat indiquant Non valide signifie qu'un ou plusieurs certificats de la chaîne se sont révélés non valides ou que leur validité n'a pas pu être déterminée. Des informations supplémentaires sont fournies dans ce cas pour indiquer quel certificat est considéré comme non valide et pourquoi. Cliquez sur **Aide** pour plus d'informations sur le motif.

Pour valider un certificat de racine approuvée :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.
4. Recherchez et cliquez sur l'objet Racine approuvée que vous souhaitez valider.

5 Cliquez sur **OK**.

6 Sélectionnez le certificat, puis cliquez sur **Valider**.

L'état du certificat est indiqué dans le champ **Certificate Status** (État du certificat). Si le certificat n'est pas valide, un motif est indiqué.

REMARQUE : si le certificat dans l'objet n'est pas auto-signé, pour que la validation réussisse, sa chaîne de certificats doit se trouver dans le conteneur de racines approuvées du conteneur de sécurité (CN=Trusted Roots.CN=Security). En règle générale, la chaîne de certificats se compose d'une seule autorité de certification au niveau de la racine ou combine une autorité de certification intermédiaire et une autorité de certification racine. Le nom du conteneur de racines approuvées doit être Trusted Roots et chaque certificat de la chaîne doit être stocké dans son propre objet Racine approuvée. Pour obtenir des instructions sur la création d'un conteneur de racines approuvées et d'objets Racine approuvée, reportez-vous aux sections « Création d'un conteneur de racines approuvées » page 722 et « Création d'un objet Racine approuvée » page 722.

Révocation d'un certificat de racine approuvée

Il est parfois nécessaire de révoquer un certificat si la clé ou l'autorité de certification est endommagée, si le certificat a été remplacé par un autre, s'il a été supprimé de la liste de révocation, s'il a cessé de fonctionner, etc.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Modifier un objet**.

4 Recherchez et cliquez sur l'objet Racine approuvée que vous souhaitez modifier.

5 Cliquez sur **OK**.

6 Sélectionnez le certificat, puis cliquez sur **Révoquer**.

L'assistant de révocation du certificat démarre. Suivez les instructions à l'écran pour révoquer le certificat.

7 Cliquez sur **Finish** (Terminer).

Tâches relatives aux listes de révocation de certificats

NetIQ Certificate Server fournit un système de gestion des listes de révocation de certificats (CRL). Ce système est facultatif, mais doit être implémenté si vous souhaitez être en mesure de révoquer les certificats créés par l'autorité de certification organisationnelle.

Une liste de révocation de certificats est une liste qui répertorie les certificats révoqués et le motif de leur révocation.

- « Création manuelle d'un conteneur CRL » page 759
- « Suppression d'un conteneur CRL » page 759
- « Création d'un objet Configuration CRL » page 760
- « Activation d'un objet Configuration CRL » page 760
- « Affichage et modification des propriétés d'un objet Configuration CRL » page 761

- « Suppression d'un objet Configuration CRL » page 762
- « Création d'un objet CRL » page 763
- « Exportation d'un fichier CRL » page 763
- « Remplacement d'un fichier CRL » page 764
- « Extension de validité du fichier CRL » page 765
- « Affichage des propriétés d'un objet CRL » page 765
- « Suppression d'un objet CRL » page 766

Création manuelle d'un conteneur CRL

Lors de l'installation de Certificate Server, un conteneur CRL est créé si l'utilisateur dispose des droits appropriés pour le créer. Dans le cas contraire, le conteneur CRL peut être créé manuellement par un utilisateur disposant des droits nécessaires une fois l'installation terminée.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

   Si un conteneur CRL existe déjà, vous êtes renvoyé à la page de propriétés de l'autorité de certification organisationnelle.

   Si aucun conteneur CRL n'existe, un assistant démarre et crée un conteneur CRL et un objet Configuration CRL à placer dans le conteneur.
4. Suivez les instructions de l'assistant jusqu'à la fin.

REMARQUE : si le conteneur CRL est créé dans un autre conteneur que le conteneur de sécurité, l'attribut `ndspkiCRLContainerDN` doit être renseigné manuellement dans l'objet CA de l'arborescence pour que l'onglet CRL répertorie les listes de révocation de certificats.

Suppression d'un conteneur CRL

La suppression d'un conteneur CRL est possible, mais pas recommandée.

La règle générale consiste à ne pas supprimer un conteneur CRL, un objet Configuration CRL, un objet CRL ni un fichier CRL tant que la date d'émission du dernier certificat qui contient un point de distribution lié n'a pas expiré.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Administration de l'annuaire** > **Supprimer l'objet**.
4. Recherchez et sélectionnez le conteneur CRL que vous souhaitez supprimer.
5. Cliquez sur **OK** > **OK**.

Création d'un objet Configuration CRL

Un objet Configuration CRL peut être créé dans le conteneur CRL. Il s'agit d'un objet qui contient les informations de configuration des objets Liste de révocation de certificats disponibles dans l'arborescence eDirectory. Normalement, l'arborescence ne compte qu'un seul objet Configuration CRL. Il se peut que vous ayez besoin de plusieurs objets Configuration CRL si vous créez ou déployez une nouvelle autorité de certification organisationnelle, mais un seul objet Configuration CRL peut être utilisé pour créer de nouveaux certificats.

L'objet Configuration CRL réside dans le conteneur CRL.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification), puis effectuez l'une des opérations suivantes :
   - Si aucun conteneur CRL n'existe, un assistant démarre et crée un conteneur CRL et un objet Configuration CRL à placer dans le conteneur. Suivez les instructions de l'assistant jusqu'à la fin.
   - Si un conteneur CRL existe, mais qu'aucun objet Configuration CRL n'existe, un assistant démarre et crée un objet Configuration CRL à placer dans le conteneur. Suivez les instructions de l'assistant jusqu'à la fin.
   - Si un conteneur CRL et un objet Configuration CRL existent déjà, vous êtes renvoyé à la page de propriétés de l'autorité de certification organisationnelle. Passez à l'Étape 4.
4. Cliquez sur l'onglet **CRL**.
5. Cliquez sur **Nouveau**.
6. Entrez le nom du nouvel objet Configuration CRL, puis cliquez sur **OK**.

   REMARQUE : assurez-vous que le chemin d'accès au fichier CRL spécifié ici correspond au chemin d'installation d'eDirectory.

   ---
7. Suivez les instructions de l'assistant jusqu'à la fin.

Activation d'un objet Configuration CRL

Une arborescence eDirectory ne peut contenir qu'un seul objet Configuration CRL à la fois. Si vous avez plusieurs objets Configuration CRL, vous devez en choisir un à activer. Par défaut, le premier objet Configuration CRL créé est actif.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).
4. Cliquez sur l'onglet **CRL**.

5 Sélectionnez un objet Configuration CRL, puis cliquez sur **Make Active** (Activer).

6 Cliquez sur **OK** ou sur **Appliquer**.

Affichage et modification des propriétés d'un objet Configuration CRL

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

4 Cliquez sur l'onglet **CRL**.

5 Cliquez sur le nom de l'objet Configuration CRL que vous souhaitez afficher ou modifier.

6 Cliquez sur **OK** ou sur **Appliquer**.

REMARQUE : vous pouvez désactiver la configuration CRL lors de la validation des certificats. Pour désactiver la configuration CRL, vous devez affecter une valeur à la variable d'environnement `NDSD_DISABLE_CRL_CONFIG`. Si l'arborescence eDirectory est déjà configurée avec CRL, veillez à supprimer les objets Configuration CRL (`objectclass: ndspkiCRLConfiguration`) et les objets Point de distribution CRL (`objectclass: CRLDistributionPoint`) manuellement avant de procéder à la mise à niveau d'eDirectory.

- « Assignation LDAP » page 761
- « Emplacement du point de distribution HTTP » page 762

Assignation LDAP

Le type LDAP standard pour les listes de révocation de certificats limite la taille des CRL à 64 Ko. Pour modifier cette limite, vous devez créer des entrées de répertoire CRL avec des types définis par NetIQ. Pour pouvoir trouver les points de distribution LDAP, vous devez assigner les types LDAP standard aux types NetIQ LDAP en procédant comme suit :

1 Lancez iManager.

2 Connectez-vous à eDirectory en tant qu'administrateur disposant des droits appropriés.

3 Dans le menu **Rôles et tâches**, sélectionnez **LDAP** > **Options LDAP**.

4 Cliquez sur l'onglet **Afficher les groupes LDAP**, puis sélectionnez le groupe LDAP à assigner.

5 Cliquez sur l'onglet **Général**, sélectionnez la page Assignation d'attribut et apportez les modifications suivantes :

   5a L'assignation par défaut de l'attribut LDAP primaire certificateRevocationList;binary (et de l'attribut secondaire certificateRevocationList) à l'attribut eDirectory certificateAuthorityList doit être modifiée en l'attribut eDirectory ndspkiCertificateRevocationList (autrement dit, modifiez l'attribut eDirectory certificateAuthorityList en ndspkiCertificateRevocationList).

   5b L'assignation par défaut de l'attribut LDAP primaire authorityRevocationList;binary (et de l'attribut secondaire authorityRevocationList) à l'attribut eDirectory authorityRevocationList doit être modifiée en l'attribut eDirectory ndspkiAuthorityRevocationList (autrement dit, modifiez l'attribut eDirectory authorityRevocationList en ndspkiAuthorityRevocationList).

   5c L'assignation par défaut de l'attribut LDAP primaire deltaRevocationList;binary (et de l'attribut secondaire deltaRevocationList) à l'attribut eDirectory deltaRevocationList doit être modifiée en l'attribut eDirectory ndspkiDeltaRevocationList (autrement dit, modifiez l'attribut eDirectory deltaRevocationList en ndspkiDeltaRevocationList).

6 Cliquez sur OK.

7 Dans le menu **Rôles et tâches**, sélectionnez **LDAP** > **Options LDAP**.

8 Cliquez sur l'onglet **Afficher les serveurs LDAP**, puis sélectionnez le serveur qui héberge le point de distribution LDAP.

9 Cliquez sur l'onglet **Général**, puis sélectionnez la page Informations.

10 Cliquez sur le bouton Rafraîchir.

   Le service LDAP redémarre et commence à utiliser l'assignation appropriée pour les attributs CRL.

Pour plus d'information sur la gestion de LDAP, reportez-vous au Chapitre 14, « Configuration des services LDAP pour NetIQ eDirectory », page 393.

Emplacement du point de distribution HTTP

Lorsque vous configurez Certificate Server pour qu'il utilise un point de distribution HTTP, veillez à spécifier un emplacement accessible aux utilisateurs qui souhaitent valider des certificats. Si un utilisateur ne peut pas localiser la CRL d'un certificat qui contient un point de distribution, le certificat est considéré comme non valide. Le point de distribution doit se trouver dans un répertoire disponible sur le serveur Web spécifié par l'adresse HTTP du point de distribution. Si ce répertoire ne se trouve pas sur le même serveur qui héberge l'autorité de certification, la CRL doit être déplacée manuellement, par le biais d'un script ou créé sur un répertoire monté.

Suppression d'un objet Configuration CRL

Bien que la suppression d'un objet Configuration CRL soit possible, elle n'est pas recommandée. Lorsqu'un objet Configuration CRL est supprimé, le serveur s'arrête et crée les fichiers CRL. Si un fichier CRL existe déjà à l'emplacement indiqué dans l'objet CRL, la validation de certificat continue de l'utiliser jusqu'à ce qu'il arrive à expiration. Une fois arrivé à expiration, la validation de tous les certificats disposant d'un point de distribution CRL faisant référence à ce fichier CRL échoue.

La règle générale consiste à ne pas supprimer un conteneur CRL, un objet Configuration CRL, un objet CRL ni un fichier CRL tant que la date d'émission du dernier certificat qui contient un point de distribution lié n'a pas expiré.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, sélectionnez **Administration de l'annuaire** > **Supprimer l'objet**.

4 Recherchez et sélectionnez l'objet Configuration CRL à supprimer.

5 Cliquez sur **OK** > **OK**.

Création d'un objet CRL

Cette tâche vous permet de créer un objet CRL (cRLDistributionPoint) pour stocker des CRL tierces dans eDirectory. Cet objet peut être créé dans n'importe quel conteneur de l'arborescence eDirectory. Toutefois, les objets CRL NetIQ se trouvent généralement dans un objet Configuration CRL et ne doivent pas être créés manuellement. Un objet CRL est créé automatiquement pour vous lorsque vous créez un objet Configuration CRL.

L'objet CRL héberge un fichier CRL qui contient des informations détaillées sur la liste de révocation des certificats. Pour chaque objet CRL NetIQ, un fichier CRL est automatiquement créé et mis à jour chaque fois que le serveur en émet un nouveau. Pour les autres objets CRL, vous devez importer un fichier CRL à partir d'une autorité de certification tierce.

REMARQUE : l'appellation Point de Distribution CRL est utilisée de différentes manières. Il s'agit du nom d'objet Schéma eDirectory pour l'objet CRL et désigne de manière générale, l'emplacement où les informations de la CRL sont publiées.

Pour créer un objet CRL :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, cliquez sur **Serveur de certificats NetIQ** > **Create CRL Object** (Créer un objet CRL).

4 Entrez un nom pour l'objet et indiquez le contexte dans lequel vous souhaitez placer l'objet.

5 Collez une copie de la liste de révocation dans le champ ou lisez-la à partir d'un fichier CRL.

6 Cliquez sur **Terminer** pour créer l'objet.

Exportation d'un fichier CRL

Vous pouvez exporter la liste de révocation de certificats contenue dans l'objet Point de Distribution CRL vers un fichier.

Pour exporter un fichier CRL NetIQ :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

4 Cliquez sur l'onglet **CRL**.

5 Cliquez sur le nom de l'objet Configuration CRL, puis cliquez sur **Détails**.

6 Cliquez sur **Exporter**.

7 Sélectionnez un format de sortie, puis cliquez sur **Suivant**.

8 Pour enregistrer la CRL exportée dans un fichier, cliquez sur **Enregistrer**, puis spécifiez l'emplacement du fichier.

9 Cliquez sur **OK** > **OK**.

Pour exporter un fichier CRL tiers :

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, sélectionnez **Administration de l'annuaire** > **Modifier un objet**.

4 Recherchez et sélectionnez l'objet Configuration CRL, puis cliquez sur **OK**.

5 Cliquez sur **Exporter**.

6 Sélectionnez un format de sortie, puis cliquez sur **Suivant**.

7 Pour enregistrer la CRL exportée dans un fichier, cliquez sur **Enregistrer**, puis spécifiez l'emplacement du fichier.

8 Cliquez sur **OK** > **OK**.

Remplacement d'un fichier CRL

Vous pouvez remplacer un fichier CRL, mais cette opération n'est pas recommandée.

1 Lancez iManager.

2 Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.

3 Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).

4 Cliquez sur l'onglet **CRL**.

5 Cliquez sur le nom de l'objet Configuration CRL, puis cliquez sur **Détails**.

6 Cliquez sur **Remplacer**.

7 Cliquez sur **OK** pour continuer.

8 Recherchez et sélectionnez le nouveau fichier CRL.

9 Cliquez sur **OK**.

Si un fichier CRL n'existe pas dans l'objet Configuration CRL, le bouton **Importer** s'affiche.

Extension de validité du fichier CRL

L'administrateur peut étendre la validité du fichier CRL à l'aide d'iManager. Pour étendre la validité, procédez comme suit :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).
4. Cliquez sur l'onglet **CRL**.
5. Cliquez sur le nom du fichier CRL.
6. Sélectionnez **Prolonger la validité en fonction du nombre d'heures suivant** sous **Prochaine émission de la liste de révocation de certificats (CRL)** et indiquez le nombre d'heures dans la zone suivante. Vous pouvez entrer dans ce champ une valeur comprise entre 1 et 12 heures.
7. Cliquez sur **Issue Now** (Émettre maintenant).

Affichage des propriétés d'un objet CRL

Pour afficher les propriétés d'un objet CRL NetIQ :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Serveur de certificats NetIQ** > **Configure Certificate Authority** (Configurer l'autorité de certification).
4. Cliquez sur l'onglet **CRL**.
5. Cliquez sur le nom de l'objet Configuration CRL, puis cliquez sur **Détails**.

   Vous pouvez à présent afficher les propriétés de l'objet CRL.
6. Après les avoir consultées, cliquez sur **OK** ou **Appliquer**.

Pour afficher les propriétés d'un objet CRL tiers :

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, sélectionnez **Administration de l'annuaire** > **Modifier un objet**.
4. Recherchez et cliquez sur l'objet CRL que vous souhaitez afficher, puis cliquez sur **OK**.
5. Cliquez sur **Éditer**.

   Vous pouvez à présent afficher les propriétés de l'objet CRL.
6. Après les avoir consultées, cliquez sur **OK** ou **Appliquer**.

Suppression d'un objet CRL

Si vous supprimez un objet CRL, il sera recréé la prochaine fois que le serveur génèrera le fichier CRL. Si vous supprimez un objet CRL créé et importé à l'aide d'iManager, il est définitivement supprimé et tous les certificats qui y font référence sont considérés comme non valides.

La règle générale consiste à ne pas supprimer un conteneur CRL, un objet Configuration CRL, un objet CRL ni un fichier CRL tant que la date d'émission du dernier certificat qui contient un point de distribution lié n'a pas expiré.

1. Lancez iManager.
2. Connectez-vous à l'arborescence eDirectory en tant qu'administrateur disposant des droits appropriés.

   Pour afficher les droits appropriés pour cette tâche, reportez-vous à la « Droits sur les entrées nécessaires à la réalisation des tâches » page 778.
3. Dans le menu **Rôles et tâches**, cliquez sur **Administration de l'annuaire** > **Supprimer l'objet**.
4. Recherchez et cliquez sur l'objet CRL que vous souhaitez supprimer.
5. Cliquez sur **OK** > **OK**.

Tâches relatives à eDirectory

- « Résolution de plusieurs conteneurs de sécurité, autorités de certification organisationnelles, conteneurs KAP et objets W0 » page 766
- « Restauration ou recréation d'un conteneur de sécurité » page 767
- « Restauration ou recréation d'objets KAP et W0 » page 767

Résolution de plusieurs conteneurs de sécurité, autorités de certification organisationnelles, conteneurs KAP et objets W0

NetIQ Certificate Server peut être installé sur plusieurs serveurs d'une arborescence eDirectory. Toutefois, pour lui permettre de fonctionner correctement, l'arborescence ne peut contenir qu'un seul conteneur de sécurité, une seule autorité de certification organisationnelle, un conteneur KAP et un objet W0.

Si vous installez NetIQ Certificate Server sur plusieurs serveurs d'une arborescence eDirectory, vous devez autoriser eDirectory à effectuer des réplications entre chaque installation de NetIQ Certificate Server. À défaut, votre installation sur un autre serveur risque de ne pas reconnaître que l'arborescence héberge déjà un conteneur de sécurité, une autorité de certification organisationnelle, un conteneur KAP et un objet W0, et pourrait recréer ces objets sur un autre serveur de la même arborescence eDirectory.

Les cas de figure suivants décrivent les scénarios possibles et comment les résoudre.

- Si la même arborescence eDirectory héberge deux ou plusieurs conteneurs de sécurité et que chacun contient une autorité de certification organisationnelle et un conteneur KAP avec un objet W0, n'émettez aucun certificat. Contactez le support technique pour vous aider à remédier à cette situation.
- Si la même arborescence eDirectory héberge un conteneur de sécurité qui contient deux conteneurs KAP, n'émettez aucun certificat. Contactez le support technique pour vous aider à remédier à cette situation.

- Si la même arborescence eDirectory héberge un conteneur de sécurité qui contient deux autorités de certification organisationnelles et un conteneur KAP avec un objet W0, supprimez tous les certificats de serveur et utilisateur émis par les deux autorités de certification organisationnelles. Supprimez ensuite les deux autorités de certification et créez une nouvelle autorité de certification organisationnelle. Émettez de nouveaux certificats de serveur et utilisateur en fonction de vos besoins.
- Si la même arborescence eDirectory héberge deux ou plusieurs conteneurs de sécurité et que chacun contient une autorité de certification organisationnelle, mais qu'un seul héberge un conteneur KAP avec un objet W0, supprimez tous les certificats de serveur et utilisateur émis par toutes les autorités de certification organisationnelles. Supprimez tous les conteneurs de sécurité à l'exception de celui hébergeant le conteneur KAP et l'objet W0. Si le nom du conteneur de sécurité restant n'est pas *Security*, renommez-le *Security*. Émettez de nouveaux certificats de serveur et utilisateur en fonction de vos besoins.
- Si la même arborescence eDirectory héberge deux ou plusieurs conteneurs de sécurité et qu'un seul contient une autorité de certification organisationnelle et un conteneur KAP avec un objet W0, supprimez tous les conteneurs de sécurité à l'exception de celui hébergeant le conteneur KAP et l'objet W0. Si le nom du conteneur de sécurité restant n'est pas *Security*, renommez-le *Security*.

Restauration ou recréation d'un conteneur de sécurité

Si vous supprimez le conteneur de sécurité, vous ne pouvez pas créer d'autorité de certification organisationnelle tant que vous n'avez pas restauré ou recréé le conteneur de sécurité.

Pour restaurer le conteneur de sécurité, vous devez restaurer la partition eDirectory hébergeant le conteneur de sécurité.

Pour recréer le conteneur de sécurité, utilisez l'une des deux méthodes suivantes :

- À l'aide d'iManager, cliquez sur **Administration de l'annuaire** > **Créer un objet**. Cliquez sur le **conteneur de sécurité de l'arborescence**, puis cliquez sur **OK**. Le nom du conteneur doit être Security.
- Réinstallez NetIQ Certificate Server sur n'importe quel serveur de l'arborescence eDirectory.

Restauration ou recréation d'objets KAP et W0

Ne supprimez pas les objets KAP ni W0. Tous les certificats utilisateur précédemment créés ne seraient alors plus valides. Si vous avez supprimé l'un de ces objets, accédez au site Web du support Novell (http://support.novell.com/) et recherchez le document TID #3032354, How to Restore or Recreate KAP and W0 Object (Comment restaurer ou recréer des objets KAP et W10) pour plus d'informations sur la procédure de résolution de ce problème. N'essayez pas de procéder à d'autres installations de NetIQ Certificate Server, Single Sign-on, NMAS ou eDirectory tant que les problèmes n'ont pas été résolus.

Tâches relatives aux applications

Cette section décrit comment configurer des applications codées pour qu'elles utilisent des certificats NetIQ.

Certaines informations de cette section sont anciennes, mais très pratiques. Pour obtenir les dernières informations sur l'utilisation de certificats avec vos applications codées, reportez-vous à la documentation correspondante.

La procédure générale pour activer la sécurisation des courriers électroniques pour les applications est la suivante :

1. Exportez le certificat auto-signé de votre autorité de certification organisationnelle (reportez-vous à la section « Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle » page 728), votre certificat utilisateur et la clé privée correspondante dans un fichier `.pfx` (reportez-vous à la section « Exportation d'un certificat utilisateur et de la clé privée » page 747).
2. Importez le fichier `.pfx` dans votre client de messagerie.
3. Configurez votre client de messagerie électronique de façon à sécuriser vos courriers électroniques.

Pour créer une connexion SSL à un serveur sur Internet à l'aide de votre navigateur, vous devez approuver l'autorité de certification qui a signé les certificats utilisateur ou de serveur. À défaut, une erreur risque de s'afficher dans votre application. Certaines applications affichent un avertissement vous permettant d'accepter ou de rejeter le certificat de serveur ou utilisateur dont l'autorité de certification n'a pas encore été approuvée pour l'application. Les certificats de serveur et utilisateur signés par l'autorité de certification organisationnelle d'une société génèrent toujours ce type d'avertissement et d'erreur. Cela est dû au fait que l'autorité de certification organisationnelle n'est pas répertoriée comme autorité de certification approuvée par votre application. Ces avertissements et erreurs peuvent être évités en installant le certificat auto-signé de l'autorité de certification organisationnelle dans votre application. L'installation de l'autorité de certification organisationnelle dans votre navigateur l'ajoute automatiquement comme autorité de certification approuvée.

Pour accepter l'autorité de certification organisationnelle en tant qu'autorité de certification approuvée dans votre application :

1. Exportez le certificat auto-signé de votre autorité de certification organisationnelle (reportez-vous à la section « Exportation d'un certificat auto-signé d'une autorité de certification organisationnelle » page 728).

   REMARQUE : les navigateurs Internet reconnaissent les certificats au format .der ou .crt.

2. Importez le certificat dans votre navigateur en suivant les instructions fournies par la documentation relative au navigateur.

Vérification de l'état de santé PKI

NetIQ Certificate Server intègre un processus qui maintient l'état de santé et l'intégrité des composants de Certificate Server. Ce processus est appelé PKI Health Check (Vérification de l'état de santé PKI) et s'exécute dans les cas suivants :

- au redémarrage du serveur ;
- lors de l'affichage d'eDirectory ;
- à la fin de l'exécution de DSRepair.

Lors de l'exécution de la vérification de l'état de santé PKI, les tâches suivantes sont effectuées :

Tableau 25-1 *Tâches de vérification de l'état de santé PKI*

Tâche	Fonction
Vérifier le lien du serveur vers l'objet Service SAS	Cette tâche vérifie s'il existe un lien entre l'objet Serveur et un objet SAS:Service. Si le lien existe, la tâche vérifie que le nom de l'objet est correct et qu'il se trouve dans le même contexte que le serveur. Si le lien n'existe pas, la tâche recherche si un objet portant le nom correct existe dans le même contexte que le serveur. Si un tel objet existe, la tâche crée un lien entre le serveur et l'objet.
Vérifier l'objet Service SAS	Cette tâche vérifie qu'un objet SAS:Service existe. S'il n'existe pas, la tâche en crée un et génère un lien entre l'objet Serveur et le nouvel objet. La tâche vérifie ensuite si l'objet SAS:Service dispose des droits eDirectory nécessaires. À défaut, la tâche tente d'octroyer à l'objet SAS:Service les droits nécessaires.
Vérifier les liens vers les objets Matériel clé	Cette tâche lit la liste des objets Certificat de serveur (ou des objets Matériel clé) qui sont liés à l'objet SAS:Service. Elle vérifie que le nom des objets Matériel clé sont tous corrects et tente de résoudre les noms incorrects. La tâche vérifie également que les objets Matériel clé se trouvent tous dans le même contexte que l'objet Serveur et tente de les déplacer vers le contexte approprié lorsque ce n'est pas le cas.
Vérifier les certificats de serveur (KMO)	Cette tâche lit tous les noms des objets Matériel clé qui se trouvent dans le même conteneur que l'objet Serveur et les place dans la liste. La tâche effectue ensuite les opérations suivantes pour chaque objet Matériel clé de la liste : ◆ Tente de compléter les attributs NDSPKI:Not Before et NDSPKI:Not After avec les dates de validité du certificat. ◆ Vérifie si Public possède le droit de lecture sur l'attribut Serveur hôte. ◆ Vérifie si le lien de l'objet Matériel clé vers un serveur est un lien en amont. Si le lien en amont est destiné à un autre serveur, la tâche ignore l'objet Matériel clé et le supprime de sa liste. ◆ Lit la clé privée et tente de la désencapsuler.
Revérifier les liens vers les objets Matériel clé	Cette tâche lit la liste des objets Certificat de serveur (ou des objets Matériel clé) qui sont liés à l'objet SAS:Service. Elle compare chaque objet Matériel clé de cette liste à la liste créée au cours de la tâche Vérifier les certificats de serveur (KMO). À l'aide des contrôles de la tâche Vérifier les certificats de serveur (KMO), la tâche détermine la présence éventuelle de problèmes concernant les certificats liés et les détache si l'objet Matériel clé devient inutilisable. La tâche détermine également si des objets Matériel clé détachés peuvent être utilisées par ce serveur et, le cas échéant, les lie.

Tâche	Fonction
Créer des certificats par défaut	Cette tâche détermine si l'auto-provisioning du serveur est activé au niveau de l'objet Autorité de certification organisationnelle. Si l'auto-provisioning du serveur n'est pas activé, cette étape est ignorée. Si l'auto-provisioning du serveur est activé, la tâche appelle l'API NPKICreateDefaultCertificates(). Cette API crée ou remplace le certificat SSL CertificateDNS dans les cas suivants : ◆ Le certificat n'existe pas. ◆ Le certificat n'est pas arrivé à expiration ou sur le point d'expirer. ◆ Le nom d'objet du certificat ne correspond pas aux adresses IP et DNS par défaut configurées pour le serveur. **REMARQUE :** eDirectory ne crée pas automatiquement le certificat SSL CertificateIP. Le nom DNS du certificat SSL contient toutes les adresses IP répertoriées dans le champ Subject Alternative Name (Autre nom de l'objet). En outre, cette API acquiert toutes les adresses IP et DNS configurées pour le serveur et crée et/ou remplace un certificat pour chacune d'elles, par exemple IP AG *adresse_ip* ou IP DNS *nom_dns* dans les cas suivants : ◆ Les certificats n'existent pas. ◆ Les certificats sont arrivés à expiration ou sur le point d'expirer.
Synchroniser les certificats pour les services externes	Cette tâche lit la configuration de l'objet SAS:Service. Pour chaque entrée configurée, la tâche acquiert les certificats et la clé privée à partir de l'objet Matériel clé spécifié. Si le répertoire spécifié n'existe pas, la tâche tente de le créer. La tâche désencapsule alors la clé privée et la convertit au format clé brute spécifié. La tâche compare chaque clé privée existante et les fichiers de certificat avec ceux de l'objet Matériel clé spécifié. Si les clés et certificats ne sont pas identiques, la tâche effectue une sauvegarde de la clé privée et des fichiers de certificat existants, puis les remplace par la clé privée et les certificats. Les clés sont écrites au format PEM.

Tâche	Fonction
Exporter le certificat de l'autorité de certification eDirectory vers le système de fichiers	Le déroulement de cette tâche dépend de votre système d'exploitation. Les fichiers `SSCert.der` et `SSCert.pem` contiennent le certificat RSA de l'autorité de certification de l'organisation. Si l'autorité de certification de l'organisation possède un certificat ECDSA, eDirectory exporte ce certificat vers les fichiers `SSECCert.der` et `SSECCert.pem` et les enregistre dans le même répertoire que les fichiers `SSCert.der` et `SSCert.pem`. ◆ **Windows :** vérifie si les fichiers `SSCert.der` et `SSCert.pem` dans le répertoire de travail PKI contiennent le même certificat que celui de l'autorité de certification de l'organisation dans eDirectory. Tente de remplacer les fichiers s'ils ne sont pas identiques. Le répertoire de travail PKI par défaut est `c:\Novell\NDS\DIBFiles\CertServ\` ◆ **Linux (pas OES Linux) :** vérifie si les fichiers `SSCert.der` et `SSCert.pem` dans le répertoire de données eDirectory contiennent le même certificat que celui de l'autorité de certification de l'organisation dans eDirectory. Tente de remplacer les fichiers s'ils ne sont pas identiques. Le répertoire de données eDirectory par défaut est `/var/opt/novell/eDirectory/data` ◆ **OES Linux :** vérifie si les fichiers `/etc/opt/novell/certs/SSCert.der` et `/etc/opt/novell/certs/SSCert.pem` contiennent le même certificat que celui de l'autorité de certification de l'organisation dans eDirectory. Si les certificats ne sont pas identiques, la tâche tente de remplacer les fichiers en ajoutant le certificat de l'autorité de certification de l'organisation dans le répertoire `/etc/ssl/certs`, puis en exécutant le programme `c_rehash`. Toutefois, avant de remplacer les fichiers, la tâche crée des sauvegardes de tous les certificats existants.

Cryptographie à clé publique - Notions

Cette section décrit les notions de base de la cryptographie à clé publique.

- « Présentation » page 772
- « Transmissions sécurisées » page 772
- « Paires de clés » page 772
- « Mise en place d'une relation de confiance » page 775

Présentation

Le contenu de la plupart des communications Internet, comme la consultation des pages Web ou les forums de discussion publics, peut être géré par tout utilisateur équipé à cet effet. Le contenu des autres transmissions de données, comme l'échange d'informations relatives aux cartes de crédit dans le cadre d'achats en ligne, doit rester confidentiel.

La cryptographie à clé publique est une méthode largement utilisée qui permet de garantir la sécurité et le caractère confidentiel des données transmises sur Internet. La particularité de la cryptographie à clé publique réside dans l'utilisation de codes numériques, appelés “clés”, qui permettent d'authentifier les expéditeurs de messages et de crypter le contenu de ces derniers.

Transmissions sécurisées

Les transmissions de données sont confidentielles et sécurisées dans les deux situations suivantes :

- **Authentification :** Le destinataire des données sait que l'expéditeur est bien celui qu'il prétend être.
- **Chiffrement :** Les données envoyées sont codées pour que seul leur destinataire puisse les lire.

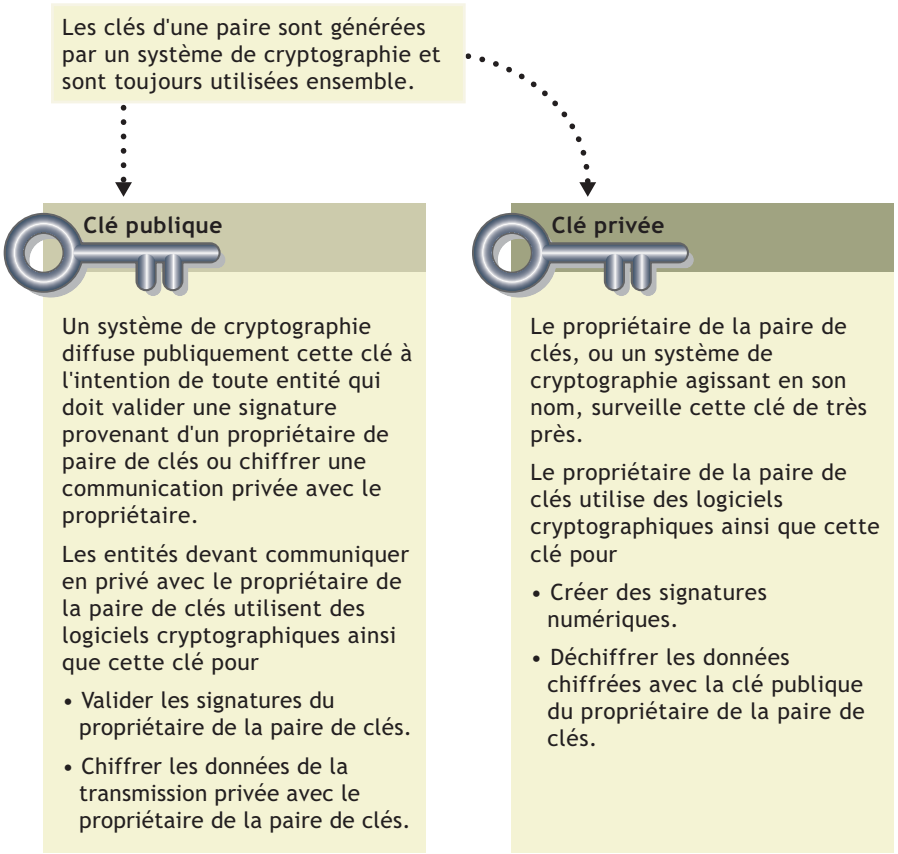
Paires de clés

L'authentification et le chiffrement se font à l'aide de paires de codes numériques liés par une relation mathématique et appelés des « clés ». Une clé de chaque paire est publique (distribuée à tous) et l'autre clé est privée.

Tout émetteur de données, qu'il s'agisse d'un individu, d'un logiciel ou d'une entité comme une banque ou une société, se voit attribuer une paire de clés par un système de cryptographie à clé publique.

L'illustration suivante propose une synthèse des principes et des fonctions de base de chaque clé d'une paire:

Figure 25-1 *Description de la paire de clés de base*



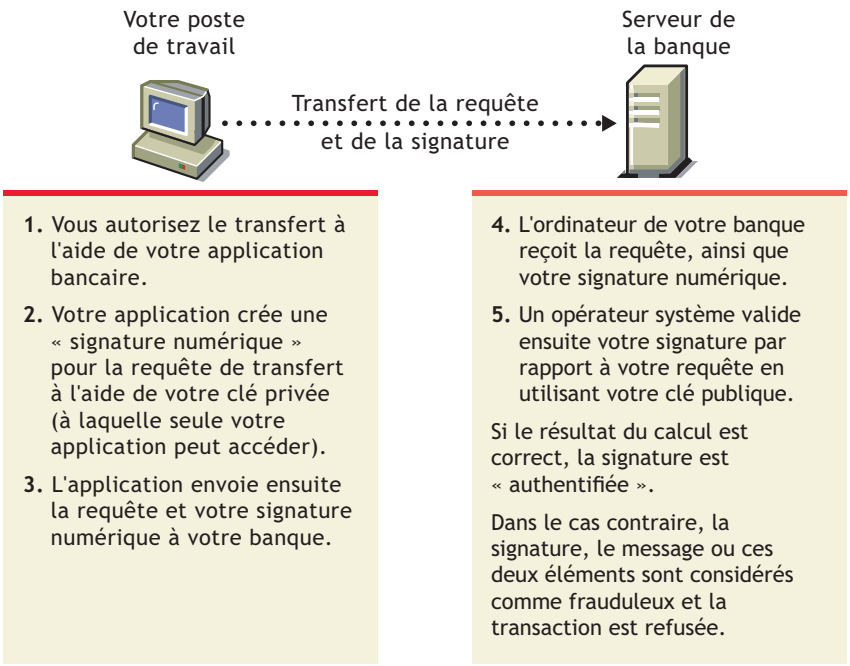
- « Paires de clés et authentification » page 773
- « Paires de clés et chiffrement » page 774

Paires de clés et authentification

L'*authentification* vise à prouver au destinataire des données que l'expéditeur est bien celui qu'il prétend être.

Supposez que vous souhaitiez autoriser votre banque à transférer des fonds de votre compte vers un autre. La banque a besoin d'une preuve selon laquelle vous êtes l'expéditeur du message et que celui-ci n'a pas été altéré pendant le transfert. La figure ci-après illustre le traitement de votre transaction en ligne au moyen de la cryptographie à clé publique.

Figure 25-2 *Processus de clé publique*



Pour plus d'informations sur les signatures digitales et leur vérification, reportez-vous à la section « Signatures digitales » page 776.

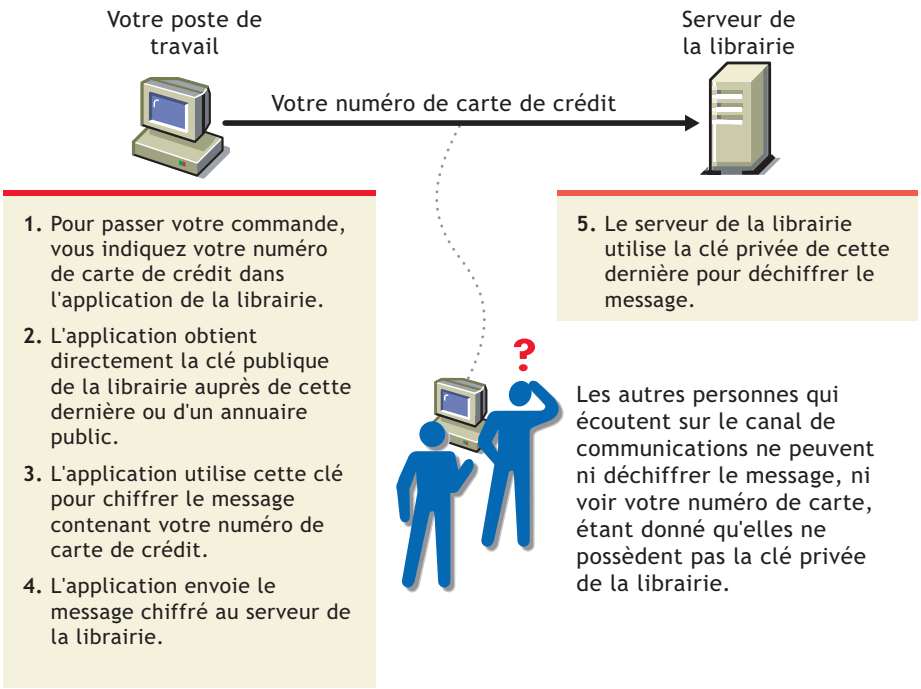
Paires de clés et chiffrement

Le chiffrement signifie que les données ne peuvent être lues que par le destinataire désigné.

Supposez que vous souhaitiez commander un ouvrage auprès d'un fournisseur Internet et utiliser votre carte de crédit pour régler le montant de la facture. Vous ne voulez pas que votre numéro de carte de crédit soit lu par une personne autre que le destinataire prévu.

L'illustration suivante représente le processus de codage par le biais duquel la transmission du numéro de votre carte de crédit peut être sécurisée.

Figure 25-3 *Processus de chiffrement*



Mise en place d'une relation de confiance

Si l'expéditeur et le destinataire se font confiance, ils peuvent se contenter d'échanger des clés publiques et d'établir une transmission de données sécurisée (authentification et codage). Pour ce faire, chacun va utiliser la clé publique de l'autre et sa propre clé privée.

Dans des circonstances normales, toutefois, les parties qui ont besoin de transmissions de données sécurisées n'ont aucun moyen de valider l'identité de leur interlocuteur. Une tierce partie de toute confiance est nécessaire pour garantir l'identité des deux parties en présence.

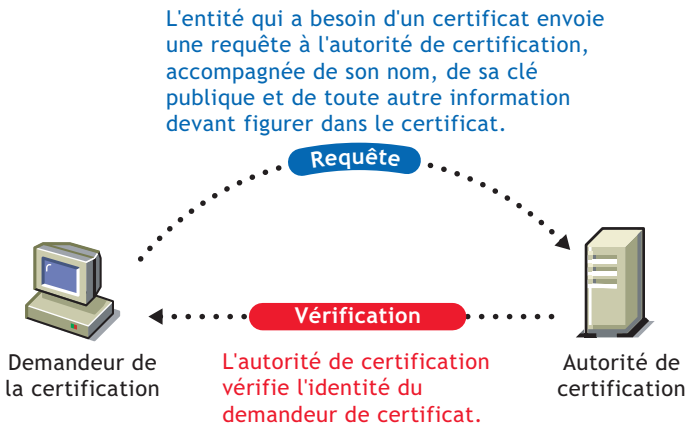
- « Autorités de certification » page 775
- « Signatures digitales » page 776
- « Chaîne de certificats » page 777
- « Racines approuvées » page 777

Autorités de certification

Une partie devant prouver son identité dans un environnement de cryptographie à clé publique fait appel aux services d'un tiers digne de confiance reconnu comme autorité de certification.

L'objectif principal de l'autorité de certification consiste à vérifier que l'identité d'une partie est bien celle qu'elle prétend être, puis à lui délivrer un certificat de clé publique. Le certificat de clé publique vérifie que la clé publique contenue dans le certificat appartient à la partie mentionnée dans ce certificat.

Figure 25-4 *Requête de certificat*



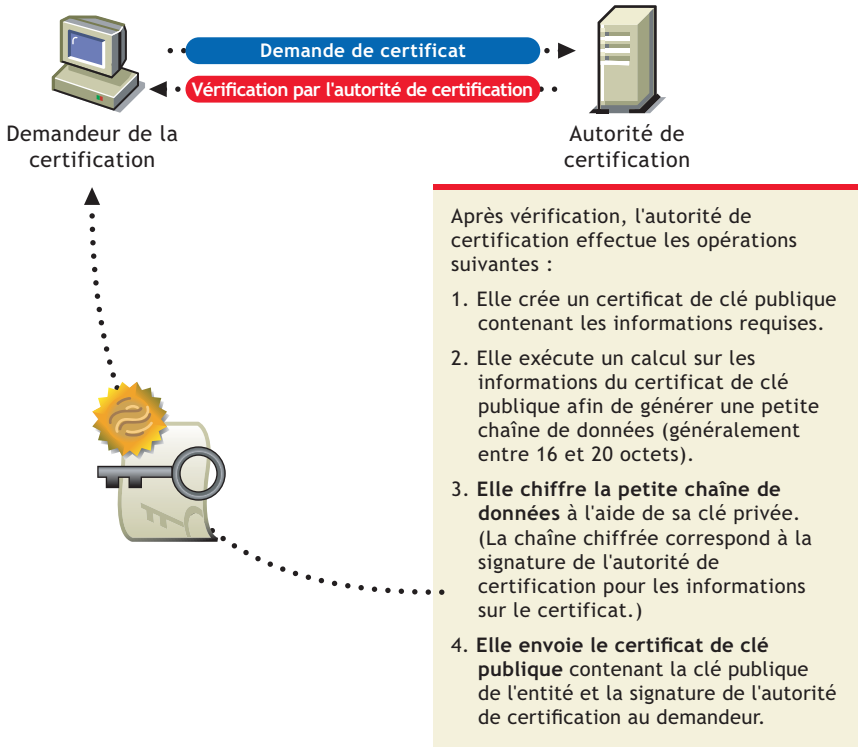
Une fois que l'autorité de certification a déterminé l'identité de la partie, elle émet un « certificat électronique » et y applique sa signature numérique.

Signatures digitales

Tout comme une signature sur un document papier en prouve l'authenticité, la signature digitale indique l'authenticité des données électroniques.

Pour créer une signature digitale, le logiciel qui sert à la générer lie les données signées à la clé privée du signataire. L'illustration suivante représente le processus que suit l'autorité de certification (CA) pour créer sa signature digitale et l'apposer sur un certificat de clé publique.

Figure 25-5 *Signature numérique*



La signature digitale est liée de manière unique au signataire et aux données. Personne d'autre ne peut reproduire la signature car personne d'autre ne possède la clé privée du signataire. Par ailleurs, le signataire ne peut pas nier avoir signé les données. Ce processus est connu sous le nom de *non-rejet*.

Lorsqu'une autorité de certification signe un certificat de clé publique, elle garantit avoir vérifié l'identité du propriétaire de cette clé conformément aux stratégies publiées et établies.

Une fois que les données signées (certificat de clé publique par exemple) sont reçues, le logiciel en vérifie l'authenticité en leur appliquant le même calcul que celui initialement utilisé par le logiciel ayant apposé sa signature. Si les données n'ont pas été altérées, les deux calculs génèrent les mêmes résultats. Il est peu probable que les données et la signature aient été modifiées pendant le transfert.

Chaîne de certificats

Une chaîne de certificats est une liste ordonnée de certificats. Les certificats sont classés de sorte que le certificat de serveur ou utilisateur apparaisse en premier, suivi par le certificat de son autorité de certification.

Les autorités de certification peuvent soit signer leurs propres certificats (les certificats sont alors auto-signés) ou les faire signer par une autre autorité de certification. Si les certificats sont auto-signés, l'autorité de certification est généralement qualifiée de racine. S'ils ne sont pas auto-signés, l'autorité de certification est généralement qualifiée de subordonnée ou intermédiaire.

Si un certificat utilisateur ou de serveur a été signé par une autorité de certification avec un certificat auto-signé, la chaîne de certificats se compose exactement de deux certificats : le certificat d'entité finale et le certificat de l'autorité de certification racine.

Si un certificat utilisateur ou de serveur a été signé par une autorité de certification intermédiaire, la chaîne de certificats est plus longue. Les deux premiers éléments sont toujours le certificat d'entité finale, suivi par le certificat de l'autorité de certification intermédiaire. Toutefois, les certificats de l'autorité de certification intermédiaire sont alors suivis du certificat de son autorité de certification. Cette liste se poursuit alors jusqu'à ce que le dernier certificat dans la liste soit destiné à une autorité de certification racine. La longueur d'une chaîne de certificats peut par conséquent être infinie. Toutefois, dans la pratique, la plupart des chaînes de certificats ne comportent que deux ou trois certificats.

Racines approuvées

Afin de valider une signature numérique, vous devez approuver au moins un des certificats de la chaîne de certificats de serveur ou utilisateur. Vous pouvez approuver directement le certificat de l'utilisateur ou du serveur, ou choisir d'approuver n'importe quel autre certificat de la chaîne. En règle générale, le certificat approuvé est le certificat de l'autorité de certification racine.

La plupart des logiciels applicatifs pouvant utiliser des certificats disposent déjà d'une liste des certificats approuvés installés. Ces certificats sont destinés à des autorités de certification racine et sont, par conséquent, appelés « racines approuvées ».Ces autorités de certification sont généralement des autorités de certification commerciales. Si vous le souhaitez, vous pouvez ajouter des certificats supplémentaires à cette liste ou en supprimer.

Droits sur les entrées nécessaires à la réalisation des tâches

La liste suivante répertorie les droits spécifiques sur les entrées dont l'administrateur a besoin pour gérer les tâches NetIQ Certificate Server au sein d'une arborescence eDirectory. Ces droits sont les droits minimum requis sur les entrées.

Cette liste devrait également être utile à l'administrateur qui souhaite accorder des droits à un autre utilisateur pour gérer une partie ou l'ensemble des besoins de la société en termes de gestion des certificats et d'autorité de certification.

Tableau 25-2 *Droits sur les entrées pour l'administrateur*

Tâches	Droits nécessaires sur les entrées
Installation de NetIQ Certificate Server	Pour la première installation sur une arborescence eDirectory : ◆ Superviseur au niveau de la [Racine] de l'arborescence Pour les installations suivantes : ◆ Superviseur sur l'objet W0 ◆ Droits requis pour créer un objet Certificat de serveur Si un utilisateur ne possède pas les droits requis pour créer un objet Certificat de serveur, l'installation se termine, mais les objets Certificat de serveur doivent être créés manuellement par un utilisateur disposant des droits appropriés, et les applications qui utilisent ces certificats doivent être configurées manuellement.
Création d'une autorité de certification organisationnelle	◆ Superviseur sur le conteneur de sécurité
Affichage des propriétés et des certificats de l'autorité de certification organisationnelle	◆ Parcourir sur l'objet de l'autorité de certification organisationnelle
Exportation de certificat(s) de l'autorité de certification organisationnelle	◆ Parcourir sur l'objet de l'autorité de certification organisationnelle
Émission d'un certificat de clé publique	◆ Lire sur l'attribut NDSPKI:Private Key de l'objet de l'autorité de certification organisationnelle Toutefois, si l'objet qui tente de délivrer le certificat de clé publique est un serveur NCP, les droits requis sont les suivants : ◆ Écrire sur l'attribut NDSPKI:Private Key de l'objet de l'autorité de certification organisationnelle
Sauvegarde et restauration d'une autorité de certification organisationnelle	◆ Superviseur sur l'objet de l'autorité de certification organisationnelle

Tâches	Droits nécessaires sur les entrées
Déplacement de l'autorité de certification organisationnelle vers un autre serveur	◆ Superviseur sur l'objet de l'autorité de certification organisationnelle
Validation des certificats de l'autorité de certification organisationnelle	◆ Parcourir sur l'objet de l'autorité de certification organisationnelle
Remplacement de l'autorité de certification organisationnelle	◆ Superviseur sur l'objet de l'autorité de certification organisationnelle
Suppression d'une autorité de certification organisationnelle	◆ Supprimer sur l'objet de l'autorité de certification organisationnelle
Création d'objets Certificat de serveur	◆ Superviseur sur le conteneur du serveur ◆ Lire sur l'attribut NDSPKI:Private Key de l'objet de l'autorité de certification organisationnelle (uniquement s'il s'agit de l'autorité de certification organisationnelle) Toutefois, si l'objet qui tente de délivrer le certificat de clé publique est un serveur NCP, les droits requis sont les suivants : ◆ Superviseur sur le conteneur du serveur ◆ Écrire sur l'attribut NDSPKI:Private Key de l'objet de l'autorité de certification organisationnelle
Importation d'un certificat de clé publique dans un objet Certificat de serveur	◆ Écrire sur l'attribut NDSPKI:Public Key Certificate de l'objet Certificat de serveur ◆ Écrire sur l'attribut NDSPKI:Certificate Chain de l'objet Certificat de serveur
Suppression d'un objet Certificat de serveur	◆ Supprimer sur l'objet Certificat de serveur
Exportation d'un certificat de racine approuvée ou d'un certificat de clé publique à partir d'un objet Certificat de serveur	◆ Parcourir sur l'objet Certificat de serveur
Affichage des propriétés et des certificats de l'objet Certificat de serveur	◆ Parcourir sur l'objet Certificat de serveur
Sauvegarde et restauration d'un objet Certificat de serveur	◆ Superviseur sur l'objet Serveur qui possède l'objet Certificat de serveur à sauvegarder ◆ Créer sur le conteneur de l'objet Serveur à restaurer.
Validation des certificats de serveur	◆ Parcourir sur l'objet Certificat de serveur
Révocation des certificats de serveur	◆ Lire sur la clé privée de l'autorité de certification, Supprimer sur l'objet Certificat de serveur ou Superviseur sur le serveur hôte (autrement dit, l'objet serveur NCP™)
Remplacement du matériel de codage d'un certificat de serveur	◆ Écrire sur l'attribut NDSPKI:PrivateKey de l'objet Certificat de serveur

Tâches	Droits nécessaires sur les entrées
Création de certificats utilisateur	◆ Lire sur l'attribut NDSPKI:Private Key de l'objet de l'autorité de certification organisationnelle ◆ Lire et Écrire sur l'attribut NDSPKI:userCertificateInfo de l'objet Utilisateur ◆ Lire et Écrire sur l'attribut SAS:SecretStore de l'objet Utilisateur ◆ Lire et Écrire sur l'attribut userCertificate de l'objet Utilisateur Toutefois, si l'objet qui tente de délivrer le certificat de clé publique est un serveur NCP, les droits requis sont les suivants : ◆ Écrire sur l'attribut NDSPKI:Private Key de l'objet de l'autorité de certification organisationnelle ◆ Lire et Écrire sur l'attribut NDSPKI:userCertificateInfo de l'objet Utilisateur ◆ Lire et Écrire sur l'attribut SAS:SecretStore de l'objet Utilisateur ◆ Lire et Écrire sur l'attribut userCertificate de l'objet Utilisateur
Importation d'un certificat de clé publique dans un objet utilisateur	◆ Lire et Écrire sur l'attribut NDSPKI:userCertificateInfo de l'objet Utilisateur ◆ Lire et Écrire sur l'attribut NDSPKI:userCertificate de l'objet Utilisateur
Affichage des propriétés d'un certificat utilisateur	◆ Parcourir sur l'objet Utilisateur
Exportation d'un certificat utilisateur	◆ Parcourir sur l'objet Utilisateur
Exportation de la clé privée et du certificat d'un utilisateur	◆ Vous devez être connecté en tant que l'utilisateur
Suppression d'un certificat utilisateur et de la clé privée	◆ Lire et Écrire sur l'attribut NDSPKI:userCertificateInfo ◆ Lire et Écrire sur l'attribut userCertificate
Validation des certificats utilisateur	◆ Parcourir sur l'objet Utilisateur
Révocation des certificats utilisateur	◆ Lire sur la clé privée de l'autorité de certification, Supprimer sur l'objet Utilisateur ou être connecté en tant que l'utilisateur et Écrire sur l'attribut userCertificate
Création d'un conteneur de racines approuvées	◆ Créer sur le conteneur de sécurité
Création d'un objet Racine approuvée	◆ Créer sur le conteneur Racine approuvée dans lequel résidera l'objet Racine approuvée

Tâches	Droits nécessaires sur les entrées
Affichage des propriétés d'un objet Racine approuvée	◆ Parcourir sur l'objet Racine approuvée
Remplacement d'un certificat de racine approuvée	◆ Lire et Écrire sur l'attribut NDSPKI:Not After de l'objet Racine approuvée ◆ Lire et Écrire sur l'attribut NDSPKI:Not Before de l'objet Racine approuvée ◆ Lire et Écrire sur l'attribut NDSPKI:Subject Name de l'objet Racine approuvée ◆ Lire et Écrire sur l'attribut NDSPKI:Trusted Root Certificate de l'objet Racine approuvée
Validation d'un certificat de racine approuvée	◆ Parcourir sur l'objet Racine approuvée
Révocation d'un certificat de racine approuvée	◆ Lire sur la clé privée de l'autorité de certification ou Supprimer sur l'objet Racine approuvée
Suppression d'un objet Racine approuvée	◆ Supprimer sur l'objet Racine approuvée
Création d'un conteneur CRL	◆ Superviseur sur le conteneur de sécurité ◆ Écrire sur l'attribut ndspkiCRLContainerDN de l'objet de l'autorité de certification organisationnelle
Suppression d'un conteneur CRL	◆ Supprimer sur le conteneur CRL
Création d'un objet Configuration CRL	◆ Superviseur sur le conteneur CRL
Activation d'un objet Configuration CRL	◆ Écrire sur l'attribut ndspkiCRLConfigurationDNList de l'objet de l'autorité de certification organisationnelle
Affichage et/ou modification des propriétés d'un objet Configuration CRL	Modification: ◆ Superviseur sur l'objet Configuration CRL ou ◆ Écrire sur l'attribut modifié de l'objet Configuration CRL Affichage: ◆ Parcourir sur l'objet Configuration CRL
Suppression d'un objet Configuration CRL	◆ Supprimer sur l'objet Configuration CRL
Création d'un objet CRL	◆ Superviseur sur l'objet Configuration CRL
Exportation d'un fichier CRL	◆ Lire pour l'attribut certificateRevocationList
Remplacement d'un fichier CRL	◆ Parcourir sur l'objet CRL
Affichage des propriétés d'un objet CRL	◆ Parcourir sur l'attribut certificateRevocationList
Suppression d'un objet CRL	◆ Supprimer sur le point de distribution CRL

Tâches	Droits nécessaires sur les entrées
Création d'un conteneur de sécurité	◆ Créer à la racine de l'arborescence eDirectory
Création d'un objet Service SAS	◆ Superviseur sur le conteneur de l'objet ◆ Écrire sur l'attribut SAS:Service DN sur le serveur pour lequel l'objet est créé.

26 Gestion des mots de passe

Cette section fournit une vue d'ensemble du mot de passe universel, des stratégies de mot de passe et du self-service des mots de passe.

- « Présentation du mot de passe universel » page 783
- « Présentation du stockage de mots de passe non réversibles » page 786
- « Stratégies de mot de passe » page 787
- « Déploiement du mot de passe universel » page 787
- « Gestion des mots de passe à l'aide de stratégies de mot de passe » page 792
- « Self-service de mot de passe » page 819
- « Application de mots de passe universels respectant la casse » page 836
- « Considérations relatives à la sécurité » page 839
- « Importation des mots de passe basés sur le hachage dans eDirectory » page 841

Présentation du mot de passe universel

Le mot de passe universel est géré par Secure Password Manager, un composant du module NMAS (NetIQ Modular Authentication Services). Secure Password Manager simplifie la gestion des modèles d'authentification par mot de passe pour une vaste gamme de solutions développées par NetIQ et ses partenaires. Les outils de gestion n'exposent qu'un mot de passe et ne montrent pas tout le traitement en arrière-plan qui s'exécute à des fins de compatibilité avec les versions précédentes.

Secure Password Manager et les autres composants qui gèrent ou utilisent le mot de passe universel sont installés avec eDirectory. Toutefois, le mot de passe universel n'est pas activé par défaut. Étant donné que toutes les API d'authentification et de définition de mots de passe évoluent pour prendre en charge le mot de passe universel, tous les outils de gestion existants fonctionnent automatiquement avec le mot de passe universel lorsqu'ils sont exécutés sur des clients dotés de ces nouvelles bibliothèques.

REMARQUE : le plug-in de gestion des mots de passe pour NetIQ eDirectory pour iManager 3.x peut être téléchargé sur le site Web de téléchargement NetIQ. Des informations sur la procédure de téléchargement et d'installation de ce plug-in sont disponibles sur le site de téléchargement.

Le logiciel Client Novell prend en charge le mot de passe universel. Il continue également de prendre en charge le mot de passe NDS pour les systèmes plus anciens du réseau. Une fois que le mot de passe universel a été configuré et activé pour un utilisateur, le client Novell a la possibilité de mettre à niveau/migrer automatiquement le mot de passe NDS vers le mot de passe universel.

Quel est le niveau de sécurité du mot de passe universel ?

Un chiffrement réversible du mot de passe universel est nécessaire pour garantir l'interopérabilité avec d'autres systèmes de mot de passe. Les administrateurs doivent évaluer les coûts et les avantages du système. L'utilisation d'un mot de passe universel stocké dans eDirectory pourrait se

révéler plus sûr ou plus pratique que de tenter de gérer plusieurs mots de passe différents. NetIQ fournit plusieurs niveaux de sécurité pour vous assurer que le mot de passe universel est protégé pendant qu'il est stocké dans eDirectory.

Un mot de passe universel est protégé par trois niveaux de sécurité :

- chiffrement du mot de passe proprement dit ;
- droits eDirectory ;
- droits du système de fichiers.

Le mot de passe universel est chiffré par une clé spécifique de l'utilisateur. Le mot de passe universel et la clé utilisateur sont stockés dans les attributs du système, uniquement lisibles par eDirectory. La clé utilisateur est stockée chiffrée avec la clé d'arborescence. Cette clé d'arborescence est protégée par une clé unique NICI (Novell International Cryptographic Infrastructure) sur chaque machine. Notez que ni la clé d'arborescence ni la clé NICI ne sont stockées dans eDirectory. Elles ne sont pas enregistrées avec les données qu'elles protègent.

La clé d'arborescence est présente sur chaque machine au sein d'une arborescence, mais chaque arborescence contient une clé d'arborescence différente. Les données chiffrées avec la clé d'arborescence ne peuvent donc être récupérées que sur un ordinateur au sein de la même arborescence. Par conséquent, lors de son stockage, le mot de passe universel est protégé par trois niveaux de chiffrement.

Chaque clé est également sécurisée via des droits eDirectory. Seuls les administrateurs avec le droit Superviseur ou les utilisateurs proprement dits disposent des droits pour modifier les mots de passe universels.

Les droits du système de fichiers permettent de garantir que seul un utilisateur disposant des droits appropriés peut accéder à ces clés.

Par défaut, la clé spécifique de l'utilisateur et la clé d'arborescence sont des clés 3DES. eDirectory 9.2 prend en charge les clés AES 256 bits. Pour créer une clé AES 256 bits, reportez-vous à la section Creating an AES 256-Bit Tree Key (Création d'une clé d'arborescence AES 256 bits) du manuel NICI Administration Guide (Guide d'administration de NICI). En tant qu'administrateur, vous pouvez rechiffrer les mots de passe à l'aide de l'utilitaire `diagpwd`. Pour plus d'informations, reportez-vous à la section « Utilitaire de diagnostic de mot de passe universel » page 817.

REMARQUE : la stratégie de mot de passe doit permettre à l'utilisateur exécutant cet utilitaire de récupérer son mot de passe universel.

Si le mot de passe universel est déployé dans un environnement nécessitant un niveau élevé de sécurité, vous pouvez prendre les précautions suivantes :

1. Vérifiez que les répertoires et fichiers suivants sont sécurisés :

Plate-forme	Répertoires/Fichiers
Windows	◆ `%SystemRoot%\SysWOW64\Novell\nici` ◆ `%SystemRoot%\System32\` où le fichier DLL NICI est installé
Linux	◆ `/var/opt/novell/nici` ◆ `/etc/opt/novell/nici64.cfg` ◆ `/opt/Novell/lib64/libccs2.so` et les bibliothèques NICI partagées dans le même répertoire

Consultez la documentation de votre système pour obtenir des détails spécifiques sur l'emplacement des fichiers NICI et eDirectory.

2. Comme avec n'importe quel système de sécurité, il est très important de restreindre l'accès physique au serveur sur lequel résident les clés.

Mot de passe universel

Auparavant, les administrateurs devaient gérer plusieurs mots de passe (mot de passe simple, mot de passe NDS, mot de passe étendu) en raison des limitations inhérentes aux mots de passe. Ils devaient également s'assurer de leur synchronisation.

- Mot de passe NDS : l'ancien mot de passe NDS est stocké dans un format haché irréversible. Ce mot de passe ne peut être utilisé que par le système NDS et ne peut pas être converti dans un autre format exploitable par un autre système.
- Mot de passe simple : à l'origine, le mot de passe simple a été implémenté pour permettre aux administrateurs d'importer des utilisateurs et des mots de passe (en texte clair et au format haché) à partir de répertoires nds-cluster-config étrangers tels qu'Active Directory et iPlanet.

  L'inconvénient du mot de passe simple est qu'il ne permet pas d'appliquer de stratégies de mot de passe (longueur minimale, expiration, etc.) .
- Mot de passe étendu : le mot de passe étendu n'est plus pris en charge par NetIQ. Le mot de passe étendu est le prédécesseur du mot de passe universel. Il permet l'implémentation de certaines stratégies de mot de passe, mais sa conception n'est pas cohérente avec d'autres mots de passe. Il fournit une synchronisation unidirectionnelle et remplace le mot de passe NDS ou simple.

NetIQ a introduit le mot de passe universel comme moyen de simplifier l'intégration et la gestion des différents systèmes de mot de passe et d'authentification dans un réseau cohérent.

Le mot de passe universel règle ces problèmes de plusieurs manières :

- Il permet d'utiliser un seul mot de passe pour tous les accès à eDirectory.
- Il permet d'utiliser des caractères étendus dans les mots de passe.
- Il permet d'appliquer des stratégies de mot de passe avancées.
- Il permet de synchroniser les mots de passe entre eDirectory et d'autres systèmes.

La plupart des fonctions de gestion des mots de passe nécessitent l'activation du mot de passe universel.

Pour plus d'informations, reportez-vous à la « Déploiement du mot de passe universel » page 787.

Stratégies de mot de passe

Le mot de passe universel offre la possibilité de créer des stratégies de mot de passe avancées. Une stratégie de mot de passe est un ensemble de règles définies par l'administrateur qui régissent les critères de création et de remplacement des mots de passe utilisateur. NMAS permet d'appliquer des stratégies de mot de passe que vous assignez à des utilisateurs dans eDirectory.

Les stratégies de mot de passe sont gérées à l'aide d'iManager.

Pour plus d'informations, reportez-vous à la « Gestion des mots de passe à l'aide de stratégies de mot de passe » page 792.

Synchronisation de mot de passe

La synchronisation de mots de passe entre plusieurs systèmes connectés est une fonctionnalité incluse avec NetIQ Identity Manager. Elle présente les avantages suivants :

- Synchronisation bidirectionnelle des mots de passe
- Application de stratégies de mot de passe sur des systèmes connectés
- Notification par message électronique en cas d'échec de la synchronisation
- Possibilité de vérifier l'état de synchronisation du mot de passe d'un utilisateur

Pour plus d'informations, reportez-vous au chapitre 3 Connected System Support for Password Synchronization (https://www.netiq.com/documentation/idm45/idm_password_management/data/bo1o7xz.html) (Prise en charge des systèmes connectés pour la synchronisation des mots de passe) du *NetIQ Identity Manager 4.5 Password Management Guide* (https://www.netiq.com/documentation/idm45/idm_password_management/data/bookinfo.html) (Guide de gestion des mots de passe NetIQ Identity Manager 4.5).

Présentation du stockage de mots de passe non réversibles

Les mots de passe universels sont stockés dans eDirectory après leur chiffrement et peuvent être récupérés par eDirectory lorsque cela est nécessaire. Par exemple, au moment de l'authentification.

Comme solution alternative aux mots de passe universels, eDirectory 9.2 prend en charge le stockage des mots de passe hachés à l'aide de l'algorithme de hachage PBKDF2 (Password-Based Key Derivation Function 2) (RFC 2898). Les mots de passe de l'utilisateur ne peuvent pas être récupérés si le hachage de mots de passe PBKDF2 est activé. Pour plus d'informations, reportez-vous à la section « Options de configuration du mot de passe universel » page 812.

IMPORTANT : À partir de la version 9.2 d'eDirectory, dans une stratégie de mot de passe, si les mots de passe universels sont désactivés, le hachage de mots de passe PBKDF2 est automatiquement activé. Les stratégies de mot de passe existantes dont les mots de passe universels sont désactivés ne sont pas appliquées aux utilisateurs avant la mise à niveau vers eDirectory 9.2. En revanche, si vous mettez à niveau votre serveur vers eDirectory 9.2, ces stratégies de mot de passe sont automatiquement appliquées à tous les utilisateurs de l'arborescence. Pour contourner ce comportement, supprimez toutes les assignations de ces stratégies de mot de passe avant d'effectuer la mise à niveau.

Si vous passez des mots de passe NDS aux mots de passe PBKDF2, vous devez également passer manuellement à la méthode de connexion SCRAM. Pour plus d'informations sur la méthode de connexion SCRAM, reportez-vous à la section « Authentification par mot de passe » page 674.

REMARQUE

- Les mots de passe créés à l'aide de l'algorithme de hachage PBKDF2 sont sensibles à la casse, contrairement contrairement aux mots de passe NDS.
- Les mots de passe créés à l'aide de l'algorithme de hachage PBKDF2 ne prennent pas en charge les règles `nspmXCharHistoryLimit` et `nspmXCharLimit` dans la stratégie de mot de passe.

- Par défaut, PBKDF2 est configuré pour utiliser SHA-256 et le nombre d'itérations de 1. Ces paramètres peuvent être modifiés à l'aide des attributs `nspmPBKDF2HashAlgorithm` et `nspmPBKDF2IterationCount`, respectivement. Les performances de la liaison LDAP diminuent si vous augmentez le nombre d'itérations.
- La méthode de connexion SCRAM ne prend pas en charge l'annexion d'un mot de passe à usage unique (OTP). Si des utilisateurs de l'arborescence utilisent la méthode de connexion NDS avec un mot de passe à usage unique basé sur le hachage (HOTP), n'autorisez pas l'utilisation de la méthode de connexion SCRAM pour ces utilisateurs.

Activation du stockage de mots de passe non réversibles

1. Démarrez NetIQ iManager.
2. Cliquez sur **Rôles et tâches** > **Mots de passe** > **Stratégie de mot de passe**.
3. Démarrez l'assistant de stratégie de mot de passe en cliquant sur **Nouveau**.
4. Entrez un nom pour la stratégie et cliquez sur **Suivant**.
5. Sélectionnez **Non** pour activer le hachage de mots de passe PBKDF2.
6. Fermez l'assistant de stratégie de mot de passe.

Stratégies de mot de passe

Le mot de passe universel offre la possibilité de créer des stratégies de mot de passe avancées. Une stratégie de mot de passe est un ensemble de règles définies par l'administrateur qui régissent les critères de création et de remplacement des mots de passe utilisateur. NMAS permet d'appliquer des stratégies de mot de passe que vous assignez à des utilisateurs dans eDirectory.

Les stratégies de mot de passe sont gérées à l'aide d'iManager.

Pour plus d'informations, reportez-vous à la « Gestion des mots de passe à l'aide de stratégies de mot de passe » page 792.

Déploiement du mot de passe universel

Cette section décrit comment déployer et gérer le mot de passe universel.

Suivez les instructions des sections 2.1 à 2.8 pour déployer le mot de passe universel :

- « Étape 1 : identifiez votre besoin d'un mot de passe universel » page 788
- « Étape 2 : vérifiez la disponibilité de votre conteneur de sécurité » page 788
- « Étape 3 : vérifiez que vos serveurs de clés de domaine SDI sont prêts pour le mot de passe universel » page 788
- « Étape 4 : vérifiez la cohérence des clés SDI pour l'arborescence » page 790
- « Étape 5 : activez le mot de passe universel » page 790
- « Compatibilité avec les versions précédentes » page 791
- « Administration des mots de passe » page 791
- « Problèmes à surveiller » page 791

Étape 1 : identifiez votre besoin d'un mot de passe universel

Si vous répondez par l'affirmative à toutes les questions suivantes, vous devriez prévoir de déployer et d'utiliser un mot de passe universel :

- Avez-vous l'intention de permettre à des utilisateurs internationaux d'accéder aux services Web de NetIQ ou d'utiliser le client Novell pour Windows pour accéder aux services de fichiers et d'impression Novell ?
- Avez-vous l'intention d'utiliser NetIQ Identity Manager, avec sa stratégie de mot de passe étendu et ses fonctionnalités de synchronisation des mots de passe ?

Étape 2 : vérifiez la disponibilité de votre conteneur de sécurité

NMAS compte stocker les stratégies globales dans l'arborescence eDirectory, qui est le domaine de sécurité effectif. Les règles de sécurité doivent être disponibles sur tous les serveurs de l'arborescence.

NMAS place les stratégies d'authentification et les données de configuration des méthodes de connexion dans le conteneur de sécurité créé au niveau de la partition [Racine]. Ces informations doivent être facilement accessibles à tous les serveurs utilisant NMAS. Le conteneur Sécurité a pour but d'héberger les stratégies globales relatives aux propriétés de sécurité telles que la connexion, l'authentification et la gestion des clés.

eDirectory 9.0 et versions ultérieures fournissent un caching du conteneur de sécurité. Cette fonctionnalité met en cache les données du conteneur de sécurité sur des serveurs locaux pour que NMAS ne soit pas obligé d'accéder au conteneur de sécurité à chaque tentative de connexion. Reportez-vous à la « Caching des objets Sécurité » page 677.

Avec NMAS et eDirectory 8.8.*x* et versions ultérieures, il est recommandé de créer le conteneur de sécurité en tant que partition distincte et de le répliquer largement. Cette partition doit être répliquée en tant que partition Lecture/écriture uniquement sur les serveurs de votre arborescence qui sont approuvés.

AVERTISSEMENT : étant donné que le conteneur Sécurité contient des règles globales, soyez attentifs à l'emplacement des répliques accessibles en écriture car ces serveurs peuvent modifier les règles de sécurité générales spécifiées dans l'arborescence eDirectory. Pour que les utilisateurs puissent se connecter avec NMAS, les répliques des objets Utilisateur et du conteneur de sécurité doivent se trouver sur le serveur NMAS.

Pour plus d'informations, consultez le document TID3393169 (http://www.novell.com/support/viewContent.do?externalId=3393169).

Étape 3 : vérifiez que vos serveurs de clés de domaine SDI sont prêts pour le mot de passe universel

Vous devez vous assurer que les serveurs de clés de domaine SDI respectent la configuration minimale requise et disposent de clés cohérentes pour la distribution et l'utilisation par d'autres serveurs au sein de l'arborescence. Ces étapes sont cruciales. Si vous ne les respectez pas comme indiqué, de sérieux problèmes de mot de passe risquent de survenir sur votre système lorsque vous activez le mot de passe universel.

1. À l'invite de commande du serveur Windows, exécutez `sdidiag.exe`.

Le fichier `sdidiag.exe` n'est pas fourni avec eDirectory. Une fois installé, exécutez `sdidiag.exe`. Le fichier est livré avec un correctif de sécurité () associé avec le document TID 2974092 (http://support.novell.com/docs/Readmes/InfoDocument/2974092.html).

2 Connectez-vous en tant qu'administrateur en entrant le serveur (contexte complet), le nom de l'arborescence, le nom d'utilisateur et le mot de passe.

3 Assurez-vous que tous vos serveurs utilisent des clés 168 bits pour la clé d'arborescence 3DES et des clés 256 bits pour la clé d'arborescence AES 256 bits.

   Suivez les instructions fournies dans le document TID 3364214 pour vous assurer que cette condition est satisfaite.

4 Entrez la commande `CHECK -v >> dossier_installation\sdinotes.txt`.

   Les résultats de la commande `CHECK` s'affichent à l'écran.

5 Si aucun problème n'est détecté, accédez à l'« Étape 4 : vérifiez la cohérence des clés SDI pour l'arborescence » page 790.

   ou

   Suivez les instructions consignées dans le fichier `dossier_installation\sdinotes.txt` pour résoudre les éventuels problèmes de configuration et de clé, puis passez à l'Étape 6.

6 Vérifiez que les serveurs de clés de domaine SDI exécutent NICI *3.0*.

   Si vous utilisez une version antérieure, mettez à niveau eDirectory vers la version 9.0 ou une version ultérieure. Cette opération mettra à niveau NICI à niveau respectivement vers la version 3.0 ou une version ultérieure :

7 (Facultatif) Exécutez de nouveau la commande `SDIDIAG CHECK`. Reportez-vous à l'Étape 4.

Pour plus d'informations sur l'utilisation de la commande SDIDIAG, reportez-vous au document TID 3364214 (http://www.novell.com/support/viewContent.do?externalId=3364214).

Ajout ou suppression d'un serveur de clés de domaine SDI

Pour supprimer un serveur de clés de domaine SDI, procédez comme suit :

1 Le fichier `sdidiag.exe` n'est pas fourni avec eDirectory. Il peut être téléchargé à partir du site de téléchargement Novell (http://download.novell.com/index.jsp). Une fois téléchargé, exécutez le fichier sdidiag.exe.

2 Connectez-vous en tant qu'administrateur doté de droits de gestion sur le conteneur de sécurité et les objets W0, KAP et Sécurité en indiquant le serveur (contexte complet), le nom de l'arborescence, le nom d'utilisateur et le mot de passe.

3 Entrez la commande `RS -s nom_serveur`.

   Par exemple, si `server1` existe dans le conteneur `PRV` de l'organisation `Novell` de l'arborescence `Novell_Inc`, entrez la valeur `.server1.PRV.Novell.Novell_Inc.` pour le nom du serveur.

Pour ajouter un serveur de clés de domaine SDI, procédez comme suit :

1 À partir d'un serveur Windows, ouvrez une fenêtre d'invite de commande et exécutez `sdidiag.exe`.

2 Connectez-vous en tant qu'administrateur en entrant le serveur (contexte complet), le nom de l'arborescence, le nom d'utilisateur et le mot de passe.

3 Entrez la commande `AS -s nom_serveur`.

   Par exemple, si `server1` existe dans le conteneur `PRV` de l'organisation `Novell` de l'arborescence `Novell_Inc`, entrez la valeur `.server1.PRV.Novell.Novell_Inc.` pour le nom du serveur.

Étape 4 : vérifiez la cohérence des clés SDI pour l'arborescence

Vérifiez que toutes les instances de clés cryptographiques sont cohérentes dans toute l'arborescence. Pour vous assurer que chaque serveur dispose des clés cryptographiques nécessaires pour communiquer en toute sécurité avec les autres serveurs de l'arborescence :

1. À l'invite de commande du serveur Windows, exécutez `sdidiag.exe`.
2. Entrez la commande `CHECK -v >> sys:system\sdinotes.txt -n DN_conteneur`.

   Par exemple, si l'utilisateur Bob existe dans le conteneur USR de l'organisation Acme de l'arborescence Acme_Inc, entrez la valeur `.USR.Acme.Acme_Inc.` pour le nom distinctif (DN) du conteneur.

   Les éventuels problèmes de cohérence de clés entre les différents serveurs et serveurs de domaines de clé sont alors signalés.

   Les résultats de la commande `CHECK` s'affichent à l'écran.
3. Si aucun problème n'est signalé, vous pouvez activer le mot de passe universel. Allez à l'« Étape 5 : activez le mot de passe universel » page 790.

   ou

   Si des problèmes sont signalés, suivez les instructions fournies dans le fichier `sdinotes.txt`.

   Dans la plupart des cas, vous êtes invité à exécuter la commande `RESYNC -T`. Cette commande peut être répétée chaque fois que NMAS signale des erreurs -1418 ou -1460 au cours de l'authentification par mot de passe universel.

   Pour plus d'informations sur les options et opérations SDIDIAG, reportez-vous aux documents suivants :

   - TID 3364214 (http://www.novell.com/support/viewContent.do?externalId=3364214)
   - TID 7005397 (http://www.novell.com/support/viewContent.do?externalId=7005397)

Étape 5 : activez le mot de passe universel

1. Démarrez NetIQ iManager.
2. Cliquez sur **Rôles et tâches** > **Mots de passe** > **Stratégie de mot de passe**.
3. Démarrez l'assistant de stratégie de mot de passe en cliquant sur **Nouveau**.
4. Entrez un nom pour la stratégie et cliquez sur **Suivant**.
5. Sélectionnez **Oui** pour activer le mot de passe universel.
6. Fermez l'assistant de stratégie de mot de passe.

IMPORTANT : Si vous assignez une règle à un conteneur qui est la racine d'une partition, l'assignation de règle est héritée par tous les utilisateurs de cette partition, y compris ceux présents dans les sous-conteneurs. Pour déterminer si un conteneur est la racine d'une partition, recherchez le conteneur et vérifiez la présence d'une icône de partition à proximité.

Si vous assignez une stratégie à un conteneur qui n'est pas la racine d'une partition, l'assignation de stratégie est héritée uniquement par les utilisateurs de ce conteneur spécifique. Elle n'est pas héritée par les utilisateurs des sous-conteneurs. Si vous souhaitez que la stratégie s'applique à tous les utilisateurs sous un conteneur qui n'est pas une racine de partition, vous devez assigner la stratégie à chaque sous-conteneur individuellement.

Compatibilité avec les versions précédentes

Le mot de passe universel est conçu pour assurer une compatibilité avec les versions précédentes des services existants. Par défaut, les mots de passe modifiés grâce à ce service peuvent être synchronisés avec les mots de passe simples et NDS sur l'objet Utilisateur. Vous pouvez choisir les mots de passe à synchroniser à l'aide du plug-in de gestion des mots de passe.

La seule exception est l'utilisation des caractères internationaux dans les mots de passe. Étant donné que les traductions de caractères sont différentes pour les clients plus anciens, les valeurs actuelles ne correspondent plus. Il est recommandé de mettre à niveau tous les logiciels Client Novell pour garantir le bon fonctionnement des mots internationaux à l'échelle du système.

L'infrastructure Novell NetWare Storage Management Services (SMS) est utilisée pour les applications de sauvegarde et de restauration NetIQ et de fabricants tiers. Les mots de passe système utilisés par ces produits NetIQ et de fabricants tiers ne peuvent pas contenir de caractères étendus s'ils doivent fonctionner dans un environnement mixte.

REMARQUE : reportez-vous au document TID 3065822 (http://www.novell.com/support/viewContent.do?externalId=3065822) pour identifier les applications et services compatibles avec le mot de passe universel, ainsi que les applications et services compatibles avec les caractères étendus. De nombreux services et applications peuvent utiliser des caractères étendus sans mot de passe universel.

Administration des mots de passe

Vous pouvez utiliser les méthodes suivantes pour administrer le mot de passe universel :

- **iManager (recommandé) :** l'administration des mots de passe à l'aide de NetIQ iManager entraîne automatiquement la synchronisation du mot de passe universel avec les mots de passe simples et NDS pour assurer la compatibilité avec les versions précédentes. La tâche NMAS dans iManager autorise la gestion granulaire des différents mots de passe et méthodes d'authentification installés et configurés sur le système.

  Dans iManager avec le plug-in de gestion des mots de passe, vous pouvez utiliser des stratégies de mot de passe pour spécifier comment le mot de passe universel est synchronisé avec les mots de passe NDS, simples et de distribution. En outre, une tâche iManager permet à l'administrateur de définir un mot de passe universel pour un utilisateur.
- **Applications de fabricants tiers :** des applications de fabricants tiers écrites dans les bibliothèques multi plates-formes NetIQ et qui assurent une gestion des mots de passe permettent également de définir le mot de passe universel et de synchroniser les autres mots de passe si les bibliothèques plus récentes sont installées sur le client Novell pour Windows.

Problèmes à surveiller

- Si vous désactivez le mot de passe NDS d'un utilisateur, il prend une valeur arbitraire inconnue de l'utilisateur. La liste suivante décrit comment certaines méthodes de connexion gèrent ce changement :
  - La méthode de mot de passe simple n'est pas désactivée si le mot de passe NDS est désactivé. La méthode de mot de passe simple utilise le mot de passe universel s'il est activé et disponible. Dans le cas contraire, elle utilise le mot de passe simple. Si le mot de passe universel est activé, mais pas défini, la méthode de mot de passe simple définit le mot de passe universel avec le mot de passe simple.

- La méthode de mot de passe étendu n'est pas désactivée si le mot de passe NDS est désactivé. Le mot de passe étendu n'utilise pas le mot de passe universel pour la connexion.
- La méthode de mot de passe NDS (mot de passe universel) n'est pas désactivée si le mot de passe NDS est désactivé. La méthode de mot de passe NDS utilise le mot de passe universel s'il est activé et disponible. Dans le cas contraire, elle utilise le mot de passe NDS. Si le mot de passe universel est activé, mais pas défini, la méthode de mot de passe NDS définit le mot de passe universel avec le mot de passe NDS.

- Lorsqu'un administrateur modifie le mot de passe universel d'un utilisateur, par exemple lors de la création d'un nouvel utilisateur ou en réponse à un appel du service d'assistance, le mot de passe précédent expire automatiquement pour des raisons de sécurité, si vous avez activé le paramètre d'expiration des mots de passe dans la stratégie de mot de passe. Il s'agit du paramètre **Number of days before password expires (0-365** (Nombre de jours avant l'expiration du mot de passe (0-365) dans la stratégie de mot de passe sous **Advanced Password Rules** (Règles de mot de passe avancées). Dans cette fonction, ce n'est pas le nombre de jours défini qui est important, c'est son activation.

  REMARQUE : pour remplacer ce comportement, sélectionnez l'option **Do not expire the user's password when the administrator sets the password** (Ne pas faire expirer le mot de passe de l'utilisateur lorsque l'administrateur l'a défini) dans la stratégie de mot de passe.

- Si vous créez une stratégie de mot de passe, activez le mot de passe universel et activez les règles de mot de passe avancées, ces dernières sont appliquées à la place des éventuels paramètres de mot de passe existants pour le mot de passe NDS. Les anciens paramètres de mot de passe sont ignorés. La fusion ou la copie des anciens paramètres est automatique lorsque vous créez des stratégies de mot de passe.

  Par exemple, si vous avez paramétré le nombre de connexions gracieuses que vous utilisez avec le mot de passe NDS, lorsque vous activez le mot de passe universel, vous devez reparamétrer les connexions gracieuses dans les règles de mot de passe avancées de la stratégie de mot de passe.

  NMAS remplace le paramètre de mot de passe NDS de l'objet Utilisateur avec les paramètres de stratégie de mot de passe correspondants. Par exemple, si le nombre de connexions gracieuses de l'objet Utilisateur correspond à 4, et à 5 pour la stratégie de mot de passe, lorsque l'utilisateur se connecte ou modifie le mot de passe, le nombre de connexions gracieuses de l'objet Utilisateur devient 5.

Gestion des mots de passe à l'aide de stratégies de mot de passe

Pour accroître la sécurité, vous pouvez utiliser des stratégies de mot de passe afin de définir des règles spécifiant comment les utilisateurs créent leur mot de passe. Pour réduire les coûts d'assistance technique, vous pouvez également fournir aux utilisateurs des options de libre service pour les mots de passe oubliés et pour la réinitialisation de mots de passe.

Cette section aborde les points suivants :

- « Présentation des fonctionnalités de la stratégie de mot de passe » page 793
- « Planification de stratégies de mot de passe » page 793
- « Tâches préalables à l'utilisation des stratégies de mot de passe » page 797
- « Création de règles de mot de passe » page 798
- « Assignation de stratégies de mot de passe aux utilisateurs » page 814

- « Recherche de la stratégie d'un utilisateur » page 816
- « Définition d'un mot de passe utilisateur » page 816
- « Utilitaire de diagnostic de mot de passe universel » page 817
- « Dépannage des stratégies de mot de passe » page 818

Pour plus d'informations sur le self-service de mot de passe oublié et le self-service de réinitialisation de mot de passe, reportez-vous à la « Self-service de mot de passe » page 819.

Présentation des fonctionnalités de la stratégie de mot de passe

Une règle de mot de passe est un ensemble de principes définis par l'administrateur et régissant les critères de création et de remplacement des mots de passe par les utilisateurs finals. NMAS permet d'appliquer des stratégies de mot de passe que vous assignez à des utilisateurs dans eDirectory.

Les stratégies de mot de passe peuvent également inclure des fonctionnalités de self-service de mot de passe oublié, afin de réduire les appels au service d'assistance concernant les mots de passe oubliés. Une autre fonctionnalité est le self-service de réinitialisation de mot de passe qui permet aux utilisateurs de modifier leur mot de passe pendant qu'ils affichent les règles que l'administrateur a définies dans la stratégie de mot de passe. Les utilisateurs accèdent à ces fonctions via l'application utilisateur Identity Manager ou la console en self-service d'iManager.

L'utilisation d'une stratégie de mot de passe exige que vous activiez le mot de passe universel pour vos utilisateurs si vous souhaitez utiliser les règles de mot de passe avancées, la synchronisation de mot de passe et bon nombre des fonctionnalités de mot de passe oublié. Pour plus d'informations sur le déploiement du mot de passe universel, reportez-vous à la « Déploiement du mot de passe universel » page 787.

Pour créer des stratégies de mot de passe, utilisez l'assistant de stratégie de mot de passe. Dans iManager, cliquez sur **Mots de passe** > **Password Policies** (Stratégies de mot de passe) > **Nouveau**. Pour plus d'informations sur la création de stratégies de mot de passe, reportez-vous à la « Création de règles de mot de passe » page 798.

Planification de stratégies de mot de passe

- « Planification de l'assignation des stratégies de mot de passe dans l'arborescence » page 793
- « Planification des règles pour vos stratégies de mot de passe » page 794
- « Planification des méthodes de connexion et de changement de mot de passe pour vos utilisateurs » page 795

Planification de l'assignation des stratégies de mot de passe dans l'arborescence

Nous vous recommandons d'assigner une stratégie par défaut à l'ensemble de l'arborescence et d'assigner les éventuelles autres stratégies que vous utilisez aussi haut que possible dans l'arborescence, afin de simplifier l'administration.

NMAS détermine la stratégie de mot de passe effective pour un utilisateur. Pour plus d'informations, reportez-vous à la « Assignation de stratégies de mot de passe aux utilisateurs » page 814.

Planification des règles pour vos stratégies de mot de passe

Vous pouvez utiliser les règles de mot de passe avancées dans une stratégie de mot de passe pour appliquer vos stratégies d'entreprise pour les mots de passe.

Rappelez-vous que Novell Client (4.9.1), l'application utilisateur Identity Manager et la console en self-service d'iManager affichent les règles de mot de passe de la stratégie de mot de passe. Si vos utilisateurs vont changer leur mot de passe via le serveur LDAP ou sur un système connecté, vous devez rendre les règles de mot de passe facilement accessibles aux utilisateurs pour aider à ces derniers à créer des mots de passe conformes.

Si vous utilisez la synchronisation de mot de passe, n'oubliez pas de vérifier que les utilisateurs à qui sont assignées des stratégies de mot de passe correspondent aux utilisateurs qui doivent participer à la synchronisation de mot de passe entre les systèmes connectés. Les stratégies de mot de passe sont assignées dans une perspective centrée sur l'arborescence. En revanche, la synchronisation de mot de passe est configurée par pilote pour chaque serveur. Pour que la synchronisation de mot de passe donne les résultats escomptés, vérifiez que les utilisateurs situés dans une réplique maîtresse ou Lecture-écriture sur le serveur sur lequel s'exécutent les pilotes pour la synchronisation correspondent aux conteneurs pour lesquels vous avez assigné des stratégies de mot de passe avec le mot de passe universel activé. L'assignation d'une stratégie de mot de passe au conteneur racine d'une partition garantit que cette stratégie s'applique à tous les utilisateurs de ces conteneurs et sous-conteneurs.

Règles de mot de passe avancées

Les règles de mot de passe avancées vous permettent de définir les critères suivants pour le mot de passe universel :

- La durée de vie du mot de passe : les règles de mot de passe offrent les mêmes fonctions de stratégie que celles offertes précédemment par eDirectory, de sorte que vous pouvez spécifier la fréquence à laquelle un mot de passe doit être changé et s'il peut être réutilisé.
- Le contenu d'un mot de passe : vous pouvez exiger une combinaison de lettres, de chiffres, de majuscules ou de minuscules et de caractères spéciaux. Vous pouvez exclure les mots de passe que vous ne jugez pas sûrs, comme le nom de votre société. Vous pouvez également exiger qu'un certain nombre de caractères dans un mot de passe soient « nouveaux », autrement dit inutilisés dans les mots de passe précédents. Vous pouvez aussi configurer le nombre de violations de stratégies de mot de passe autorisées dans un mot de passe spécifié.

Pour utiliser les règles de mot de passe avancées dans une stratégie de mot de passe, vous devez activer le mot de passe universel. Si vous n'activez pas pour une stratégie de mot de passe universel, les restrictions de mot de passe défini pour le mot de passe NDS® sont appliquées à la place.

REMARQUE : lorsque vous créez une stratégie de mot de passe et que vous activez le mot de passe universel, les règles de mot de passe avancées sont appliquées à la place des paramètres de mot de passe existants pour le mot de passe NDS. Les anciens paramètres de mot de passe sont ignorés. La fusion ou la copie des anciens paramètres est automatique lorsque vous créez des stratégies de mot de passe.

Par exemple, si vous avez paramétré le nombre de connexions gracieuses que vous utilisez avec le mot de passe NDS, lorsque vous activez le mot de passe universel, vous devez reparamétrer les connexions gracieuses dans les règles de mot de passe avancées de la stratégie de mot de passe.

Si, par la suite, vous désactivez le mot de passe universel dans la stratégie de mot de passe, les paramètres de mot de passe existants que vous aviez ne sont plus ignorés et sont appliqués pour le mot de passe NDS.

Les versions 3.1 et ultérieures de NMAS remplacent le paramètre de mot de passe NDS de l'objet Utilisateur avec les paramètres de stratégie de mot de passe correspondants. Par exemple, si le nombre de connexions gracieuses de l'objet Utilisateur correspond à 4, et à 5 pour la stratégie de mot de passe, lorsque l'utilisateur se connecte ou modifie le mot de passe, le nombre de connexions gracieuses de l'objet Utilisateur devient 5.

Application des stratégies

Lorsque vous assignez une stratégie de mot de passe aux utilisateurs de l'arborescence, les changements de mot de passe suivants doivent respecter les règles de mot de passe avancées dans cette stratégie. Dans le client Novell 4.9 SP2 ou version ultérieure, les règles sont également affichées. Dans les deux méthodes d'accès, un mot de passe non conforme est rejeté. NMAS est l'application qui applique ces règles.

Vous pouvez spécifier dans la stratégie que la conformité des mots de passe existants est vérifiée et que les utilisateurs sont tenus de changer les mots de passe non conformes existants. Un mot de passe est considéré comme ayant expiré lorsque l'option de vérification de la conformité est activée et que le mot de passe ne satisfait pas aux règles de stratégie de mot de passe.

Vous pouvez également spécifier que lorsque les utilisateurs s'authentifient via un portail, ils sont invités à configurer les fonctions de mot de passe oublié que vous avez activées. Il s'agit des services de post-authentification. Par exemple, si vous voulez que les utilisateurs créent un indice de mot de passe pouvant être envoyé par message électronique lorsqu'ils oublient un mot de passe, vous pouvez utiliser les services de post-authentification pour inviter les utilisateurs à créer cet indice au moment de la connexion.

Le paramètre post-authentification est la dernière option sur la page de propriétés du mot de passe oublié.

Planification des méthodes de connexion et de changement de mot de passe pour vos utilisateurs

Un utilisateur peut se connecter ou changer un mot de passe de différentes manières. Pour plus d'informations sur la mise à niveau pour la prise en charge du mot de passe universel, reportez-vous à la « Déploiement du mot de passe universel » page 787.

Cette section décrit la configuration requise pour la prise en charge du mot de passe universel dans les différents cas :

- « Client Novell » page 795
- « Application utilisateur Identity Manager et iManager » page 796
- « Autres protocoles » page 797
- « Systèmes connectés » page 797

Client Novell

Si vous utilisez le client Novell, mettez-le à niveau vers la version 4.9 SP2 ou une version ultérieure.

Rappelez-vous que l'utilisation du client Novell n'est pas obligatoire étant donné que les utilisateurs peuvent se connecter via la console en self-service d'iManager ou d'autres portails d'entreprise en fonction de votre environnement. De plus, le client Novell n'est plus requis pour la synchronisation de mot de passe sous Active Directory.

Le tableau suivant décrit les différences entre les versions du client Novell concernant le mot de passe universel et émet des suggestions pour la gestion des clients Novell hérités.

Tableau 26-1 Mot de passe universel avec les clients Novell hérités

Version du client Novell	Connexion	Modifier le mot de passe
Antérieure à 4.9	Ne passe pas par NMAS et ne prend donc pas en charge le mot de passe universel. La connexion est établie directement à l'aide du mot de passe NDS.	Change le mot de passe NDS directement, sans passer par NMAS. Si vous utilisez le mot de passe universel, cela peut signifier que le mot de passe NDS et le mot de passe universel ne sont pas synchronisées. Pour éviter cela, vous avez trois possibilités : ◆ Mettez à niveau tous les clients vers la version 4.9 ou une version ultérieure. ◆ Empêchez les clients hérités de changer les mots de passe à l'aide d'une valeur d'attribut sur un conteneur. Dans ce cas, les clients hérités peuvent toujours se connecter, mais ils ne peuvent plus changer le mot de passe. Les changements de mot de passe doivent être effectués à l'aide d'une version plus récente d'iManager ou du client Novell. ◆ Utilisez le paramètre de stratégie de mot de passe pour l'option **Retirer le mot de passe NDS lors de la définition du mot de passe universel**. Il s'agit d'une mesure drastique, car elle empêche à la fois la connexion et le changement de mot de passe via le mot de passe NDS.
4.9	Prend en charge le mot de passe universel.	Applique les règles de stratégie de mot de passe pour le mot de passe universel. Si un utilisateur tente de créer un mot de passe non conforme, le changement de mot de passe est rejeté. La liste des règles n'est cependant pas présentée aux utilisateurs.
4.9 SP2 ou version ultérieure	Prend en charge le mot de passe universel.	Applique les règles de stratégie de mot de passe pour le mot de passe universel. Présente en outre les règles aux utilisateurs pour leur permettre de créer des mots de passe conformes.

Application utilisateur Identity Manager et iManager

L'application utilisateur Identity Manager et iManager proposent un self-service de mot de passe qui permet aux utilisateurs de réinitialiser des mots de passe et de configurer une fonction en self-service de mot de passe oublié si la stratégie de mot de passe la prévoit. Pour plus d'informations sur la configuration du self-service de mot de passe, reportez-vous à la « Self-service de mot de passe » page 819.

- Dans les stratégies de mot de passe, il est recommandé d'accepter le paramètre par défaut pour l'option **Synchroniser le mot de passe NDS lors de la définition du mot de passe universel**.

Autres protocoles

Assurez-vous qu'eDirectory, le serveur LDAP, NMAS et iManager sont mis à niveau pour prendre en charge le mot de passe universel.

Pour plus d'informations sur l'utilisation de CIFS, d'AFP et d'autres protocoles avec le mot de passe universel, reportez-vous à la « Déploiement du mot de passe universel » page 787.

Systèmes connectés

Si vous utilisez la synchronisation de mot de passe Identity Manager, assurez-vous que les conditions suivantes sont satisfaites afin que les changements de mot de passe utilisateur réussissent :

- Tous les pilotes Identity Manager du système ont été mis à niveau au format Identity Manager.
- La configuration des pilotes Identity Manager comprend les nouvelles stratégies de synchronisation de mot de passe.
- Les paramètres de synchronisation de mot de passe doivent indiquer que le mot de passe universel est à utiliser, ainsi que le mot de passe de distribution si vous souhaitez une synchronisation de mot de passe bidirectionnelle.
- Les filtres de mot de passe ont été déployés sur le système connecté pour capturer les mots de passe, si nécessaire.

Pour plus d'informations, reportez-vous au chapitre Connected System Support for Password Synchronization (Prise en charge des systèmes connectés pour la synchronisation des mots de passe) du *NetIQ Identity Manager 5 Password Management Guide* (Guide de gestion des mots de passe NetIQ Identity Manager 4.5).

Tâches préalables à l'utilisation des stratégies de mot de passe

Si vous souhaitez bénéficier de toutes les fonctionnalités des stratégies de mot de passe, vous devez effectuer certaines opérations pour préparer votre environnement.

1. Mettez à niveau votre environnement pour prendre en charge le mot de passe universel.

   Pour plus d'informations, reportez-vous à la « Déploiement du mot de passe universel » page 787.

2. Mettez à niveau votre environnement client pour prendre en charge le mot de passe universel.

   Reportez-vous à la section « Planification des méthodes de connexion et de changement de mot de passe pour vos utilisateurs » page 795 ainsi qu'à la « Déploiement du mot de passe universel » page 787.

3. Si vous n'avez pas exécuté l'assistant de configuration d'iManager précédemment lors de la configuration d'iManager, dans le cadre de son installation ou ultérieurement, vous devez l'exécuter maintenant. Pour plus d'informations sur l'exécution de cet assistant, reportez-vous à la section Services basés sur le rôle du *Guide d'administration de NetIQ iManager*.

   IMPORTANT : après avoir exécuté l'assistant de configuration d'iManager, le programme s'exécute en mode RBS. Cela signifie que les administrateurs ne voient aucune tâche, sauf s'ils se sont assignés à des rôles spécifiques. Assurez-vous que vous assignez des administrateurs aux rôles pour leur donner accès à toutes les tâches d'iManager.

   ---

4. Installez le plug-in de gestion des mots de passe de NetIQ iManager.

Il est disponible pour téléchargement sur le site Web de téléchargement NetIQ (http://dl.netiq.com/).

IMPORTANT : si vous effectuez la mise à niveau vers la dernière version du plug-in de gestion des mots de passe de NetIQ iManager sans réaliser au préalable la mise à niveau d'eDirectory et que vous essayez ensuite de modifier ou de créer une stratégie de mot de passe, iManager affiche un message d'erreur.

---

5 Configurez SSL entre le serveur Web iManager et eDirectory, même s'ils s'exécutent sur le même ordinateur.

6 Configurez l'objet Groupe-Serveur LDAP dans eDirectory de manière à exiger TLS en cas de liaison simple.

Il s'agit du paramètre par défaut lorsque vous configurez iManager. Il est fortement recommandé d'exiger TLS en cas de liaison simple pour la fonction de self-service de mot de passe. C'est par ailleurs une nécessité pour pouvoir utiliser la tâche iManager **Mots de passe** > **Set Universal Password** (Définir le mot de passe universel).

Si vous exigez TLS en cas de liaison simple, aucune configuration supplémentaire n'est nécessaire pour le port SSL LDAP.

IMPORTANT : si vous choisissez de ne pas exiger TLS en cas de liaison simple, cela signifie que les utilisateurs sont autorisés à se connecter à la console en self-service d'iManager à l'aide d'un mot de passe en texte clair.

Vous pouvez utiliser cette option, mais une étape supplémentaire est nécessaire.

Par défaut, la fonction de self-service de mot de passe suppose que le port SSL LDAP est celui indiqué dans le paramètre `System.DirectoryAddress` du fichier `PortalServlet.properties`. Si votre port SSL LDAP est différent, vous devez indiquer le port approprié en ajoutant la paire de clés suivante pour le fichier `PortalServlet.properties` :

`LDAPSSLPort=`*`your_port_number`*

Par exemple, si vous exécutez Tomcat, vous devez ajouter cette paire de clés dans le fichier `PortalServlet.properties` contenu dans le répertoire `tomcat\webapps\nps\WEB_INF`.

---

7 Pour activer la notification par message électronique pour les fonctions de mot de passe oublié, suivez la procédure de la « Configuration de la notification par message électronique pour le self-service de mot de passe » page 833.

Vous devez configurer le serveur SMTP et personnaliser les modèles de message électronique.

Vous êtes maintenant prêt à utiliser toutes les fonctions des stratégies de mot de passe. Créez les règles comme indiqué à la « Création de règles de mot de passe » page 798.

Création de règles de mot de passe

L'assistant de stratégie de mot de passe dans iManager permet de créer des stratégies de mot de passe.

Reportez-vous à l'aide en ligne pour obtenir des informations sur chaque étape de l'assistant, ainsi qu'aux informations contenues dans la « Gestion des mots de passe à l'aide de stratégies de mot de passe » page 792 et la « Self-service de mot de passe » page 819.

1 Assurez-vous d'avoir effectué les étapes de la « Tâches préalables à l'utilisation des stratégies de mot de passe » page 797.

Ces étapes préparent votre système pour pouvoir utiliser toutes les fonctions des stratégies de mot de passe.

2 Dans iManager, dans la vue **Rôles et tâches**, cliquez sur **Mots de passe** > **Stratégie de mot de passe**.

3 Cliquez sur **Nouveau** pour créer une stratégie de mot de passe.

4 Suivez les procédures décrites dans l'Assistant pour créer des règles de mot de passe avancées, des options de configuration du mot de passe universel et des sélections de mot de passe oublié pour la règle.

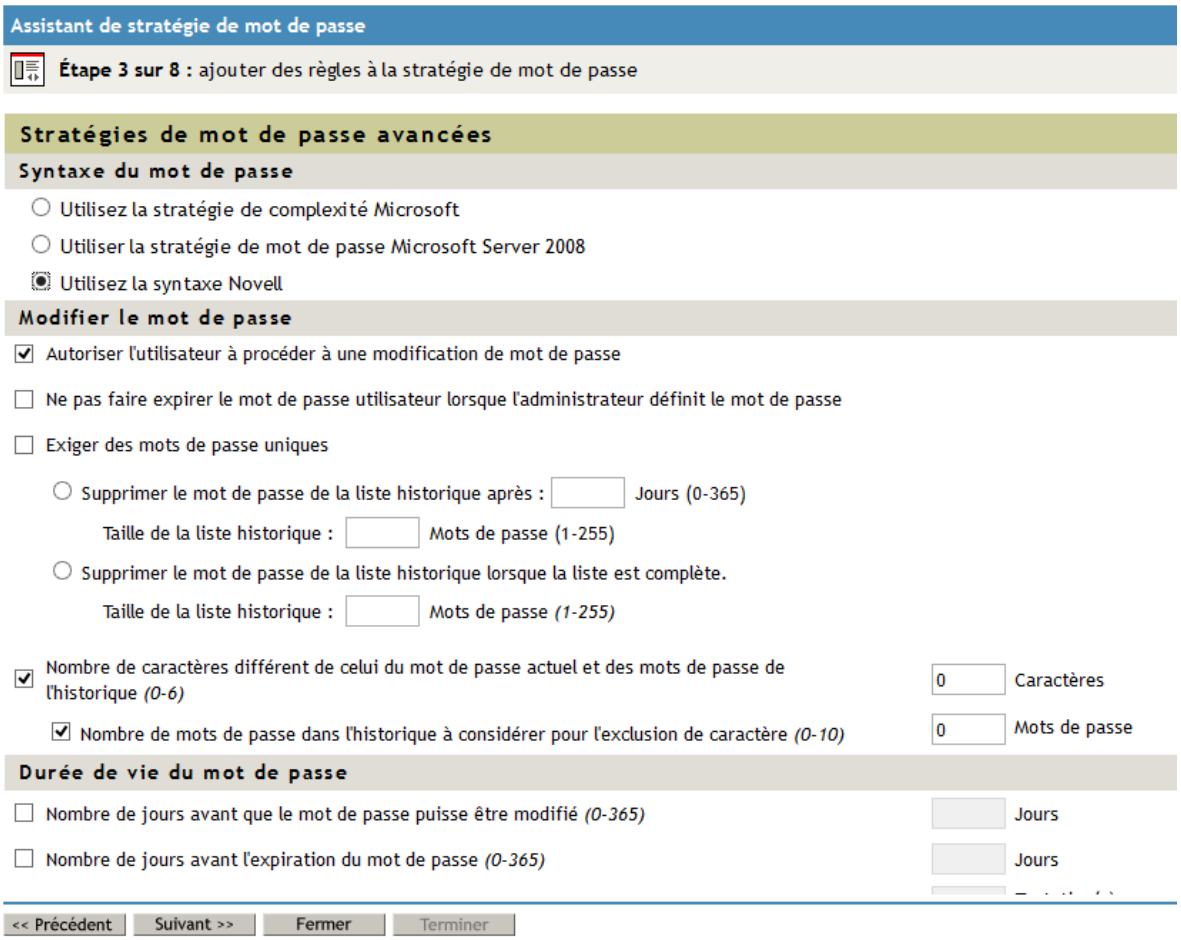
5 Assignez la stratégie de mot de passe à des utilisateurs, des organisations ou à l'ensemble de votre entreprise, selon vos besoins.

6 Passez en revue les paramètres de la nouvelle stratégie, puis cliquez sur **Terminer**, puis sur **Fermer** pour fermer l'assistant.

Règles de mot de passe avancées

La Figure 26-1 affiche la première section des règles de mot de passe avancées :

Figure 26-1 *Règles de mot de passe avancées*



Syntaxe de mot de passe

Vous pouvez spécifier l'une des trois options de syntaxe de mot de passe à utiliser pour une stratégie de mot de passe :

- **Utiliser la stratégie de complexité Windows**

- **Utiliser la stratégie de mot de passe de Microsoft Server 2008**
- **Utiliser la syntaxe Novell**

AVERTISSEMENT : iManager permet de créer une stratégie à l'aide du type de stratégie de mot de passe Microsoft Server 2008, quelle que soit la version de NMAS installée sur votre serveur. Toutefois, vous devez disposer de NMAS 3.3.4 ou version ultérieure pour utiliser cette option. Si une version antérieure de NMAS est installée, la nouvelle stratégie de mot de passe ne fonctionne pas correctement.

- **Utiliser la stratégie de complexité Windows**

  Ce paramètre vous permet d'utiliser la configuration requise pour la stratégie de complexité Microsoft*. Utilisez cette option si vous devez synchroniser des mots de passe entre eDirectory et Microsoft Active Directory.

  Si vous sélectionnez cette option pour une stratégie, tous les utilisateurs auxquels la stratégie est assignée doivent créer des mots de passe répondant aux critères de la stratégie de complexité Microsoft telle qu'implémentée dans le mot de passe universel. Les critères sont notamment :

  - La longueur minimale du mot de passe est de 6 caractères.
  - La longueur maximale du mot de passe est de 128 caractères.
  - Le mot de passe doit contenir au moins un caractère de trois des quatre types de caractères suivants, à savoir, caractères majuscules, minuscules, numériques et spéciaux :
    - Caractères majuscules : tous les caractères majuscules des ensembles Latin de base et Latin-1.
    - Caractères minuscules : tous les caractères minuscules des ensembles Latin de base et Latin-1.
    - Caractères numériques : 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9.
    - Caractères spéciaux : tous les autres caractères.
  - Les valeurs des attributs utilisateur suivants ne peuvent pas être contenues dans le mot de passe : `CN` (nom commun), `Given Name` (Prénom), `Surname` (Nom), `Full Name` (Nom complet) et `displayName` (Nom d'affichage).
  - Le mot de passe ne peut pas contenir la valeur complète de l'attribut utilisateur `CN` pour le compte eDirectory. NMAS n'effectue pas cette vérification si la longueur de l'attribut est inférieure à trois caractères.

- **Utiliser la stratégie de mot de passe de Microsoft Server 2008**

  Ce paramètre vous permet d'utiliser les exigences de complexité de stratégie de mot de passe Microsoft* Windows Server 2008. Utilisez cette option si vous devez synchroniser des mots de passe entre eDirectory et Microsoft Active Directory.

  Si vous sélectionnez cette option pour une stratégie, tous les utilisateurs auxquels la stratégie est assignée doivent créer des mots de passe répondant aux critères de la stratégie de complexité Microsoft Windows Server 2008 telle qu'implémentée dans le mot de passe universel. Si vous sélectionnez cette option, plusieurs options sur la page Règles de mot de passe avancées sont définies pour respecter les critères de la stratégie de complexité. Les critères sont notamment :

  - La longueur minimale du mot de passe est, par défaut, de 7 caractères. Vous pouvez configurer la longueur minimale du mot de passe dans votre environnement à l'aide de l'option **Nombre minimum de caractères dans le mot de passe (1-512)**. Pour plus d'informations sur la configuration du nombre minimal de caractères, reportez-vous à la section « Longueur du mot de passe » page 807.

- La longueur maximale du mot de passe est de 512 caractères.
- Le mot de passe doit contenir au moins un caractère de trois des cinq types de caractères suivants, à savoir, caractères majuscules, minuscules, numériques, non-alphanumériques et autres :
  - Caractères majuscules : tous les caractères en majuscules de langues européennes, comportant des marques diacritiques, ainsi que des caractères grecs et cyrilliques.
  - Caractères minuscules : tous les caractères en minuscules de langues européennes, comportant des marques diacritiques, ainsi que des caractères grecs et cyrilliques.
  - Caractères numériques : 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9.
  - Caractères non alphanumériques : un des caractères spéciaux suivants: () ' ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / _.
  - Autres caractères : un ou plusieurs caractères Unicode classés parmi les caractères alphabétiques, mais pas en majuscules ni en minuscules. Cela comprend les caractères Unicode des langues asiatiques.
- Le mot de passe ne peut contenir aucun mot de la liste des mots de passe exclus. NMAS n'effectue pas cette vérification si la longueur du mot de passe exclu est inférieure à trois caractères. Pour plus d'informations sur les mots de passe exclus, reportez-vous à la section « Exclusions de mots de passe » page 805.
- Le mot de passe ne peut pas contenir la valeur complète de l'attribut `CN` ni l'intégralité ou une partie de la valeur de l'attribut `Full Name` (Nom complet), si l'attribut contient au moins trois caractères et forme un seul mot. Une partie de la valeur d'attribut est définie comme au moins trois caractères consécutifs délimités aux deux extrémités par les caractères suivants : des virgules, des points, des tirets, des traits d'union, des traits de soulignement, des espaces, des dièses ou des tabulations.

  REMARQUE : lors de l'utilisation de la stratégie de mot de passe 2008 de Microsoft, les attributs `CN` et `displayName` sont considérés comme étant similaires à la règle `samAccountName` et `displayName` dans AD.

- Le nombre maximal de violations de stratégie de complexité autorisé dans un mot de passe est, par défaut, de 2. Vous pouvez configurer le nombre de violations de la complexité autorisées à l'aide de l'option **Maximum number of complexity policy violations in password (0-5)** (Nombre maximal de violations de stratégie de complexité de mot de passe [0-5]). Pour plus d'informations sur la configuration du nombre maximal de violations autorisées, reportez-vous à la section « Violations de la complexité du mot de passe » page 807.

- **Utiliser la syntaxe Novell**

  Cette option vous permet d'utiliser la syntaxe Novell pour la stratégie de mot de passe. Cette option est sélectionnée par défaut. Les paramètres standard pour les stratégies utilisant la syntaxe Novell sont les suivants :

  - La longueur minimale du mot de passe est, par défaut, de 4 caractères. Vous pouvez configurer la longueur minimale du mot de passe dans votre environnement à l'aide de l'option **Nombre minimum de caractères dans le mot de passe (1-512)**. Pour plus d'informations sur la configuration du nombre minimal de caractères, reportez-vous à la section « Longueur du mot de passe » page 807.
  - La longueur maximale du mot de passe est, par défaut, de 12 caractères. Vous pouvez configurer la longueur maximale du mot de passe dans votre environnement à l'aide de l'option **Nombre maximum de caractères dans le mot de passe (1-512)**. Pour plus d'informations sur la configuration du nombre maximal de caractères, reportez-vous à la section « Longueur du mot de passe » page 807.

Priorité pour la syntaxe de mot de passe

Si vous modifiez les attributs d'une stratégie de mot de passe à l'aide de l'Administration de l'annuaire ou de LDAP, en dehors de l'interface de plug-in de gestion des mots de passe iManager, vous pouvez configurer un conflit entre un ou plusieurs types de stratégies de mot de passe. Par exemple, vous pouvez utiliser LDAP pour activer les deux types de stratégie : la stratégie de complexité Microsoft et la stratégie de mot de passe de Microsoft Windows 2008 pour la même stratégie.

En cas de conflit, eDirectory utilise l'ordre de priorité suivant :

- Stratégie de mot de passe de Microsoft Windows 2008
- Stratégie de complexité de Microsoft
- Syntaxe Novell

Pour plus d'informations sur la modification des stratégies de mot de passe en dehors de l'interface de gestion des mots de passe, reportez-vous à la section « Modification des stratégies de mot de passe en dehors de l'interface de stratégies de mot de passe » page 811.

Modifier le mot de passe

- **Permettre à l'utilisateur d'initier le changement de mot de passe**

  Cette option permet à l'utilisateur d'utiliser les fonctions de self-service de mot de passe. Cette option est sélectionnée par défaut. Pour plus d'informations sur le self-service de mot de passe, reportez-vous à la « Self-service de mot de passe » page 819.

- **Do not expire the user's password when the administrator sets the password** (Ne pas faire expirer le mot de passe de l'utilisateur lorsque l'administrateur l'a défini)

  Cette option demande à l'utilisateur de modifier son mot de passe. Cette fonction permet de remplacer le paramètre par défaut. Le comportement par défaut dans eDirectory, lorsque l'expiration du mot de passe est définie, est de faire expirer le mot de passe lorsque l'administrateur l'a défini.

- **Exiger des mots de passe uniques**

  Lorsque cette option est sélectionnée, l'utilisateur n'est pas autorisé à réutiliser un mot de passe qui figure déjà dans l'historique. Si un utilisateur tente de changer le mot de passe et de réutiliser un mot de passe de l'historique, la stratégie de mot de passe refuse le mot de passe et l'utilisateur est invité à en spécifier un autre.

  Vous pouvez préciser dans quelle mesure les mots de passe uniques doivent être appliqués à l'aide d'une des deux valeurs suivantes :

  - **Supprimer le mot de passe de l'historique après un certain nombre de jours (0-365)** et **Taille de l'historique (1-255)**.

    Si vous avez besoin de mots de passe uniques, vous pouvez spécifier le nombre de jours pendant lequel un mot de passe précédent reste stocké dans l'historique à des fins de comparaison.

    Par exemple, si vous spécifiez une limite de 30 jours et que le précédent mot de passe de l'utilisateur était « montagnes99 », ce mot de passe est conservé dans l'historique pendant 30 jours. Au cours de cette période, si l'utilisateur tente de modifier son mot de passe et de réutiliser « montagnes99 », la stratégie de mot de passe refuse ce mot de passe et l'utilisateur est invité à en spécifier un autre. À l'issue de la période de 30 jours, l'ancien mot de passe n'est plus stocké à des fins de comparaison et la stratégie de mot de passe vous autorise donc à le réutiliser.

Si vous avez besoin de mots de passe uniques, vous pouvez également indiquer le nombre de mots de passe stockés dans l'historique à des fins de comparaison. Par exemple, si vous spécifiez 3, les trois derniers mots de passe de l'utilisateur sont conservés. Si un utilisateur tente de modifier son mot de passe et d'en réutiliser un qui figure dans l'historique avant le nombre de jours spécifié pour être supprimé de l'historique, la stratégie de mot de passe refuse le mot de passe et l'utilisateur est invité à en spécifier un autre.

REMARQUE

- Si l'option **Use Microsoft Server 2008 Password Policy** (Utiliser la stratégie de mot de passe Microsoft Server 2008) est sélectionnée, l'option **Exiger des mots de passe uniques** est également sélectionnée par défaut.
- Si l'option **Exiger des mots de passe uniques** est sélectionnée et que vous sélectionnez l'option **Supprimer le mot de passe de l'historique après un certain nombre de jours (0-365)** sans spécifier le nombre de jours, le mot de passe est conservé dans l'historique 8 fois plus longtemps que la valeur définie dans le champ **Nombre de jours avant l'expiration du mot de passe (0-365)** dans la section Durée de vie du mot de passe. Si aucune valeur n'est spécifiée dans ces champs, le mot de passe est conservé dans l'historique pendant 365 jours.
- Si vous spécifiez une taille pour l'historique des mots de passe et un nombre de jours, et que le nombre de mots de passe indiqué dans le champ Taille de l'historique de mot de passe a été atteint, l'utilisateur n'est pas autorisé à changer son mot de passe, sauf s'il a expiré. Un administrateur peut modifier ou définir un mot de passe utilisateur, même si la taille autorisée pour l'historique des mots de passe a été atteinte.
- Après l'expiration d'un ou plusieurs mots de passe de la liste de l'historique des mots de passe, la liste n'est plus complète, et l'utilisateur est de nouveau en mesure de modifier son mot de passe. Cette limitation est incluse pour empêcher que les utilisateurs ne modifient leur mot de passe plusieurs fois jusqu'à ce que leur mot de passe ne figure plus dans l'historique des mots de passe et qu'ils puissent ainsi le réutiliser.
- Si aucune taille n'est spécifiée pour l'historique de mot de passe, l'historique n'est jamais complet.
- Lors de la comparaison d'un mot de passe spécifié aux anciens mots de passe de l'historique, eDirectory fonctionne différemment d'Active Directory. Si la taille de l'historique des mots de passe est « N », Active Directory compare le mot de passe spécifié aux « N » derniers mots de passe. Toutefois, eDirectory compare le mot de passe spécifié aux « N + 1 » derniers mots de passe.

- **Supprimer le mot de passe de l'historique lorsqu'il est plein** et le nombre de mots de passe atteint la **taille spécifiée dans l'historique** (1-255).

  Si vous avez besoin de mots de passe uniques, vous pouvez indiquer le nombre de mots de passe stockés dans l'historique à des fins de comparaison. Cette option fonctionne selon le principe « premier entré, premier sorti », où les mots de passe plus anciens sont supprimés en premier de l'historique. Par exemple, lorsqu'un utilisateur crée un nouveau mot de passe qui ne figure pas actuellement dans l'historique, le plus ancien mot de passe de l'historique est supprimé si l'historique est plein.

REMARQUE

- Si l'option **Use Microsoft Server 2008 Password Policy** (Utiliser la stratégie de mot de passe de Microsoft Server 2008) est sélectionnée, alors l'option **Supprimer le mot de passe de l'historique lorsqu'il est plein** est également sélectionnée par défaut. Lorsque la syntaxe de Microsoft Server 2008 est activée, la plage **Taille de l'historique** s'étend de 0 à 24 mots de passe.

- Si cette option est sélectionnée, vous devez également sélectionner les deux options **Nombre de jours restant avant que le mot de passe puisse être changé** et **Nombre de jours avant l'expiration du mot de passe** et indiquer le nombre minimal de jours pour chacune.
- Si vous spécifiez une taille de 0 pour l'historique de mots de passe, NMAS compare uniquement tout nouveau mot de passe créé par un utilisateur au mot de passe actuel de cet utilisateur.

- **Number of characters different from current password and passwords from history (0-6)** (Nombre de caractères différents entre le mot de passe actuel et les mots de passe de l'historique [0-6]) et un certain nombre de caractères.

  Lorsque cette option est sélectionnée, l'utilisateur doit spécifier un mot de passe qui inclut plusieurs « nouveaux » caractères inutilisés dans les mots de passe précédents, comme indiqué dans le paramètre. Cette option est sélectionnée par défaut.

  Vous pouvez préciser dans quelle mesure les caractères inutilisés doivent être uniques à l'aide de la valeur suivante :

  - **Number of passwords in history to be considered for character exclusion (0-10)** (Nombre de mots de passe dans l'historique à prendre en considération pour l'exclusion de caractères [0-10]) et un certain nombre de caractères

    Si vous avez besoin d'un certain nombre de caractères inutilisés pour tout nouveau mot de passe, vous pouvez spécifier le nombre d'anciens mots de passe à prendre en considération lors de la vérification des caractères précédemment utilisés pour un mot de passe.

    Par exemple, si vous spécifiez un minimum de trois nouveaux caractères et spécifiez que les cinq derniers mots de passe doivent être pris en compte pour l'exclusion de caractères, et si un utilisateur crée le nouveau mot de passe « montagnes99 », ce mot de passe doit inclure au moins trois caractères ne figurant dans aucun des cinq mots de passe précédents. Si l'avant-dernier mot de passe de l'utilisateur était « lantagnes99 », avec seulement deux caractères de différence par rapport au nouveau mot de passe, la stratégie de mot de passe refuse ce mot de passe, et l'utilisateur est invité à en spécifier un autre.

REMARQUE

- Les deux options **Number of characters different from current password and passwords from history (0-6)** (Nombre de caractères différents entre le mot de passe actuel et les mots de passe de l'historique [0-6]) et **Number of passwords in history to be considered for character exclusion (0-10)** (Nombre de mots de passe dans l'historique à prendre en considération pour l'exclusion de caractères [0-10]) sont sélectionnées par défaut. Toutefois, les valeurs de ces deux options sont définies sur 0 par défaut.
- Si la valeur de l'option **Number of characters different from current password and passwords from history (0-6)** (Nombre de caractères différents entre le mot de passe actuel et les mots de passe de l'historique [0-6]) est définie sur 0, l'option est désactivée.
- Si la valeur de l'option **Number of passwords in history to be considered for character exclusion (0-10)** (Nombre de mots de passe dans l'historique à prendre en considération pour l'exclusion de caractères [0-10]) est définie sur 0, seul le mot de passe actuel est pris en compte lorsqu'eDirectory vérifie les « nouveaux » caractères.
- Pour ces options, le mot de passe universel doit être activé dans la stratégie de mot de passe.

Durée de vie du mot de passe

- **Nombre de jours restant avant que le mot de passe puisse être changé (0-365)**

Cette option empêche l'utilisateur de modifier son mot de passe universel avant l'expiration du délai spécifié. Par exemple, si cette valeur est définie sur 30, un utilisateur doit conserver le même mot de passe pendant 30 jours avant de pouvoir le changer.

- **Nombre de jours avant l'expiration du mot de passe (0-365)**

  Cette option entraîne l'expiration du mot de passe d'un utilisateur passé le délai spécifié. Par exemple, si cette valeur est définie sur 90, le mot de passe d'un utilisateur expire 90 jours après sa création. Si vous activez les connexions gracieuses, l'utilisateur peut se connecter avec un mot de passe ayant expiré le nombre de fois spécifié. En outre, si vous n'avez pas sélectionné l'option Limiter le nombre de connexions gracieuses autorisées, un nombre illimité de connexions gracieuses est autorisé.

REMARQUE

- Si l'option **Use Microsoft Server 2008 Password Policy** (Utiliser la stratégie de mot de passe de Microsoft Server 2008) est sélectionnée, les options **Nombre de jours restant avant que le mot de passe puisse être changé** et **Nombre de jours avant l'expiration du mot de passe** sont également sélectionnées par défaut. Lorsque la syntaxe de Microsoft Server 2008 est activée, la plage pour ces deux options s'étend de 0 à 999 jours.
- Lorsqu'un administrateur modifie le mot de passe d'un utilisateur, par exemple lors de la création d'un nouvel utilisateur ou en réponse à un appel de dépannage, le mot de passe précédent expire automatiquement si vous avez activé le paramètre d'expiration des mots de passe dans la stratégie de mots de passe. Pour cette fonction, le nombre de jours défini n'est pas important, mais ce paramètre doit être activé. Sélectionner l'option **Do not expire the user's password when the administrator sets the password** (Ne pas faire expirer le mot de passe de l'utilisateur lorsque l'administrateur l'a défini) remplace cette amélioration de sécurité.

- **Limiter le nombre de connexions bonus autorisées (0-254)**

  Lorsque le mot de passe expire, cette valeur indique le nombre de fois qu'un utilisateur est autorisé à se connecter à eDirectory à l'aide d'un mot de passe ayant expiré. Si les connexions gracieuses ne sont pas activées, l'utilisateur ne pourra plus se connecter si son mot de passe a expiré et il devra contacter l'administrateur pour réinitialiser son mot de passe. Si la valeur est 1 ou plus, l'utilisateur a peut se connecter le nombre de fois indiqué avant d'être forcé à changer le mot de passe. Toutefois, si l'utilisateur ne modifie pas le mot de passe avant que toutes les connexions gracieuses soient utilisées, il est verrouillé et ne parvient plus à se connecter à eDirectory. En outre, si vous n'avez pas sélectionné l'option **Limiter le nombre de connexions gracieuses autorisées**, un nombre de connexions gracieuses illimitées est autorisé.

Exclusions de mots de passe

- **Exclure les mots de passe suivants**

  Cette option vous permet d'entrer manuellement les mots de passe que vous souhaitez exclure. Elle permet d'exclure des mots ou des caractères spécifiques, mais pas un modèle ni un attribut eDirectory. Vous pouvez également exclure des mots de passe qui contiennent un caractère spécial spécifique, notamment *, +, %, ou un espace. Par exemple, si vous ajoutez le caractère * à la liste des mots de passe exclus, un utilisateur qui a tenté d'entrer le mot de passe « Pa55w0rd*! » reçoit une erreur indiquant que le mot de passe spécifié n'est pas valide. Cela peut être utile si vous devez empêcher les utilisateurs de spécifier des mots de passe qui contiennent des caractères spéciaux qui provoquent des problèmes avec les applications dans votre environnement.

Pour NMAS 3.1.3 et version ultérieure, les chaînes dans la liste d'exclusion ne peuvent pas être contenues dans le mot de passe et la comparaison ne tient pas compte de la casse. Par exemple, si « test » figure dans la liste d'exclusion, les éléments suivants ne peuvent pas être des mots de passe : Test, TEST, ltest, test1, etc.

N'oubliez pas que les exclusions de mots de passe peuvent être utiles pour quelques mots qui représentent selon vous des risques en matière de sécurité. Bien qu'une fonctionnalité de liste d'exclusion soit fournie, elle n'est pas conçue pour devenir une longue liste de termes de type dictionnaire. Une longueur excessive des listes de termes exclus peut perturber les performances du serveur. Plutôt que de configurer une longue liste d'exclusions pour vous protéger contre les « attaques de dictionnaire » perpétrées sur les mots de passe, nous recommandons d'utiliser les règles de mot de passe avancées pour imposer l'emploi de nombres dans les mots de passe.

- **Excluez les mots de passe qui concordent avec les valeurs d'attribut**

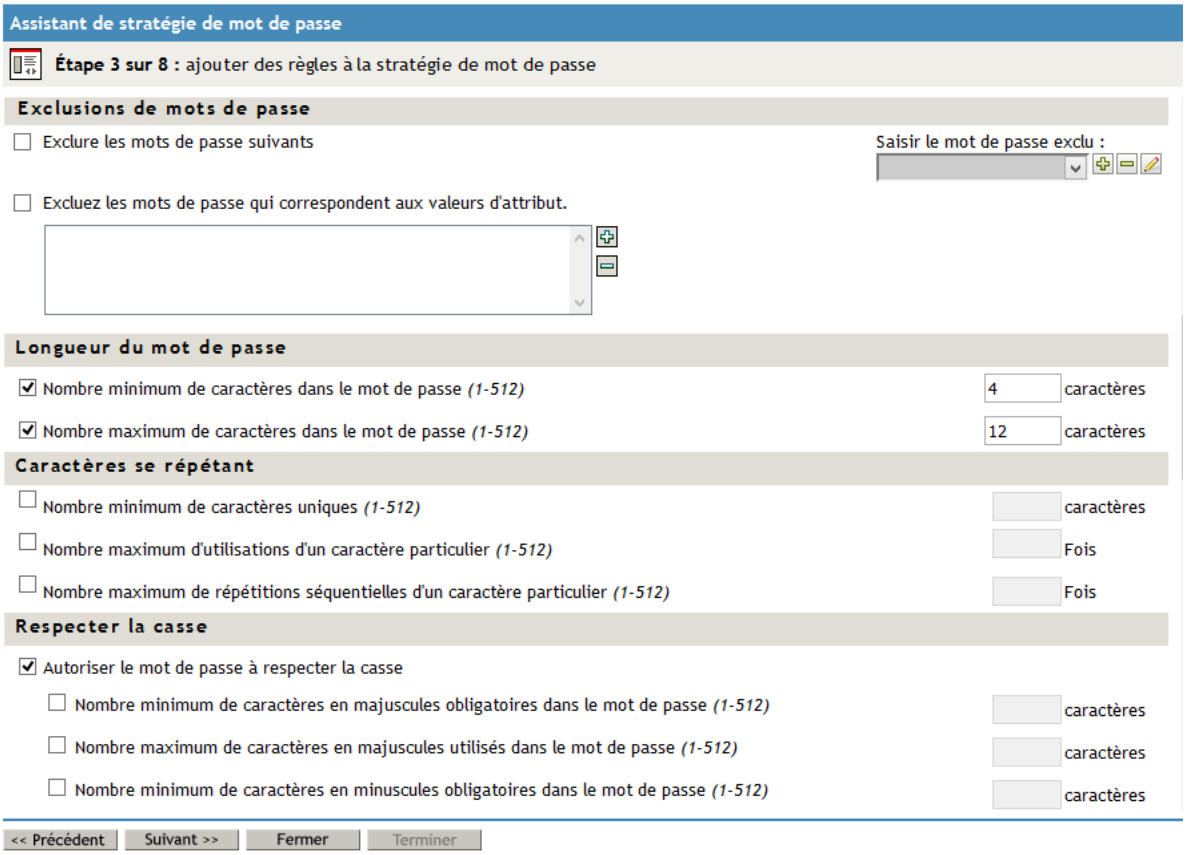
  Cette option vous permet de sélectionner les attributs des objets Utilisateur dont vous voulez empêcher l'utilisation en tant que mots de passe. Par exemple, si vous ajoutez l'attribut Nom Donné à la liste, et si l'attribut Nom Donné contenait la valeur de Franck, alors franck, franck1 ou 1franck ne pourraient pas être utilisés comme mot de passe.

  NMAS n'effectue pas cette vérification si la longueur du mot de passe exclu est inférieure à trois caractères.

  Utilisez les boutons plus ou moins pour ajouter et supprimer des valeurs d'attribut de la liste.

REMARQUE : si l'option **Utiliser la stratégie de complexité Microsoft**, l'option **Excluez les mots de passe qui concordent avec les valeurs d'attribut** est également sélectionnée par défaut. Lorsque la syntaxe de stratégie de complexité Microsoft est activée, la liste des valeurs d'attribut à faire correspondre est pré-remplie avec les attributs suivants : `Nom commun`, `Nom d'affichage`, `Nom complet`, `Prénom` et `Nom de famille`.

Figure 26-2 *Règles de mot de passe avancées (Suite)*



Longueur du mot de passe

- **Nombre minimum de caractères dans le mot de passe (1-512)**
- **Nombre maximum de caractères dans le mot de passe (1-512)**

REMARQUE

- La longueur maximale de tout mot de passe créé à l'aide de NMAS est de 512 caractères.
- Si l'option **Utiliser la stratégie de complexité Microsoft** est sélectionnée, ni l'option **Nombre minimum de caractères dans le mot de passe** ni l'option **Nombre maximum de caractères dans le mot de passe** ne sont disponibles.
- Si l'option **Use Microsoft Server 2008 Password Policy** (Utiliser la stratégie de mot de passe de Microsoft Server 2008) est sélectionnée, seule l'option **Nombre minimum de caractères dans le mot de passe** est disponible. Cette option est sélectionnée par défaut.
- Si l'option **Utiliser la syntaxe Novell** est sélectionnée, les options **Nombre minimum de caractères dans le mot de passe** et **Nombre maximum de caractères dans le mot de passe** sont également sélectionnées par défaut.

Violations de la complexité du mot de passe

- **Nombre maximum de violations de la stratégie de complexité dans le mot de passe (0-5)**

Cette option vous permet, en tant qu'administrateur, de configurer le nombre de violations de stratégie de complexité que vous souhaitez autoriser pour les mots de passe dans votre environnement. Par défaut, la stratégie de mot de passe de Microsoft Server 2008 requiert qu'un mot de passe contienne au moins un caractère provenant de trois des cinq types de caractères, à savoir des caractères en majuscules, en minuscules, numériques, non alphanumériques et autres. Par conséquent, le nombre de violations autorisé par défaut est de 2. Pour plus d'informations sur les exigences de stratégie pour la stratégie de mot de passe de Microsoft Server 2008, reportez-vous à la section « Syntaxe de mot de passe » page 799.

Toutefois, si vous souhaitez rendre votre stratégie de mot de passe plus ou moins restrictive, vous pouvez modifier le nombre de violations autorisé par défaut. Par exemple, si vous modifiez le paramètre par défaut et le définissez sur 1, tous les mots de passe doivent inclure au moins un caractère provenant de quatre types des cinq types de caractères indiqués ci-dessus. Si la valeur est de 4, les mots de passe doivent inclure un caractère provenant d'un seul des cinq types de caractères.

REMARQUE : L'option **Maximum number of complexity policy violations in password (0-5)** (Nombre maximum de violations de la stratégie de complexité dans le mot de passe [0-5]) n'est disponible que si vous sélectionnez l'option **Use Microsoft Server 2008 Password Policy** (Utiliser la stratégie de mot de passe de Microsoft Server 2008). Cette option est sélectionnée par défaut.

Caractères répétés

- **Nombre minimum de caractères uniques (1-512)**
- **Nombre maximum d'utilisations d'un caractère particulier (1-512)**
- **Nombre maximum de répétitions séquentielles d'un caractère particulier (1-512)**

REMARQUE : Si l'option **Utiliser la stratégie de complexité Microsoft** ou l'option **Use Microsoft Server 2008 Password Policy** (Utiliser la stratégie de mot de passe de Microsoft Server 2008) est sélectionnée, alors les options **Nombre minimum de caractères uniques**, **Nombre maximum d'utilisations d'un caractère particulier** et **Nombre maximum de répétitions séquentielles d'un caractère particulier (1-512)** ne sont pas disponibles.

Sensible à la casse

Dans eDirectory, vous pouvez utiliser l'option **Autoriser le mot de passe à respecter la casse** pour que vos mots de passe respectent la casse pour tous les clients mis à niveau vers eDirectory 9.2.

REMARQUE

- L'option **Autoriser le mot de passe à respecter la casse** n'est disponible que si vous sélectionnez l'option **Utiliser la syntaxe Novell**. Cette option est sélectionnée par défaut.
- Si vous avez choisi de désactiver le mot de passe universel, l'option de respect de la casse est vérifiée et désactivée par défaut.

L'option **Autoriser le mot de passe à respecter la casse** n'est disponible que si vous sélectionnez l'option **Utiliser la syntaxe Novell**. Cette option est sélectionnée par défaut.

Si l'option **Autoriser le mot de passe à respecter la casse** est sélectionnée, vous disposez de quatre options :

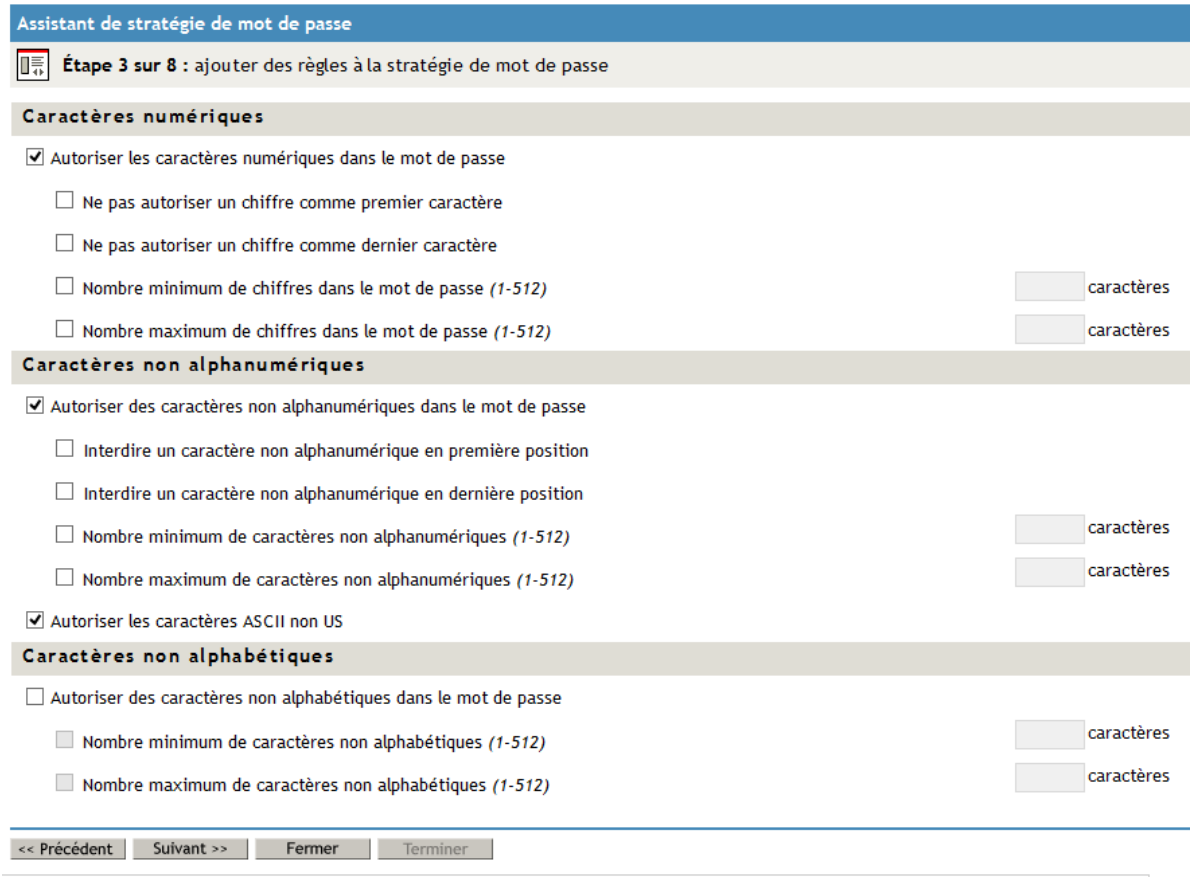
- **Autoriser le mot de passe à respecter la casse**
  - **Nombre minimum de caractères en majuscules obligatoires dans le mot de passe (1-512)**
  - **Nombre maximum de caractères en majuscules autorisés dans le mot de passe (1-512)**
  - **Nombre minimum de caractères en minuscules obligatoires dans le mot de passe (1-512)**
  - **Nombre maximum de caractères en minuscules autorisés dans le mot de passe (1-512)**

Lorsque l'option **Autoriser le mot de passe à respecter la casse** n'est pas sélectionnée, les mots de passe respectent la casse et vous disposez de deux options :

- **Nombre minimum de caractères alphabétiques autorisés dans le mot de passe (1-512)**
- **Nombre maximum de caractères alphabétiques autorisés dans le mot de passe (1-512)**

IMPORTANT : les mots de passe sont conservés avec la casse et sont synchronisés entre les systèmes en respectant la casse, même si l'option **Allow passwords to be case sensitive** (Autoriser les mots de passe à être sensibles à la casse) n'est pas sélectionnée. La casse de caractères du mot de passe est ignorée si l'option **Autoriser le mot de passe à respecter la casse** n'est pas sélectionnée.

Figure 26-3 *Règles de mot de passe avancées (Fin)*



Caractères numériques

- **Autoriser les caractères numériques dans le mot de passe**
  - **Ne pas autoriser un chiffre comme premier caractère**
  - **Ne pas autoriser un chiffre comme dernier caractère**
  - **Nombre minimum de chiffres dans le mot de passe (1-512)**
  - **Nombre maximum de chiffres dans le mot de passe (1-512)**

REMARQUE : l'option **Autoriser les caractères numériques dans le mot de passe** n'est disponible que si vous sélectionnez l'option **Utiliser la syntaxe Novell**. Cette option est sélectionnée par défaut.

Caractères non alphanumériques

Les caractères non alphanumériques sont des caractères qui ne sont ni des chiffres (0-9) ni des caractères alphabétiques. Les caractères alphabétiques comprennent les lettres a-z, A-Z et les caractères alphabétiques de la page 850 de codes Latin-1.

- **Autoriser des caractères non alphanumériques dans le mot de passe**
  - **Interdire un caractère non alphanumérique en première position**
  - **Interdire un caractère non alphanumérique en dernière position**
  - **Nombre minimum de caractères non alphanumériques (1-512)**
  - **Nombre maximum de caractères non alphanumériques (1-512)**
- **Autoriser les caractères ASCII non US**

  Cette option permet d'inclure dans le mot de passe des caractères ne figurant pas dans le jeu de caractères latins de base, également appelés « caractères étendus ».

REMARQUE : l'option **Autoriser des caractères non alphanumériques dans le mot de passe** n'est disponible que si vous sélectionnez l'option **Utiliser la syntaxe Novell**. Cette option est sélectionnée par défaut.

Caractères non alphabétiques

Les caractères non alphabétiques sont les caractères qui ne sont pas des caractères alphabétiques. Les caractères alphabétiques comprennent les lettres a-z, A-Z et les caractères alphabétiques de la page 850 de codes Latin-1.

- **Autoriser des caractères non alphabétiques dans le mot de passe**
  - **Nombre minimum de caractères non alphabétiques (1-512)**
  - **Nombre maximum de caractères non alphabétiques (1-512)**

REMARQUE

- L'option **Autoriser des caractères non alphabétiques dans le mot de passe** n'est disponible que si vous sélectionnez l'option **Utiliser la syntaxe Novell**.
- Si vous utilisez l'option **Autoriser des caractères non alphabétiques dans le mot de passe**, vérifiez que votre stratégie ne limite pas à tort les mots de passe possibles. Par exemple, vous pouvez créer une stratégie qui requiert plusieurs caractères non alphabétiques ou des chiffres, mais aussi des *limites* du nombre de caractères non alphabétiques autorisé.

Modification des stratégies de mot de passe en dehors de l'interface de stratégies de mot de passe

Outre la création, la modification et l'assignation de stratégies de mot de passe à l'aide du plug-in de gestion de mot de passe d'iManager, vous pouvez modifier les stratégies en dehors de l'interface des stratégies de mot de passe de l'une des manières suivantes :

- Modification de l'objet Stratégie directement à l'aide de l'interface d'administration de l'annuaire.
- Modification de l'objet Stratégie directement à l'aide de l'outil de ligne de commande ldapmodify.

Toutefois, il est déconseillé de manipuler les stratégies de mot de passe en dehors de l'interface de stratégies de mot de passe, étant donné que cette manipulation risque d'entraîner des problèmes dans votre environnement si tous les attributs ne sont pas correctement définis. Si vous définissez plusieurs types de stratégie pour une seule stratégie par exemple, seul le type le plus élevé de stratégies est pris en compte et eDirectory ignore toutes les règles de stratégies de niveau inférieur appliquées. Pour plus d'informations sur la priorité de type de stratégie de mot de passe, reportez-vous à la section « Priorité pour la syntaxe de mot de passe » page 802.

En outre, si vous remplacez le type de stratégie de mot de passe Microsoft Server 2008 par le type de stratégie de complexité de Microsoft sans utiliser l'interface de stratégie de mot de passe, iManager ne supprime pas l'attribut de la stratégie de mot de passe Microsoft Server 2008 (`nspmAD2K8Syntax`) existant de l'objet Stratégie. À la place, iManager définit la valeur de l'attribut sur `False` (Faux). Dans ce cas, eDirectory ignore toutes les stratégies et règles définies pour chaque type de stratégie.

Un autre problème peut se produire lorsque vous utilisez LDAP pour modifier les règles spécifiques d'une stratégie. Si la modification d'une stratégie entraîne un conflit entre deux règles, eDirectory applique une règle sélectionnée ou définie sur `True` (Vrai) dans la stratégie au lieu d'une règle en conflit qui n'est pas sélectionnée ni définie sur `False` (Faux).

Par exemple, vous pouvez créer une stratégie et ensuite la modifier pour ne pas autoriser les caractères numériques et autoriser les caractères non alphabétiques. Étant donné que la valeur de l'attribut `nspmNonAlphaCharactersAllowed` est définie sur `True` (Vrai), tous les caractères non alphabétiques sont autorisés, y compris les caractères numériques, même si l'attribut `nspmNumericCharactersAllowed` est défini sur `False` (Faux).

Génération de mot de passe aléatoire

Au lieu d'indiquer un mot de passe spécifique, les utilisateurs peuvent également demander un mot de passe généré de façon aléatoire. Les mots de passe généré de façon aléatoire respectent automatiquement les exigences de complexité et autres restrictions de la stratégie de mot de passe assignée à l'utilisateur.

Mots de passe de Microsoft Server 2008 générés de façon aléatoire

Les mots de passe générés de façon aléatoire pour les stratégies de mot de passe de Microsoft Server 2008 diffèrent des mots de passe générés de façon aléatoire utilisant d'autres types de stratégie de mot de passe. Les différences sont les suivantes :

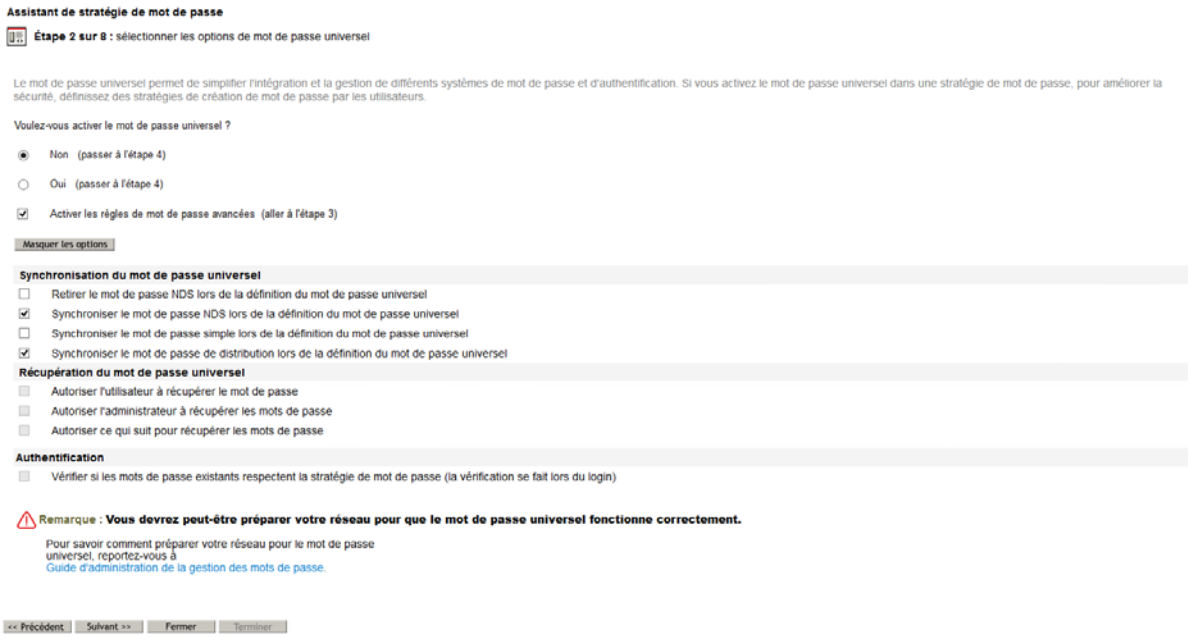
- Si un utilisateur se voit assigner une stratégie de mot de passe qui utilise le type de stratégie de mot de passe de Microsoft Server 2008 et demande un mot de passe généré de façon aléatoire, NMAS génère le mot de passe en fonction du nombre de violations de la complexité de mot de passe autorisé pour la stratégie.

- Si le nombre de violations de la complexité de mot de passe autorisé est défini sur la valeur maximale de 5, tous les mots de passe générés de façon aléatoire se composent uniquement de caractères alphabétiques en majuscules ou en minuscules.
- Si les exigences de la complexité de mot de passe configurées sont extrêmement strictes, même les mots de passe générés de façon aléatoire pourraient ne pas être valides pour la stratégie de mot de passe.
- La longueur maximale de tout mot de passe généré de façon aléatoire par la stratégie de mot de passe de Microsoft Server 2008 est de 16 caractères, sauf si la longueur minimale configurée dans la stratégie est de plus de 16 caractères. Si la longueur minimale est supérieure à 16 caractères, la longueur du mot de passe généré est la longueur minimale définie dans la stratégie. Par exemple, si la longueur minimale d'un mot de passe est définie sur 20 caractères à l'aide d'une stratégie de Microsoft Server 2008, le mot de passe généré de façon aléatoire est toujours de 20 caractères.

Options de configuration du mot de passe universel

La figure suivante illustre un exemple des options de configuration de mot de passe universel :

Figure 26-4 *Options de configuration*



- **Activer le mot de passe universel**

  Active le mot de passe universel pour cette stratégie. Vous pouvez activer ou désactiver le mot de passe universel.

- **Activer les règles de mots de passe avancées**

  Active les règles de mot de passe avancées définies sur la page des règles de mot de passe avancées pour cette stratégie. Ces règles de mots de passe avancées vous aident à sécuriser votre environnement, en vous permettant de contrôler la durée de vie et le contenu des mots de passe.

- **Synchronisation de mot de passe**
  - **Retirer le mot de passe NDS lors de la définition du mot de passe universel**

Si cette option est cochée, le mot de passe NDS est désactivé lorsque le mot de passe universel est défini. En outre, lorsque le mot de passe NDS est défini, la valeur de hachage du mot de passe NDS est défini sur une valeur aléatoire inconnue, sauf pour eDirectory. Une valeur de mot de passe pourrait éventuellement être hachée sur la base d'une valeur aléatoire.

- **Synchroniser le mot de passe NDS lors de la définition du mot de passe universel**

  Si cette option est sélectionnée et que le mot de passe universel est défini, le mot de passe NDS est défini simultanément avec le même mot de passe.

- **Synchroniser le mot de passe simple lors de la définition du mot de passe universel**

  REMARQUE : la définition de cette option n'affecte pas votre capacité à importer des mots de passe utilisateur à l'aide d'ICE.

  Si cette option est sélectionnée et que le mot de passe universel est défini, le mot de passe simple est défini simultanément et utilise le même mot de passe.

- **Synchroniser le mot de passe de distribution lors de la définition du mot de passe universel**

  Détermine si le moteur méta-annuaire d'Identity Manager peut récupérer ou définir le mot de passe universel d'un utilisateur dans eDirectory.

  Si cette option est sélectionnée et que le mot de passe universel est défini, le mot de passe de distribution est défini simultanément et utilise le même mot de passe.

  Le mot de passe de distribution peut être utilisé avec Identity Manager pour effectuer la synchronisation de mot de passe sur les systèmes connectés. Cette option permet également au moteur méta-annuaire de récupérer le mot de passe universel d'un utilisateur dans eDirectory.

- **Récupération du mot de passe universel**

  REMARQUE : si vous avez choisi de désactiver le mot de passe universel, les options ci-dessous sont désactivées par défaut.

  - **Autoriser l'utilisateur à récupérer le mot de passe**

    Détermine si la fonction de self-service de mot de passe oublié peut récupérer un mot de passe pour le compte d'un utilisateur de sorte à pouvoir lui envoyer par message électronique. Si cette option n'est pas sélectionnée, la fonction correspondante apparaît en grisé sur la page des mots de passe oublié de la stratégie de mot de passe.

    Cette option permet aux utilisateurs de récupérer leurs propres mots de passe à l'aide des extensions LDAP et NMAS.

  - **Autoriser l'administrateur à récupérer les mots de passe**

    Vous permet de récupérer les mots de passe des utilisateurs à l'aide d'un produit ou d'un service tiers qui utilise cette fonctionnalité.

    Cette option n'est pas recommandée. Au lieu de cela, vous devriez utiliser l'option **Autoriser ce qui suit pour récupérer les mots de passe** pour assigner des droits de lecture de mot de passe à des objets spécifiques, tels que les objets Service SAMBA ou freeRADIUS qui ont besoin de ces droits pour exécuter leurs fonctions.

    Si l'option **Autoriser l'administrateur à récupérer les mots de passe** est sélectionnée, les utilisateurs disposant de privilèges d'écriture sur l'attribut ACL de l'objet cible peuvent récupérer le mot de passe de l'objet cible.

  - **Autoriser ce qui suit pour récupérer les mots de passe**

    Vous permet d'insérer un objet capable de récupérer les mots de passe.

REMARQUE : les membres avec des privilèges insuffisants reçoivent une erreur `-672` lors de l'utilisation de la tâche **Check Password Status** (Vérifier l'état du mot de passe) sur un utilisateur donné.

- **Authentification**
  - **Vérifier si les mots de passe existants respectent la stratégie de mot de passe (la vérification se fait lors de la connexion)**

    Si cette option est sélectionnée et que les utilisateurs se connectent via iManager, leurs mots de passe existants sont analysés pour vérifier qu'ils respectent les règles de mot de passe avancées dans la stratégie de mot de passe des utilisateurs. Si un mot de passe existant n'est pas conforme, les utilisateurs sont invités à le changer. Si le mot de passe universel est désactivé, cette option est également désactivée par défaut.

Assignation de stratégies de mot de passe aux utilisateurs

Dans eDirectory, vous pouvez assigner une stratégie de mot de passe à des utilisateurs en assignant celle-ci à l'ensemble de l'arborescence (à l'aide de l'objet Stratégie de connexion), à des partitions ou conteneurs spécifiques, ou à certains utilisateurs. Pour simplifier l'administration, il est recommandé de définir des stratégies de mot de passe au niveau le plus élevé possible de l'arborescence.

IMPORTANT : l'assignation d'une stratégie de mot de passe à une arborescence eDirectory entière ou à un conteneur dans une arborescence qui contient une grande quantité d'utilisateurs (des dizaines de milliers) dans les sous-conteneurs risque de provoquer le blocage du plug-in iManager et de l'application proprement dite.

Dans ce cas, vous souhaiterez peut-être envisager d'assigner individuellement les stratégies de mot de passe à des conteneurs de niveau inférieur afin de contrôler le nombre d'utilisateurs pour chaque assignation de stratégie de mot de passe.

Une stratégie ne prend effet qu'une fois assignée à un ou plusieurs objets. Vous pouvez assigner une stratégie de mot de passe aux objets suivants:

- Objet Stratégie de connexion

  Nous préconisons de créer une stratégie Mot de passe par défaut pour tous les utilisateurs de l'arborescence. Pour cela, créez une stratégie et assignez-la à l'objet Stratégie de connexion. L'objet Stratégie de connexion se trouve dans le conteneur Sécurité situé juste en dessous de la racine de l'arborescence.
- Conteneur constituant la racine d'une partition

  Si vous assignez une règle à un conteneur qui est la racine d'une partition, l'assignation de règle est héritée par tous les utilisateurs de cette partition, y compris ceux présents dans les sous-conteneurs. Pour déterminer si un conteneur est la racine d'une partition, recherchez le conteneur et vérifiez la présence d'une icône de partition à proximité.
- Conteneur ne constituant pas la racine d'une partition

  Si vous assignez une stratégie à un conteneur qui n'est pas la racine d'une partition, l'assignation de stratégie est héritée uniquement par les utilisateurs de ce conteneur spécifique. Elle n'est pas héritée par les utilisateurs des sous-conteneurs. Si vous souhaitez que la stratégie s'applique à tous les utilisateurs sous un conteneur qui n'est pas une racine de partition, vous devez assigner la stratégie à chaque sous-conteneur individuellement.
- Utilisateur spécifique

Une seule stratégie à la fois peut être appliquée à un utilisateur. NMAS détermine la stratégie applicable à un utilisateur en recherchant des stratégies dans l'ordre suivant, puis en appliquant la première trouvée.

1. **Assignation spécifique à l'utilisateur :** si une règle de mot de passe a été assignée spécialement à l'utilisateur, elle est appliquée.
2. **Conteneur:** si aucune assignation spécifique ne cible l'utilisateur, NMAS applique la règle assignée au conteneur dans lequel se trouve l'utilisateur.
3. **Conteneur de la racine de partition :** si aucune règle n'est assignée à l'utilisateur ou au conteneur au niveau immédiatement supérieur à l'utilisateur, la règle assignée au conteneur de la racine de partition est appliquée.
4. **Objet Stratégie de connexion:** si aucune stratégie n'est assignée à l'utilisateur ou à d'autres conteneurs, c'est celle assignée à l'objet Stratégie de connexion qui est appliquée. Il s'agit de la stratégie par défaut pour tous les utilisateurs de l'arborescence.

La figure suivante illustre un exemple de la page de propriétés dans laquelle vous spécifiez quelle stratégie de mot de passe pour objet est assignée à :

Figure 26-5 *Assignation d'une stratégie de mot de passe aux objets*

Recherche de la stratégie d'un utilisateur

Un utilisateur ne peut avoir qu'une seule stratégie appliquée à la fois. Pour savoir quelle stratégie est applicable à un utilisateur ou un conteneur en particulier, procédez comme suit :

1. Dans iManager, dans la vue **Rôles et tâches**, cliquez sur **Mots de passe** > **View Policy Assignments** (Afficher les assignations de stratégie).
2. Recherchez l'utilisateur souhaité et sélectionnez-le.
3. Cliquez sur **OK**.

Si l'arborescence contient plusieurs stratégies, NMAS détermine la stratégie à appliquer à un utilisateur, conformément aux indications de la « Assignation de stratégies de mot de passe aux utilisateurs » page 814.

Définition d'un mot de passe utilisateur

Les administrateurs ou le personnel du service d'assistance peuvent définir le mot de passe universel d'un utilisateur en utilisant une tâche dans iManager. La tâche affiche les règles de mot de passe pour la stratégie de mot de passe applicable à cet utilisateur.

1. Dans iManager, dans la vue **Rôles et tâches**, cliquez sur **Mots de passe** > **Définir un mot de passe universel**.
2. Recherchez l'utilisateur souhaité et sélectionnez-le.
3. Cliquez sur **OK**.

   Si l'utilisateur s'est vu assigner une stratégie de mot de passe et qu'il dispose d'un mot de passe universel activé, cette tâche vous permet de modifier son mot de passe.

   Si les règles de mot de passe avancées sont activées dans la stratégie, une liste de règles à suivre s'affiche.

   Si le mot de passe universel n'est pas activé pour un utilisateur, iManager affiche un message d'erreur. Vous devez soit assigner une stratégie à l'utilisateur puis revenir à cette tâche, soit modifier le mot de passe NDS de l'utilisateur à l'aide de la tâche **Administration eDirectory** > **Modifier un objet**.
4. Créez un mot de passe pour l'utilisateur et assurez-vous qu'il soit compatible avec toutes les règles de mot de passe affichées.
5. Cliquez sur **OK**.

   Le mot de passe universel est modifié pour l'utilisateur.

   Si la synchronisation de mot de passe est définie dans votre environnement, le nouveau mot de passe utilisateur est distribué aux systèmes connectés configurés pour l'accepter.

REMARQUE : Lorsqu'un administrateur modifie le mot de passe d'un utilisateur, par exemple lors de la création d'un nouvel utilisateur ou en réponse à un appel de dépannage, le mot de passe précédent expire automatiquement si vous avez activé le paramètre d'expiration des mots de passe dans la stratégie de mots de passe. Le paramètre **Nombre de jours avant l'expiration du mot de passe** se trouve dans les règles de mot de passe avancées. Dans cette fonction, ce n'est pas le nombre de jours défini qui est important, c'est son activation.

L'option **Do not expire the user's password when the administrator sets the password** (Ne pas faire expirer le mot de passe de l'utilisateur lorsque l'administrateur définit le mot de passe) remplace cette fonction.

Utilitaire de diagnostic de mot de passe universel

eDirectory intègre un utilitaire qui vérifie l'état et rechiffre le mot de passe universel. L'utilitaire de diagnostic de mot de passe universel (`diagpwd`) est un outil qui permet à un administrateur d'afficher l'état du mot de passe universelctif), du mot de passe simple, du mot de passe NDS et du mot de passe de distribution (DP) d'un utilisateur. Il indique également l'état de la synchronisation de ces mots de passe. Vous trouverez ci-dessous un exemple de syntaxe de l'utilitaire `diagpwd` :

```
diagpwd LDAP_SERVER_ADDR TLS_PORT CA_CERT_FILE SEARCH_BASE SEARCH_SCOPE BIND_DN
[BIND_PWD] -t
```

Option	Description
`LDAP_SERVER_ADDR`	Indique l'adresse du serveur LDAP cible.
`TLS_PORT`	Indique le port sécurisé LDAP (TLS) du serveur LDAP cible.
`CA_CERT_FILE`	Indique le chemin du fichier codé PEM qui contient le certificat de racine approuvée du serveur LDAP cible.
`SEARCH_BASE`	Utilise la base de recherche comme point de départ de la recherche.
`SEARCH_SCOPE`	Définit l'étendue de la recherche. L'étendue peut être « base », « one » ou « sub » pour spécifier une recherche portant respectivement sur un objet de base, sur un niveau ou sur une sous-arborescence.
`BIND_DN`	DN LDAP de l'administrateur. Par exemple, `cn=admin,o=company`.
`BIND_PWD`	Mot de passe LDAP de l'administrateur. **REMARQUE :** Ce paramètre est facultatif. S'il n'est pas inclus dans la ligne de commande, l'utilisateur est invité à le spécifier.
`-t`	Cette option rechiffre le mot de passe universel, le mot de passe de distribution et le mot de passe simple, ainsi que l'historique des mots de passe avec des clés AES 256 bits. Utilisez cette option après avoir créé la clé d'arborescence AES 256 bits. **REMARQUE :** Lorsque vous utilisez cette option, assurez-vous que la stratégie de mot de passe permet à l'utilisateur qui exécute cet utilitaire de récupérer le mot de passe universel de l'utilisateur.

Exemples

Pour vérifier l'état des mots de passe pour l'utilisateur `cn=user1,ou=users,o=company` sur le serveur `192.168.1.1`, exécutez la commande suivante :

```
diagpwd 192.168.1.1 636 /home/user1/cert.pem cn=user1,ou=users,o=company base
cn=admin,o=company
```

Pour vérifier l'état des mots de passe pour tous les utilisateurs dans la sous-arborescence `ou=users,o=company`, exécutez la commande suivante :

```
diagpwd 192.168.1.1 636 /home/user1/cert.pem ou=users,o=company sub
cn=admin,o=company
```

Pour rechiffrer les mots de passe de tous les utilisateurs dans la sous-arborescence `ou=users,o=company` avec une clé AES 256 bits, exécutez la commande suivante :

```
diagpwd 192.168.1.1 636 /home/user1/cert.pem ou=users,o=company sub
cn=admin,o=company -t
```

Dépannage des stratégies de mot de passe

- « Ces erreurs indiquent qu'une stratégie de mot de passe n'est pas assignée à un utilisateur » page 818
- « Utilisation des questions et réponses de vérification d'identité » page 818
- « Octroi d'accès pour les nouveaux conteneurs » page 818
- « Erreur de transport NMAS LDAP » page 819

Ces erreurs indiquent qu'une stratégie de mot de passe n'est pas assignée à un utilisateur

Si vous détectez une erreur indiquant qu'une stratégie de mot de passe n'est pas assignée à un utilisateur à partir de la tâche de définition du mot de passe universel et que vous savez que l'utilisateur dispose d'une stratégie de mot de passe assignée, le problème peut venir de SSL. Pour diagnostiquer et résoudre les problèmes liés à SSL, procédez comme suit :

- Pour vérifier que la configuration de SSL est bien à l'origine du problème, utilisez la tâche d'affichage des assignations de stratégies pour vérifier la stratégie de cet utilisateur. Si la tâche d'affichage des assignations de stratégies renvoie une erreur de transport NMAS, cela peut indiquer que SSL n'est pas configuré correctement.
- Vérifiez que SSL est correctement configuré entre le serveur Web qui exécute iManager et l'arborescence eDirectory principale. Vérifiez que vous disposez d'un certificat configuré entre le serveur Web et eDirectory.
- Si vous ne faites pas appel à TLS en cas de liaison simple, vous devez veiller à indiquer le port SSL LDAP correct, comme expliqué dans la remarque à l'Étape 6 page 798.

Utilisation des questions et réponses de vérification d'identité

Assurez-vous que vous utilisez un navigateur pris en charge par iManager.

Octroi d'accès pour les nouveaux conteneurs

Lorsque vous configurez iManager ou un des produits du portail de NetIQ, tels que l'application utilisateur, vous spécifiez le conteneur des utilisateurs du portail. Généralement, vous spécifiez un conteneur d'un niveau élevé dans l'arborescence, afin que tous les utilisateurs de l'arborescence puissent accéder aux fonctionnalités du portail. Si tous les utilisateurs sont situés sous ce conteneur, alors ils ont tous accès au self-service de mot de passe oublié et du self-service de réinitialisation de mot de passe.

Erreur de transport NMAS LDAP

Si vous installez Identity Manager dans un environnement multiserveur et utilisez certains plug-ins de gestion des mots de passe dans iManager, une erreur de type `Erreur de transport NMAS LDAP` risque de s'afficher.

Une cause fréquente de cette erreur est que le fichier `PortalServlet.properties` pointe vers un serveur LDAP qui ne dispose pas des extensions NMAS nécessaires pour Identity Manager. Ouvrez le fichier `PortalServlet.properties` et assurez-vous que l'adresse du serveur LDAP est la même que celle du serveur sur lequel vous avez installé Identity Manager.

Autres causes possibles :

- Le serveur LDAP n'est pas en cours d'exécution.
- SSL n'est pas configuré pour LDAP entre le serveur iManager qui exécute les plug-ins et le serveur LDAP.
- Lorsque vous vous connectez avec iManager à d'autres arborescences pour gérer les serveurs distants Identity Manager, des erreurs risquent de se produire si vous utilisez le nom du serveur au lieu de l'adresse IP du serveur distant.
- Le certificat de racine approuvée de l'arborescence auprès de laquelle vous vous authentifiez doit être importé en tant que certificat approuvé sur le serveur Web. Vous pouvez utiliser `keytool.exe` pour exporter le certificat vers le serveur Web.

Self-service de mot de passe

Cette section fournit des informations sur la configuration et la gestion du self-service de mot de passe.

- « Présentation du self-service de mot de passe » page 819
- « Conditions préalables à l'utilisation du self-service de mot de passe » page 820
- « Gestion des mots de passe oubliés » page 820
- « Self-service de réinitialisation de mot de passe proposé aux utilisateurs » page 833
- « Ajout d'un message de changement de mot de passe » page 833
- « Configuration de la notification par message électronique pour le self-service de mot de passe » page 833
- « Test du self-service de mot de passe » page 835
- « Ajout du self-service de mot de passe à votre portail d'entreprise » page 835
- « Dépannage du self-service de mot de passe » page 836

Présentation du self-service de mot de passe

Vous pouvez réduire les frais d'assistance en configurant des options en self-service afin que les utilisateurs puissent récupérer les mots de passe oubliés ou réinitialiser leur mot de passe en ayant accès aux règles que vous avez spécifiées dans la stratégie de mot de passe.

Vous gérez la stratégie du self-service de mot de passe en utilisant l'une des méthodes suivantes :

- iManager

  La majeure partie de ce chapitre décrit comment gérer le self-service de mot de passe à l'aide d'iManager.

- Application utilisateur Identity Manager

  Pour plus d'informations sur la gestion du self-service de mot de passe avec l'application utilisateur Identity Manager, reportez-vous à la section Using the Identity Self-Service Tab (Utilisation de l'onglet Self-service d'identité) du *NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide* (Guide de l'utilisateur pour l'application utilisateur du module RBPM 4.5 de NetIQ Identity Manager).

Les utilisateurs peuvent accéder aux fonctionnalités du self-service de mot de passe par le biais de l'une des opérations suivantes :

- Portail iManager
- Portlet de l'application utilisateur Identity Manager

  Pour plus d'informations sur l'utilisation du self-service de mot de passe avec l'application utilisateur Identity Manager, reportez-vous à la section Using the Identity Self-Service Tab (Utilisation de l'onglet Self-service d'identité) du *NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide* (Guide de l'utilisateur pour l'application utilisateur du module RBPM 4.5 de NetIQ Identity Manager).
- Client Novell

  Pour plus d'informations sur l'utilisation du self-service de mot de passe avec le client Novell, reportez-vous à la section Using Forgotten Password Self-Service (Utilisation du self-service de mot de passe oublié) du *Novell Client for Windows Administration Guide* (Guide d'administration du client Novell pour Windows).

Conditions préalables à l'utilisation du self-service de mot de passe

Passez en revue les informations de la « Gestion des mots de passe à l'aide de stratégies de mot de passe » page 792 et respectez les conditions préalables mentionnées à la « Tâches préalables à l'utilisation des stratégies de mot de passe » page 797.

Bien que certaines fonctions du self-service de mot de passe soient disponibles sans déployer le mot de passe universel, nous vous recommandons de préparer votre environnement et d'activer le mot de passe universel pour pouvoir utiliser toutes les fonctionnalités des stratégies de mot de passe.

Le client Novell tire également parti des fonctions du self-service de mot de passe. Reportez-vous à la section Using Forgotten Password Self-Service (Utilisation du self-service de mot de passe oublié) du *Novell Client for Windows Administration Guide* (Guide d'administration du client Novell pour Windows).

Gestion des mots de passe oubliés

Les sections suivantes décrivent la façon de gérer des mots de passe oubliés à l'aide d'iManager.

Pour plus d'informations sur la gestion des mots de passe oubliés à l'aide de l'application utilisateur Identity Manager, reportez-vous à la section Password Management Configuration (Configuration de la gestion des mots de passe) du *NetIQ Identity Manager 4.5 Password Management Guide* (Guide de gestion des mots de passe NetIQ Identity Manager 4.5).

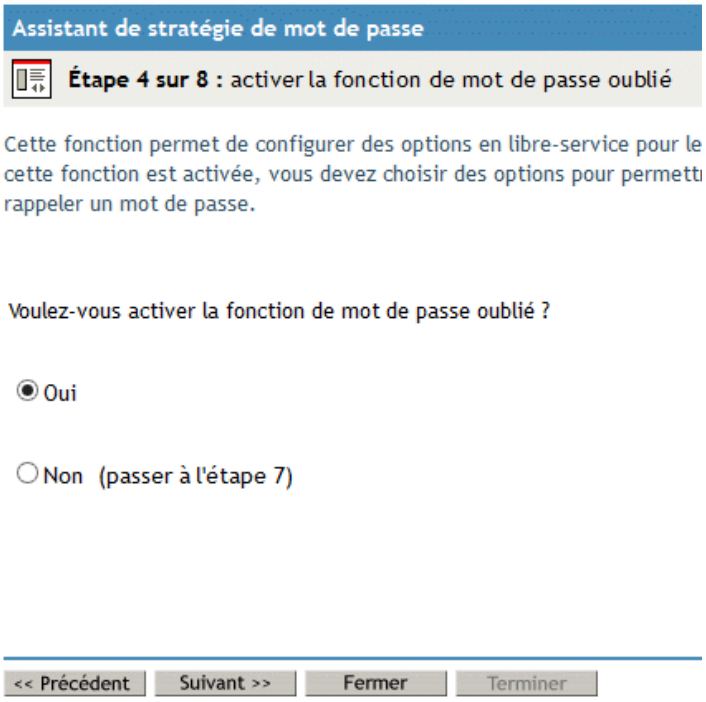
- « Activation du mot de passe oublié » page 821
- « Création ou modification d'ensembles de stimulations » page 822
- « Sélection d'une opération de mot de passe oublié » page 824

- « Configuration du self-service de mot de passe oublié » page 825
- « Écran d'oubli de mot de passe » page 830

Activation du mot de passe oublié

Pour permettre aux utilisateurs de récupérer un mot de passe oublié sans contacter le service d'assistance, activez la fonction de mot de passe oublié. Comme le montre la figure suivante, cette option apparaît lorsque vous utilisez l'assistant de stratégie de mot de passe pour créer une stratégie de mot de passe. Pour plus d'informations sur l'assistant de stratégie de mot de passe, reportez-vous à la section « Pour créer un ensemble de questions de stimulations lors de l'utilisation de l'assistant de stratégie de mot de passe, procédez comme suit : » page 823

Figure 26-6 *Activez la fonction de mot de passe oublié.*



Vous pouvez également activer le mot de passe oublié pour une stratégie de mot de passe existante :

1. Dans iManager, sélectionnez **Mots de passe** > **Stratégie de mot de passe**.
2. Cliquez sur le nom de la stratégie.
3. Cliquez sur l'onglet **Mot de passe oublié**.
4. Sélectionnez **Activer la fonction de mot de passe oublié**, sélectionnez ou créez un ensemble de stimulations, spécifiez une action, sélectionnez l'option **Authentification**, puis cliquez sur **OK**.

Création ou modification d'ensembles de stimulations

Un ensemble de stimulations est une série de questions auxquelles répond un utilisateur pour prouver son identité, au lieu d'utiliser un mot de passe. L'ensemble de questions de stimulations est assigné à une stratégie de mot de passe et est utilisé dans le cadre de la méthode d'une stratégie de mot de passe d'authentification. Les réponses des utilisateurs à ces questions de stimulations ne respectent pas la casse.

Vous pouvez utiliser des ensembles de stimulations au sein du self-service de mot de passe oublié pour les utilisateurs. Exiger d'un utilisateur qu'il réponde à des questions de stimulations avant de recevoir de l'aide pour un mot de passe oublié contribue à accroître le niveau de sécurité.

Lorsque vous créez une stratégie de mot de passe, vous pouvez activer la fonctionnalité du self-service de mot de passe oublié pour que les utilisateurs puissent obtenir de l'aide sans appeler le service d'assistance. Pour renforcer la sécurité du self-service, vous pouvez créer un ensemble de questions de stimulations et exiger des utilisateurs qu'ils répondent aux questions correspondantes avant d'obtenir de l'aide pour les mots de passe oubliés. Vous indiquez également quelle opération a lieu pour aider les utilisateurs une fois qu'ils répondent aux questions, telles que l'affichage d'un indice permettant à l'utilisateur de deviner le mot de passe. Ces fonctions de self-service sont accessibles aux utilisateurs via iManager. Les choix disponibles sont expliqués à la section « Sélection d'une opération de mot de passe oublié » page 824.

Pour créer un ensemble de questions de stimulations :

1. Dans iManager, cliquez sur **Mots de passe** > **Ensembles de stimulations**.
2. Cliquez sur **Nouveau**.
3. Saisissez un nom dans le champ **Nom de l'ensemble de stimulations**, sélectionnez un conteneur pour l'ensemble de questions de stimulations devant être créé, puis sélectionnez ou créez des stimulations.

   Pour sélectionner une question par défaut dans l'ensemble de questions de stimulations, cochez la case correspondante.

   Pour modifier une question ou le nombre de caractères (minimum ou maximum) autorisés dans les réponses, cliquez sur la question.

   Pour créer une question et l'ajouter à l'ensemble de stimulations, cliquez sur **Add Question** (Ajouter une question).

   Défini par l'utilisateur: si vous sélectionnez cette option, les utilisateurs peuvent créer leurs propres questions de stimulations.

   NMAS stocke les questions et réponses définies par l'utilisateur dans eDirectory.

   Questions obligatoires : les questions de cette liste apparaissent toujours lorsqu'un utilisateur utilise le self-service de mot de passe.

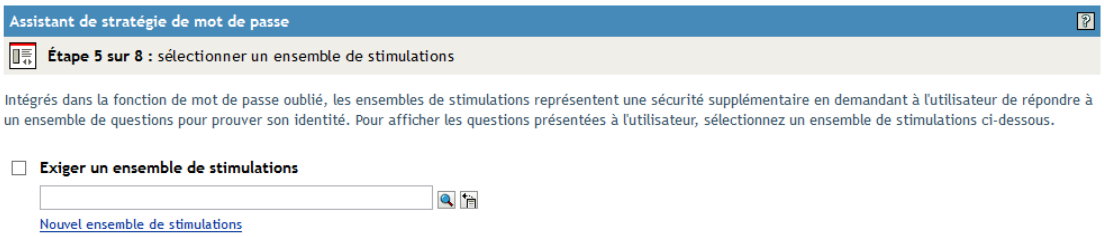
   Questions aléatoires : les questions de cette liste n'apparaissent qu'une seule fois et en tant qu'ensemble complet, au moment où l'utilisateur configure la fonctionnalité de mot de passe oublié en répondant à l'ensemble des questions de stimulations pour la première fois. Lorsque l'utilisateur doit ensuite utiliser la fonction de mot de passe oublié, seules quelques-unes des questions lui sont posées. Le nombre de questions aléatoires qui apparaît varie en fonction de la valeur que vous spécifiez.
4. Cliquez sur **OK**.

Pour créer un ensemble de questions de stimulations lors de l'utilisation de l'assistant de stratégie de mot de passe, procédez comme suit :

1 Dans iManager, lancez l'assistant en cliquant sur **Mots de passe** > **Stratégie de mot de passe** > **Nouveau**.

2 À l'étape 4, cliquez sur **Oui** pour activer la fonction de mot de passe oublié.

3 À l'étape 5, sélectionnez Exiger un ensemble de stimulations, puis cliquez sur Nouvel ensemble de stimulations.



Pour utiliser un ensemble de questions de stimulations existant, recherchez-le et sélectionnez-le.

4 Spécifiez le conteneur dans lequel créer l'ensemble de questions de stimulations. Saisissez un nom dans le champ **Nom de l'ensemble de stimulations**, puis cliquez sur **Suivant**.

5 Sélectionnez ou créez des questions de stimulations obligatoires ou aléatoires.

Si vous ne souhaitez pas créer de nouvelles questions, sélectionnez des questions existantes.

Pour permettre aux utilisateurs d'ajouter leurs propres questions, sélectionnez **Défini par l'utilisateur**.

Pour créer une nouvelle question :

5a Cliquez sur **Add Question** (Ajouter une question).

5b Sélectionnez **Administrator Defines the Question** (L'administrateur définit la question), cliquez sur **Ajouter**, spécifiez une langue dans le menu déroulant, entrez votre question, puis cliquez sur **OK**.

5c Indiquez si la question est obligatoire ou aléatoire.

5d Spécifiez le nombre minimal et maximal de caractères requis, puis cliquez sur **OK**

6 Indiquez le nombre de questions aléatoires, puis cliquez sur **Suivant**.

7 Suivez les étapes restantes de l'assistant de stratégie de mot de passe.

Pour créer un ensemble de stimulations pour une stratégie de mot de passe existante, procédez comme suit :

1 Dans iManager, sélectionnez **Mots de passe** > **Stratégie de mot de passe**.

2 Cliquez sur le nom d'une stratégie.

3 Cliquez sur l'onglet **Forgotten Password** (Mot de passe oublié).

4 Sélectionnez **Activer la fonction de mot de passe oublié** > **Exiger un ensemble de stimulations**.

5 Recherchez et sélectionnez un ensemble de questions de stimulations existant ou créez-en un nouveau, puis cliquez sur le nouvel ensemble.

Pour créer un nouvel ensemble :

5a Cliquez sur le lien **Ensembles de stimulations**.

5b Dans la boîte de dialogue Ensembles de stimulations, cliquez sur **Nouveau**.

5c Dans la boîte de dialogue Ensembles de stimulations, nommez l'ensemble de stimulation, spécifiez un conteneur dans lequel créer l'ensemble, sélectionnez ou ajoutez des questions obligatoires ou aléatoires, puis indiquez le nombre de questions aléatoires à poser.

5d Cliquez sur **OK**.

Sélection d'une opération de mot de passe oublié

1. Dans iManager, sélectionnez **Mots de passe** > **Stratégie de mot de passe**.
2. Cliquez sur le nom de la stratégie.
3. Cliquez sur l'onglet **Forgotten Password** (Mot de passe oublié).
4. Sélectionnez la case à cocher **Activer la fonction de mot de passe oublié**.
5. Sélectionnez une action :
   - **Autoriser l'utilisateur à réinitialiser le mot de passe:** après avoir répondu aux questions de stimulations pour établir son identité, l'utilisateur est autorisé à définir un nouveau mot de passe. Authentifié par le biais de ses réponses aux questions de stimulations, l'utilisateur peut modifier son mot de passe sans avoir à fournir l'ancien. Pour utiliser cette option, vous devez exiger un ensemble de stimulations. Quant à l'utilisateur, il doit avoir configuré la fonction de mot de passe oublié dans le portail iManager en répondant aux questions de stimulations.
   - **Envoyer par messagerie électronique le mot de passe actuel à l'utilisateur:** après avoir répondu à l'ensemble de questions de stimulations pour établir son identité, l'utilisateur reçoit le mot de passe actuel par courrier électronique. Pour utiliser cette option, vous devez effectuer les opérations suivantes :
     - Activer le mot de passe universel pour la stratégie. Cette option se trouve dans **Options de configuration** sous **Mot de passe universel**.
     - Activer l'option **Autoriser l'utilisateur à récupérer le mot de passe** qui se trouve dans **Options de configuration** sous **Mot de passe universel**.
     - Configurer la notification par message électronique conformément aux indications de la « Configuration de la notification par message électronique pour le self-service de mot de passe » page 833.

     En outre, l'utilisateur doit avoir configuré la fonction de mot de passe oublié dans iManager en répondant aux questions de stimulations.
   - **Envoyer par messagerie électronique l'indice à l'utilisateur:** l'utilisateur reçoit l'indice de mot de passe dans un message électronique. Pour utiliser cette option, vous devez configurer la notification par message électronique conformément aux indications de la « Configuration de la notification par message électronique pour le self-service de mot de passe » page 833.

     En outre, l'utilisateur doit avoir configuré la fonction de mot de passe oublié dans iManager en fournissant un indice de mot de passe.
   - **Afficher l'indice sur la page:** l'utilisateur peut accéder à l'indice de mot de passe sur le portail iManager. Pour utiliser cette option, l'utilisateur doit avoir configuré la fonction de mot de passe oublié en fournissant un indice de mot de passe.

Indices de mot de passe

Si vous spécifiez une tâche de mot de passe oublié qui requiert l'indice de mot de passe, l'utilisateur peut saisir un indice qui lui rappellera le mot de passe.

- « Indice du mot de passe » page 825
- « Indice sécurisé » page 825

Indice du mot de passe

L'attribut Indice de mot de passe (`nsimHint`) est lisible par tous, ce qui permet aux utilisateurs non authentifiés qui ont oublié leur mot de passe d'accéder à leur indice. Les indices de mots de passe peuvent contribuer à réduire considérablement le nombre d'appels au service d'assistance.

Pour des raisons de sécurité, ces indices sont contrôlés afin de vérifier qu'ils ne contiennent pas le mot de passe de l'utilisateur. Toutefois, un utilisateur peut toujours créer un indice de mot de passe fournissant trop d'informations sur le mot de passe.

Afin d'accroître la sécurité lors de l'utilisation des indices de mots de passe :

- Autorisez l'utilisateur à accéder uniquement à l'attribut nsimHint sur le serveur nds-cluster-config utilisé pour les options de self-service de mot de passe.
- Rappelez aux utilisateurs qu'ils doivent créer des indices de mots de passe qu'eux seuls peuvent comprendre. L'option Message de modification du mot de passe, dans la stratégie de mot de passe, est l'une des manières de le faire. Reportez-vous à la « Ajout d'un message de changement de mot de passe » page 833.

Indice sécurisé

L'attribut Indice sécurisé (`nsimPasswordReminder`) est plus sûr, car il n'est pas lisible par tous. L'utilisateur doit répondre aux questions de stimulations avant que l'indice ne s'affiche.

Les exigences relatives à la réponse aux questions de stimulations sont définies dans la section des mots de passe oubliés des propriétés de la stratégie de mot de passe.

Si vous choisissez de ne pas utiliser d'indice de mot de passe, vérifiez que vous n'utilisez cette fonction dans aucune des stratégies de mot de passe.

Configuration du self-service de mot de passe oublié

L'utilisateur ne peut pas cliquer sur le lien **Vous avez oublié votre mot de passe ?** lors d'une connexion au portail (`https://www.`*`nom_serveur`*`.com/nps` par défaut), sauf si les conditions suivantes sont réunies :

- L'administrateur a défini une stratégie de mot de passe avec la fonction de mot de passe oublié activée.
- L'utilisateur a configuré les questions de stimulations ou un indice de mot de passe, si l'un d'entre eux est spécifié dans le paramètre de mot de passe oublié.

- « Utilisateurs invités à configurer la fonction de mot de passe oublié » page 826
- « Configuration de l'utilisateur pour la fonction de mot de passe oublié » page 827
- « Conformité des mots de passe existants exigée » page 828

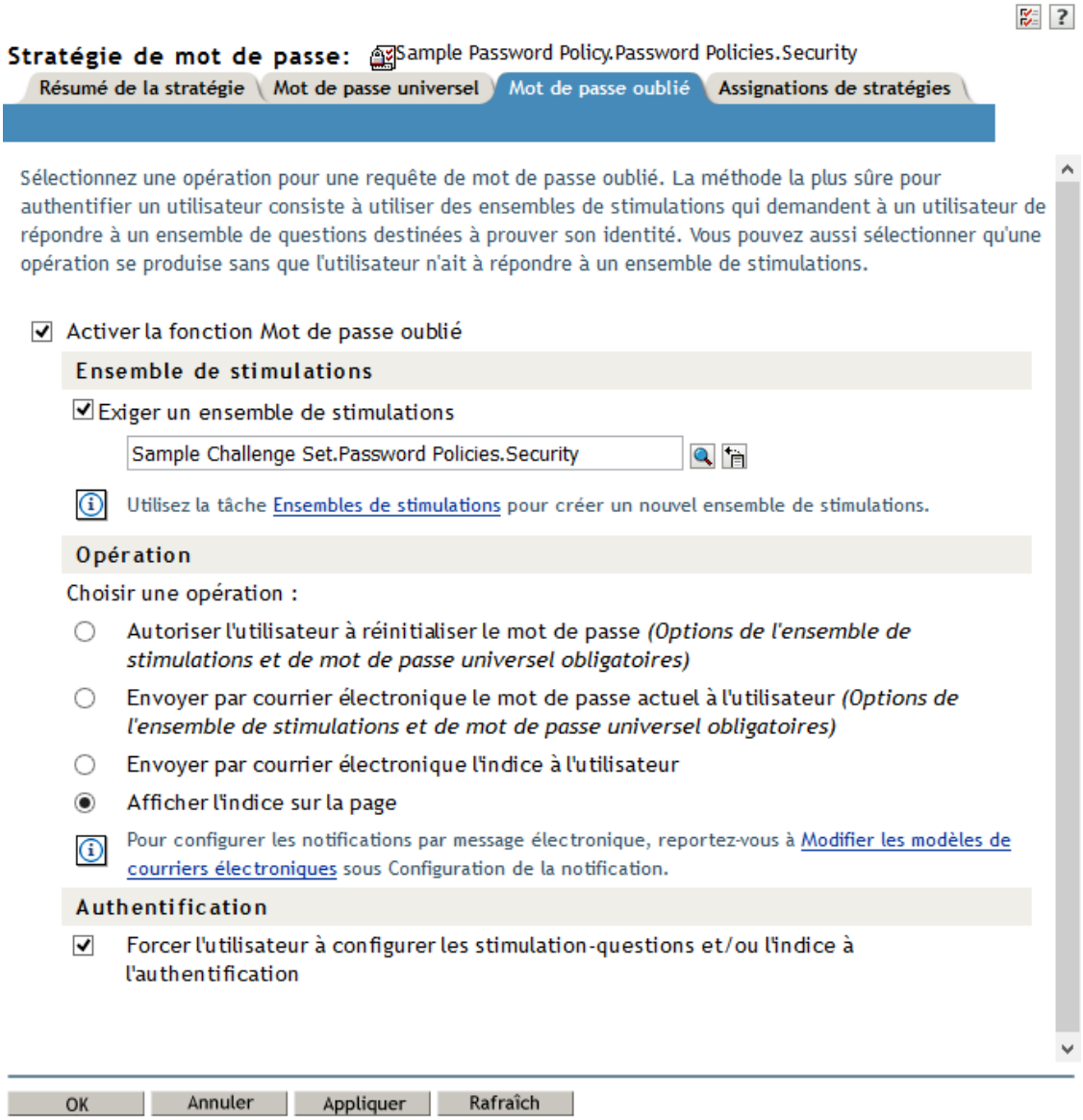
Utilisateurs invités à configurer la fonction de mot de passe oublié

Pour certaines opérations liées à un mot de passe oublié, l'utilisateur doit réaliser quelques opérations de configuration avant d'utiliser le self-service de mot de passe oublié. Par exemple, si la stratégie de mot de passe indique qu'un ensemble de stimulations est utilisé pour permettre à un utilisateur de prouver son identité et si l'opération liée au mot de passe oublié consiste à envoyer par courrier électronique un indice de mot de passe à l'utilisateur, ce dernier doit tout d'abord répondre aux questions de stimulations et créer un indice de mot de passe avant de pouvoir utiliser le self-service de mot de passe oublié.

Les utilisateurs peuvent commencer à configurer ces fonctions sur le portail, ou vous pouvez exiger que les utilisateurs les configurent à l'aide des services de post-authentification, c'est-à-dire des pages affichées lorsqu'ils se connectent au portail.

Pour demander aux utilisateurs de configurer ces fonctions au moment de la connexion, sélectionnez l'option **Forcer l'utilisateur à configurer les stimulation-questions et/ou l'indice à l'authentification** dans l'interface des stratégies de mot de passe au bas de la page des mots de passe oubliés. Cette option est sélectionnée par défaut lorsque vous créez une stratégie.

Figure 26-7 *Stratégie de mot de passe*



Pour permettre aux utilisateurs de configurer la fonction de mot de passe oublié à un moment de leur choix, vous devez leur fournir l'URL du portail, par exemple `https://www.`*`mon_serveur_iManager`*`.com/nps`.

Configuration de l'utilisateur pour la fonction de mot de passe oublié

La configuration de l'utilisateur peut être exécutée de deux façons :

- « Post-authentification » page 828
- « Via le portail » page 828

Post-authentification

L'administrateur peut demander à l'utilisateur de configurer les fonctions de mot de passe oublié après une connexion réussie en sélectionnant l'option **Mot de passe oublié** pour forcer l'utilisateur à configurer les questions de stimulations ou l'indice lors de l'authentification. Si cette option est sélectionnée, mais qu'un utilisateur n'a pas configuré de questions ou d'indice, les gadgets de configuration de mot de passe oublié seront présentés à l'utilisateur lors de sa prochaine connexion via le portail (`https://www.nom_serveur.com/nps` by default). Il s'agit de la configuration post-authentification.

Via le portail

Lorsque les utilisateurs se connectent via le portail iManager, iManager leur donne accès aux gadgets de configuration ou de modification des ensembles de stimulations et des indices de mot de passe pour le self-service de mot de passe oublié. Il s'agit du même emplacement que celui dans lequel les utilisateurs peuvent entamer un changement de mot de passe. De là, ils peuvent accéder à cet endroit aux gadgets suivants :

- Configuration de l'indice
- Réponse aux questions de stimulations
- Modification de mot de passe (universel)

L'utilisateur peut démarrer sa modification à tout moment. Toutefois, si un indice ou un ensemble de stimulations n'est pas requis pour la stratégie de mot de passe de l'utilisateur, ce dernier ne peut pas les définir. La page affiche un message indiquant que les options ne sont pas accessibles.

Pour consulter des exemples spécifiques de l'apparence de ces options utilisateur dans chaque application (iManager 2.02 ou version ultérieure, portlet de l'application utilisateur et client Novell), reportez-vous à la documentation de chaque application comme décrit dans la « Présentation du self-service de mot de passe » page 819.

Conformité des mots de passe existants exigée

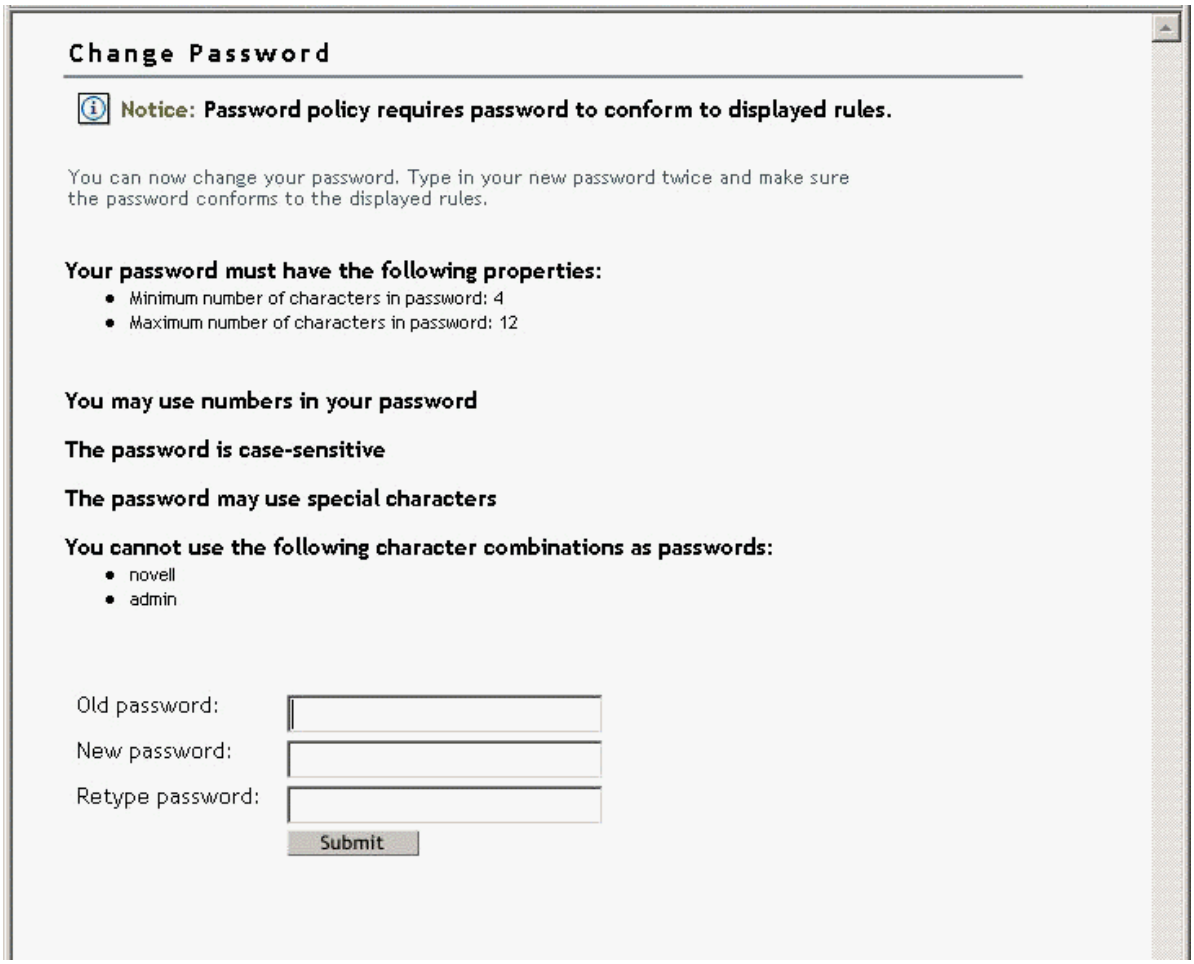
Si vous créez ou modifiez une stratégie de mot de passe, vous pouvez exiger des utilisateurs qu'ils modifient les mots de passe existants qui ne sont pas conformes lors de leur prochaine connexion via le portail.

Pour ce faire, définissez une option dans la stratégie de mot de passe à l'aide de l'onglet **Mot de passe universel** sous **Options de configuration**. Cette option s'appelle **Vérifier si les mots de passe existants respectent la stratégie de mot de passe (la vérification se fait lors de la connexion)**. Par défaut, cette option est désactivée lorsque vous créez une nouvelle stratégie de mot de passe. La figure suivante illustre la page sur laquelle vous définissez cette option :

Figure 26-8 *Conformité des mots de passe existants exigée*

Si cette option est définie, la prochaine fois que les utilisateurs se connecteront via le portail, leurs mots de passe seront analysés pour vérifier leur conformité avec la stratégie de mot de passe. Si le mot de passe n'est pas conforme, une page similaire à la suivante s'affiche et l'utilisateur n'est pas autorisé à se connecter s'il ne change pas le mot de passe.

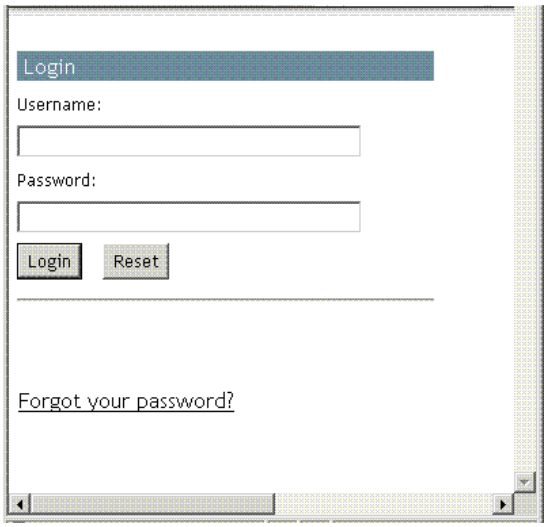
Figure 26-9 *Modifier le mot de passe*



Écran d'oubli de mot de passe

Une fois que vous avez installé les plug-ins d'iManager fournis avec Identity Manager, le lien **Mot de passe oublié** s'affiche dans le portail iManager (`https://www.`*`nom_serveur`*`.com/nps` par défaut), comme illustré sur la figure suivante.

Figure 26-10 *Fonction de mot de passe oublié dans iManager*



Un lien similaire s'affiche lors de l'authentification via le client Novell.

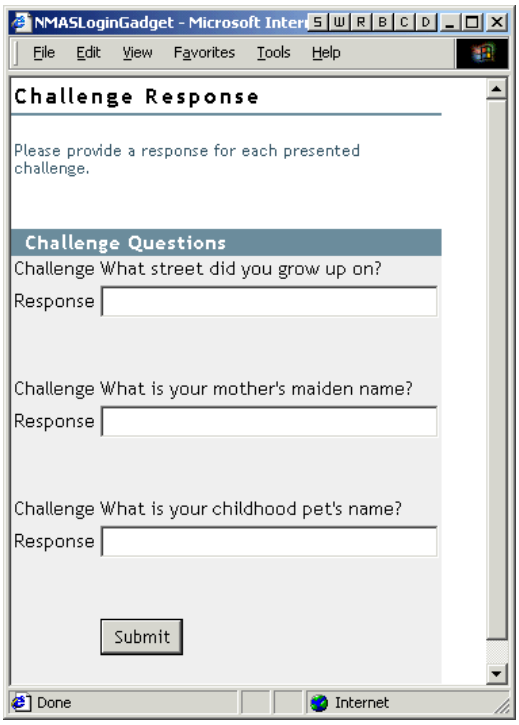
Si un utilisateur clique sur ce lien, la page suivante s'affiche et demande le nom d'utilisateur :

Figure 26-11 *Mot de passe oublié dans Virtual Office et le client Novell*

Lorsque vous avez entré le nom d'utilisateur, les paramètres de mot de passe oublié déterminent ce que voit l'utilisateur.

Par exemple, si l'administrateur spécifie dans la stratégie de mot de passe qu'un ensemble de stimulations est utilisé, une page similaire à la suivante s'affiche. L'utilisateur doit alors répondre aux questions de stimulations pour prouver son identité.

Figure 26-12 Questions de stimulations liées au mot de passe oublié



Si l'administrateur a spécifié que l'opération liée au mot de passe oublié est **Afficher l'indice sur la page**, une page similaire à la suivante s'affiche :

Figure 26-13 Indice de mot de passe oublié

Si l'administrateur a spécifié que l'opération liée au mot de passe oublié est **Envoyer par courrier électronique le mot de passe actuel à l'utilisateur** ou **Envoyer par courrier électronique l'indice à l'utilisateur**, le système indique que le mot de passe ou un indice a été envoyé par courrier électronique.

Self-service de réinitialisation de mot de passe proposé aux utilisateurs

Vous pouvez configurer la stratégie de mot de passe pour permettre aux utilisateurs de réinitialiser leur mot de passe. Le mode d'affichage pour l'utilisateur dépend de l'application qu'il utilise pour exécuter cette tâche. Reportez-vous à la « Présentation du self-service de mot de passe » page 819 pour obtenir des liens vers la documentation des différentes applications.

Ajout d'un message de changement de mot de passe

Bien que les utilisateurs puissent modifier leur mot de passe chaque fois qu'ils le souhaitent, ils utilisent généralement les mêmes mots de passe aussi longtemps que possible. Pour renforcer la sécurité, vous pouvez utiliser une stratégie de mot de passe pour les forcer à le modifier. Cette stratégie peut contenir un message de changement de mot de passe et les règles de mot de passe. Chaque fois que les utilisateurs modifient un mot de passe, ils voient ce message ainsi que les règles.

Pour modifier la stratégie de mot de passe et créer ce message :

1. Dans iManager, sélectionnez **Mots de passe** > **Stratégie de mot de passe**.
2. Cliquez sur le nom de la stratégie de mot de passe à laquelle vous souhaitez ajouter un message.
3. Cliquez sur **Policy Summary** (Résumé de la stratégie) > **Password Change Message** (Message de changement de mot de passe).
4. Saisissez le message qui doit s'afficher pour les utilisateurs, puis cliquez sur **OK**.

Configuration de la notification par message électronique pour le self-service de mot de passe

Le rôle iManager nommé Configuration de la notification vous permet de spécifier le serveur de messagerie et de personnaliser les modèles de notifications par courrier électronique.

Des modèles de messages sont prévus pour permettre aux fonctions de synchronisation des mots de passe et de self-service des mots de passe d'envoyer automatiquement des messages électroniques aux utilisateurs.

Vous ne créez pas de modèles. Ils sont en effet fournis par l'application qui les utilise. Les modèles de message électronique sont des objets Modèle dans eDirectory. Ils sont placés dans le conteneur Sécurité, qui se trouve généralement à la racine de votre arborescence. Même s'il s'agit d'objets eDirectory, vous ne pouvez les modifier que dans l'interface iManager.

Ce cadre est modulaire. À mesure que vous ajoutez de nouvelles applications qui utilisent les modèles de messages électroniques, les modèles peuvent être installés en même temps que les applications qui les utilisent.

Identity Manager fournit des modèles pour les notifications de synchronisation de mot de passe et de mot de passe oublié. Vous contrôlez l'envoi éventuel de messages, en fonction des choix que vous avez faits dans l'interface iManager.

En ce qui concerne les oublis de mots de passe, les notifications ne sont envoyées que si vous choisissez d'utiliser l'une des opérations Mot de passe oublié amenant à l'envoi d'un message électronique : envoyer le mot de passe à l'utilisateur par courrier électronique ou lui envoyer un indice.

Cette section aborde les points suivants :

- « Conditions préalables » page 834
- « Configuration du serveur SMTP pour envoyer la notification par message électronique » page 834
- « Configuration des modèles de message électronique destinés à la notification » page 834

Conditions préalables

- Vérifiez que les utilisateurs eDirectory ont rempli l'attribut Adresse de messagerie Internet.

Configuration du serveur SMTP pour envoyer la notification par message électronique

1. Dans iManager, sélectionnez **Mots de passe** > **Email Server Options** (Options du serveur de messagerie électronique).
2. Indiquez les informations suivantes :
   - Nom d'hôte
   - Nom qui doit apparaître dans le champ De du message électronique, par exemple « Administrateur »
   - Nom d'utilisateur et mot de passe permettant de s'authentifier auprès du serveur, le cas échéant
3. Cliquez sur **OK**.
4. Personnalisez les modèles de message électronique comme décrit à la section « Configuration des modèles de message électronique destinés à la notification » page 834.

Une fois le serveur de messagerie configuré, les messages électroniques peuvent être envoyés par les applications qui les utilisent, si vous faites appel aux fonctionnalités qui entraînent l'envoi des messages.

Configuration des modèles de message électronique destinés à la notification

Vous pouvez personnaliser ces modèles avec le texte de votre choix. Le nom du modèle traduit son utilisation. Les modèles de message électronique offrent une prise en charge linguistique.

1. Dans iManager, sélectionnez **Mots de passe** > **Edit Email Templates** (Modifier les modèles de message électronique). Une liste de modèles s'affiche.
2. Modifiez les modèles comme vous le souhaitez.

   N'oubliez pas que, si vous souhaitez ajouter des balises de remplacement, vous aurez peut-être besoin de tâches complémentaires.

Test du self-service de mot de passe

Pour vous assurer que les fonctions sont configurées correctement, suivez la procédure suivante pour tester le self-service de mot de passe :

1. Créez une stratégie avec les caractéristiques suivantes. Pour plus d'informations sur cette opération, reportez-vous à la section « Création ou modification d'ensembles de stimulations » page 822.
   - Activez la fonction de mot de passe oublié.
   - Exigez un ensemble de stimulations.
   - Sélectionnez l'option pour vérifier que la réponse aux question de stimulations et de l'indice sont configurés lors de la connexion.
   - Assignez la stratégie de mot de passe à un conteneur comportant au moins un utilisateur que vous pouvez utiliser pour réaliser le test. Cet utilisateur est celui dont l'adresse électronique est indiquée dans l'objet Utilisateur sous l'attribut `Internet EMail Address` (Adresse électronique Internet).
2. Vérifiez que vous disposez, pour le test, d'un autre utilisateur auquel aucune stratégie de mot de passe n'est assignée.
3. Pour tester le self-service de mot de passe, utilisez l'application utilisateur Identity Manager. Pour plus d'informations sur la procédure à suivre, reportez-vous à la section Using the Identity Self-Service Tab *(Utiliser l'onglet Self-service d'identité) du NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide* (Guide de l'utilisateur pour l'application utilisateur du module RBPM 4.5 de NetIQ Identity Manager).

   Pour les utilisateurs Windows, testez le self-service de mot de passe à l'aide du client Novell. Pour plus d'informations sur la procédure à suivre, reportez-vous à la section Using Forgotten Password Self-Service (Utiliser la fonction de self-service de mot de passe oublié) du *Novell Client for Windows Administration Guide* (Guide d'administration du client Novell pour Windows).

Ajout du self-service de mot de passe à votre portail d'entreprise

La plupart des procédures décrites à la section Self-service de mot de passe supposent que vous utilisez les fonctions du self-service de mot de passe sur un serveur iManager 2.0.2, qui est la dernière version d'iManager, pour prendre en charge le self-service de mot de passe. Si vous disposez d'une version d'iManager ultérieure à 2.0.2, vous ne pouvez utiliser la fonction de self-service de mot de passe que par le biais de l'application utilisateur de NetIQ. Pour plus d'informations sur l'utilisation du self-service de mot de passe à l'aide de l'application utilisateur de NetIQ, reportez-vous à la section Using the Identity Self-Service Tab (Utilisation de l'onglet Self-service d'identité) du *NetIQ Identity Manager Roles Based Provisioning Module 4.5 User Application User Guide* (Guide de l'utilisateur de l'application utilisateur du module RBPM 4.5 de NetIQ Identity Manager).

Reportez-vous au tableau ci-dessous pour obtenir des instructions sur l'utilisation des fonctions du self-service de mot de passe avec les produits du portail, y compris des produits autres qu'iManager.

Vérification de la configuration des fonctions de mot de passe par les utilisateurs

Lorsque les utilisateurs se connectent sur le portail iManager à l'adresse `https://adresse_IP_serveur_iManager/nps`, ils sont invités à prendre des mesures sur diverses pages post-authentification en présence de conditions semblables aux suivantes :

- Le mot de passe utilisateur ne respecte pas les règles de mot de passe avancées dans la stratégie de mot de passe
- La stratégie de mot de passe nécessite des questions de stimulations lorsque vous utilisez la fonction de self-service de mot de passe oublié et que l'utilisateur n'a pas configuré ces questions
- La stratégie de mot de passe utilise la fonction de mot de passe oublié avec l'action « Display Password Hint » (Afficher l'indice de mot de passe) et l'utilisateur n'a pas créé d'indice

Par exemple, ces invites sont nécessaires pour vous assurer que l'utilisateur peut utiliser la fonction de self-service de mot de passe oublié. Si la stratégie de mot de passe exige des utilisateurs qu'ils répondent à des questions de stimulations et si l'utilisateur ne les a jamais configurées, il ne peut pas accéder au self-service de mot de passe oublié. Si l'utilisateur n'a pas créé d'indice de mot de passe, il ne peut pas le récupérer pour l'aider à se rappeler du mot de passe.

Étant donné que d'autres produits du portail ne proposent pas automatiquement les fonctions post-authentification, vous devez vous assurer que les utilisateurs se connectent au portail iManager au moins une fois afin de créer des mots de passe conformes et de configurer la gestion des mots de passe, puis une nouvelle fois lorsque que vous modifiez les stratégies de mot de passe.

Dépannage du self-service de mot de passe

- Pour utiliser les questions et réponses de stimulations, vérifiez que vous utilisez un navigateur pris en charge par iManager 2.02.
- Si votre protocole SSL n'est pas correctement configuré, vous ne pourrez pas vous connecter à iManager ni au portail. Si vous pouvez vous connecter à iManager et que vous avez besoin de TLS pour la liaison simple, SSL est correctement configuré et vous pouvez éliminer les problèmes associés au protocole SSL lors du dépannage du self-service de mot de passe.

Application de mots de passe universels respectant la casse

Dans NetIQ eDirectory , vous pouvez activer la fonctionnalité de mot de passe universel et rendre votre mot de passe sensible à la casse lorsque vous accédez au serveur eDirectory par le biais des clients et utilitaires suivants :

- Novell Client 4.9 et versions ultérieures ;
- Utilitaires d'administration mis à niveau vers eDirectory 9.0 ; ou ultérieur
- NetIQ iManager 3.0 et versions ultérieures, sauf s'il s'exécute sous Windows.

Vous pouvez utiliser n'importe quelle version du SDK LDAP pour obtenir des mots de passe respectant la casse.

Le tableau suivant liste les plates-formes prenant en charge la fonction des mots de passe respectant la casse :

Fonction	Linux	Windows
Application de mots de passe universels respectant la casse	✓	✓

Ce chapitre comprend les informations suivantes :

- « Avantage des mots de passe respectant la casse » page 837
- « Déploiement des mots de passe respectant la casse » page 837
- « Mise à niveau des anciens clients et utilitaires Novell » page 838
- « Pour plus d'informations » page 839

Avantage des mots de passe respectant la casse

L'utilisation de mots de passe sensibles à la casse renforce la sécurité de la connexion à l'annuaire. Par exemple, si vous avez un mot de passe aBc sensible à la casse, toutes les tentatives de connexion avec des combinaisons telles que abc, Abc ou ABC échoueront.

Dans eDirectory, vous pouvez exiger que vos mots de passe respectent la casse pour tous les clients mis à niveau vers eDirectory 9.0 ou version ultérieure.

En imposant l'utilisation de mots de passe sensibles à la casse, vous pouvez empêcher les anciens clients Novell d'accéder au serveur eDirectory.

Déploiement des mots de passe respectant la casse

Dans eDirectory, vous pouvez rendre vos mots de passe sensibles à la casse pour tous les clients en activant la fonction de mot de passe universel. La fonction du mot de passe universel est désactivée par défaut.

Conditions préalables

Par défaut, les utilitaires LDAP et autres utilitaires côté serveur utilisent d'abord la connexion NDS, et en cas d'échec, la connexion avec mot de passe simple. Pour que les mots de passe respectent la casse, vous devez vous connecter via NMAS (NetIQ Modular Authentication Service). Par conséquent, vous devez définir la variable d'environnement `NDSD_TRY_NMASLOGIN_FIRST` sur Vrai pour que la fonctionnalité de mot de passe respectant la casse soit disponible. La connexion NMAS est activée par défaut dans eDirectory. Pour désactiver la connexion NMAS, définissez `NDSD_TRY_NMASLOGIN_FIRST` sur `false`.

REMARQUE : L'utilisation de NMAS pour l'authentification augmente le temps nécessaire à la connexion.

Procédure pour rendre votre mot de passe sensible à la casse

1. Connectez-vous à eDirectory en utilisant le mot de passe existant.

   Dans le cas d'une nouvelle installation, le mot de passe existant est celui que vous avez défini pendant la configuration d'eDirectory 9.2.

   Par exemple, votre mot de passe est “novell”.

REMARQUE : Ce mot de passe n'est pas sensible à la casse.

2 Activer le mot de passe universel.

   Pour plus d'informations, reportez-vous à la « Déploiement du mot de passe universel » page 787.

3 Déconnectez-vous d'eDirectory.

4 Connectez-vous à eDirectory en saisissant le mot de passe existant dans la casse de votre choix.

   Le mot de passe que vous venez d'entrer sera désormais sensible à la casse.

   Par exemple, entrez “NoVELL”.

   Votre mot de passe sera désormais “NoVELL”. Par conséquent, “novell” ou toute autre combinaison de majuscules et de minuscules autre que “NoVELL” ne sera pas valide.

Si vous migrez vers des mots de passe respectant la casse, reportez-vous à la section « Migration vers des mots de passe respectant la casse » page 838.

Tout nouveau mot de passe que vous définissez sera sensible à la casse selon le niveau (objet ou partition) auquel vous avez activé la fonction du mot de passe universel.

Gestion des mots de passe respectant la casse

Vous pouvez gérer le respect de la casse de vos mots de passe en activant ou en désactivant la fonction du mot de passe universel via iManager. Pour plus d'informations, reportez-vous à la « Déploiement du mot de passe universel » page 787.

Mise à niveau des anciens clients et utilitaires Novell

Les dernières versions des clients Novell et utilitaires NetIQ sont les suivantes :

- Novell Client 4.9
- Utilitaires d'administration avec eDirectory 9.2
- NetIQ iManager 3.2 et versions ultérieures

Les clients et utilitaires antérieurs aux versions susmentionnés sont d'anciens clients Novell.

Pour obtenir des mots de passe respectant la casse pour les anciens clients Novell, vous devez d'abord mettre ces derniers à niveau vers leur dernière version. Grâce à eDirectory , la migration de vos mots de passe existants vers des mots de passe respectant la casse est aisée et souple. Pour plus d'informations, reportez-vous à la section « Migration vers des mots de passe respectant la casse » page 838.

Si vous ne mettez pas à niveau les anciens clients vers leur dernière version, leur utilisation d'eDirectory 9.2 peut être bloquée au niveau du serveur.

Migration vers des mots de passe respectant la casse

La fonction du mot de passe universel étant désactivée par défaut, vos mots de passe existants ne seront pas affectés tant que vous n'activez pas cette fonction dans iManager. Pour des instructions pas à pas, reportez-vous à la « Déploiement des mots de passe respectant la casse » page 837.

L'exemple suivant explique la migration vers des mots de passe respectant la casse :

Ouverture de session 1 : le mot de passe universel est désactivé par défaut.

- Vous vous connectez en utilisant votre mot de passe existant. Supposons, par exemple, que vous utilisez le mot de passe netiq.
- Ce mot de passe n'est pas sensible à la casse. Par conséquent, netiq et NetIQ sont tous deux des mots de passe valides.
- Après vous être connecté, vous activez la fonction de mot de passe universel. Pour plus d'informations, reportez-vous à la « Déploiement du mot de passe universel » page 787.

Ouverture de session 2 : la fonction de mot de passe universel a été activée lors de la session précédente.

- Vous vous connectez en utilisant votre mot de passe existant. Supposons, par exemple, que vous tapez le mot de passe noVell.
- Lorsque la fonction du mot de passe universel est activée, ce mot de passe devient sensible à la casse. Vous devez donc vous rappeler comment vous avez entré votre mot de passe la première fois.

Session de connexion 3 et connexions suivantes.

- Si vous vous connectez en utilisant le mot de passe netIQ, il est valide.
- Si vous vous connectez en utilisant le mot de passe NetIQ (ou toute autre variante, à l'exception de noVell), il n'est pas valide.

Pour plus d'informations

Pour plus d'informations sur les mots de passe respectant la casse, reportez-vous à l'aide en ligne d'iManager.

Considérations relatives à la sécurité

Un chiffrement réversible du mot de passe universel est nécessaire pour garantir l'interopérabilité avec d'autres systèmes de mot de passe. Les administrateurs doivent évaluer les coûts et les avantages du système. L'utilisation d'un mot de passe universel stocké dans eDirectory pourrait se révéler plus sûr ou plus pratique que de tenter de gérer plusieurs mots de passe.

Un mot de passe universel dans eDirectory est protégé par trois niveaux de sécurité : un chiffrement triple DES, des droits eDirectory et des droits du système de fichiers.

- Avant NICI 3.0, le mot de passe universel était chiffré par une clé triple DES propre à l'utilisateur. Le mot de passe universel et la clé utilisateur étaient stockés dans les attributs du système, uniquement lisibles par eDirectory. La clé utilisateur (3DES) était chiffrée avec la clé d'arborescence et cette dernière était protégée par une clé NICI unique sur chaque machine. Notez que ni la clé d'arborescence ni la clé NICI n'était stockée dans eDirectory. Elles n'étaient pas enregistrées avec les données qu'elles protègent. La clé d'arborescence était présente sur chaque machine au sein d'une arborescence, mais chaque arborescence avait une clé d'arborescence différente, de sorte que les données chiffrées avec la clé d'arborescence pouvaient être récupérées uniquement sur un ordinateur au sein de la même arborescence. Par conséquent, lors de son stockage, le mot de passe universel était protégé par trois niveaux de chiffrement.

NICI 3.0 prend en charge des clés de stockage AES 256 bits. Par conséquent, toute application utilisant les clés de stockage pour encapsuler en toute sécurité d'autres clés doit être en mesure de traiter le nouvel algorithme. Cependant, toutes les données qui sont actuellement encapsulées à l'aide des clés 3-DES plus anciennes peuvent toujours être évaluées sans modification.

NICI 3.0 prend en charge la clé d'arborescence AES 256 bits. Cependant, eDirectory ne crée pas la clé d'arborescence AES 256 bits par défaut. La création de cette clé dans un environnement eDirectory 9.0 et versions antérieures peut entraîner des problèmes au niveau des services qui dépendent de la clé d'arborescence. Il est recommandé de mettre à jour tous les serveurs eDirectory vers la version 9.2 avant de créer la clé. Pour plus d'informations, reportez-vous à la section Création d'une clé d'arborescence AES 256 bits.

- Chaque clé est également sécurisée via des droits eDirectory. Seuls les administrateurs avec le droit Superviseur ou les utilisateurs proprement dits disposent des droits pour modifier les mots de passe universels.

REMARQUE : la stratégie de mot de passe peut être configurée pour permettre aux administrateurs de lire le mot de passe universel et aux utilisateurs de lire leurs propres mots de passe à l'aide des extensions NMAS/nds-cluster-config. Cette option n'est pas activée par défaut.

- Les droits du système de fichiers garantissent que seul un utilisateur disposant des droits appropriés puisse accéder aux clés.

  Si le mot de passe universel est déployé dans un environnement nécessitant un niveau élevé de sécurité, vous pouvez prendre les précautions supplémentaires suivantes :

  - Vérifiez que les répertoires et fichiers suivants sont sécurisés :

Windows	`%SystemRoot%\SysWOW64\Novell\nici`
	`%SystemRoot%\System32\` où le fichier DLL NICI est installé
Linux	`/var/opt/novell/nici`
	`/etc/opt/novell/nici64.cfg`
	`/opt/Novell/lib64/libccs2.so` et les bibliothèques NICI partagées dans le même répertoire

  Consultez la documentation de votre système pour obtenir des détails spécifiques sur l'emplacement des fichiers NICI et eDirectory.

  - Comme avec n'importe quel système de sécurité, il est très important de restreindre l'accès physique au serveur sur lequel résident les clés.

Pour des consignes de sécurité concernant la gestion des mots de passe, reportez-vous à la « Considérations relatives à la sécurité » page 701.

Importation des mots de passe basés sur le hachage dans eDirectory

Les mots de passe peuvent être importés dans eDirectory par le biais d'un format `LDIF` dans les hachages `DIGEST-MD5`, `crypt`, `SHA` et `SSHA`. Procédez comme suit pour importer les mots de passe basés sur le hachage MD5 dans eDirectory :

1. Créez un hachage `MD5` au format `base64` à l'aide de la commande suivante :

   ```
   echo -n <password> | openssl md5 -binary | base64
   ```

   REMARQUE : eDirectory prend en charge les mots de passe basés sur le hachage uniquement au format `base64`.

2. Ajoutez le texte qui est renvoyé lors de la création du hachage `MD5` dans un fichier `LDIF` comme illustré dans l'exemple ci-dessous :

   ```
   dn: cn=sp1,o=novell
   control: 2.16.840.1.113719.1.27.101.5
   changetype: modify
   replace: userPassword
   userPassword: {md5}CSbJUP4kfDtGXrE+JY7kaNI5oGU=
   ```

   REMARQUE : assurez-vous qu'aucune stratégie de mot de passe n'est appliquée à l'utilisateur modifié via le fichier `LDIF`.

3. Ajoutez les variables suivantes au script `pre_ndsd_start`, puis redémarrez eDirectory. Par défaut, le script se trouve à l'emplacement `/opt/novell/eDirectory/sbin`.

   ```
   NDSD_TRY_NMASLOGIN_FIRST=true
   export NDSD_TRY_NMASLOGIN_FIRST
   ```

4. Installez les deux méthodes (mot de passe simple et DIGEST-MD5 NMAS) et assurez-vous d'utiliser la méthode de mot de passe simple comme méthode par défaut.

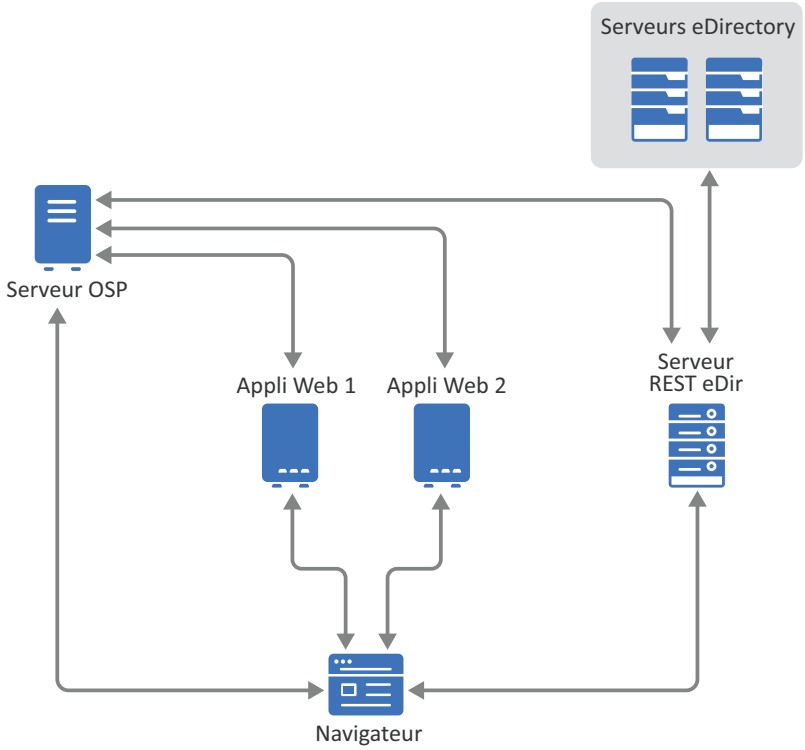
5. Utilisez ice avec l'option `-l` du gestionnaire cible LDAP à l'aide de la commande suivante :

   ```
   ice -S LDIF -f ./change_pass.ldiff -D LDAP -s 164.99.163.236 -p 636 -d
   cn=admin,o=novell -w n -l -L /var/opt/novell/eDirectory/data/SSCert.der
   ```

27 Services REST

eDirectory intègre plusieurs API REST qui permettent d'accéder à diverses fonctionnalités d'eDirectory par le biais des services Web REST. Grâce aux API, vous pouvez appeler n'importe quelle requête afin d'obtenir la réponse appropriée du serveur eDirectory. Les services Web REST peuvent être déployés en tant que conteneur Docker. Pour plus d'informations, reportez-vous au schéma ci-dessous, qui illustre l'architecture des services Web REST pour eDirectory :

Figure 27-1 *Architecture des services Web REST avec eDirectory*



REMARQUE : les services REST pour eDirectory utilisent le protocole OAUTH2 pour fournir l'authentification avec One SSO Provider (OSP).

Ce document vous explique comment effectuer les tâches suivantes :

- « Planification de l'installation des services REST pour eDirectory » page 844
- « Configuration des services REST pour eDirectory » page 846
- « Gestion de la persistance des données » page 848
- « Audit avec les services REST » page 848
- « Modification d'un mot de passe LDAP à l'aide d'un conteneur REST » page 849
- « Modification d'un certificat de serveur à l'aide d'un conteneur REST » page 850

Planification de l'installation des services REST pour eDirectory

Cette section explique comment préparer l'installation avant d'installer les services REST. Pour installer et configurer REST, vous devez effectuer les tâches suivantes :

- Veillez à obtenir un certificat de serveur au format `.pfx`. Vous pouvez utiliser des certificats de serveur générés par une autorité de certification externe ou iManager. Par exemple, vous pouvez générer un certificat de serveur `keys.pfx` à l'aide d'iManager. Pour plus d'informations, reportez-vous à la section « Création d'un objet Certificat de serveur » page 720.
- Veillez à obtenir un fichier de certificat d'une autorité de certification au format `.pem`. Par exemple, vous pouvez utiliser le certificat d'autorité de certification eDirectory (`SSCert.pem`).
- (Facultatif) Installez et configurez OSP avant d'installer les services REST. Pour plus d'informations, reportez-vous à la section Création d'un conteneur OSP.
- Créez un fichier de configuration à l'aide des paramètres de configuration ci-dessous. Par exemple, créez un fichier `edirapi.conf`. Vous pouvez modifier les valeurs du fichier de configuration en fonction de vos besoins.

```
listen = ":9000"
ldapserver = "192.168.1.1:636"
ldapuser = "cn=admin,o=novell"
pfxpassword = "novell"
ldappassword = "novell"
osp-token-endpoint = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/
getattributes"
osp-authorize-url = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/grant"
osp-logout-url = "http://10.10.10.10:8543/osp/a/idm/auth/app/logout"
osp-redirect-url = "https://10.10.10.10:9000/eDirAPI/v1/edirtree/
authcoderedirect"
osp-client-id = "edirapi"
ospclientpass = "novell"
ospcert = "/etc/opt/novell/eDirAPI/conf/ssl/trustedcert/SSCert.pem"
bcert = "/etc/opt/novell/eDirAPI/conf/ssl/trustedcert/SSCert.pem"
loglevel = "error"
check-origin = "true"
origin = "https://10.10.10.10:9000,https://192.168.1.1:9000"
enableaudit = "true"
enableservicestartaudit = "true"
enableservicestopaudit = "true"
enablelogsessioncreationaudit = "true"
enablelogsessionterminationaudit = "true"
auditlogmaxsize = "50 MB"
edirapilogmaxsize = "50 MB"
scope = "ism"
```

Tableau 27-1 *Description des paramètres de configuration dans le fichier de configuration*

Paramètre de configuration	Description
listen	Spécification du port 9000 en tant que port d'écoute du serveur REST dans le conteneur.
ldapserver	Spécification de l'adresse IP du serveur hôte eDirectory.

Paramètre de configuration	Description
ldapuser	Spécification du nom de l'utilisateur qui dispose des droits d'administration pour l'arborescence eDirectory.
pfxpassword	Spécification du mot de passe du fichier de certificat .pfx.
ldappassword	Spécification du mot de passe du serveur LDAP.
osp-token-endpoint	Cette URL est utilisée pour extraire certains attributs du serveur OSP afin de vérifier la validité du jeton d'authentification.
osp-authorize-url	Cette URL est utilisée par l'utilisateur pour fournir les informations d'identification permettant d'obtenir un jeton d'authentification.
osp-logout-url	Cette URL permet de mettre fin à la session entre l'utilisateur et le serveur OSP.
osp-redirect-url	Le serveur OSP redirige l'utilisateur vers cette URL une fois le jeton d'authentification accordé.
osp-client-id	Spécification de l'ID du client OSP qui a été fourni lors de l'enregistrement d'Identity Console avec OSP.
ospclientpass	Spécification du mot de passe du client OSP qui a été fourni lors de l'enregistrement d'Identity Console avec OSP.
ospcert	Spécification de l'emplacement du certificat CA du serveur OSP.
bcert	Spécification de l'emplacement du certificat CA du serveur REST.
loglevel	Spécification des niveaux à inclure dans le fichier journal uniquement. Par exemple, Debug, Error, Panic, etc.
check-origin	Si ce paramètre a la valeur true, le serveur Identity Console compare la valeur d'origine des requêtes. Les options disponibles sont true (vrai) et false (faux).
origin	Si le paramètre `check-origin` a la valeur true, Identity Console compare la valeur d'origine des requêtes avec les valeurs spécifiées dans ce champ.
enableaudit	L'affectation de la valeur true à cette option active l'audit pour les services REST. Les options disponibles sont true (vrai) et false (faux).
enableservicestartaudit	L'affectation de la valeur true à cette option permet de recevoir une notification pour les événements de démarrage des services REST. Les options disponibles sont true (vrai) et false (faux).
enableservicestopaudit	L'affectation de la valeur true à cette option permet de recevoir une notification pour les événements d'arrêt des services REST. Les options disponibles sont true (vrai) et false (faux).

Paramètre de configuration	Description
enablelogsessioncreationaudit	L'affectation de la valeur true à cette option permet de recevoir une notification pour les événements de création de session des services REST. Les options disponibles sont true (vrai) et false (faux).
enablelogsessionterminationaudit	L'affectation de la valeur true à cette option permet de recevoir une notification pour les événements de fin de session des services REST. Les options disponibles sont true (vrai) et false (faux).
auditlogmaxsize	Spécification de la limite maximale de la taille du fichier journal d'audit de chaque service REST. Par défaut, la taille du fichier est de 50 Mo.
edirapilogmaxsize	Spécification de la limite maximale de la taille du fichier journal de chaque serveur REST.
scope	Spécification de l'étendue du serveur REST lorsqu'il est utilisé en tant que serveur de ressources selon la terminologie OAuth. Par défaut, ce paramètre est défini sur edirapi *<nom_arborescence>*.

IMPORTANT

- Les paramètres de configuration liés à OSP ne doivent être utilisés que si vous envisagez d'intégrer OSP avec les services REST.
- Pour activer l'audit pour les services REST, vous devez configurer les paramètres liés à l'audit dans le fichier de configuration.
- L'URL HTTPS OSP doit être validée avec des certificats contenant une clé 2 048 bits. Cette validation échoue avec les certificats contenant une clé 4 096 ou 8 192 bits.

Configuration des services REST pour eDirectory

Procédez comme suit pour configurer les API REST pour eDirectory :

1. Chargez l'image Docker à partir de tarball dans votre registre Docker local à l'aide de la commande suivante :

   ```
   docker load --input <tarball of the image>
   ```

   Exemple :

   ```
   docker load --input edirapi.tar.gz
   ```

2. Créez un conteneur Docker à l'aide de la commande suivante :

   ```
   docker create --name edirapi-container -v <volune name> –p <host port>:9000 -e
   ACCEPT_EULA=Y edirapi:<version>
   ```

   Exemple :

   ```
   docker create --name edirapi-container -v my-volume-1 –p 9000:9000 -e
   ACCEPT_EULA=Y edirapi:1.0.0
   ```

REMARQUE : vous pouvez accepter l'accord de licence EULA en affectant la valeur `Y` à la variable d'environnement `ACCEPT_EULA`. Vous pouvez également accepter cet accord dans l'invite qui s'affiche au démarrage du conteneur à l'aide de l'option `-it` de la commande docker create en mode interactif.

3 Copiez le fichier de certificat de serveur (`.pfx`) de votre système de fichiers local vers le conteneur dans `/etc/opt/novell/eDirAPI/cert/keys.pfx` à l'aide de la commande suivante :

```
docker cp <absolute path of server certificate file> edirapi-container:/etc/
opt/novell/eDirAPI/cert/keys.pfx
```

Exemple :

```
docker cp /home/user/keys.pfx edirapi-container:/etc/opt/novell/eDirAPI/cert/
keys.pfx
```

4 Copiez le fichier de certificat d'autorité de certification (`.pem`) de votre système de fichiers local vers le conteneur dans `/etc/opt/novell/eDirAPI/cert/SSCert.pem` à l'aide de la commande suivante :

```
docker cp <absolute path of CA certificate file> edirapi-container:/etc/opt/
novell/eDirAPI/cert/SSCert.pem
```

Exemple :

```
docker cp /home/user/SSCert.pem edirapi-container:/etc/opt/novell/eDirAPI/
cert/SSCert.pem
```

5 Copiez le fichier de configuration (`edirapi.conf`) de votre système de fichiers local vers le conteneur dans `/etc/opt/novell/eDirAPI/conf/edirapi.conf` à l'aide de la commande suivante :

```
docker cp <absolute path of CA certificate file> edirapi-container:/etc/opt/
novell/eDirAPI/conf/edirapi.conf
```

Par exemple :

```
docker cp /home/user/edirapi.conf edirapi-container:/etc/opt/novell/eDirAPI/
conf/edirapi.conf
```

6 Démarrez le conteneur Docker à l'aide de la commande suivante :

```
docker start -i edirapi-container
```

7 (Facultatif) Vous pouvez également installer et configurer le conteneur REST en exécutant le script suivant (passez les étapes 2 à 6) :

```
configure-edirapi --sscert-file <absolute path of CA certificate file> --conf-
file <absolute path of configuration file> --pfx-file <absolute path of server
certificate file> --name edirapi-container –p <hosts port>:9000 -v <name of the
volume> edirapi:<version>
```

Exemple :

```
configure-edirapi --sscert-file my-SSCert.pem --conf-file my-edirapi.conf --
pfx-file my-keys.pfx –-name edirapi-container –p 9000:9000 –v myvolume:/config
edirapi:1.0.0
```

REMARQUE

- Le certificat de l'autorité de certification du serveur REST doit commencer par `BEGIN CERTIFICATE` et se terminer par `END CERTIFICATE`. Si vous indiquez une autre valeur, le serveur REST affiche un message d'erreur.
- Pour prendre en charge un nombre maximal de 42 000 connexions dans le conteneur REST, vous devez augmenter la plage de ports en exécutant les trois commandes suivantes :

```
ulimit -n 999999
cat /proc/sys/net/ipv4/ip_local_port_range
echo 1024 65535 > /proc/sys/net/ipv4/ip_local_port_range
```

Gestion de la persistance des données

En plus des conteneurs REST, des volumes sont également créés pour la persistance des données. Pour utiliser les paramètres de configuration d'un ancien conteneur qui utilise les volumes, procédez comme suit :

1. (Facultatif) Arrêtez le conteneur Docker actuel à l'aide de la commande suivante :

   ```
   docker stop edirapi-container
   ```

2. Créez le second conteneur à l'aide de la commande suivante :

   ```
   docker create --name container-2 –p 9000:9000 -v my-volume-1:/config
   edirapi:1.0.0
   ```

3. Démarrez le second conteneur à l'aide de la commande suivante :

   ```
   docker start container-2
   ```

4. (Facultatif) Vous pouvez à présent supprimer le premier conteneur à l'aide de la commande suivante :

   ```
   docker rm edirapi-container
   ```

Audit avec les services REST

Le serveur REST eDirectory peut envoyer les journaux des événements d'audit CEF au serveur Sentinel. Le serveur REST envoie les données d'audit à l'aide de connecteurs ArcSight SmartConnector. Pour plus d'informations sur la configuration et sur l'utilisation des connecteurs SmartConnector, reportez-vous au manuel ArcSight SmartConnector User Guide (Guide de l'utilisateur d'ArcSight SmartConnector).

Pour activer l'audit pour les services REST, vous devez configurer les paramètres liés à l'audit dans le fichier de configuration. Pour plus d'informations, reportez-vous à la section « Planification de l'installation des services REST pour eDirectory » page 844.

Présentation des événements REST

Par défaut, tous les événements REST sont activés. Vous pouvez désactiver un événement s'il n'est pas nécessaire pour votre organisation. Le serveur REST eDirectory peut auditer les événements suivants :

Événement	Description
ENABLESERVICESTARTAUDIT	Génère un événement en cas de démarrage du service REST.
ENABLESERVICESTOPAUDIT	Génère un événement en cas d'arrêt du service REST.
ENABLELOGSESSIONCREATIONAUDIT	Génère un événement en cas de création d'une session REST.
ENABLELOGSESSIONTERMINATIONAUDIT	Génère un événement en cas de fin d'une session REST.

REMARQUE : les fichiers journaux se trouvent dans `/var/opt/novell/eDirAPI/log/edirapi_auditlog.log`.

Exemple

Voici un exemple d'événement **Créer une session** :

```
Oct 10 15:37:17 eDirAPI
CEF:0|NetIQ|eDirAPI|1.0|000B0510|SESSION_CREATE|3|dvc=10.71.128.233
dvchost=SLES12SP3-SHREYAS-128233 rt=Oct 10 2019 15:37:17 dtz=IST src=164.99.136.60
spt=59132 suser=cn\=admin,o\=novell duser=cn\=admin,o\=novell
cn1Label=CorrelationID cn1=rtpL9xt-tzBR92fEGt9rrczA_1M2vHrGM4Q_8AjEmSU=
cs1Label=Client Address cs1=164.99.136.60 cs2Label=Tree Name cs2=SHREYAS_TREE2
sproc=eDirAPI sourceServiceName=edirapi reason=201 outcome=Success
```

Modification d'un mot de passe LDAP à l'aide d'un conteneur REST

Procédez comme suit pour modifier un mot de passe LDAP à l'aide d'un conteneur REST :

1. Connectez-vous au conteneur à l'aide de la commande suivante :

   ```
   docker exec -it <container_name> bash
   ```

2. Stockez un nouveau mot de passe dans la zone de stockage des mots de passe à l'aide de la commande suivante :

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/netiq/
   common/openssl/lib64/ /opt/novell/eDirAPI/sbin/passwdstore -a <Admin DN>
   ```

   La commande ci-dessus vous invite à entrer un mot de passe. Entrez le nouveau mot de passe.

   Exemple :

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/netiq/
   common/openssl/lib64/ /opt/novell/eDirAPI/sbin/passwdstore -a admin.novell
   ```

3. Quittez la console du conteneur à l'aide de la commande suivante :

   ```
   exit
   ```

4. Redémarrez le conteneur.

   ```
   docker restart <container name>
   ```

Modification d'un certificat de serveur à l'aide d'un conteneur REST

Procédez comme suit pour modifier un certificat de serveur à l'aide d'un conteneur REST :

1. Exécutez la commande suivante pour copier le nouveau certificat de serveur (par exemple, `new-keys.pfx`) dans un emplacement du conteneur :

   ```
   docker cp /path/to/new-keys.pfx <container_id/name>:/tmp/new-keys.pfx
   ```

2. Connectez-vous au conteneur à l'aide de la commande suivante :

   ```
   docker exec -it <container_name> bash
   ```

3. Exécutez `NLPCERT` pour stocker les clés.

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/netiq/
   common/openssl/lib64/ /opt/novell/eDirAPI/sbin/nlpcert -i /tmp/new-keys.pfx -o
   /etc/opt/novell/eDirAPI/conf/ssl/private/cert.pem
   ```

   La commande ci-dessus vous invite également à entrer le mot de passe du certificat de serveur. Entrez votre mot de passe.

4. Quittez la console du conteneur à l'aide de la commande suivante :

   ```
   exit
   ```

5. Redémarrez le conteneur.

   ```
   docker restart <container name>
   ```

A Considérations relatives à NMAS

Cette annexe comprend les rubriques suivantes :

- « Configuration d'un conteneur Sécurité en tant que partition distincte » page 851
- « Fusion des arborescences avec conteneurs de sécurité multiples » page 851

Configuration d'un conteneur Sécurité en tant que partition distincte

NMAS* (NetIQ Modular Authentication Services*) repose sur le stockage des stratégies communes à l'arborescence NetIQ eDirectory. L'arborescence eDirectory représente en réalité le domaine de sécurité. Les règles de sécurité doivent être disponibles sur tous les serveurs de l'arborescence.

NMAS place les stratégies d'authentification et les données de configuration des méthodes de connexion dans le conteneur de sécurité créé au niveau de la [Racine] des arborescences eDirectory. Ces informations doivent être facilement accessibles à tous les serveurs utilisant NMAS. Le conteneur Sécurité a pour but d'héberger les stratégies globales relatives aux propriétés de sécurité telles que la connexion, l'authentification et la gestion des clés.

Avec NMAS, il est recommandé de créer le conteneur de sécurité en tant que partition séparée, et de le répliquer largement. Cette partition doit être répliquée en tant que partition Lecture/écriture uniquement sur les serveurs de votre arborescence qui sont approuvés.

REMARQUE : étant donné que le conteneur Sécurité contient des règles globales, soyez attentifs à l'emplacement des répliques accessibles en écriture car ces serveurs peuvent modifier les règles de sécurité générales spécifiées dans l'arborescence eDirectory. Pour que les utilisateurs se connectent avec NMAS, les répliques de leurs objets Utilisateur doivent se trouver sur le serveur NMAS.

Fusion des arborescences avec conteneurs de sécurité multiples

Il convient d'être particulièrement prudent lors de la fusion d'arborescences eDirectory lorsque l'une au moins comporte un conteneur Sécurité. Vérifiez qu'il s'agit bien d'une opération que vous souhaitez vraiment réaliser. Cette procédure peut en effet être longue et fastidieuse.

Pour fusionner des arborescences avec plusieurs conteneurs Sécurité :

1. Dans iManager, identifiez les arborescences à fusionner.
2. Identifiez l'arborescence source et l'arborescence cible.

   Tenez compte des remarques suivantes concernant la sécurité pour les arborescences source et cible :

   - Tous les certificats signés par l'autorité de certificat organisationnelle de l'arborescence source doivent être supprimés.
   - L'autorité de certificat organisationnelle de l'arborescence source doit être supprimée.

- Tous les secrets d'utilisateur enregistrés dans NetIQ SecretStore sur l'arborescence source doivent être supprimés.
- Toutes les méthodes de connexion NMAS de l'arborescence source doivent être supprimées et réinstallées dans l'arborescence cible.
- Tous les utilisateurs NMAS de l'arborescence source doivent être de nouveau enrôlés une fois les arborescences fusionnées.
- Tous les utilisateurs et serveurs qui se trouvaient dans l'arborescence source doivent disposer de nouveaux certificats créés une fois les arborescences fusionnées.
- Les secrets de tous les utilisateurs qui se trouvaient dans l'arborescence source doivent être réinstallés dans SecretStore.

Si aucune des arborescences source ou cible ne possède de conteneur appelé Sécurité à la racine de l'arborescence, ou si seule une arborescence dispose d'un conteneur de sécurité, aucune autre action n'est nécessaire. Sinon, poursuivez la procédure.

REMARQUE : veillez à ne pas fusionner deux arborescences eDirectory contenant des serveurs activés pour l'authentification EBA.

Opérations à effectuer par produit avant une fusion d'arborescences

Ce chapitre comprend les informations suivantes :

- « NetIQ Certificate Server » page 852
- « NetIQ Single Sign-on » page 853
- « NMAS » page 854
- « Infrastructure du domaine de sécurité NetIQ » page 855
- « Autres opérations de sécurité » page 855

NetIQ Certificate Server

selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. Si les objets et éléments cités dans une étape donnée ne sont pas présents dans l'arborescence source, vous pouvez ignorer l'étape.

1. Tous les certificats de racine approuvée de l'arborescence source doivent être installés dans l'arborescence cible.

   Les certificats de racine approuvée sont stockés dans des objets Racine approuvée, stockés dans des conteneurs Racine approuvée. Les conteneurs de racine approuvée peuvent être créés à tout emplacement de l'arborescence. Cependant, seuls les certificats de racine approuvée se trouvant dans les conteneurs de racine approuvée du conteneur de sécurité doivent être déplacés manuellement depuis l'arborescence source vers l'arborescence cible.

2. Installez les certificats de racine approuvée dans l'arborescence cible.

   2a Sélectionnez un conteneur Racine approuvée du conteneur de sécurité dans l'arborescence source.

   2b Créez un conteneur Racine approuvée dans le conteneur Sécurité de l'arborescence cible, portant le nom exact utilisé dans l'arborescence source (Étape 2a).

   2c Dans l'arborescence source, ouvrez un objet Racine approuvée dans le conteneur du même nom sélectionné et exportez le certificat.

IMPORTANT : notez l'emplacement et le nom du fichier utilisé. Vous en aurez besoin à la prochaine étape.

2d Dans l'arborescence cible, créez un objet Racine approuvée dans le conteneur créé à l'Étape 2b. Spécifiez le même nom que pour l'arborescence source et, lorsque vous êtes invité à préciser le certificat, spécifiez le fichier créé à Étape 2c.

2e Supprimez l'objet Racine approuvée de l'arborescence source.

2f Reprenez la procédure de l'Étape 2c à l'Étape 2e jusqu'à ce que tous les objets Racine approuvée du conteneur Racine approuvée sélectionné soient installés dans l'arborescence cible.

2g Supprimez le conteneur Racine approuvée de l'arborescence source.

2h Répétez la procédure de l'Étape 2a à l'Étape 2f jusqu'à ce que tous les conteneurs de racine approuvée soient supprimés de l'arborescence source.

3 Supprimez l'autorité de certificat organisationnelle de l'arborescence source.

L'objet Autorité de certificat organisationnelle se trouve dans le conteneur de sécurité.

IMPORTANT : après cette étape, tous les certificats signés par l'autorité de certification organisationnelle de l'arborescence source sont inutilisables. Cela comprend les certificats serveur et les certificats utilisateur signés par l'autorité de certificat organisationnelle de l'arborescence source.

4 Supprimez tous les objets Matériel clé (KMO – Key Material Object) de l'arborescence source possédant un certificat signé par l'autorité de certification organisationnelle de l'arborescence source.

Les objets Matériel clé de l'arborescence source possédant des certificats signés par d'autres autorités de certificat restent valides et n'ont pas à être supprimés.

Si vous n'êtes pas sûr de l'identité de l'autorité de certification apposant sa signature pour un objet Matériel clé, consultez la section Certificat de racine approuvée de l'onglet Certificats sur la page de propriétés de l'objet Matériel clé.

5 Supprimez tous les certificats utilisateur de l'arborescence source signés par l'autorité de certificat organisationnelle de l'arborescence source.

Si les utilisateurs de l'arborescence source ont déjà exporté leurs certificats et clés privées, ces certificats et clés exportés seront toujours utilisables. Les clés privées et les certificats restant dans eDirectory ne peuvent plus être utilisés après l'Étape 3.

Pour chaque utilisateur disposant de certificats, ouvrez les propriétés de l'objet Utilisateur. La liste de tous les certificats pour l'utilisateur s'affiche dans la section Certificats de l'onglet Sécurité. Tous les certificats dont l'émetteur est l'autorité de certificat organisationnelle doivent être supprimés.

NetIQ Single Sign-on

Si NetIQ Single Sign-on est installé sur un ou plusieurs serveurs de l'arborescence source, vous devez supprimer tous les secrets NetIQ Single Sign-on pour les utilisateurs de l'arborescence source.

Pour chaque utilisateur qui emploie NetIQ Single Sign-on dans l'arborescence source, ouvrez les propriétés de l'objet Utilisateur. Tous les secrets de l'utilisateur sont répertoriés dans la section SecretStore de l'onglet Sécurité. Supprimez tous les secrets répertoriés.

REMARQUE : selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. S'ils ne se trouvent pas dans l'arborescence source, vous pouvez ignorer cette étape.

NMAS

selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. S'ils ne se trouvent pas dans l'arborescence source, vous pouvez ignorer cette étape.

1. Dans l'arborescence cible, installez toutes les méthodes de connexion NMAS de l'arborescence source qui n'y figurent pas encore.

   Pour vous assurer que tous les composants de connexion client et serveur nécessaires sont correctement installés dans l'arborescence cible, il est recommandé d'installer toutes les nouvelles méthodes de connexion à partir des sources NetIQ d'origine ou des sources fournies par le revendeur.

   Bien que les méthodes *puissent* être réinstallées à partir des fichiers de serveur existants, il est généralement plus simple et plus fiable de procéder à une installation à partir de paquetages fournis par NetIQ ou par le fournisseur.

2. Pour être sûr que les séquences de connexion établies précédemment dans l'arborescence source seront bien disponibles dans l'arborescence cible, migrez les séquences de connexion souhaitées.

   2a Dans iManager, sélectionnez le conteneur de sécurité de l'arborescence source.

   2b Cliquez avec le bouton droit sur l'objet **Login Policy** (Stratégie de connexion) et sélectionnez **Propriétés**.

   2c Pour chaque séquence de connexion figurant dans la liste déroulante **Defined Login Sequences** (Séquences de connexion définies), notez les méthodes de connexion utilisées (affichées dans le volet de droite).

   2d Sélectionnez le conteneur de sécurité dans l'arborescence cible et répliquez les séquences de connexion en utilisant les mêmes méthodes de connexion qu'à l'Étape 2c.

   2e Pour terminer, cliquez sur **OK**.

3. Supprimez les attributs de sécurité des connexions NMAS dans l'arborescence source.

   3a Dans le conteneur Sécurité de l'arborescence source, supprimez l'objet Stratégie de connexion.

   3b Dans le conteneur Méthodes de connexion autorisées de l'arborescence source, supprimez toutes les méthodes de connexion.

   3c Supprimez le conteneur Méthodes de connexion autorisées de l'arborescence source.

   3d Dans le conteneur Méthodes de post-connexion autorisées de l'arborescence source, supprimez toutes les méthodes de connexion.

   3e Supprimez ensuite le conteneur Méthodes de post-login autorisées de l'arborescence source.

   REMARQUE : pour supprimer les méthodes de connexion autorisées, utilisez ldapdelete.

Infrastructure du domaine de sécurité NetIQ

selon l'utilisation du produit, les objets et éléments auxquels il est fait référence peuvent ne pas être présents. S'ils ne se trouvent pas dans l'arborescence source, vous pouvez ignorer cette étape.

1. Supprimez l'objet W0 et le conteneur KAP de l'arborescence source.

   Le conteneur KAP se trouve dans le conteneur de sécurité. L'objet W0 se trouve dans le conteneur KAP.

2. Sur tous les serveurs de l'arborescence source, supprimez les clés de l'infrastructure du domaine de sécurité (Security Domain Infrastructure, SDI) en supprimant le fichier `/var/opt/novell/nici/uid/nicisdi.key` sous Linux et le fichier %SystemRoot%\SysWOW64\Novell\NICI\nicisdi.key sous Windows.

   IMPORTANT : Veillez à supprimer ce fichier sur *tous* les serveurs de l'arborescence source.

Autres opérations de sécurité

Si un conteneur de sécurité existe dans l'arborescence source, supprimez-le avant de fusionner les arborescences.

Fusion des arborescences

L'utilitaire DSMerge permet de fusionner les arborescences eDirectory. Pour plus d'informations, reportez-vous au Chapitre 10, « Fusion d'arborescences NetIQ eDirectory », page 297 et à l'Annexe B, « Commandes et syntaxe NetIQ eDirectory Linux », page 857.

Opérations à effectuer par produit après la fusion

Ce chapitre comprend les informations suivantes :

- « NetIQ Certificate Server » page 855
- « NetIQ Single Sign-on » page 855
- « NMAS » page 856

NetIQ Certificate Server

Si vous utilisez NetIQ Certificate Server, après la fusion des arborescences, réémettez, si nécessaire, des certificats pour les serveurs et les utilisateurs qui se trouvaient auparavant dans l'arborescence source.

NetIQ Single Sign-on

Si vous utilisez NetIQ Single Sign-on, après la fusion des arborescences, recréez, si nécessaire, des secrets SecretStore pour les utilisateurs qui se trouvaient auparavant dans l'arborescence source.

NMAS

Si vous utilisez NMAS, après la fusion des arborescences, réinscrivez si nécessaire les utilisateurs NMAS qui se trouvaient auparavant dans l'arborescence source.

Pour plus d'informations, reportez-vous au Chapitre 24, « Présentation de l'infrastructure d'authentification d'eDirectory », page 673.

B Commandes et syntaxe NetIQ eDirectory Linux

Ce chapitre présente les utilitaires de NetIQ eDirectory sous Linux et décrit leur syntaxe :

- « Utilitaires généraux » page 857
- « Commandes spécifiques de LDAP » page 862

Utilitaires généraux

Cette section contient la liste des utilitaires eDirectory sous Linux et décrit leur syntaxe.

REMARQUE : après l'installation, veillez à exécuter les utilitaires ndsconfig, ndscheck et ndslogin à partir de l'emplacement d'installation sur le serveur (par défaut, `/opt/novell/eDirectory/bin`). N'exécutez pas ndsconfig à partir du paquetage d'installation.

Pour plus d'informations sur l'utilisation des utilitaires eDirectory, reportez-vous à la page du manuel de chaque utilitaire et à la « Utilitaires de dépannage sous Linux » page 973.

Commande	Description	Utilisation
`nds-install`	Utilitaire qui installe NetIQ eDirectory.	`nds-install [-h] [--help] [-i] [-j] [-u]`

Commande	Description	Utilisation
ndsconfig	Configure NetIQ eDirectory.	ndsconfig <new> [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <password>] [-B ip_address1|interface1@port1,ip_address2|interface2@port2....] [-b port to bind] [-i] [-S <server name>] [-D <instance path>] [-d <path for dib>] [-m <module>] [-e] [-R|-r] [-c] [-L <ldap port>] [-l <SSL port>] [-P <LDAP URLs>] [-o http port] [-O https port] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig <def> [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <password>] [-B ip_address1|interface1@port1,ip_address2|interface2@port2....] [-b port to bind] [-i] [-S <server name>] [-D <instance path>] [-d <path for dib>] [-m <module>] [-e] [-R|-r] [-c] [-L <ldap port>] [-l <SSL port>] [-P <LDAP URLs>] [-o http port] [-O https port] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig add [-t <treename>] [-n <server context>] [-a <admin FDN>] [-w <password>] [-B ip_address1|interface1@port1,ip_address2|interface2@port2....] [-b port to bind] [-E] [-e] [-R|-r] [-c] [-L <ldap port>] [-l <SSL port>] [-P <LDAP URLs>] [-o http port] -O [https port] [-S <server name>] [-D <instance path >] [-d <path for dib>] [-p <IP address[:port]>] [-m <module>] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig rm [-a <*admin FDN*>] [-w <*admin password*>] [-W <*obfuscated_password_file*>] [-c] [--config-file <*configuration file*>] ndsconfig upgrade [-a <admin FDN>] [-w <password>] [-c] [-j] [--config-file <absolute path for configuration file>] [--configure-eba-now <yes/no>] ndsconfig {set <*valuelist*> | get [<*paramlist*>] | get help [<*paramlist*>]}

Commande	Description	Utilisation
ndscheck	Utilitaire qui vérifie l'état de santé de l'arborescence.	ndscheck [--help | -?] Display command usage ndscheck [--version | -v] Display version information ndscheck [-h <*hostname port*>] [-a <*admin FDN*>] [-F <*log file*>] [-D] [-q] [-w <*admin password*>] [-W] [--config-file <*file name*>] ndscheck [-a <*admin FDN*>] [-W] [--config-file <*file name*>] Par exemple : ndscheck -a admin.novell -W --config-file /etc/opt/novell/eDirectory/conf-1/nds.conf
ndsmanage	Utilitaire listant les instances eDirectory.	ndsmanage [-a] ndsmanage [<*username*>]

Commande	Description	Utilisation
ndsbackup	Crée des archives d'objets eDirectory et ajoute ou extrait des objets eDirectory	ndsbackup c [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <*admin-user*>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup r [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <admin-user>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup t [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <admin-user>] [-I <*include-file*>] [-E <*password*>] [--config-file <configuration_file_path>]... [eDirectoryobject] ndsbackup x [f <*ndsbackupfile*>] [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <admin-user>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup s [e] [v] [w] [X<*exclude-file*>] [R] [Replica-server-name] [-a <*admin-user*>] [-I <*include-file*>] [-E <*password*>] [--config-file <*configuration_file_path*>]... [eDirectoryobject] ndsbackup --version ndsbackup [option] [file] [-a <*admin FDN*>] [-p passstore] [--config-file <*file name*>] Par exemple : ndsbackup cvf /tmp/test.bak -a admin.novell -p passstore --config-file /etc/opt/novell/eDirectory/conf-1/nds.conf
ndslogin	Utilitaire de diagnostic pour la vérification de l'authentification NetIQ eDirectory.	ndslogin [-t treename] [-p password] [-s] [-n] [-c] [[-i] | [-I]] [[-h hostname[:port]] | [--config-file <configuration file>]] <userFDN>
ndsd	Daemon NDS.	/opt/novell/eDirectory/sbin/ndsd [--config-file *configfile*]

Commande	Description	Utilisation
ndsimonitor	Surveille et diagnostique les serveurs de l'arborescence NetIQ eDirectory à l'aide de HTTP.	/opt/novell/eDirectory/bin/ndsimonitor [-l [-d <*path of ndsimonitor conf files*>] | u] [-h <*local_interface:port*>] [--config-file <*configuration_file_path*>]
ndsmerge	Utilitaire de fusion de deux arborescences NetIQ eDirectory.	ndsmerge [-m target-tree target-admin source-admin [target-container]] [-c] [-t] [-r target-tree source-admin] [-h <*local_interface:port*>] [--config-file <*configuration_file_path*>]
ndsrepair	Utilitaire de réparation et de résolution des problèmes de la base de données eDirectory, au niveau des enregistrements, du schéma, des objets de Bindery et des références externes	ndsrepair {-U |-E |-C |-P [Ad] |-S [Ad]|-N |-T |-J <*entry_id*>} [-A <*yes/no*>] [-O <*yes/no*>][-F <*filename*>] [-h <*local_interface:port*>] [--config-file <*configuration_file_path*>] ndsrepair -R [-l <*yes/no*>][-u <*yes/no*>][-m <*yes/no*>][-i <*yes/no*>][-f <*yes/no*>][-d <*yes/no*>][-t <yes/no>][-o <yes/no>][-r <yes/no>][-v <yes/no>][-c <yes/no>][-A <yes/no>][-O <yes/no>][-F <*filename*>] [-h <*local_interface*>] [--config-file <*configuration_file_path*>] ndsrepair –I [--config-file <*configuration_file_path*>]
	Vous pouvez demander à ndsrepair d'afficher des informations sur l'espace disponible dans la base de données qui peut être libéré pour votre usage.	
ndssch	Utilitaire d'extension de schéma NetIQ eDirectory.	ndssch [-h <*hostname*>[:<port>]][-t <*treename*>][-F <*logfile*>] <*admin-FDN*> <*schemafile*> ... ndssch [-h <*hostname*>[:<port>]][-t <*treename*>] [-d] <*admin-FDN*> <*schemafile*> [schema description] ...
ndssnmp	Module de services SNMP pour NetIQ eDirectory.	/opt/novell/eDirectory/bin/ndssnmp
ndssnmpconfig	Utilitaire de configuration des trappes SNMP	ndssnmpconfig [-h <*hostname[:port]*>] [-p <*password*>] [-a <*userFDN*>] [-c <*command*>]
ndssnmpsa	Daemon de sous-agent SNMP eDirectory	/opt/novell/eDirectory/bin/ndssnmpsa
ndsstat	Utilitaire d'affichage des informations sur le serveur	ndsstat { -r -s -p <*partitionname*>} [-n] [[-h <*hostname | IP address*>:<*port*>] | [--config-file <*configuration file*>]]
ndstrace	Utilitaire d'affichage des messages de débogage du serveur	ndstrace [-l|-u|-c "command1;....."|--version] [-h <*local_interface:port*>] [--config-file <*configuration_file_path*>]

Commande	Description	Utilisation
nds-uninstall	Utilitaire de désinstallation de NetIQ eDirectory.	nds-uninstall [-s][-h]
nldap	Services LDAP pour le daemon NDS	/opt/novell/eDirectory/sbin/nldap
nmasinst	Utilitaire de configuration de NMAS.	nmasinst -i <*admin-FDN*> <*treename*> [-h <*hostname*>[:port]] nmasinst -addmethod <*admin-FDN*> <*treename*> <*config.txt file*> [-h <*hostname*>[:port]]
npki	Services PKI (Public Key Infrastructure) Novell.	/opt/novell/eDirectory/sbin/npki

Commandes spécifiques de LDAP

Commande	Description	Utilisation
ldapconfig	Utilitaire de configuration des objets Serveur LDAP et Groupe LDAP	ldapconfig get [...] | set <*attribute-value-list*> [-t <*treename*> | -p <*hostname*>[:port] | --config-file <*configuration file*>] [-w <*password*>] [-a <*user FDN*>] [-f] ldapconfig [-t <*treename*> | -p <*hostname*>[:port]] [-w <*password*> | --config-file <*configuration file*>] [-a <*user FDN*>] [-V] [-R] [-H] [-f] -v <*attribute*>,<*attribute2*>... ldapconfig [-t <*treename*> | -p hostname[:port] | --config-file <*configuration file*>] [-w <*password*>] [-a <*admin FDN*>] [-V] [-R] [-H] [-f] -s <*attribute*>=<*value*>,...
ldapadd ldapmodify	Ajoute ou modifie des entrées d'un serveur LDAP	ldapmodify [-a] [-c] [-C] [-M] [-P] [-r] [-n] [-v] [-F] [-l <*limit*>] [-M[M]] [-d <*debuglevel*>] [-e <*key filename*>] [-D <*binddn*>] [[-W]|[-w <*passwd*>]] [-h <*ldaphost*>] [-p <*ldap-port*>] [-P <*version*>] [-Z[Z]] [-f <*file*>] ldapadd [-c] [-C] [-l] [-M] [-P] [-r] [-n] [-v] [-F] [-l <*limit*>] [-M[M]] [-d <*debuglevel*>] [-e <*key filename*>] [-D <*binddn*>] [[-W]| [-w <*passwd*>]] [-h <*ldaphost*>] [-p <*ldapport*>] [-P <*version*>] [-Z[Z]] [-f <*file*>]

Commande	Description	Utilisation
`ldapdelete`	Supprime les entrées d'un serveur LDAP	`ldapdelete [-n] [-v] [-c] [-r] [-l] [-C] [-M] [-d <debuglevel>] [-e <key filename>] [-f <file>] [-D <binddn>] [[-W]| [-w <passwd>]] [-h <ldaphost>] [-p <ldapport>] [-Z[Z]] [dn]...`
`ldapmodrdn`	Outil de modification du nom distinctif relatif (RDN) des entrées LDAP	`ldapmodrdn [-r] [-n] [-v] [-c] [-C] [-l] [-M] [-s <newsuperior>] [-d <debuglevel>] [-e <key filename>] [-D <binddn>] [[-W]|[-w <passwd>]] [-h <ldaphost>] [-p <ldapport>] [-Z[Z]] [-f <file>] [dn <newrdn>]`
`ldapsearch`	Outil de recherche LDAP	`ldapsearch [-n] [-u] [-v] [-t] [-A] [-T] [-C] [-V] [-M] [-P] [-L] [-d <debuglevel>] [-e <key filename>] [-f <file>] [-D <binddn>] [[-W]| [-w <bindpasswd>]] [-h <ldaphost>] [-p <ldapport>] [-b <searchbase>] [-s <scope>] [-a <deref>] [-l <time limit>] [-z <size limit>] [-Z[Z]] filter [attrs....]`

`ndsindex`	Utilitaire permettant de créer, lister, suspendre, reprendre ou supprimer des index de base de données NetIQ eDirectory	`ndsindex list [-h <hostname>] [-p <port>] [-D <bind DN>] [-W|[-w <password>]] [-l <limit>] [-s <eDirectory Server DN>] [-Z[Z]] [<indexName1>, <indexName2>.....]`
		
		`ndsindex add [-h <hostname>] [-p <port>] [-D <bind DN>] -W|[-w <password>] [-l <limit>] [-s <eDirectory Server DN>] [-Z[Z]] <indexDefinintion1> [<indexDefinintion2>.....]`
		
		`ndsindex delete [-h <hostname>] [-p <port>] [-D <bind DN>] [-W|[-w <password>]] [-l <limit>] [-s <eDirectory Server DN>] [-Z[Z]] <indexName1> [<indexName2>.....]`
		
		`ndsindex resume [-h <hostname>] [-p <port>] -D <bind DN> [-W|[-w <password>]] [-l <limit>] [-s <eDirectory Server DN>] [-Z[Z]] <indexName1> [<indexName2>.....]`
		
		`ndsindex suspend [-h <hostname>] [-p <port>] [-D <bind DN>] [-W|[-w <password>]] [-l <limit>] [-s <eDirectory Server DN>] [-Z[Z]] <indexName1> [<indexName2>.....]`

Commande	Description	Utilisation

`ice`	Utilitaire d'importation des entrées d'un fichier vers un annuaire LDAP, de modification des entrées d'un fichier dans un annuaire, d'exportation des entrées vers un fichier et d'ajout des définitions de classes et d'attributs à partir d'un fichier.	`ice -S LDAP -s server1.acme.com -p 636 -L cert-server1.pem -d cn=admin,c=us -w password -F objectClass=* -c sub -D LDIF -f server1.ldif -e des -E secret`
		
		`ice -S LDIF -f server1.ldif -e des -E secret -D LDAP -s server2.acme.com -p 636 -L cert-server2.pem -d cn=admin,c=us -w password`

Caractères spéciaux dans les noms d'utilisateur et mots de passe

L'utilisation de caractères spéciaux dans les noms d'utilisateur et les mots de passe peut créer des problèmes lors de la transmission des valeurs au cours d'une d'installation d'eDirectory ou d'une extension de schéma. Si le nom d'utilisateur ou le mot de passe contient des caractères spéciaux, tels que $, #, etc., insérez devant une barre oblique inverse (\) comme caractère d'échappement.

Exemple : un nom d'administrateur `cn=admin$name.o=container` doit être transféré sous la forme `cn=admin\$name.o=container`.

Lorsque vous entrez des valeurs de paramètre sur la ligne de commande, vous pouvez soit utiliser un caractère d'échappement, soit placer des guillemets simples autour de la valeur.

Par exemple,

```
cn=admin\$name.o=container
```

ou

```
'cn=admin$name.o=container'
```

C Configuration de OpenSLP pour eDirectory

Destinée aux administrateurs, cette annexe contient des informations sur la configuration des installations OpenSLP pour NetIQ eDirectory sans Novell Client.

- « Protocole SLP » page 865
- « Concepts fondamentaux de SLP » page 865
- « Paramètres de configuration » page 868

Protocole SLP

OpenSLP est une mise en œuvre open-source de la convention IETF Service Location Protocol version 2.0, documentée sur le site IETF Request-For-Comments (RFC) 2608 (http://www.ietf.org/rfc/rfc2608.txt?number=2608).

Outre la mise en œuvre du protocole SLP v2, l'interface fournie par le code source OpenSLP est une implémentation d'une autre norme de l'IETF concernant l'accès par programme à la fonctionnalité SLP, documentée dans le fichier RFC 2614 (http://www.ietf.org/rfc/rfc2614.txt?number=2614).

Pour bien comprendre le fonctionnement de SLP, il est recommandé de lire ces deux documents et de les assimiler. Leur lecture peut s'avérer laborieuse, mais ils sont essentiels pour procéder à une configuration correcte de SLP sur un intranet.

Pour plus d'informations sur le projet OpenSLP, consultez les sites Web OpenSLP (http://www.OpenSLP.org) et SourceForge (http://sourceforge.net/projects/openslp). Le site Web OpenSLP contient plusieurs documents qui offrent de précieux conseils de configuration. Un grand nombre de ces documents sont encore incomplets à la date de rédaction de la présente documentation.

Concepts fondamentaux de SLP

Le protocole SLP spécifie trois composants :

- L'agent Utilisateur (UA)
- L'agent de service (SA)
- L'agent Annuaire (DA)

La fonction de l'agent Utilisateur est de fournir une interface par programmation aux clients pour leurs requêtes de services, et aux services pour leur permettre de publier leurs annonces. Un agent Utilisateur contacte un agent Annuaire pour interroger des services enregistrés d'une classe de service et d'une étendue spécifiées.

La fonction de l'agent Service consiste à fournir des points de stockage et de maintenance persistants pour des services locaux s'étant enregistrés auprès de SLP. L'agent de service a pour tâche principale de gérer une base de données en mémoire des services locaux enregistrés. En fait, un service ne peut pas s'enregistrer auprès de SLP tant qu'un agent de service local n'est pas présent. Les clients peuvent identifier les services au moyen d'une seule bibliothèque d'agent

Utilisateur, mais l'enregistrement nécessite obligatoirement un agent de service (SA), principalement parce que cet agent doit régulièrement vérifier l'existence de services enregistrés pour maintenir l'enregistrement des agents Annuaire à l'écoute.

Le fonction de l'agent Annuaire consiste à fournir un cache persistant à long terme pour les services annoncés, ainsi qu'un point d'accès permettant aux agents Utilisateur de rechercher des services. En tant que cache, l'agent Annuaire reste à l'écoute de l'annonce de nouveaux services par les agents de service et met en cache ces notifications. À court terme, le cache d'un agent Annuaire se complète. Les agents Annuaire utilisent un algorithme d'expiration pour faire expirer les entrées de cache. Lorsqu'un agent Annuaire s'active, il lit le cache du stockage persistant (en général un disque dur), puis commence à faire expirer les entrées selon l'algorithme. Lorsqu'un nouvel agent Annuaire arrive ou lorsqu'un cache a été supprimé, l'agent Annuaire détecte cette condition et envoie une notification spéciale à tous les agents Service à l'écoute pour qu'ils vident leurs bases de données locales, de manière à ce que l'agent Annuaire puisse rapidement créer son cache.

En l'absence d'agents Annuaire, l'agent Utilisateur effectue une requête de multidiffusion générale à laquelle les agents de service peuvent répondre listant ainsi les services demandés de la même manière que les agents Annuaire créent leur cache. La liste des services renvoyée par une telle requête est incomplète et bien plus localisée que celle fournie par un agent Annuaire, notamment en présence d'un filtrage multidiffusion mis en œuvre par un grand nombre d'administrateurs réseaux, lesquels limitent les diffusions et les multidiffusions au sous-réseau local seulement.

En bref, tout s'articule autour de l'agent Annuaire trouvé par un agent Utilisateur dans une étendue donnée.

Protocole SLP NetIQ

La version NetIQ de SLP prend certaines libertés vis-à-vis de la norme SLP afin de fournir un environnement d'annonce de service renforcé, mais au prix d'une certaine évolutivité.

Par exemple, pour améliorer l'évolutivité d'une structure d'annonce de service, nous cherchons à limiter le nombre de paquets diffusés ou multidiffusés sur un sous-réseau. La norme SLP gère ce facteur en imposant des limitations aux agents de service et Utilisateur concernant les requêtes à l'agent Annuaire. Le premier agent Annuaire identifié qui dessert l'étendue souhaitée est celui qu'un agent de service (et par conséquent des agents Utilisateur locaux) utilisera pour toutes les requêtes futures sur cette étendue.

La mise en œuvre de NetIQ SLP permet d'analyser tous les agents Annuaire connus, à la recherche des informations de la requête. Un acheminement AR de 300 millisecondes étant considéré comme trop long, 10 serveurs peuvent être analysés en 3 à 5 secondes. Il n'est pas nécessaire d'effectuer cette opération si SLP est configuré correctement sur le réseau et que OpenSLP considère le réseau comme configuré correctement pour le trafic SLP. Les valeurs de timeout de réponse de OpenSLP sont supérieures à celles du fournisseur de services SLP de NetIQ et cela limite le nombre d'agents Annuaire au premier qui répond, que les informations de celui-ci soient ou non précises et complètes.

Agents Utilisateur

Un agent utilisateur prend la forme physique d'une bibliothèque statique ou dynamique liée à une application. Il permet à l'application d'émettre des requêtes de services SLP.

Les agents Utilisateur suivent un algorithme pour obtenir l'adresse d'un agent Annuaire auquel les requêtes seront envoyées. Une fois qu'ils ont obtenu une adresse d'agent Annuaire sur une étendue spécifiée, ils continuent à utiliser cette adresse pour cette étendue jusqu'à ce qu'elle ne réponde plus. Là, ils se procurent une autre adresse pour l'étendue. Les agents Utilisateur localisent l'adresse d'un agent Annuaire sur une étendue spécifiée en :

1. vérifiant si l'identificateur de socket de la requête en cours est connecté à un agent Annuaire pour l'étendue indiquée ; S'il se trouve que la requête fait partie d'une requête en plusieurs parties, elle peut déjà contenir une connexion en cache.
2. recherchant dans le cache de l'agent Annuaire connu un agent Annuaire correspondant à l'étendue indiquée ;
3. recherchant auprès de l'agent de service local un agent Annuaire de l'étendue spécifiée et en ajoutant de nouvelles adresses au cache ;
4. interrogeant DHCP pour obtenir des adresses d'agents Annuaire configurées pour le réseau et correspondant à l'étendue indiquée, et en ajoutant de nouvelles adresses au cache ;
5. envoyant une requête de découverte d'agent Annuaire par multidiffusion sur un port connu et en ajoutant de nouvelles adresses au cache.

Sauf spécification contraire, l'étendue indiquée est celle « par défaut ». Cela signifie que si aucune étendue n'est définie de façon statique dans le fichier de configuration SLP et qu'aucune étendue n'est indiquée dans la requête, l'étendue utilisée est le mot « default ». Notez également que eDirectory n'indique jamais d'étendue dans ses enregistrements. Cela ne signifie pas pour autant que l'étendue utilisée avec eDirectory soit toujours « default ». En fait, s'il existe une étendue configurée statiquement, celle-ci devient l'étendue par défaut pour les requêtes à l'agent Utilisateur local et les enregistrements de l'agent Service en l'absence d'une étendue spécifiée.

Agents Service

Les agents de service prennent la forme physique d'un processus distinct exécuté sur l'ordinateur hôte. Dans le cas de Windows, `slpd.exe` s'exécute en tant que service sur l'ordinateur local. Des agents utilisateur interrogent l'agent de service local en envoyant des messages à l'adresse de bouclage sur un port connu.

Un agent de service localise et met en cache les agents Annuaire et la liste de l'étendue qu'ils prennent en charge en envoyant directement une requête d'identification d'agent Annuaire à des adresses d'agent Annuaire potentielles en :

1. vérifiant toutes les adresses d'agent Annuaire configurées statiquement (et en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
2. demandant la liste des agents Annuaire et des étendues à DHCP (et en en ajoutant de nouveaux au cache d'agent Annuaire connu de l'agent de service) ;
3. envoyant une requête d'identification d'agent Annuaire par multidiffusion sur un port connu (et en en ajoutant de nouvelles au cache d'agent Annuaire connu de l'agent de service) ;
4. recevant les paquets d'annonce régulièrement diffusés par les agents Annuaire (et en ajoutant les nouveaux au cache d'agent Annuaire connu de l'agent de service).

Puisqu'un agent utilisateur interroge toujours l'agent de service local en premier, cela est important, car la réponse de l'agent de service local détermine si l'agent utilisateur passe ou non à l'étape suivante de la découverte (dans ce cas, DHCP-- voir étapes 3 et 4 de la section « Agents Utilisateur » page 867).

Paramètres de configuration

Les paramètres de configuration SLP sont stockés dans le fichier `slp.conf`, qui se trouve dans le dossier `/etc` sur les plates-formes UNIX et Linux, et dans `%systemroot%/slp.conf` sur les plates-formes Windows. Ces paramètres peuvent être modifiés pour régler les opérations sur le réseau. Par exemple, les paramètres suivants contrôlent la découverte d'agents Annuaire :

```
net.slp.useScopes = <comma-delimited scope list>
net.slp.DAAddresses = <comma-delimited address list>
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

L'option useScopes indique à quelles étendues l'agent Service va s'annoncer et à quelles étendues les requêtes seront adressées en l'absence d'une étendue spécifique lors de l'enregistrement ou de la requête effectuée par le service ou l'application client. Comme eDirectory envoie toujours ses annonces et requêtes à partir de l'étendue par défaut, cette liste sera considérée comme la liste d'étendues par défaut pour l'ensemble des enregistrements et des requêtes eDirectory.

L'option DAAddresses est une liste d'adresses IP décimales avec points, séparées par une virgule, qui doivent être préférées à toutes les autres. Si cette liste des agents Annuaire configurés ne prend pas en charge l'étendue d'un enregistrement ou d'une requête, les agents de service et Utilisateur font alors appel à l'identification d'agent Annuaire multidiffusion, sauf si cette fonction a été désactivée.

L'option passiveDADetection a par défaut la valeur Vrai. Les agents Annuaire annoncent régulièrement leur existence sur le sous-réseau au moyen d'un port connu si celui-ci est configuré à cet effet. Ils s'intitulent paquets DAAdvert. Si cette option a pour valeur Faux, tous les paquets DAAdvert diffusés sont ignorés par l'agent de service.

L'option activeDADetection a également par défaut la valeur Vrai. Elle permet à l'agent de service de diffuser régulièrement une requête à tous les agents Annuaire pour qu'ils répondent au moyen d'un paquet DAAdvert dirigé. Un paquet dirigé n'est pas diffusé, mais envoyé directement à l'agent de service en réponse à ces requêtes. Si cette option a pour valeur False (faux), aucune requête régulière de découverte d'agents Annuaire n'est diffusée par l'agent de service.

L'option DAActiveDiscoveryInterval est un paramètre de vérification d'état. La valeur par défaut est 1. Cela signifie que l'agent de service doit seulement envoyer une requête de découverte d'agent Annuaire à l'initialisation. Si vous attribuez la valeur 0 à cette option, cela revient à attribuer la valeur « false » à l'option activeDADetection. Toute autre valeur indique un nombre de secondes entre les diffusions d'identification.

Employées correctement, ces options assurent une utilisation appropriée de la bande passante du réseau pour l'annonce de services. En fait, les paramètres par défaut sont conçus pour optimiser l'évolutivité d'un réseau moyen.

REMARQUE : par défaut, le protocole IPV4 est activé pour SLP et IPV6 est désactivé. Pour activer IPV6, supprimez les marques de commentaire de la ligne suivante dans le fichier `slp.conf` :

```
net.slp.useIPv6 = true
```

Cette remarque n'est valable que pour Windows, car OpenSLP 2.0 est fourni uniquement pour ce système d'exploitation.

Utilitaire slptool

Il s'agit d'un utilitaire de ligne de commande fourni par OpenSLP. Vous pouvez utiliser slptool pour enregistrer les services ou annuler leur enregistrement, ainsi que pour interroger les étendues, les types de service, les attributs et les services disponibles.

Par exemple :

- Pour enregistrer les services

  Syntaxe : `slptool register URL [attrs]`

  ```
  slptool register service:myserv.x://myhost.com "(attr1=val1),(attr2=val2)"
  ```

- Pour annuler l'enregistrement d'un service

  Syntaxe : `slptool deregister URL`

  ```
  slptool deregister service:myserv.x://myhost.com
  ```

- Pour rechercher les services disponibles

  Syntaxe : `slptool findsrvs type_service [filtre]`

  ```
  slptool findsrvs service:myserv.x
  slptool findsrvs service:myserv.x "(attr1=val1)"
  ```

- Pour rechercher les étendues configurées

  Syntaxe : `slptool findscopes`

D Fonctionnement de NetIQ eDirectory avec DNS

Si un client demande à un serveur de résoudre un nom complet (par exemple, admin.novell.novell_inc) qui n'existe pas dans l'arborescence NetIQ eDirectory, ou si vous utilisez une application autonome telle que NetIQ iManager pour Linux ou l'application d'installation d'eDirectory pour résoudre un nom dans l'arborescence et que vous n'avez encore aucun serveur à contacter, eDirectory utilise des protocoles de découverte de services pour la résolution. Ces protocoles correspondent à une classe d'applications réseau qui permettent à des composants distribués de rechercher et d'utiliser les services appropriés sur un réseau.

eDirectory utilisait jusqu'à présent SAP et SLP pour rechercher et annoncer les services réseau. DNS a été intégré à eDirectory 8.7.1 en tant que protocole de découverte. Grâce à cette nouvelle fonctionnalité, si vous demandez un nom d'arborescence qu'eDirectory ne comprend pas (parce que vous communiquez avec un serveur qui ne détient pas de copie de l'arborescence ou que vous utilisez une application autonome), la machine qui tente la découverte (qu'il s'agisse d'une machine exécutant une application autonome, d'une application JClient telle que NetIQ iManager ou d'un serveur) utilise les protocoles de découverte d'eDirectory dans l'ordre suivant :

1. Nom d'hôte du Système de nom de domaine (DNS)
2. SLP (Service Location Protocol)
3. Protocole SAP (Service Advertising Protocol - Annonce du service)

Lorsque vous utilisez le protocole DNS, eDirectory utilise le nom tel qu'il a été transmis (par exemple, un nom de serveur comme prod_server4.provo.novell.novell-_inc) et tente de résoudre le nom complet tel qu'il est. Ensuite, eDirectory ajoute chaque nom dans la liste de recherche DNS de la machine de découverte et demande au serveur DNS de la machine s'il dispose d'une adresse pour ce nom. Par exemple, si la liste de recherche DNS contient dev.novell.com et test.novell.com, eDirectory recherche prod_server4.provo.novell.novell_inc.dev.novell.com et prod_server4.provo.novell.novell_inc.test.novell.com.

eDirectory considère ensuite les composants du nom qui lui a été transmis. Par exemple, lors de la résolution de prod_server4.provo.novell.novell_inc, eDirectory essaie d'abord provo.novell.novell_inc, puis novell.novell_inc, puis novell_inc. Il procède ainsi pour chacun des contextes de recherche et essaie pour finir le composant unique qui constitue la racine de l'arborescence. Le client essaie chacune des adresses jusqu'à ce qu'il parvienne à établir une connexion. Il effectue les tentatives en suivant l'ordre des enregistrements renvoyés par le serveur DNS. La révision de code exécutée par les serveurs de l'anneau de répliques importe peu, l'essentiel étant que la version eDirectory 8.7.1 (ou une version ultérieure) soit installée sur la machine qui tente d'effectuer l'identification.

Nous vous recommandons de placer le nom de votre arborescence eDirectory dans DNS au moyen d'un enregistrement de ressource de type A, AAAA ou service (SRV) sous le domaine DNS que les clients vont utiliser pour résoudre les noms. Dans le cas d'enregistrements A ou AAAA, les serveurs eDirectory doivent utiliser le port par défaut 524. S'ils utilisent un autre port, vous devez recourir à un enregistrement SRV.

Dans les exemples d'enregistrements de ressources ci-dessous, novell_inc est le nom de l'arborescence et provo.novell.com le contexte de recherche DNS :

Enregistrer	Exemple
A	novell_inc.provo.novell.com. EN A 192.168.1.2
AAAA	novell_inc.provo.novell.com. EN AAAA 4321:0:1:2:3:4:567:89ab
SRV	_ldap._tcp.novell_inc.provo.novell.com. SRV 0 0 389 server1.novell_inc.provo.novell.com SRV 10 0 389 server2.novell_inc.provo.novell.com

Pour assurer la redondance ou pour spécifier plusieurs hôtes (serveurs de l'anneau de répliques) pour l'enregistrement A, créez plusieurs enregistrements de ce type. eDirectory les examinera tous. Pour plus d'informations sur les enregistrements A, AAAA et SRV, consultez la page Web « DNS Resource Records » (Enregistrements de ressources DNS).

L'entrée de l'enregistrement du serveur DNS ne doit pas nécessairement pointer sur un élément qui comporte une racine de partition correspondante. Dès que la machine d'identification parvient à contacter un serveur qui connaît l'arborescence, elle peut parcourir cette dernière pour résoudre le nom. Par exemple, si vous placez novell_inc sur votre DNS, vous n'avez pas à inclure les serveurs contenant la racine novell_inc. Il vous suffit de pointer sur n'importe quel serveur de l'arborescence novell_inc car, après avoir accédé à ce dernier dans l'arborescence, celui-ci vous fera connaître dans l'ensemble de l'arborescence.

E Configuration de GSSAPI avec eDirectory

Le mécanisme SASL-GSSAPI pour NetIQ eDirectory permet de s'authentifier auprès d'eDirectory via LDAP à l'aide d'un ticket Kerberos. Il n'est pas nécessaire de saisir le mot de passe utilisateur eDirectory. Le ticket Kerberos peut être obtenu en s'authentifiant auprès d'un serveur Kerberos.

Cette fonctionnalité est surtout utile aux utilisateurs d'applications LDAP dans des environnements disposant d'une infrastructure Kerberos existante. Ces utilisateurs peuvent ainsi s'authentifier auprès du serveur LDAP sans devoir fournir un mot de passe utilisateur LDAP distinct.

La mise en oeuvre actuelle de SASL-GSSAPI est compatible avec la convention RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) et ne prend en charge que le mécanisme d'authentification Kerberos v5.

Les sections suivantes expliquent comment configurer GSSAPI, décrivent les différentes tâches pouvant être effectuées avec Kerberos dans eDirectory et fournissent d'autres informations utiles :

- « Concepts » page 873
- « Fonctionnement de GSSAPI avec eDirectory » page 874
- « Conditions préalables à la configuration de GSSAPI » page 875
- « Configuration de la méthode SASL-GSSAPI » page 879
- « Gestion de la méthode SASL-GSSAPI » page 879
- « Création d'une séquence de connexion » page 887
- « Utilisation de SASL-GSSAPI par LDAP » page 887
- « Messages d'erreur » page 887
- « Terminologie courante » page 887

Concepts

- « Définition de Kerberos » page 873
- « Définition de SASL » page 874
- « Définition de GSSAPI » page 874

Définition de Kerberos

Kerberos est un protocole standard qui permet d'authentifier des entités sur un réseau. Basé sur un modèle tiers approuvé, il inclut des secrets partagés et utilise la cryptographie à clé symétrique.

Pour plus d'informations, reportez-vous au fichier RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

Définition de SASL

SASL (Simple Authentication and Security Layer) offre aux applications une couche d'abstraction d'authentification. Il s'agit d'un cadre auquel les modules d'authentification peuvent être connectés.

Pour plus d'informations, reportez-vous au fichier RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

Définition de GSSAPI

L'interface GSSAPI (Generic Security Services Application Program Interface) propose des services d'authentification et autres services de sécurité via un ensemble standard d'API. Elle prend en charge différents mécanismes d'authentification, le plus courant étant Kerberos v5.

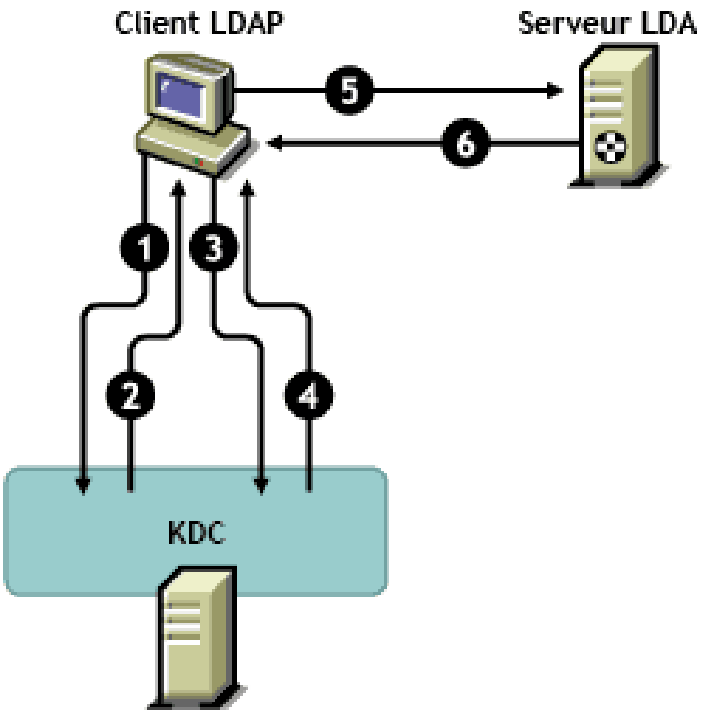
Pour plus d'informations sur les API GSS, reportez-vous au fichier RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964).

Cette mise en oeuvre de SASL-GSSAPI commence à la section 7.2 du fichier RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

Fonctionnement de GSSAPI avec eDirectory

Le schéma ci-dessous illustre le fonctionnement de GSSAPI avec un serveur LDAP.

Figure E-1 *Fonctionnement de GSSAPI*



Sur la figure ci-dessus, les numéros correspondent aux éléments suivants :

1. Un utilisateur eDirectory envoie une requête via un client LDAP au serveur KDC (Key Distribution Center) Kerberos concernant un ticket initial appelé TGT (Ticket Granting Ticket).

Un KDC Kerberos peut être de type MIT ou Microsoft*.

2 En réponse, le KDC envoie un TGT au client LDAP.

3 Le client LDAP renvoie le TGT au KDC et demande un ticket de service LDAP.

4 En réponse, le KDC envoie le ticket de service LDAP au client LDAP.

5 Le client LDAP établit une liaison ldap_sasl_bind avec le serveur LDAP et envoie le ticket de service LDAP.

6 Le serveur LDAP valide le ticket de service LDAP à l'aide du mécanisme GSSAPI et, en fonction du résultat, renvoie la liaison ldap_sasl_bind réussie ou échouée au client LDAP.

Conditions préalables à la configuration de GSSAPI

La configuration de GSSAPI implique d'effectuer préalablement les opérations suivantes :

- **Méthode SASL-GSSAPI :** installez la méthode SASL-GSSAPI. Reportez-vous à la section Installing a Login Method (Installation d'une méthode de connexion) du *NetIQ Modular Authentication Services 3.3 Administration Guide* (https://www.netiq.com/documentation/edir88/nmas88/data/bookinfo.html) (Guide d'administration de NetIQ Modular Authentication Services 3.3).

  REMARQUE : la méthode SASL-GSSAPI d'eDirectory ne fonctionne pas sur les installations d'Open Enterprise Server (OES) version 2 ou 11 dotées des services de domaine pour Windows.

  Pour vérifier que SASL-GSSAPI est installé sur votre machine, entrez la commande suivante :

  ```
  ldapsearch -x -h osg-dt-srv9 -b " " -s base | grep -i sasl
  ```

  Si SASL-GSSAPI est installé, la commande donne un résultat similaire à celui-ci :

  ```
  supportedSASLMechanisms: NMAS_LOGIN
  ```

  ```
  supportedSASLMechanisms: GSSAPI
  ```

- **Plug-in Kerberos pour iManager :** installez le plug-in Kerberos pour iManager. Reportez-vous à la section « Installation du plug-in Kerberos pour iManager. » page 876 pour plus d'informations.

- **KDC (Key Distribution Center) :** installez le centre de distribution de clés KDC Kerberos (MIT, Active Directory) sur le réseau.

  Les outils Kerberos doivent être installés pour le KDC Microsoft (Active Directory). Ces outils font partie de l'installation de Windows et peuvent être installés à partir des fichiers `\support\tools\setup.exe` (Windows XP) et `\support\tools\suptools.msi` (Windows 2003) disponibles sur le CD d'installation Windows.

- **Synchronisation horaire:** pour que cette méthode fonctionne, synchronisez l'heure du poste client NMAS, du serveur NMAS et de la machine KDC. Pour plus d'informations sur la synchronisation de l'heure réseau, reportez-vous à la « Synchronisation des heures réseau » page 100.

- **Extensions LDAP Kerberos :** ajoutez les extensions LDAP Kerberos. Pour plus d'informations, reportez-vous à la « Ajout d'extensions LDAP Kerberos » page 877.

IMPORTANT

- Sous Open Enterprise Server, n'ajoutez pas les extensions LDAP Kerberos sur les serveurs sur lesquels les services de domaine pour Windows ou les services DNS sont configurés.
- toutes les informations Kerberos collectées auprès de votre système d'administration Kerberos tiennent compte de la casse et doivent la respecter.

Hypothèses concernant les caractéristiques réseau

Le mécanisme SASL-GSSAPI se base sur les hypothèses suivantes :

- La synchronisation horaire de toutes les machines du réseau présente une souplesse relative, ce qui signifie que les heures des différentes machines diffèrent tout au plus de plus de cinq minutes.
- Le mécanisme SASL-GSSAPI est censé être utilisé principalement dans un environnement LAN vu la difficulté à respecter l'exigence de synchronisation horaire, mentionnée ci-dessus, dans des environnements MAN et/ou WAN. Ce mécanisme ne se limite toutefois pas au LAN.
- Vous faites entièrement et systématiquement confiance aux serveurs et administrateurs Kerberos.
- Une attaque de refus de service n'est pas contrée. Pour plus d'informations, reportez-vous au fichier RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

Installation du plug-in Kerberos pour iManager.

1. Ouvrez le navigateur.
2. Saisissez l'URL suivante dans le champ Adresse de la fenêtre du navigateur :

   `http://hostname/nps/`

   où *`nom_hôte`* est le nom ou l'adresse IP du serveur iManager sur lequel installer le plug-in iManager pour SASL-GSSAPI.

   REMARQUE : en cas de problèmes, vérifiez que les serveurs Web et Tomcat sont configurés correctement. Pour plus d'informations, reportez-vous au *Guide d'administration de NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html).

3. Indiquez le nom d'utilisateur et le mot de passe pour vous connecter à eDirectory, puis cliquez sur **Connexion**.
4. Cliquez sur le bouton **Configurer** dans la barre d'outils iManager.
5. Dans le volet de gauche, cliquez sur **Installation de plug-ins** > **Modules de plug-in NetIQ disponibles**.
6. Cliquez sur **Ajouter**.
7. Indiquez l'emplacement du fichier `kerberosPlugin.npm` ou cliquez sur **Parcourir** pour le sélectionner.

   Le plug-in Administration Kerberos fait partie du NPM unique d'eDirectory 88 (`eDir_88_iMan27_Plugins.npm`) et peut être téléchargé à partir du site de téléchargement Novell (https://download.novell.com/Download?buildid=G_8Eymx0QtI~).

   Si vous avez déplacé le fichier `kerberosPlugin.npm`, accédez à son nouvel emplacement et sélectionnez le fichier.

8 Cliquez sur **Ouvrir**, puis sur **OK**.

9 Cliquez sur **Installer**.

Cette installation prendra quelques minutes.

10 Redémarrez le serveur iManager après avoir reçu un message indiquant la réussite de l'enregistrement du module.

Si vous exécutez iManager en mode d'accès illimité (aucune collection RBS dans l'arborescence), ignorez la procédure de l'Étape 11 à l'Étape 17.

REMARQUE : pour plus d'informations sur le redémarrage du serveur iManager, consultez le *Guide d'administration de NetIQ iManager*.

---

11 Connectez-vous à iManager, puis cliquez sur le bouton **Configurer** .

12 Dans le volet de gauche, cliquez sur **Services basés sur le rôle** > **Configuration RBS**.

13 (Conditionnel) Si vous n'avez pas de collection RBS, procédez comme suit :

13a Cliquez sur **Nouveau** > **Collection**.

13b Spécifiez le nom que vous souhaitez utiliser pour la collection.

13c Sélectionnez le conteneur dans lequel vous souhaitez créer les services basés sur le rôle, puis cliquez sur **OK**.

13d Cliquez à nouveau sur **OK**.

14 Sous l'onglet **Collections iManager 2.x**, cliquez sur le chiffre dans la colonne **Modules** de la collection que vous souhaitez utiliser.

15 Sélectionnez **Module Kerberos**, puis cliquez sur **Installer**.

16 Cliquez sur **OK** pour continuer.

17 Lorsqu'iManager termine l'installation du module, cliquez sur **OK**.

18 Dans la barre d'outils d'iManager, cliquez sur **Rôles et tâches**.

Le rôle Kerberos Management s'affiche dans le volet gauche.

Si le rôle Administration Kerberos ne s'affiche pas, redémarrez le serveur iManager.

Ajout d'extensions LDAP Kerberos

Les extensions LDAP Kerberos permettent de gérer les clés Kerberos.

L'utilisation des extensions LDAP Kerberos nécessite l'installation de LDAP Libraries for C. Pour plus d'informations, consultez la documentation LDAP Libraries for C (http://www.novell.com/developer/ndk/ldap_libraries_for_c.html).

Pour ajouter ou supprimer les extensions LDAP Kerberos, employez l'utilitaire krbLdapConfig. Lorsque le paquetage eDirectory autonome est extrait dans un répertoire, le chemin d'accès de ce fichier est `dossier_extraction/nmas/NmasMethods/Novell/GSSAPI/extensions_LDAP_Kerberos/Linux/krbLdapConfig`.

Par exemple : `/misc/eDir88/Linux/nmas/NmasMethods/Novell/GSSAPI/extensions_LDAP_Kerberos/Linux/krbLdapConfig`.

Pour ajouter les extensions LDAP Kerberos, utilisez la syntaxe suivante :

```
krbldapconfig {-i | -u} -D bind_DN [-w bind_DN_password] [-h ldap_host] [-p
ldap_port] [-e trusted_root_cert]
```

Le tableau suivant décrit les paramètres de l'utilitaire krbldapconfig :

Paramètre	Description
`-i`	Ajoute les extensions LDAP Kerberos à eDirectory.
`-u`	Supprime les extensions LDAP Kerberos d'eDirectory.
`-D` *`FDN_liaison`*	Indique le FDN de l'administrateur ou de l'utilisateur disposant de droits équivalents. Il doit avoir le format `cn=admin,o=org`.
`-w` *`mot_de_passe_FDN_liaison`*	Indique le mot de passe du FDN de liaison (`FDN_liaison`).
`-h` *`serveur_LDAP`*	Indique le nom d'hôte ou l'adresse IP du serveur LDAP où doivent être installées les extensions LDAP Kerberos.
`-p` *`port`*	Indique le port sur lequel est exécuté le serveur LDAP.
`-e` *`fichier_racine_approuvée`*	Indique le nom du fichier de certificat de racine approuvée pour la liaison SSL. Si vous utilisez un port SSL, spécifiez l'option `-e`. Pour plus d'informations, reportez-vous à la « Exportation du certificat de racine approuvée » page 878.

REMARQUE : si l'option `-h` n'est pas spécifiée, le nom de l'hôte local à partir duquel le fichier krbldapconfig est appelé est utilisé par défaut.

Si aucun port de serveur LDAP ni certificat de racine approuvée ne sont spécifiés, le port 389 est utilisé par défaut.

Si aucun port de serveur LDAP n'est spécifié, mais qu'un certificat de racine approuvée est indiqué, le port 636 est utilisé par défaut.

Par exemple, entrez la commande suivante pour ajouter les extensions :

```
krbldapconfig -i -D cn=admin,o=org -w password -h ldapserver -p 389
```

Entrez la commande suivante pour supprimer des extensions :

```
krbldapconfig -u -D cn=admin,o=org -w password -h ldapserver -p 389
```

IMPORTANT : le serveur LDAP doit être actualisé manuellement pour que les modifications apportées à l'installation soient prises en compte. Pour plus d'informations, reportez-vous à la « Rafraîchissement du serveur LDAP » page 410.

Exportation du certificat de racine approuvée

1. Dans iManager, cliquez sur **Administration de l'annuaire** > **Modifier un objet** pour ouvrir la page correspondante.
2. Utilisez le sélecteur d'objet pour sélectionner l'objet Certificat de serveur.
3. Cliquez sur **OK**.

4 Cliquez sur l'onglet **Certificats**, puis sélectionnez **Certificat de racine approuvée** pour afficher les informations relatives au certificat.

5 Cliquez sur **Exporter**.

6 Cliquez sur le menu déroulant **Certificats** et sélectionnez le certificat à exporter.

7 Spécifiez si vous souhaitez ou non exporter la clé privée. Si vous souhaitez exporter la clé privée, vous devrez peut-être spécifier un mot de passe pour protéger cette dernière.

8 Cliquez sur **Suivant**.

9 Cliquez sur **Save the exported certificate** (Enregistrer le certificat exporté).

10 Cliquez sur **Save File** (Enregistrer le fichier).

11 Cliquez sur **Fermer**.

Configuration de la méthode SASL-GSSAPI

1 Le plug-in iManager pour SASL-GSSAPI ne fonctionnera pas si iManager n'est pas configuré pour utiliser une connexion à eDirectory de type SSL/TLS. Une connexion sécurisée est obligatoire pour protéger la clé principale et les clés maîtresses du domaine.

   iManager est généralement configuré par défaut pour une connexion à eDirectory de type SSL/TLS. Vous devez toutefois lui ajouter les certificats de racine approuvée SSL du serveur LDAP que vous utilisez pour l'administration Kerberos.

   Pour plus d'informations sur la configuration d'iManager avec connexion SSL/TLS à eDirectory, reportez-vous au *Guide d'administration de NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/bookinfo.html).

2 Effectuez les procédures suivantes dans l'ordre indiqué :

   2a Étendez le schéma Kerberos.

   2b Créez un conteneur de domaine.

   2c Créez le principal de service LDAP.

   2d Extrayez une clé de principal de service ou une clé partagée du KDC.

   2e Créez un objet Principal de service dans eDirectory.

   2f Associez un nom de principal Kerberos à l'objet Utilisateur.

Fusion d'arborescences eDirectory configurées avec la méthode SASL-GSSAPI

Lorsque vous fusionnez deux arborescences, dont l'une ou les deux ont été configurées avec la méthode SASL-GSSAPI, vous devez créer manuellement tous les objets Kerberos de l'arborescence source dans l'arborescence cible.

Gestion de la méthode SASL-GSSAPI

iManager vous permet d'effectuer les opérations Kerberos suivantes :

- « Extension du schéma Kerberos » page 880
- « Gestion de l'objet Domaine Kerberos » page 880
- « Gestion d'un principal de service » page 882

- « Édition de principaux étrangers » page 886
- « Configuration de l'authentification SASL GSSAPI si le KDC Kerberos MIT utilise eDirectory comme interface dorsale » page 886

Extension du schéma Kerberos

Cette tâche permet d'étendre votre schéma eDirectory en ajoutant des définitions d'attributs et une classe d'objet Kerberos.

1. Si le schéma n'a pas déjà été étendu, cliquez sur **OK** pour l'étendre.
2. Dans iManager, cliquez sur **Administration Kerberos** > **Étendre le schéma** pour ouvrir la page correspondante.

   Si le schéma a été étendu, un message affiche son état.
3. Cliquez sur **Fermer**.

Gestion de l'objet Domaine Kerberos

Un domaine est un réseau logique desservi par un ensemble de centres de distribution de clés (KDC - Key Distribution Center). En d'autres termes, un domaine est un espace ou un groupement de principaux desservis par un ensemble de KDC. L'usage veut que les noms de domaine Kerberos soient en lettres majuscules pour les distinguer des domaines Internet. Pour plus d'informations, reportez-vous au fichier RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

Cette section fournit les informations suivantes :

- « Création d'un objet Domaine » page 880
- « Édition d'un objet Domaine » page 881
- « Suppression d'un objet Domaine » page 882

Création d'un objet Domaine

Le type de chiffrement par défaut pris en charge est DES-CBC-CRC.

1. Dans iManager, cliquez sur **Administration Kerberos** > **Nouveau domaine** pour ouvrir la page correspondante.
2. Indiquez un nom pour le domaine Kerberos à créer.

   Le nom de domaine doit être le même que celui avec lequel vous voulez configurer cette méthode de connexion, et il doit être conforme aux conventions RFC 1510.
3. Indiquez un mot de passe principal pour le domaine, puis confirmez-le.

   REMARQUE : veillez à utiliser un mot de passe principal complexe.
4. Spécifiez les sous-arborescences et la référence du conteneur principal avec lesquelles vous souhaitez configurer le domaine Kerberos, ou utilisez l'icône **Sélecteur d'objet** pour effectuer votre sélection.

   Il s'agit du FDN de la sous-arborescence ou du conteneur qui renferme les principaux de service eDirectory de ce domaine. Cette sous-arborescence n'est pas applicable aux principaux Utilisateur.

5 Indiquez l'étendue de la recherche dans la sous-arborescence :

- **Un niveau :** effectue la recherche dans les subordonnés immédiats de la sous-arborescence de domaine.
- **Sous-arborescence :** effectue la recherche dans l'ensemble de la sous-arborescence en commençant par la sous-arborescence du domaine.

6 Cliquez sur **OK**.

REMARQUE : la case **Services KDC** n'est pas utilisée dans SASL-GSSAPI.

REMARQUE : Si un domaine Kerberos pour l'authentification LDAP SASL GSSAPI doit être configuré dans l'arborescence par un administrateur de conteneurs eDirectory, l'administrateur de l'arborescence doit effectuer les opérations suivantes :

1. Veillez à ce que l'objet Conteneur de sécurité (cn=security) possède la classe d'objet krbContainerRefAux et à ce que l'attribut krbContainerReference soit défini sur le conteneur Kerberos.
2. Accordez à l'administrateur des conteneurs un droit d'accès en lecture sur l'attribut krbContainerReference.
3. Créez un conteneur de domaine dans le conteneur Kerberos. Le nom du conteneur doit être identique au nom du nouveau domaine en cours de création et la classe d'objet doit être krbRealmContainer.
4. Accordez à l'administrateur des conteneurs un droit Superviseur sur le conteneur de domaine.

Connectez-vous à iManager en tant qu'administrateur des conteneurs, sélectionnez **Administration Kerberos** > **Définir la clé maîtresse** pour ouvrir la page correspondante. Sélectionnez le **domaine KDC MIT** et spécifiez un mot de passe principal.

Édition d'un objet Domaine

1 Dans iManager, cliquez sur **Administration Kerberos** > **Éditer le domaine** pour ouvrir la page correspondante.

2 Indiquez un nom pour le domaine Kerberos à éditer ou utilisez l'icône **Sélecteur d'objet** pour le sélectionner.

3 Cliquez sur **OK**.

4 Spécifiez la sous-arborescence à utiliser pour configurer le domaine Kerberos ou utilisez l'icône **Sélecteur d'objet** pour la sélectionner.

Il s'agit du FDN de la sous-arborescence ou du conteneur qui renferme les principaux de service eDirectory de ce domaine. Cette sous-arborescence n'est pas applicable aux principaux Utilisateur.

5 Indiquez l'étendue de la recherche de la sous-arborescence.

- **Un niveau :** effectue la recherche dans les subordonnés immédiats de la sous-arborescence de domaine.
- **Sous-arborescence :** effectue la recherche dans l'ensemble de la sous-arborescence en commençant par la sous-arborescence du domaine.

6 Cliquez sur **OK**.

7 (Facultatif) Pour éditer un autre domaine, cliquez sur **Répéter la tâche**.

REMARQUE : la case **Services KDC** n'est pas utilisée dans SASL-GSSAPI.

Suppression d'un objet Domaine

1. Dans iManager, cliquez sur **Administration Kerberos** > **Supprimer le domaine** pour ouvrir la page correspondante.
2. Sélectionnez les domaines à supprimer.

   Pour en sélectionner plusieurs, appuyez sur la touche Maj et sélectionnez les domaines ou appuyez sur Maj et sur les touches fléchées.
3. Cliquez sur **OK**.
4. Cliquez de nouveau sur **OK** pour confirmer la suppression ou sur **Annuler** pour l'arrêter.

IMPORTANT : la suppression d'un objet Domaine efface également tous les objets Principal de service qu'il contient.

Gestion d'un principal de service

Cette section fournit les informations suivantes :

- « Création d'un principal de service pour un serveur LDAP » page 882
- « Extraction de la clé du principal de service pour eDirectory » page 883
- « Création d'un objet Principal de service dans eDirectory. » page 883
- « Affichage des clés de principal de service Kerberos » page 884
- « Suppression d'un objet Principal de service Kerberos » page 884
- « Définition d'un mot de passe pour le principal de service Kerberos » page 885

Création d'un principal de service pour un serveur LDAP

L'outil d'administration Kerberos disponible avec votre KDC permet de créer le principal de service eDirectory avec AES256-CTS comme type de chiffrement et Normal comme type de valeur aléatoire (salt).

Le nom du principal doit être ldap/*MONHÔTE.MONDOMAINEDNS@NOMDOMAINE*.

Par exemple, si vous utilisez un KDC MIT, exécutez la commande suivante :

```
kadmin:addprinc -randkey -e aes256-cts:normal ldap/server.novell.com@MITREALM
```

IMPORTANT : le nom d'hôte du principal de service créé doit être en minuscules. L'authentification échoue si le nom d'hôte est en majuscules. Par exemple, si le nom d'hôte est myHost.com, la syntaxe de nom d'hôte du principal de service LDAP doit ressembler à ce qui suit : `ldap/myhost.com@<nom_domaine>`.

Recommandation

- Toutes les clés doivent être de préférence de type AES256.
- Modifiez régulièrement les clés de principal de service LDAP. Lors de leur changement, veillez à mettre à jour l'objet Principal dans eDirectory.

Extraction de la clé du principal de service pour eDirectory

L'outil d'administration Kerberos disponible avec votre KDC permet d'extraire la clé du principal de service LDAP créé à la section « Création d'un principal de service pour un serveur LDAP » page 882, puis de la stocker dans le système de fichiers local. Votre administrateur Kerberos peut vous aider à effectuer cette opération.

Par exemple, si vous utilisez un KDC MIT, exécutez la commande suivante :

```
kadmin: ktadd -k /chemin_répertoire/nom_fichier_KeyTab -e aes256-cts:normal ldap/
server.novell.com@MITREALM
```

Par exemple, si vous utilisez un KDC Microsoft, créez un utilisateur ldapMONHÔTE dans Active Directory, puis exécutez la commande suivante :

```
ktpass -princ ldap/MONHÔTE.MONDOMAINEDNS@MONDOMAINE -mapuser ldapMONHÔTE -pass
mon_mot_de_passe -out MONHÔTE.keytab
```

Cette commande assigne le principal (ldap/MONHÔTE.MONDOMAINEDNS@MONDOMAINE) au compte utilisateur (ldapMONHÔTE), définit le mot de passe de principal hôte sur `mon_mot_de_passe` et extrait la clé dans le fichier `MONHÔTE.keytab`.

Création d'un objet Principal de service dans eDirectory.

Vous devez créer un principal de service Kerberos avec un nom identique (ldap/*MONHÔTE.MONDOMAINEDNS@MONDOMAINE*) à celui indiqué à la section « Création d'un principal de service pour un serveur LDAP » page 882.

Recommandation

Les principaux de service pour eDirectory doivent être aisément accessibles à tous les serveurs activés pour le mécanisme SASL-GSSAPI. S'ils ne sont pas créés sous le conteneur Domaine Kerberos dans le conteneur Sécurité, il est vivement recommandé de créer le conteneur qui les renferme en tant que partition distincte et de le répliquer largement.

1. Dans iManager, cliquez sur **Administration Kerberos** > **Nouveau principal** pour ouvrir la page correspondante.
2. Indiquez le nom du principal à créer.

   Le nom du principal doit avoir le format suivant : ldap/*MONDOMAINEDNS@NOMDOMAINE*.
3. Indiquez le nom du conteneur qui renfermera l'objet Principal créé ou utilisez l'icône **Sélecteur d'objet** pour le sélectionner.
4. Indiquez le nom du domaine.

   Si vous l'avez déjà spécifié à l'Étape 2, laissez ce champ vide.
5. Effectuez l'une des opérations suivantes :
   - Indiquez le nom du fichier KeyTab ou cliquez sur **Parcourir** pour sélectionner son emplacement de stockage.

     Il s'agit du fichier qui contient la clé extraite à la section « Extraction de la clé du principal de service pour eDirectory » page 883.

- Spécifiez le mot de passe, confirmez-le, puis sélectionnez le type de chiffrement et le type de valeur aléatoire (salt).

  Le mot de passe et la combinaison type de chiffrement/type de valeur aléatoire doivent être identiques à ceux spécifiés lors de la création du principal de service dans la base de données KDC.

6 Cliquez sur **OK**.

Affichage des clés de principal de service Kerberos

1 Dans iManager, cliquez sur **Administration Kerberos** > **Afficher les informations sur la clé** pour ouvrir la page correspondante.

2 Indiquez le nom de la clé de principal à afficher ou utilisez l'icône **Sélecteur d'objet** pour la sélectionner.

  Les informations suivantes sur les clés de principal s'affichent :

  - Principal name (Nom du principal)
  - Informations sur la clé
    - Number (Numéro) : numéro de série de la clé dans la table
    - Version : version de la clé
    - Key Type (Type de clé) : type de la clé de principal
    - Salt Type (Type de valeur aléatoire) : type de valeur aléatoire de la clé de principal

3 Cliquez sur **OK**.

Suppression d'un objet Principal de service Kerberos

Vous pouvez supprimer un ou plusieurs objets, ou encore, effectuer une sélection avancée des objets Principal à effacer.

Pour supprimer un seul objet Principal :

1 Dans iManager, cliquez sur **Administration Kerberos** > **Supprimer le principal** pour ouvrir la page correspondante.

2 Cliquez sur **Sélectionner un seul objet**.

3 Indiquez le nom de l'objet Principal à supprimer ou utilisez l'icône **Sélecteur d'objet** pour le sélectionner.

4 Cliquez sur **OK**.

5 Cliquez de nouveau sur **OK** pour confirmer la suppression ou sur **Annuler** pour l'arrêter.

Pour supprimer plusieurs objets Principal :

1 Dans iManager, cliquez sur **Administration Kerberos** > **Supprimer le principal** pour ouvrir la page correspondante.

2 Cliquez sur **Sélectionner plusieurs objets**.

3 Indiquez le nom des objets Principal à supprimer ou utilisez l'icône **Sélecteur d'objet** pour les sélectionner.

4 Sélectionnez les objets Principal à supprimer.

5 Cliquez sur **OK**.

6 Cliquez de nouveau sur **OK** pour confirmer la suppression ou sur **Annuler** pour l'arrêter.

Pour supprimer un principal en utilisant la sélection avancée :

1. Dans iManager, cliquez sur **Administration Kerberos** > **Supprimer le principal** pour ouvrir la page correspondante.
2. Cliquez sur **Sélection avancée**.
3. Sélectionnez la classe d'objet.
4. Indiquez le conteneur qui renferme l'objet Principal ou utilisez l'icône **Sélecteur d'objet** pour le sélectionner.
5. Cliquez sur **Inclure les sous-conteneurs** pour englober les sous-conteneurs du conteneur spécifié à l'Étape 3.
6. Cliquez sur pour ouvrir la fenêtre Critères de sélection avancés.
7. Sélectionnez le type d'attribut et l'opérateur dans la liste déroulante, puis fournissez les valeurs correspondantes.
8. Cliquez sur le bouton **Ajouter une ligne** pour inclure d'autres groupes logiques à la sélection.
9. Cliquez sur **OK** pour configurer le filtre.
10. Cliquez sur **Afficher l'aperçu** pour afficher un aperçu de la sélection avancée.
11. Cliquez sur **OK**.
12. Cliquez de nouveau sur **OK** pour confirmer la suppression ou sur **Annuler** pour l'arrêter.

Définition d'un mot de passe pour le principal de service Kerberos

Si la clé de principal de service eDirectory a été réinitialisée dans votre KDC, vous devez également la mettre à jour dans eDirectory.

Pour plus d'informations sur l'extraction de clé, reportez-vous à la section « Extraction de la clé du principal de service pour eDirectory » page 883.

1. Dans iManager, cliquez sur **Administration Kerberos** > **Définir le mot de passe du principal** pour ouvrir la page correspondante.
2. Indiquez le nom de l'objet Principal pour lequel définir un mot de passe individuel ou utilisez l'icône **Sélecteur d'objet** pour le sélectionner.
3. Indiquez le nom du fichier KeyTab ou cliquez sur **Parcourir** pour accéder à son emplacement de stockage.
4. Effectuez l'une des opérations suivantes :
   - Indiquez le nom du fichier KeyTab qui contient la clé de principal ou cliquez sur **Parcourir** pour sélectionner son emplacement de stockage.

     Pour plus d'informations sur la création de principaux de service et l'extraction de clés, reportez-vous aux sections « Création d'un principal de service pour un serveur LDAP » page 882 et « Extraction de la clé du principal de service pour eDirectory » page 883.
   - Spécifiez le mot de passe, confirmez-le, puis sélectionnez le type de chiffrement et le type de valeur aléatoire.
5. Cliquez sur **OK** pour configurer le mot de passe.
6. (Facultatif) Pour définir le mot de passe d'un autre principal, cliquez sur **Répéter la tâche**.

Édition de principaux étrangers

iManager permet d'ajouter des noms de principaux Kerberos aux utilisateurs d'eDirectory.

1 Dans iManager, cliquez sur **Administration Kerberos** > **Éditer des principaux étrangers** pour ouvrir la page correspondante.

2 Indiquez le FDN d'un objet Utilisateur valide ou utilisez l'icône **Sélecteur d'objet** pour sélectionner la référence à l'objet Utilisateur.

3 Cliquez sur **OK**.

4 Indiquez les noms de principaux étrangers, puis cliquez sur le bouton **Ajouter**.

   Le nom du principal doit avoir le format `nomprincipal@NOMDOMAINE`.

   Pour supprimer le nom de principal étranger, sélectionnez-le, puis cliquez sur le bouton **Supprimer**.

5 Cliquez sur **OK**.

REMARQUE : les noms de principaux Kerberos doivent être uniques dans l'arborescence. Si eDirectory est configuré en tant qu'interface dorsale LDAP pour un domaine KDC, les noms de principaux étrangers ne doivent pas être configurés dans eDirectory pour ce domaine. Au lieu de cela, vous pouvez associer un nom de principal Kerberos existant avec un DN d'utilisateur eDirectory à l'aide de la commande suivante :

```
kadmin.local -q 'modprinc -x linkdn=<DN_eDir> <principal>@<domaine>'
```

Vous pouvez également associer un nom de principal Kerberos à un DN d'utilisateur eDirectory au moment de la création du principal, à l'aide de l'une des commandes suivantes :

```
kadmin.local -q 'ank -x dn=<DN_eDir> <principal>@<domaine>'
kadmin.local -q 'ank -x linkdn=<DN_eDir> <principal>@<domaine>'
```

Configuration de l'authentification SASL GSSAPI si le KDC Kerberos MIT utilise eDirectory comme interface dorsale

Si un KDC Kerberos MIT utilise eDirectory comme interface dorsale, pour que les principaux de KDC MIT s'authentifient auprès d'eDirectory via SASL GSSAPI, effectuez la procédure suivante après avoir configuré le KDC MIT :

1 Dans iManager, modifiez l'objet Conteneur de sécurité (cn=security) :

   1a Ajoutez la classe d'objet krbContainerRefAux au conteneur de sécurité.

   1b Définissez l'attribut krbContainerReference afin qu'il pointe vers le conteneur Kerberos.

   Par exemple :

   `cn=Kerberos,cn=Security`

2 Dans iManager, sélectionnez **Administration Kerberos** > **Définir la clé maîtresse** pour ouvrir la page correspondante.

IMPORTANT : sélectionnez la clé principale utilisée par le KDC MIT.

---

3 Sélectionnez le domaine KDC MIT et spécifiez le mot de passe. Ce doit être le mot de passe que vous avez utilisé comme mot de passe principal lorsque vous avez créé le domaine KDC MIT à l'aide de kdb5_ldap_util.

REMARQUE : si le domaine Kerberos est créé par un utilisateur qui n'est pas l'administrateur de l'arborescence, ce dernier doit lui accorder le droit Créer une entrée pour le conteneur Kerberos.

Création d'une séquence de connexion

Pour plus d'informations sur la création d'une séquence de connexion, reportez-vous à la « Gestion des méthodes et des séquences de connexion et de post-connexion » page 679.

Utilisation de SASL-GSSAPI par LDAP

Après avoir configuré la méthode SASL-GSSAPI, elle est ajoutée avec d'autres méthodes SASL à l'attribut supportedSASLMechanisms dans rootDSE.

Le serveur LDAP interroge SASL pour connaître les mécanismes installés lors de sa configuration et prend automatiquement en charge les éléments installés. Le serveur LDAP signale également les mécanismes SASL pris en charge dans son entrée rootDSE à l'aide de l'attribut supportedSASLMechanisms.

Par conséquent, une fois configuré, GSSAPI devient le mécanisme par défaut.

Toutefois, pour effectuer spécifiquement une opération LDAP sur le mécanisme SASL-GSSAPI, vous pouvez mentionner GSSAPI dans la ligne de commande.

Par exemple, pour effectuer une recherche à l'aide du mécanisme GSSAPI dans OpenLDAP, entrez la commande suivante :

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

Messages d'erreur

Les messages d'erreur SASL-GSSAPI sont consignés aux emplacements suivants :

- Linux : `ndsd.log`

Pour plus d'informations, reportez-vous à la « Gestion de la consignation des erreurs dans eDirectory » page 984.

Terminologie courante

Le tableau suivant définit les termes couramment utilisés avec Kerberos et GSSAPI.

Tableau E-1 *Terminologie Kerberos/GSSAPI*

Terme	Définition
KDC (Key Distribution Center)	Serveur Kerberos qui authentifie des utilisateurs et délivre des tickets.
Principal	Entité (instance service ou utilisateur) enregistrée auprès du KDC.
Domaine	Domaine ou groupe de principaux desservis par un ensemble de KDC.

Terme	Définition
ST (Service Ticket)	Enregistrement contenant des informations sur le client et le service ainsi qu'une clé de session codée avec la clé partagée du principal d'un service spécifique
TGT (Ticket Granting Ticket)	Type de ticket permettant au client d'obtenir d'autres tickets Kerberos.

F Considérations relatives à la sécurité

Cette annexe comprend les rubriques suivantes :

- « Liaisons LDAP » page 889
- « Résultats de l'analyse Nessus » page 889

Liaisons LDAP

Les liaisons LDAP doivent s'effectuer via une connexion sécurisée. Il est recommandé de toujours utiliser une connexion SSL/TLS et de tenir compte des points suivants :

- La clé transmise sur le réseau peut être détectée. Par conséquent, sécurisez physiquement le réseau de l'entreprise contre l'écoute électronique ou le « reniflage de paquets ».
- Gardez les serveurs à un emplacement sécurisé physiquement, uniquement accessible par le personnel autorisé.
- Si le produit est employé par des utilisateurs en dehors du pare-feu de l'entreprise, utilisez un réseau privé virtuel (VPN – Virtual Private Network).
- Si un serveur est accessible à l'extérieur du réseau de l'entreprise, configurez un pare-feu de manière à empêcher l'accès direct au serveur.
- Vérifiez régulièrement les journaux d'audit.
- Attribuez les différentes responsabilités administratives à des personnes distinctes. La délégation de l'administration permet un contrôle granulaire des objets d'annuaire.
- Il est recommandé de désigner un serveur LDAP particulier pour la gestion Kerberos. Le nom de ce serveur peut être spécifié dans iManager.

IMPORTANT : l'utilisateur doit pouvoir accéder au serveur LDAP à l'aide du nom DNS au lieu de l'adresse IP du serveur, car la conversion de cette dernière en nom DNS n'est pas sécurisée.

Résultats de l'analyse Nessus

L'analyse Nessus des ports a signalé les problèmes suivants :

◆ Les serveurs LDAP qui ne sont pas configurés correctement autorisent les utilisateurs à se connecter au serveur et à demander des informations

Explication : la liaison NULL est activée par défaut sur le serveur LDAP eDirectory, mais elle peut être désactivée. Afin d'améliorer la sécurité du serveur, désactivez la liaison NULL sur le port 389 du serveur LDAP. Pour plus d'informations, reportez-vous à la « Configuration des objets LDAP » page 397.

Solution: désactivez la liaison NULL sur le serveur.

◆ Les serveurs LDAP qui ne sont pas configurés correctement définissent la base de l'annuaire comme nulle

Explication : des informations peuvent être obtenues même sans connaître au préalable la structure de l'annuaire. Par le biais de la liaison NULL, un utilisateur anonyme peut interroger le serveur LDAP à l'aide d'outils tels que « LdapMiner ».

Solution: bien qu'il n'existe aucun moyen pour éliminer ce type de menaces de sécurité, il est possible de les limiter en désactivant la liaison NULL.

◆ Le service à distance prend en charge l'utilisation de suites de chiffrement SSL faibles

Explication : l'hôte distant prend en charge des ciphers SSL qui assurent un chiffrement faible, voire nul.

Solution: si possible, reconfigurez l'application concernée, afin d'éviter l'utilisation de ciphers faibles.

◆ Le serveur d'annuaire à distance laisse passer des informations

Explication : cet hôte est un serveur NetIQ eDirectory et possède des droits Parcourir sur l'objet PUBLIC.

Solution: si les applications qui utilisent eDirectory n'ont pas besoin de disposer de droits PUBLIC, assignez les droits accordés à PUBLIC uniquement aux utilisateurs authentifiés (ROOT). S'il s'agit d'un système externe, il est recommandé de bloquer l'accès au port 524 à partir d'Internet. Toutefois, le nom de l'arborescence et du serveur reste accessible, même si vous supprimez les droits Parcourir publics.

◆ Le certificat SSL est signé par une autorité de certification inconnue

Explication : le certificat X.509 de l'hôte distant n'est pas signé par une autorité de certification publique connue. Si l'hôte à distance est un hôte public en production, cela annule l'utilisation de SSL étant donné que n'importe qui peut établir une connexion entre les deux et attaquer l'hôte distant.

Solution: cela se produit lorsque l'application cliente ne dispose pas du certificat de l'autorité de certification qui a signé le certificat du serveur dans son emplacement de stockage des certificats approuvés. Procurez-vous un certificat pour le serveur auprès d'une autorité de certification connue et déployez-le. Si le certificat du serveur a été émis par l'autorité de certification organisationnelle de l'arborescence ou par une autorité de certification externe ou tierce, vous pouvez également importer ou ajouter le certificat de l'autorité de certification à l'emplacement de stockage des certificats approuvés des applications.

Pour plus d'informations, reportez-vous à la « Choix du type d'autorité de certification à utiliser » page 713.

G Configuration de l'agent de mot de passe Kerberos

Vous pouvez configurer le centre de distribution de clés (KDC, Key Distribution Center) Kerberos MIT de manière à ce qu'il utilise eDirectory pour le stockage des principaux Kerberos. Les principaux Kerberos sont associés aux utilisateurs eDirectory et chaque principal Kerberos comporte des clés Kerberos requises par le KDC. Ces clés sont dérivées des mots de passe Kerberos des utilisateurs et peuvent être différentes des mots de passe eDirectory des utilisateurs.

L'agent de mot de passe Kerberos (KPA, Kerberos Password Agent) est un module que vous pouvez charger à l'intérieur d'un serveur eDirectory. Il synchronise les clés Kerberos des utilisateurs avec leur mot de passe eDirectory.

Pour plus d'informations sur les mots de passe universels, reportez-vous au Chapitre 26, « Gestion des mots de passe », page 783.

Conditions préalables à la configuration de mot de passe Kerberos

- ❒ Un KDC Kerberos MIT doit être configuré pour utiliser eDirectory afin de stocker ses principaux.

  Pour plus d'informations sur la configuration de Kerberos, reportez-vous à la « Extension du schéma Kerberos » page 880 et à la *documentation de Kerberos MIT*.

- ❒ La fonction de mot de passe universel doit être activée pour les utilisateurs eDirectory qui sont associé à des principaux Kerberos.

  Pour plus d'informations sur l'activation de la fonction de mot de passe universel, reportez-vous à la section « Deploying Universal Password » (Déploiement du mot de passe universel) du *NetIQ Password Management Administration Guide* (https://www.netiq.com/documentation/edir88/pwm_administration88/data/bookinfo.html) (Guide d'administration de la gestion des mots de passe NetIQ).

Activation de la fonctionnalité KPA pour un domaine Kerberos

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches**.
2. Cliquez sur **Administration Kerberos** > **Éditer le domaine**.
3. Recherchez et sélectionnez l'objet Conteneur de domaine à l'aide du sélecteur d'objet.
4. Dans la fenêtre Éditer le domaine, sélectionnez **Utiliser un mot de passe universel**.

Pour plus d'informations, reportez-vous à l'aide en ligne d'iManager.

REMARQUE : en cas d'ajout d'un nouveau principal, le mot de passe Kerberos et le mot de passe universel ne sont pas synchronisés. Les clés Kerberos sont générées à partir du mot de passe spécifié lors de l'ajout du principal. Pour que le mot de passe Kerberos soit identique au mot de passe universel, modifiez ce dernier après la création du principal. Vous pouvez définir ou modifier le mot de passe universel dans eDirectory.

Agent de mot de passe Kerberos

L'agent de mot de passe Kerberos (KPA, Kerberos Password Agent) doit être installé et chargé sur le serveur eDirectory sur lequel intervient le changement de mot de passe.

Pour démarrer le KPA, entrez `kpa -l`.

Pour arrêter le KPA, entrez `kpa -u`.

Les messages consignés par l'agent de mot de passe sont affichés lorsque la balise `Misc` est activée dans `ndstrace`. Les messages sont également consignés dans le fichier journal configuré pour le serveur eDirectory.

IMPORTANT : l'agent de mot de passe Kerberos n'est pas chargé automatiquement lors du redémarrage de la machine ou d'eDirectory. Vous devez le charger manuellement.

Génération de clés

Les types de chiffrement et le type de valeur aléatoire (salt) utilisés par l'agent de mot de passe Kerberos pour générer les clés Kerberos à partir du mot de passe universel sont basés sur les éléments suivants :

- Si le principal a des clés Kerberos, les types de chiffrement et de valeur aléatoire utilisés pour la génération des clés existantes sont employés afin de générer les nouvelles clés à partir du mot de passe universel.
- Si le mot de passe Kerberos n'est pas défini pour le principal, les types de chiffrement et de valeur aléatoire par défaut configurés pour le domaine sont utilisés pour la génération des clés.

Si les types de clé par défaut ne sont pas configurés pour le domaine, ceux utilisés sont `DES3-HMAC-SHAI:NORMAL` et `DES-CBC-CRC:NORMAL`.

Voici les types de chiffrement et de valeur aléatoire pris en charge :

Types de chiffrement

- `DES-CBC-CRC` : mode DES cbc avec CRC-32
- `DES-CBC-MD4` : mode DES cbc avec RSA-MD4
- `DES-CBC-MD5` : mode DES cbc avec RSA-MD5
- `DES3-CBC-SHA1-KD` : mode triple DES cbc avec HMAC/sha1
- `AES128-CTS-HMAC-SHA1-96`
- `AES256-CTS-HMAC-SHA1-96`
- `RC4-HMAC`

Types de valeur aléatoire (salt)

- `normal` : valeur par défaut pour la version 5 de Kerberos
- `v4` : le seul type utilisé par la version 4 de Kerberos, aucune valeur aléatoire
- `norealm` : identique à la valeur par défaut, sans utiliser les informations de domaine
- `onlyrealm` : utilise uniquement les informations de domaine comme la valeur aléatoire
- `special` : utilisé uniquement dans des cas très spéciaux ; n'est pas entièrement pris en charge

Remarques relatives au mot de passe universel

- Si le mot de passe universel est activé, vous ne pouvez pas utiliser l'option `randkey` pour définir le mot de passe universel pendant le changement de mot de passe d'un principal.
- Si vous définissez le mot de passe d'un principal associé à un objet Utilisateur, le mot de passe universel est défini en tant que mot de passe Kerberos pour tous les principaux dont le mot de passe universel est activé et qui sont associés à cet objet Utilisateur.
- Si le mot de passe universel est activé, vous devez charger le module de l'agent de mot de passe Kerberos (KPA, Kerberos Password Agent) à chaque redémarrage de l'ordinateur ou d'eDirectory.
- Le KPA ne prend pas en charge les caractères étendus dans un mot de passe. Si le mot de passe Kerberos est intégré à un mot de passe universel, ce dernier ne peut pas non plus comporter des caractères étendus.

H Assignation d'événements eDirectory à des événements XDAS

Cette section contient les informations suivantes :

- « Assignation d'événements eDirectory à des événements XDAS » page 895
- « Événements XDAS » page 904

Assignation d'événements eDirectory à des événements XDAS

Le Tableau H-1 répertorie les événements internes eDirectory assignés aux événements XDAS correspondants. Pour plus d'informations sur les événements eDirectory et leur description, reportez-vous à la page des services eDirectory. Pour plus d'informations sur les événements XDAS, reportez-vous à la « Événements XDAS » page 904.

REMARQUE :

- eDirectory 9.0 SP3 et versions ultérieures suivent la taxinomie Sentinel pour les événements XDAS. Pour plus d'informations, consultez le site https://www.novell.com/developer/plugin-sdk/sentinel_taxonomy.html.
- Les événements NMAS et eDirectory peuvent être configurés à l'aide de la page de configuration de XDAS. Pour plus d'informations, reportez-vous au « Audit avec XDAS » page 629.
- Le collecteur eDirectory permet de surveiller les événements NMAS et eDirectory. Le collecteur NMAS est requis uniquement pour les instances de Platform Agent.

Tableau H-1 *Événements XDAS assignés à des événements eDirectory*

Événements XDAS	Événement eDirectory
CREATE_ACCOUNT Pour obtenir un exemple de cet événement, reportez-vous à la section « Créer un compte » page 907.	DSE_CREATE_ENTRY DSE_ADD_ENTRY
DELETE_ACCOUNT Pour obtenir un exemple de cet événement, reportez-vous à la section « Supprimer le compte » page 908.	DSE_REMOVE_ENTRY
ENABLE_ACCOUNT Pour obtenir un exemple de cet événement, reportez-vous à la section « Activer le compte » page 908.	DSE_ADD_VALUE

Événements XDAS	Événement eDirectory
DISABLE_ACCOUNT Pour obtenir un exemple de cet événement, reportez-vous à la section « Désactiver le compte » page 908.	DSE_ADD_VALUE
QUERY_ACCOUNT Pour obtenir un exemple de cet événement, reportez-vous à la section « Compte de requête » page 909.	DSE_INSPECT_ENTRY DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_SEARCH DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM
MODIFY_ACCOUNT Pour obtenir un exemple de cet événement, reportez-vous à la section « Modifier le compte » page 909.	DSE_ADD_VALUE DSE_MOVE_SOURCE_ENTRY DSE_DELETE_VALUE DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_RENAME_ENTRY DSE_ADD_PROPERTY DSE_MODIFY_ENTRY DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK
CREATE_TRUST Pour obtenir un exemple de cet événement, reportez-vous à la section « Création d'une approbation » page 911.	DSE_CREATE_ENTRY DSE_ADD_ENTRY
DELETE_TRUST Pour obtenir un exemple de cet événement, reportez-vous à la section « Suppression d'une approbation » page 912.	DSE_REMOVE_ENTRY

Événements XDAS	Événement eDirectory
QUERY_TRUST Pour obtenir un exemple de cet événement, reportez-vous à la section « Approbation de requête » page 912.	DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM
MODIFY_TRUST Pour obtenir un exemple de cet événement, reportez-vous à la section « Modification de l'approbation » page 912.	DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_RENAME_ENTRY DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_ADD_VALUE DSE_ADD_PROPERTY DSE_DELETE_VALUE DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK DSE_MODIFY_ENTRY
CREATE_DATA_ITEM Pour obtenir un exemple de cet événement, reportez-vous à la section « Créer un élément de données » page 915.	DSE_CREATE_ENTRY DSE_ADD_ENTRY DSE_ADD_REPLICA DSE_DEFINE_ATTR_DEF DSE_DEFINE_CLASS_DEF
DELETE_DATA_ITEM Pour obtenir un exemple de cet événement, reportez-vous à la section « Supprimer l'élément de données » page 915.	DSE_REMOVE_ENTRY DSE_REMOVE_REPLICA DSE_REMOVE_CLASS_DEF DSE_REMOVE_ATTR_DEF

Événements XDAS	Événement eDirectory
QUERY_DATA_ITEM_ATTRIBUTE Pour obtenir un exemple de cet événement, reportez-vous à la section « Attribut d'élément de données de requête » page 915.	DSE_DSA_READ DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_PARTITIONS DSE_LIST_CONT_CLASSES DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM

Événements XDAS	Événement eDirectory
MODIFY_DATA_ITEM_ATTRIBUTE Pour obtenir un exemple de cet événement, reportez-vous à la section « Modifier l'attribut d'élément de données » page 915.	DSE_UPDATE_SCHEMA DSE_CHANGE_TREE_NAME DSE_MOVE_SUBTREE DSE_MOVE_TREE DSE_MERGE_ENTRIES DSE_RENAME_ENTRY DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_ADD_VALUE DSE_REMOVE_BACKLINK DSE_ADD_PROPERTY DSE_DELETE_VALUE DSE_DELETE_PROPERTY DSE_UPDATE_CLASS_DEF DSE_UPDATE_ATTR_DEF DSE_CHANGE_REPLICA_TYPE DSE_MODIFY_CLASS_DEF DSE_RESEND_ENTRY DSE_MERGE_TREE DSE_CREATE_SUBREF DSE_CREATE_BACKLINK DSE_MODIFY_ENTRY
ASSOCIATE_TRUST Pour obtenir un exemple de cet événement, reportez-vous à la section « Associer l'approbation » page 920.	DSE_ADD_MEMBER DSE_ADD_VALUE
DEASSOCIATE_TRUST Pour obtenir un exemple de cet événement, reportez-vous à la section « Dissocier l'approbation » page 921.	DSE_DELETE_MEMBER DSE_DELETE_VALUE

Événements XDAS	Événement eDirectory
MODIFY_ACCOUNT_SECURITY_TOKEN Pour obtenir un exemple de cet événement, reportez-vous à la section « Modifier le jeton de sécurité du compte » page 921.	DSE_CHGPASS DSE_NMAS_LOG_SET_PWD DSE_NMAS_LOG_SET_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_SECRET DSE_NMAS_LOG_SET_LOGIN_SECRET DSE_NMAS_LOG_SET_DIST_PWD DSE_NMAS_LOG_DELETE_DIST_PWD DSE_NMAS_LOG_DELETE_PWD DSE_NMAS_LOG_CHANGE_PWD DSE_NMAS_LOG_DELETE_ALL_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_ALL_LOGIN_SECRET
QUERY_ACCOUNT_SECURITY_TOKEN Pour obtenir un exemple de cet événement, reportez-vous à la section, « Jeton de sécurité du compte de requête » page 921.	DSE_NMAS_LOG_GET_LOGIN_CONFIG DSE_NMAS_LOG_GET_PWD_STATUS DSE_NMAS_LOG_GET_DIST_PWD DSE_NMAS_LOG_GET_PWD DSE_NMAS_LOG_GET_PWD_HISTORY DSE_NMAS_LOG_GET_ALL_LOGIN_CONFIG DSE_NMAS_LOG_GET_ALL_LOGIN_SECRET DSE_NMAS_LOG_CHECK_PWD_SYNTAX_POLICY
CREATE_CONNECTION Pour obtenir un exemple de cet événement, reportez-vous à la section, « Créer une connexion » page 922.	DSE_CONNECTION
TERMINATE_CONNECTION Pour obtenir un exemple de cet événement, reportez-vous à la section, « Mettre fin à la connexion » page 922.	DSE_CONNECTION
CREATE_SESSION Pour obtenir un exemple de cet événement, reportez-vous à la section « Créer une session » page 922.	DSE_LOGIN_EX DSE_NMAS_LOG_SRVR_BEGIN_LOGIN DSE_NMAS_LOG_FINISH_LOGIN_STATUS DSE_NMAS_LOG_SASL_MECHANISM_RESULT

Événements XDAS	Événement eDirectory
TERMINATE_SESSION Pour obtenir un exemple de cet événement, reportez-vous à la section, « Terminer la session » page 922.	DSE_LOGOUT
AUTHENTICATE_SESSION Pour obtenir un exemple de cet événement, reportez-vous à la section « Authentifier la session » page 923.	DSE_AUTHENTICATE DSE_IMPERSONATE DSE_EBA_BA_FAILURE DSE_VERIFY_PASS
GRANT_TRUST_ACCESS Pour obtenir un exemple de cet événement, reportez-vous à la section, « Accorder l'accès à l'approbation » page 923.	DSE_ADD_VALUE
REVOKE_TRUST_ACCESS Pour obtenir un exemple de cet événement, reportez-vous à la section, « Révoquer l'accès à l'approbation » page 923.	DSE_DELETE_VALUE
INTRUDER_LOCKOUT Pour obtenir un exemple de cet événement, reportez-vous à la section, « Verrouillage en cas d'intrusion » page 924	DSE_ADD_VALUE
ACCOUNT_UNLOCK Pour obtenir un exemple de cet événement, reportez-vous à la section, « Déverrouillage du compte » page 924.	DSE_DELETE_VALUE
GRANT_ACCOUNT_ACCESS Pour obtenir un exemple de cet événement, reportez-vous à la section, « Accorder l'accès au compte » page 924.	DSE_ADD_VALUE
REVOKE_ACCOUNT_ACCESS Pour obtenir un exemple de cet événement, reportez-vous à la section, « Révoquer l'accès au compte » page 925.	DSE_DELETE_VALUE
AUDIT_CONFIG Pour obtenir un exemple de cet événement, reportez-vous à la section, « Configuration de l'audit » page 925.	DSE_ADD_VALUE DSE_DELETE_VALUE

Événements XDAS	Événement eDirectory
ENABLE_SERVICE Pour obtenir un exemple de cet événement, reportez-vous à la section « Activer le service » page 928.	DSE_CHANGE_MODULE_STATE DSE_NMAS_LOG_PWD_POLICY_AGENT_REG DSE_NMAS_LOG_DIST_PWD_AGENT_REG DSE_NMAS_LOG_PWD_AGENT_REG DSE_NMAS_LOG_LTSS_AGENT_REG DSE_NMAS_LOG_PWD_CHANGE_AGENT_REG
DISABLE_SERVICE Pour obtenir un exemple de cet événement, reportez-vous à la section « Désactiver le service » page 928.	DSE_CHANGE_MODULE_STATE DSE_REMOTE_SERVER_DOWN DSE_NMAS_LOG_PWD_POLICY_AGENT_DEREG DSE_NMAS_LOG_DIST_PWD_AGENT_DEREG DSE_NMAS_LOG_PWD_AGENT_DEREG DSE_NMAS_LOG_LTSS_AGENT_DEREG DSE_NMAS_LOG_PWD_CHANGE_AGENT_DEREG
INVOKE_SERVICE Pour obtenir un exemple de cet événement, reportez-vous à la section « Invoquer le service » page 928.	DSE_BACKLINK_PROC_DONE DSE_LIMBER_DONE DSE_MOVE_TREE_START DSE_PURGE_START DSE_RECV_REPLICA_UPDATES DSE_SEND_REPLICA_UPDATES DSE_START_JOIN DSE_START_UPDATE_REPLICA DSE_START_UPDATE_SCHEMA DSE_SYNC_PART_START DSE_SYNC_SVR_OUT_START

Événements XDAS	Événement eDirectory
TERMINATE_SERVICE Pour obtenir un exemple de cet événement, reportez-vous à la section « Terminer le service » page 928.	DSE_REMOVE_ATTR_DEF DSE_ABORT_JOIN DSE_END_UPDATE_REPLICA DSE_END_UPDATE_SCHEMA DSE_JOIN_DONE DSE_MOVE_TREE_END DSE_PURGE_END DSE_SCHEMA_SYNC DSE_SYNC_PART_END DSE_SYNC_SVR_OUT_END
MODIFY_SERVICE_CONFIG Pour obtenir un exemple de cet événement, reportez-vous à la section, « Modifier la configuration du service » page 929.	DSE_ALLOW_LOGIN DSE_UPDATE_REPLICA DSE_EBA_MOVE_EBA_CA DSE_GEN_CA_KEYS DSE_RECERT_PUB_KEY DSE_EBA_REQ_BA_MATERIAL DSE_EBA_REQ_SERVER_BA_MATERIAL DSE_NAME_COLLISION DSE_SERVER_RENAME DSE_SERVER_ADDRESS_CHANGE DSE_SYNC_PARTITION DSE_SYNC_SCHEMA DSE_EBA_ENABLE_PURE_MODE DSE_EBA_ISSUE_NCPCA_CERT DSE_EBA_REVOKE_NCPCA_CERT
START_SYSTEM Pour obtenir un exemple de cet événement, reportez-vous à la section « Démarrer le système » page 931.	DSE_AGENT_OPEN_LOCAL DSE_RELOAD_DS
SHUTDOWN_SYSTEM Pour obtenir un exemple de cet événement, reportez-vous à la section « Arrêter le système » page 931.	DSE_AGENT_CLOSE_LOCAL

Événements XDAS	Événement eDirectory
BACKUP_DATA_STORE Pour obtenir un exemple de cet événement, reportez-vous à la section, « Sauvegarder le stockage de données » page 931.	DSE_BACKUP_ENTRY
RECOVER_DATA_STORE Pour obtenir un exemple de cet événement, reportez-vous à la section « Récupérer la zone de stockage de données » page 931.	DSE_RESTORE_ENTRY
INTERNAL_OPERATIONS Pour obtenir un exemple de cet événement, reportez-vous à la section, « Opérations internes » page 932.	DSE_CRC_FAILURE DSE_DELETE_SUBTREE DSE_DELETE_UNUSED_EXTREF DSE_DSA_BAD_VERB DSE_LOST_ENTRY DSE_NEW_SCHEMA_EPOCH DSE_NO_REPLICA_PTR DSE_PURGE_ENTRY_FAIL DSE_EBA_ISSUE_CRL
MODIFY_PROCESS_CONTEXT Pour obtenir un exemple de cet événement, reportez-vous à la section « Modifier le contexte du processus » page 932.	DSE_PARTITION_STATE_CHG DSE_LDAP_MODLDAPSERVER DSE_PART_STATE_CHG_REQ DSE_REPAIR_TIME_STAMPS DSE_RESET_DS_COUNTERS DSE_SET_NEW_MASTER DSE_SYNTHETIC_TIME DSE_SPLIT_DONE DSE_SPLIT_PARTITION DSE_JOIN_PARTITIONS DSE_ABORT_PARTITION_OP DSE_LOW_LEVEL_JOIN

Événements XDAS

Les événements XDAS sont classés dans les catégories suivantes :

- « Événements de gestion de compte » page 905
- « Événements de gestion des approbations » page 910
- « Événements de gestion des éléments de données » page 913

- « Événements de sécurité » page 916
- « Événements de gestion de service ou d'application » page 926
- « Événements opérationnels » page 929

Événements de gestion de compte

Les événements de gestion des comptes s'appliquent à la gestion des comptes de principal. Un principal peut être un utilisateur final. Par défaut, les classes d'objet Personne organisationnelle, Personne et Utilisateur sont assignées aux comptes.

REMARQUE : l'événement `Modifier le jeton de sécurité du compte` aurait pu être défini dans le cadre de l'événement `Modifier le compte`, mais la modification des jetons de sécurité de compte est considérée comme un aspect très important de l'audit de sécurité et bénéficie dès lors de son propre événement.

Tableau H-2 *Taxinomie des événements de gestion des comptes*

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Cliquez sur
Créer un compte	0.0.0.0	DSE_CREATE_ENTRY DSE_ADD_ENTRY	Créer un compte	Cet événement est généré lors de la création d'un compte.
Supprimer le compte	0.0.0.1	DSE_REMOVE_ENTRY	Supprimer un compte existant	Cet événement a un sens sémantique opposé à la création d'un compte. Cet événement est généré lors de la suppression d'un compte.
Désactiver le compte	0.0.0.2	DSE_ADD_VALUE	Désactiver un compte existant	Cet événement est généré lorsqu'un compte est désactivé par un administrateur ou un processus de sécurité automatisé et ne peut pas être utilisé tant qu'il n'a pas été réactivé.
Activer le compte	0.0.0.3	DSE_ADD_VALUE	Activer un compte désactivé existant	Il s'agit de l'événement contraire à l'événement Désactiver le compte défini ci-dessus.

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Cliquez sur
Compte de requête	0.0.0.4	DSE_INSPECT_ENTRY DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_SEARCH DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM	Interroger un compte existant	Cet événement est généré lors d'une requête pour les informations d'attribut d'un compte en particulier.
Modifier le compte	0.0.0.5	DSE_ADD_VALUE DSE_MOVE_SOURCE_ENTRY DSE_DELETE_VALUE DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_RENAME_ENTRY DSE_ADD_PROPERTY DSE_MODIFY_ENTRY DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK	Modifier un compte existant	Cet événement est généré lors d'une requête de modification des informations d'attribut d'un compte en particulier.

Exemples d'événements de gestion des comptes

Cette section présente des exemples pour les événements de gestion de compte suivants :

- « Créer un compte » page 907
- « Supprimer le compte » page 908
- « Désactiver le compte » page 908
- « Activer le compte » page 908
- « Compte de requête » page 909
- « Modifier le compte » page 909

REMARQUE : les exemples contenus dans les sections suivantes sont uniquement fournis à titre de référence.

Créer un compte

Cliquez sur **Créer un compte** pour générer un événement de création d'un compte utilisateur. Une sortie au format JSON, semblable à ce qui suit, est générée :


```
Mar 15 12:08:35 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"ClassName" : "User"},"Account" : {"Domain"
: "TREEUPGRADE","Name" : "CN=user1,O=novell","Id" : "32864"}},"Action" : {"Event" :
{"Id" : "0.0.2.0","Name" : "CREATE_ACCOUNT","CorrelationID" :
"eDirectory#29#87e32af4-e717-4607-a541-f42ae38717e7","SubEvent" :
"DSE_CREATE_ENTRY"},"Time" : {"Offset" : 1489559915},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


L'exemple précédent apparaît au format XML (lorsque vous le convertissez depuis le format JSON) comme suit :


```
<Source>eDirectory#DS</Source>
  <Observer>
    <Account>
      <Domain>MYTREE</Domain>
      <Name>CN=SLES11-SP2,O=mycom</Name>
    </Account>
    <Entity>
      <SysAddr>100.1.1.2</SysAddr>
      <SysName>SLES11-SP2.my.com</SysName>
    </Entity>
  </Observer>
  <Initiator>
    <Account>
      <Name>CN=admin,O=mycom</Name>
      <Id>32805</Id>
    </Account>
  </Initiator>
  <Target>
    <Data>
      <ClassName>User</ClassName>
      <Name>CN=USER,O=mycom</Name>
    </Data>
  </Target>
  <Action>
    <Event>
      <Id>0.0.2.0</Id>
```

```
      <Name>CREATE_ACCOUNT</Name>
      <CorrelationID>eDirectory#25#0ef05b4c-e864-4d4c-f7a9-4c5bf00e64e8</
CorrelationID>
      <SubEvent>DSE_CREATE_ENTRY</SubEvent>
    </Event>
    <Time>
      <Offset>1389173763</Offset>
    </Time>
    <Log>
      <Severity>7</Severity>
    </Log>
    <Outcome>0</Outcome>
    <ExtendedOutcome>0</ExtendedOutcome>
  </Action>
```


Supprimer le compte

Cliquez sur **Supprimer le compte** pour générer un événement de suppression d'un compte utilisateur, comme illustré dans l'exemple suivant :


```
Mar 13 16:40:50 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:16600"}},"Target" : {"Data" : {"ClassName" : "User","Version" :
"2"},"Account" : {"Domain" : "VLV_MEM","Name" : "CN=user1,O=novell","Id" :
"203366"}},"Action" : {"Event" : {"Id" : "0.0.0.1","Name" :
"DELETE_ACCOUNT","CorrelationID" : "eDirectory#18#f2bb6a04-b1a5-43c2-a990-
046abbf2a5b1","SubEvent" : "DSE_REMOVE_ENTRY"},"Time" : {"Offset" :
1489403450},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Désactiver le compte

Cliquez sur **Désactiver le compte** pour générer un événement de désactivation d'un compte utilisateur, comme illustré dans l'exemple suivant :


```
Mar 08 17:39:31 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:39382"}},"Target" : {"Data" : {"Attribute Name" : "Login
Disabled","ClassName" : "User","Version" : "2"},"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=rrrr,OU=novell,OU=co,O=in","Id" : "32906"}},"Action" :
{"Event" : {"Id" : "0.0.0.2","Name" : "DISABLE_ACCOUNT","CorrelationID" :
"eDirectory#91#2a382b1e-9d96-4990-9341-1e2b382a969d","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1488974971},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Activer le compte

Cliquez sur **Activer le compte** pour générer un événement d'activation d'un compte utilisateur, comme illustré dans l'exemple suivant :

```
Mar 07 18:13:09 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:18902"}},"Target" : {"Data" : {"Attribute Name" : "Login
Disabled","ClassName" : "User","Version" : "2"},"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=raghu,OU=novell,OU=co,O=in","Id" : "32893"}},"Action" :
{"Event" : {"Id" : "0.0.0.3","Name" : "ENABLE_ACCOUNT","CorrelationID" :
"eDirectory#72#eecfbf13-9f36-4c09-b468-13bfcfee369f","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1488890589},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Compte de requête

Cliquez sur **Compte de requête** pour générer un événement permettant d'interroger un compte utilisateur, comme illustré dans l'exemple suivant :


```
Mar 06 16:40:00 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "ACL","ClassName" :
"User","Version" : "2"},"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"}},"Action" : {"Event" : {"Id" :
"0.0.0.4","Name" : "QUERY_ACCOUNT","CorrelationID" : "eDirectory#59#","SubEvent" :
"DSE_READ_ATTR"},"Time" : {"Offset" : 1488798600},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Modifier le compte

Cliquez sur **Modifier le compte** pour générer un événement permettant de modifier un compte utilisateur, comme illustré dans l'exemple suivant :


```
Mar 07 16:24:45 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" :
"pwdFailureTime","ClassName" : "User","Syntax" : "24","Version" : "2"},"Account" :
{"Domain" : "LNX-TREE-BUILD101","Name" : "CN=admin,OU=novell,OU=co,O=in","Id" :
"32863"}},"Action" : {"Event" : {"Id" : "0.0.0.5","Name" :
"MODIFY_ACCOUNT","CorrelationID" : "eDirectory#0#678d790d-c19f-4364-b821-
0d798d679fc1","SubEvent" : "DSE_DELETE_ATTRIBUTE"},"Time" : {"Offset" :
1488884085},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

Événements de gestion des approbations

Les événements de gestion des approbations permettent de gérer les relations de confiance. Une approbation peut être instanciée par un groupe ou un rôle. Par défaut, les classes d'objet dynamicGroup, dynamicGroupAux, Groupe, Groupe LDAP et Rôle organisationnel sont assignées aux approbations.

Par exemple, lorsqu'une identité située dans le domaine A demande un service qui relève du domaine B, une association approuvée est requise entre les deux domaines. Cela s'appelle une relation de confiance. Vous avez configuré une relation de confiance en établissant une identité dans le domaine B, qui est utilisée en tant que proxy pour toutes les requêtes venant de n'importe quelle identité du domaine A.

Tableau H-3 *Taxinomie des événements de gestion des approbations*

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Utilisation
Créer l'approbation	0.0.1.0	DSE_CREATE_ENTRY DSE_ADD_ENTRY	Création d'une approbation.	Cet événement est signalé lors de la création d'une approbation.
Supprimer l'approbation	0.0.1.1	DSE_REMOVE_ENTRY	Suppression d'une approbation.	Cet événement est signalé lors de la suppression d'une approbation.
Approbation de requête	0.0.1.2	DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM	Demande d'attributs associés à une approbation.	Cet événement est signalé lors d'une requête d'attributs associés à une approbation.

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Utilisation
Modifier l'approbation	0.0.1.3	DSE_MOVE_SUBTREE DSE_MERGE_ENTRIES DSE_RENAME_ENTRY DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_ADD_VALUE DSE_ADD_PROPERTY DSE_DELETE_VALUE DSE_DELETE_PROPERTY DSE_RESEND_ENTRY DSE_CREATE_BACKLINK DSE_REMOVE_BACKLINK DSE_MODIFY_ENTRY	Modification des attributs associés à une approbation.	Cet événement est signalé en cas de modification apportée aux attributs associés à une approbation.

Exemples d'événements de gestion des approbations

Les sections suivantes présentent des exemples pour les événements de gestion des approbations.

- « Création d'une approbation » page 911
- « Suppression d'une approbation » page 912
- « Approbation de requête » page 912
- « Modification de l'approbation » page 912

Création d'une approbation

Cliquez sur **Créer une approbation** pour générer un événement lors de la création d'une nouvelle approbation, comme illustré dans l'exemple suivant :


```
Mar 16 20:56:39 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:43936"}},"Target" : {"Data" : {"ClassName" : "LDAP Group","Name" :
"CN=LDAP Group - server2,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.1.0","Name" : "CREATE_TRUST","CorrelationID" : "eDirectory#41#2a670625-1950-
48cf-8abf-2506672a5019","SubEvent" : "DSE_CREATE_ENTRY"},"Time" : {"Offset" :
1489677999},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

Suppression d'une approbation

Cliquez sur **Supprimer l'approbation** pour générer un événement lors de la suppression d'une approbation existante, comme illustré dans l'exemple suivant :


```
Mar 16 22:02:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:26571"}},"Target" : {"Data" : {"ClassName" : "dynamicGroup","Name" :
"CN=group1,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.1.1","Name" : "DELETE_TRUST","CorrelationID" : "eDirectory#55#8f230203-1c8f-
41f7-8456-0302238f8f1c","SubEvent" : "DSE_REMOVE_ENTRY"},"Time" : {"Offset" :
1489681966},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Approbation de requête

Cliquez sur **Approbation de requête** pour générer un événement lorsqu'une requête est déclenchée pour les attributs qui sont associés à une approbation, comme illustré dans l'exemple suivant :


```
Mar 16 16:49:35 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:31967"}},"Target" : {"Data" : {"Attribute Name" : "LDAP Allow Clear
Text Password","ClassName" : "LDAP Group","Name" : "CN=LDAP Group - SLE12-
142,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.1.4","Name" :
"QUERY_TRUST","CorrelationID" : "eDirectory#46#","SubEvent" :
"DSE_READ_ATTR"},"Time" : {"Offset" : 1489663175},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Modification de l'approbation

Cliquez sur **Modifier l'approbation** pour générer un événement lorsqu'une modification est apportée aux attributs qui sont associés à une approbation, comme illustré dans l'exemple suivant :


```
Mar 16 22:02:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:26571"}},"Target" : {"Data" : {"Attribute Name" :
"Obituary","Attribute Value" : "72061996379406335","ClassName" :
"dynamicGroup","Name" : "CN=group1,O=novell","Syntax" : "9","Version" :
"2"}},"Action" : {"Event" : {"Id" : "0.0.1.5","Name" :
"MODIFY_TRUST","CorrelationID" : "eDirectory#55#8f230203-1c8f-41f7-8456-
0302238f8f1c","SubEvent" : "DSE_DELETE_VALUE"},"Time" : {"Offset" :
1489681966},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

Événements de gestion des éléments de données

Cet ensemble d'événements fait référence à la création et à la gestion d'éléments de données et de ressources au sein d'un domaine. Le type d'élément de données ou de ressources dépend entièrement du domaine. Par défaut, une classe d'objet qui n'est assignée à aucun compte ou aucune approbation sera assignée aux éléments de données.

par exemple, les fichiers et répertoires, les fichiers de périphérique spéciaux et les segments de mémoire partagée au sein d'un système d'exploitation, les tables et les enregistrements au sein d'une base de données, ou encore les messages au sein d'un système de messagerie. Le terme « élément de données » est utilisé dans ce contexte pour faire référence à tout type d'élément de ressource.

Tableau H-4 *Taxinomie de l'événement de gestion des éléments de données*

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Cliquez sur
Créer un élément de données	0.0.3.0	DSE_CREATE_ENTRY DSE_ADD_ENTRY DSE_ADD_REPLICA DSE_DEFINE_ATTR_DEF DSE_DEFINE_CLASS_DEF	Créer un élément de données	Cet événement est signalé lors de la création d'un élément de données.
Supprimer l'élément de données	0.0.3.1	DSE_REMOVE_ENTRY DSE_REMOVE_REPLICA DSE_REMOVE_CLASS_DEF DSE_REMOVE_ATTR_DEF	Supprimer un élément de données	Cet événement est signalé chaque fois qu'un élément de ressources ou de données lié à la sécurité est supprimé..
Attribut d'élément de données de requête	0.0.3.2	DSE_DSA_READ DSE_INSPECT_ENTRY DSE_SEARCH DSE_LIST_PARTITIONS DSE_LIST_CONT_CLASSES DSE_LIST_SUBORDINATES DSE_READ_REFERENCES DSE_REFERRAL DSE_COMPARE_ATTR_VALUE DSE_READ_ATTR DSE_STREAM	Demande d'attributs associés à des éléments de données.	Cet événement est consigné chaque fois qu'un élément de ressources ou de données lié à la sécurité est interrogé (que ce soit pour la valeur ou un attribut de l'élément de données).

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Cliquez sur
Modifier l'attribut d'élément de données	0.0.3.3	DSE_UPDATE_SCHEMA DSE_CHANGE_TREE_NAME DSE_MOVE_SUBTREE DSE_MOVE_TREE DSE_MERGE_ENTRIES DSE_RENAME_ENTRY DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY DSE_MUTATE_ENTRY DSE_ADD_VALUE DSE_REMOVE_BACKLINK DSE_ADD_PROPERTY DSE_DELETE_VALUE DSE_DELETE_PROPERTY DSE_UPDATE_CLASS_DEF DSE_UPDATE_ATTR_DEF DSE_CHANGE_REPLICA_TYPE DSE_MODIFY_CLASS_DEF DSE_RESEND_ENTRY DSE_MERGE_TREE DSE_CREATE_SUBREF DSE_CREATE_BACKLINK DSE_MODIFY_ENTRY	Modification des attributs associés à des éléments de données.	Cet événement est signalé en cas de modification d'un élément de ressources ou de données lié à la sécurité (la valeur ou un attribut de l'élément de données).

Exemples des événements de gestion des éléments de données

Les sections suivantes présentent des exemples de génération des événements de gestion des éléments de données.

- « Créer un élément de données » page 915
- « Supprimer l'élément de données » page 915
- « Attribut d'élément de données de requête » page 915
- « Modifier l'attribut d'élément de données » page 915

Créer un élément de données

Cliquez sur **Créer un élément de données** pour générer un événement de création d'un élément de données, comme illustré dans l'exemple suivant :


```
Mar 16 20:56:24 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:42144"}},"Target" : {"Data" : {"ClassName" : "NCP Server","Name" :
"CN=server2,O=novell","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.3.0","Name" : "CREATE_DATA_ITEM","CorrelationID" : "eDirectory#39#7e296d99-
d6a7-4206-8f23-996d297ea7d6","SubEvent" : "DSE_CREATE_ENTRY"},"Time" : {"Offset" :
1489677984},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Supprimer l'élément de données

Cliquez sur **Supprimer l'élément de données** pour générer un événement de suppression d'un élément de données, comme illustré dans l'exemple suivant :


```
Mar 16 21:46:32 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:26571"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.3.1","Name" : "DELETE_DATA_ITEM","CorrelationID" :
"eDirectory#55#9509dc1f-ecf1-4306-8fec-1fdc0995f1ec","SubEvent" :
"DSE_REMOVE_ENTRY"},"Time" : {"Offset" : 1489680992},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Attribut d'élément de données de requête

Cliquez sur **Attribut d'élément de données de requête** pour générer un événement d'interrogation d'un attribut d'élément de données, comme illustré dans l'exemple suivant :


```
Mar 03 14:01:36 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" :
"EBATreeConfiguration","ClassName" : "Tree Root","Name" : "LNX-TREE-
BUILD101","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.2","Name" :
"QUERY_DATA_ITEM_ATTRIBUTE","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_READ_ATTR"},"Time" : {"Offset" : 1488529896},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Modifier l'attribut d'élément de données

Cliquez sur **Modifier l'attribut d'élément de données** pour générer un événement de modification d'un attribut d'élément de données, comme illustré dans l'exemple suivant :

```
Mar 03 14:05:06 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:214"}},"Target" : {"Data" : {"Attribute Name" :
"modifiersName","Attribute Value" : "CN=admin,OU=novell,OU=co,O=in","ClassName" :
"NCP Server","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in","Syntax" :
"3","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.3.3","Name" :
"MODIFY_DATA_ITEM_ATTRIBUTE","CorrelationID" : "eDirectory#32#f2dbd583-1f5c-459a-
8c37-83d5dbf25c1f","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" :
1488530106},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Événements de sécurité

Les événements de cet ensemble ne sont applicables que dans le cadre d'opérations d'audit de sécurité d'eDirectory. Une opération de sécurité peut accorder/révoquer un accès ou une connexion, mais aussi autoriser/refuser une requête ou une modification de mot de passe. Cet ensemble d'événements aide également à détecter les tentatives d'intrusion sur le système eDirectory.

Tableau H-5 *Taxinomie des événements de sécurité*

Nom de l'événement	Identificateur de l'événement	Événement eDirectory correspondant	Description	Utilisation
Associer l'approbation	0.0.1.2	DSE_ADD_MEMBER DSE_ADD_VALUE	Association d'un compte à l'approbation, ce qui confère les autorisations d'approbation au compte.	Cet événement est signalé lors de la création d'une association approuvée. Par exemple, l'ajout d'un membre à un groupe.
Dissocier l'approbation	0.0.1.3	DSE_DELETE_MEMBER DSE_DELETE_VALUE	Dissociation d'un compte et d'une approbation.	Cet événement est signalé lors de la suppression d'une association approuvée existante. Par exemple, la suppression d'un membre d'un groupe.

Nom de l'événement	Identificateur de l'événement	Événement eDirectory correspondant	Description	Utilisation
Modifier le jeton de sécurité du compte	0.0.0.6	DSE_CHGPASS DSE_NMAS_LOG_SET_PWD DSE_NMAS_LOG_SET_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_SECRET DSE_NMAS_LOG_SET_LOGIN_SECRET DSE_NMAS_LOG_SET_DIST_PWD DSE_NMAS_LOG_DELETE_DIST_PWD DSE_NMAS_LOG_DELETE_PWD DSE_NMAS_LOG_CHANGE_PWD DSE_NMAS_LOG_DELETE_ALL_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_ALL_LOGIN_SECRET	Modifier le jeton de sécurité d'un compte existant.	Un jeton de sécurité d'un compte peut être un mot de passe ou tout autre type d'authentification associé à un compte utilisateur. Dans ce cas, un compte utilisateur signifie tout type de compte sous lequel un utilisateur, une application ou un service système peut s'authentifier, puis agir en fonction des droits de ce compte.
Jeton de sécurité du compte de requête	0.0.12.3	DSE_NMAS_LOG_GET_LOGIN_CONFIG DSE_NMAS_LOG_GET_PWD_STATUS DSE_NMAS_LOG_GET_DIST_PWD DSE_NMAS_LOG_GET_PWD DSE_NMAS_LOG_GET_PWD_HISTORY DSE_NMAS_LOG_GET_ALL_LOGIN_CONFIG DSE_NMAS_LOG_GET_ALL_LOGIN_SECRET DSE_NMAS_LOG_CHECK_PWD_SYNTAX_POLICY	Demande d'un jeton de sécurité pour un compte existant.	Un jeton de sécurité d'un compte peut être un mot de passe ou tout autre type d'authentification associé à un compte utilisateur. Dans ce cas, un compte utilisateur signifie tout type de compte sous lequel un utilisateur, une application ou un service système peut s'authentifier, puis agir en fonction des droits de ce compte.

Nom de l'événement	Identificateur de l'événement	Événement eDirectory correspondant	Description	Utilisation
Créer une connexion	0.0.12.4	DSE_CONNECTION	Création d'un canal de communication entre les composants du système.	Cet événement est signalé lors de la création d'un canal de communication entre les composants du système.
Mettre fin à la connexion	0.0.12.5	DSE_CONNECTION	Fermeture d'un canal de communication entre les composants du système.	Cet événement est signalé lors de la fermeture d'un canal de communication existant entre les composants du système.
Créer une session	0.0.2.0	DSE_LOGIN_EX DSE_NMAS_LOG_SRVR_BEGIN_LOGIN DSE_NMAS_LOG_FINISH_LOGIN_STATUS DSE_NMAS_LOG_SASL_MECHANISM_RESULT	Créer une session.	Cet événement doit être signalé lors de la création d'une nouvelle session. Par exemple, une connexion au système eDirectory.
Terminer la session	0.0.2.1	DSE_LOGOUT	Terminer une session existante.	Cet événement doit être signalé chaque fois qu'une session existante (telle que définie ci-dessus) est terminée. Par exemple, une déconnexion du système eDirectory.

Nom de l'événement	Identificateur de l'événement	Événement eDirectory correspondant	Description	Utilisation
Authentifier la session	0.0.2.4	DSE_AUTHENTICATE DSE_IMPERSONATE DSE_EBA_BA_FAILURE DSE_VERIFY_PASS	Une nouvelle identité est associée à une session.	Lorsqu'un utilisateur s'authentifie pour une session, une nouvelle identité est associée à cette session. Cette identité est ensuite utilisée afin d'autoriser les requêtes pour des ressources protégées.
Accorder l'accès à l'approbation	0.0.1.7	DSE_ADD_VALUE	Octroi d'accès à une approbation pour un objet.	Cet événement est signalé lorsqu'un accès est accordé à une approbation pour un objet.
Révoquer l'accès à l'approbation	0.0.1.8	DSE_DELETE_VALUE	Révocation de l'accès à une approbation pour un objet.	Cet événement est signalé lors de la suppression d'un accès à une ressource à partir d'une approbation.
Verrouillage en cas d'intrus	0.0.0.9	DSE_ADD_VALUE	Verrouillage d'un compte.	Cet événement est signalé lors du verrouillage d'un compte.
Déverrouillage du compte	0.0.0.10	DSE_DELETE_VALUE	Déverrouillage d'un compte verrouillé.	Cet événement est signalé lors du déverrouillage d'un compte verrouillé.
Accorder l'accès au compte	0.0.0.7	DSE_ADD_VALUE	Octroi d'accès à un compte pour un objet.	Cet événement est signalé lorsqu'un accès à un compte est accordé à un objet.

Nom de l'événement	Identificateur de l'événement	Événement eDirectory correspondant	Description	Utilisation
Révoquer l'accès au compte	0.0.0.8	DSE_DELETE_VALUE	Révocation de l'accès à un compte pour un objet.	Cet événement est signalé lors de la suppression d'un objet d'un compte.
Configuration de l'audit	0.0.9.0	DSE_ADD_VALUE DSE_DELETE_VALUE	Modification des paramètres de contrôle du fonctionnement du service d'audit.	Cet événement est signalé en cas de modification apportée aux paramètres qui contrôlent le service d'audit.

Exemples d'événements de sécurité

Les sections suivantes sont des exemples d'événements de sécurité.

- « Associer l'approbation » page 920
- « Dissocier l'approbation » page 921
- « Modifier le jeton de sécurité du compte » page 921
- « Jeton de sécurité du compte de requête » page 921
- « Créer une connexion » page 922
- « Mettre fin à la connexion » page 922
- « Créer une session » page 922
- « Terminer la session » page 922
- « Authentifier la session » page 923
- « Accorder l'accès à l'approbation » page 923
- « Révoquer l'accès à l'approbation » page 923
- « Verrouillage en cas d'intrusion » page 924
- « Déverrouillage du compte » page 924
- « Accorder l'accès au compte » page 924
- « Révoquer l'accès au compte » page 925
- « Configuration de l'audit » page 925

Associer l'approbation

Cliquez sur **Associer l'approbation** pour générer un événement lors de la création d'une nouvelle association approuvée, comme illustré dans l'exemple suivant :

```
Mar 16 21:57:28 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:26571"}},"Target" : {"Data" : {"Attribute Name" : "Member","Name" :
"CN=group1,O=novell","Syntax" : "1","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.1.2","Name" : "ASSOCIATE_TRUST","CorrelationID" : "eDirectory#55#b22140b4-
ad56-4592-942a-b44021b256ad","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" :
1489681648},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Dissocier l'approbation

Cliquez sur **Dissocier l'approbation** pour générer un événement lors de la suppression d'une association approuvée existante, comme illustré dans l'exemple suivant :


```
Mar 07 22:20:41 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:31446"}},"Target" : {"Data" : {"Attribute Name" : "Member","Attribute
Value" : "CN=raghu,OU=novell,OU=co,O=in","ClassName" : "Group","Name" :
"CN=RG,OU=novell,OU=co,O=in","SubTarget" :
"CN=raghu,OU=novell,OU=co,O=in","Syntax" : "1","Version" : "2"}},"Action" :
{"Event" : {"Id" : "0.0.1.3","Name" : "DEASSOCIATE_TRUST","CorrelationID" :
"eDirectory#74#55e2ccc4-d99a-4a6a-b3dd-c4cce2559ad9","SubEvent" :
"DSE_DELETE_VALUE"},"Time" : {"Offset" : 1488905441},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Modifier le jeton de sécurité du compte

Cliquez sur **Modifier le jeton de sécurité du compte** pour générer un événement permettant de modifier le jeton de sécurité du compte utilisateur, comme illustré dans l'exemple suivant :


```
Mar 15 13:19:34 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"ClassName" : "User","Version" :
"2"},"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=user7,O=novell","Id" :
"32869"}},"Action" : {"Event" : {"Id" : "0.0.0.6","Name" :
"MODIFY_ACCOUNT_SECURITY_TOKEN","CorrelationID" : "eDirectory#25#db042b31-ea70-
49d8-8b7b-312b04db70ea","SubEvent" : "DSE_CHGPASS"},"Time" : {"Offset" :
1489564174},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Jeton de sécurité du compte de requête

Cliquez sur **Jeton de sécurité du compte de requête** pour générer un événement permettant d'interroger le jeton de sécurité du compte utilisateur, comme illustré dans l'exemple suivant :


```
Mar 15 13:19:34 eDirectory : INFO {"Source" : "eDirectory#NMAS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell","Id" :
"0"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" : "SLE12-142","SvcName" :
"nmas"}},"Initiator" : {"Account" : {"Name" : "CN=admin,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"},"Account" :
{"Domain" : "TREEUPGRADE","Name" : "CN=user8,O=novell"}},"Action" : {"Event" :
{"Id" : "0.0.12.3","Name" : "QUERY_ACCOUNT_SECURITY_TOKEN","CorrelationID" :
"nmas#0#","SubEvent" : "DSE_NMAS_LOG_GET_PWD_STATUS"},"Time" : {"Offset" :
1489564174},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

Créer une connexion

Cliquez sur **Créer une connexion** pour générer un événement lors de la création d'un canal de communication entre les composants du système, comme illustré dans l'exemple suivant :


```
Mar 07 15:53:25 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101"},"Entity" : {"SysAddr" : "1100.1.2.194:64708"}},"Target" : {"Data" :
{"ConnID" : "63","Module" : "NCP Engine","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","State" : "Create","Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.13.1","Name" : "CREATE_CONNECTION","CorrelationID" :
"eDirectory#4294967295#","SubEvent" : "DSE_CONNECTION"},"Time" : {"Offset" :
1488882205},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Mettre fin à la connexion

Cliquez sur **Mettre fin à la connexion** pour générer un événement en cas d'arrêt d'un canal de communication existant entre les composants du système, comme illustré dans l'exemple suivant :


```
Mar 07 15:46:44 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101"},"Entity" : {"SysAddr" : "100.1.2.194:63684"}},"Target" : {"Data" :
{"ConnID" : "65","Module" : "NCP Engine","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","State" : "Destroy","Version" : "2"}},"Action" : {"Event"
: {"Id" : "0.0.13.2","Name" : "TERMINATE_CONNECTION","CorrelationID" :
"eDirectory#4294967295#","SubEvent" : "DSE_CONNECTION"},"Time" : {"Offset" :
1488881804},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Créer une session

Cliquez sur **Créer une session** pour générer un événement de création d'une session, comme illustré dans l'exemple suivant :


```
Mar 06 16:21:47 eDirectory : INFO {"Source" : "eDirectory#NMAS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","Id" : "nds:7"},"Entity" : {"SysAddr" :
"100.1.2.194","SysName" : "SLES12-194-12","SvcName" : "nmas"}},"Initiator" :
{"Account" : {"Name" : "CN=admin,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" :
"100.1.2.194:54823"}},"Target" : {"Data" : {"Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.2.0","Name" : "CREATE_SESSION","CorrelationID" : "nmas#262183#","SubEvent" :
"DSE_NMAS_LOG_FINISH_LOGIN_STATUS"},"Time" : {"Offset" : 1488797507},"Log" :
{"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Terminer la session

Cliquez sur **Terminer la session** pour générer un événement d'arrêt d'une session, comme illustré dans l'exemple suivant :

```
Mar 16 21:02:23 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"[Public]"},"Entity" : {"SysAddr" : "164.99.91.92:8147"},"Assertions" :
{"NetAddress" : "100.1.2.194"}},"Target" : {"Data" : {"Name" : "CN=stdir-vm-
53,O=novell","SubTarget" : "CN=JPass,OU=users,O=novell","Version" : "2"}},"Action"
: {"Event" : {"Id" : "0.0.2.1","Name" : "TERMINATE_SESSION","CorrelationID" :
"eDirectory#42#","SubEvent" : "DSE_LOGOUT"},"Time" : {"Offset" : 1489678343},"Log"
: {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Authentifier la session

Cliquez sur **Authentifier la session** pour générer un événement lorsqu'une nouvelle identité est associée à la session, comme illustré dans l'exemple suivant :


```
Mar 03 15:45:51 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:30404"},"Assertions" : {"NetAddress" :
"1100.1.2.194","NullPassword" : "FALSE","bindery login" : "FALSE"}},"Target" :
{"Data" : {"ClassName" : "NCP Server","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","SubTarget" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.2.4","Name" : "AUTHENTICATE_SESSION","CorrelationID" :
"eDirectory#28#","SubEvent" : "DSE_AUTHENTICATE"},"Time" : {"Offset" :
1488536151},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Accorder l'accès à l'approbation

Cliquez sur **Accorder l'accès à l'approbation** pour générer un événement lorsqu'un accès est accordé à une approbation pour un objet, comme illustré dans l'exemple suivant :


```
Mar 03 14:33:06 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:214"}},"Target" : {"Data" : {"Attribute Name" : "Message
Server","Attribute Value" : "Attribute Read","Name" : "[Public]","SubTarget" :
"CN=raghu,OU=novell,OU=co,O=in","Syntax" : "17","Version" : "2"}},"Action" :
{"Event" : {"Id" : "0.0.1.7","Name" : "GRANT_TRUST_ACCESS","CorrelationID" :
"eDirectory#32#9a868af1-7b8d-4426-ae41-f18a869a8d7b","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1488531786},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Révoquer l'accès à l'approbation

Cliquez sur **Révoquer l'accès à l'approbation** pour générer un événement lorsque l'accès à une ressource est supprimé d'une approbation, comme illustré dans l'exemple suivant :

```
Mar 16 20:57:33 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:43936"}},"Target" : {"Data" : {"Attribute Name" :
"nsimHint","Attribute Value" : "Attribute Write, Attribute Self, Attribute Inherit
CTL","Syntax" : "17","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.1.8","Name" : "REVOKE_TRUST_ACCESS","CorrelationID" :
"eDirectory#41#156c162f-245b-4751-90da-2f166c155b24","SubEvent" :
"DSE_DELETE_VALUE"},"Time" : {"Offset" : 1489678053},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Verrouillage en cas d'intrusion

Cliquez sur **Verrouillage en cas d'intrusion** pour générer un événement lors du verrouillage d'un compte, comme illustré dans l'exemple suivant :


```
Mar 21 09:25:29 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "NET-REPORT","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" : "CN=novell-
emp222,OU=novell,OU=co,O=in","Id" : "33795"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Account Locked" : "TRUE","Attribute Name"
: "Login Intruder Address","ClassName" : "User","Intruder Address" : "TCP:
164.99.179.164:49121","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in","Reset
Time" : "03/21/17 09:27:29","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.0.9","Name" : "INTRUDER_LOCKOUT","CorrelationID" : "eDirectory#0#0ae8da6e-
208f-4c44-b515-6edae80a8f20","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" :
1490068529},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Déverrouillage du compte

Cliquez sur **Déverrouillage du compte** pour générer un événement lors du déverrouillage d'un compte verrouillé, comme illustré dans l'exemple suivant :


```
Mar 21 12:09:00 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "NET-REPORT","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "NET-REPORT","Name" :
"CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "Locked By
Intruder","Attribute Value" : "True","ClassName" : "User","Name" : "CN=novell-
emp312,OU=novell,OU=co,O=in","Syntax" : "7","Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.0.10","Name" : "ACCOUNT_UNLOCK","CorrelationID" :
"eDirectory#0#f5fdd0c4-0595-4e82-8b8f-c4d0fdf59505","SubEvent" :
"DSE_DELETE_VALUE"},"Time" : {"Offset" : 1490078340},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Accorder l'accès au compte

Cliquez sur **Accorder l'accès au compte** pour générer un événement lorsque l'accès est accordé à un compte pour un objet, comme illustré dans l'exemple suivant :

```
Mar 16 15:23:16 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Name" : "CN=admin,O=novell","Id" : "32834"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Attribute Name" : "Print Job
Configuration","Attribute Value" : "Attribute Read, Attribute Write","ClassName" :
"User","Name" : "CN=usr54412,O=novell","SubTarget" :
"CN=usr54412,O=novell","Syntax" : "17","Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.0.7","Name" : "GRANT_ACCOUNT_ACCESS","CorrelationID" :
"eDirectory#40#1718277b-ed75-41f2-8610-7b27181775ed","SubEvent" :
"DSE_ADD_VALUE"},"Time" : {"Offset" : 1489657996},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


REMARQUE : lorsqu'un compte utilisateur est considéré comme un ayant droit sur les ACL, l'événement **Accorder l'accès au compte** est généré.

Révoquer l'accès au compte

Cliquez sur **Révoquer l'accès au compte** pour générer un événement lorsqu'un objet est supprimé à partir d'un compte, comme illustré dans l'exemple suivant :


```
Mar 18 22:44:40 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:20966"}},"Target" : {"Data" : {"Attribute Name" :
"Description","Attribute Value" : "Attribute Supervisor","ClassName" :
"User","Name" : "CN=user1,O=novell","SubTarget" : "CN=pc2,O=novell","Syntax" :
"17","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.0.8","Name" :
"REVOKE_ACCOUNT_ACCESS","CorrelationID" : "eDirectory#57#67ba4065-a7de-4581-b62e-
6540ba67dea7","SubEvent" : "DSE_DELETE_VALUE"},"Time" : {"Offset" :
1489857280},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


REMARQUE : lorsqu'un compte utilisateur est considéré comme un ayant droit sur les ACL, l'événement **Révoquer l'accès au compte** est généré.

Configuration de l'audit

Cliquez sur **Configuration de l'audit** pour générer un événement lors de toute modification des paramètres qui contrôlent le service d'audit, comme illustré dans l'exemple suivant :


```
Mar 03 11:00:23 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,OU=novell,OU=co,O=in","Id" : "32863"},"Entity" : {"SysAddr" :
"100.1.2.194:64213"}},"Target" : {"Data" : {"Attribute Name" :
"xdasConfiguration","Attribute Value" :
"dsaccount=Computer$Organization$Organizational Person$Person$User$$","ClassName"
: "NCP Server","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in","Syntax" :
"3","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.9.0","Name" :
"AUDIT_CONFIG","CorrelationID" : "eDirectory#28#a56628e8-38fc-43c5-93c2-
e82866a5fc38","SubEvent" : "DSE_ADD_VALUE"},"Time" : {"Offset" : 1488519023},"Log"
: {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

Événements de gestion de service ou d'application

Cet ensemble d'événements est associé à la gestion des services ou des applications. Les services ou les applications incluent des modules, des agents et des processus en arrière-plan.

Tableau H-6 *Taxinomie des événements de gestion de service ou d'application*

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Cliquez sur
Activer le service	0.0.4.5	DSE_CHANGE_MODULE_STATE DSE_NMAS_LOG_PWD_POLICY_AGENT_REG DSE_NMAS_LOG_DIST_PWD_AGENT_REG DSE_NMAS_LOG_PWD_AGENT_REG DSE_NMAS_LOG_LTSS_AGENT_REG DSE_NMAS_LOG_PWD_CHANGE_AGENT_REG	Activer un service ou une application.	Cet événement est signalé en cas d'activation d'un service, d'une opération ou d'une fonction. Par exemple, le chargement d'un module eDirectory.
Désactiver le service	0.0.4.4	DSE_REMOTE_SERVER_DOWN DSE_CHANGE_MODULE_STATE DSE_NMAS_LOG_PWD_POLICY_AGENT_DEREG DSE_NMAS_LOG_DIST_PWD_AGENT_DEREG DSE_NMAS_LOG_PWD_AGENT_DEREG DSE_NMAS_LOG_LTSS_AGENT_DEREG DSE_NMAS_LOG_PWD_CHANGE_AGENT_DEREG	Désactiver un service ou une application.	Cet événement est signalé en cas de désactivation d'un service, d'une opération ou d'une fonction. Par exemple, le déchargement d'un module eDirectory.
Invoquer le service	0.0.5.0	DSE_BACKLINK_PROC_DONE DSE_LIMBER_DONE DSE_MOVE_TREE_START DSE_PURGE_START DSE_RECV_REPLICA_UPDATES DSE_SEND_REPLICA_UPDATES DSE_START_JOIN DSE_START_UPDATE_REPLICA DSE_START_UPDATE_SCHEMA DSE_SYNC_PART_START DSE_SYNC_SVR_OUT_START	Invoquer un service ou une application.	Cet événement est signalé lorsqu'un service lié à la sécurité est invoqué. Par exemple, le déclenchement d'un processus en arrière-plan.

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Cliquez sur
Terminer le service	0.0.5.1	DSE_REMOVE_ATTR_DEF DSE_ABORT_JOIN DSE_END_UPDATE_REPLICA DSE_END_UPDATE_SCHEMA DSE_JOIN_DONE DSE_MOVE_TREE_END DSE_PURGE_END DSE_SCHEMA_SYNC DSE_SYNC_PART_END DSE_SYNC_SVR_OUT_END	Arrêter un service ou une application.	Cet événement est signalé en cas d'arrêt d'un service. Par exemple, l'arrêt d'un processus en arrière-plan.
Modifier la configuration du service	0.0.4.2	DSE_ALLOW_LOGIN DSE_UPDATE_REPLICA DSE_EBA_MOVE_EBA_CA DSE_GEN_CA_KEYS DSE_RECERT_PUB_KEY DSE_EBA_REQ_BA_MATERIAL DSE_EBA_REQ_SERVER_BA_MATERIAL DSE_NAME_COLLISION DSE_SERVER_RENAME DSE_SERVER_ADDRESS_CHANGE DSE_SYNC_PARTITION DSE_SYNC_SCHEMA DSE_EBA_ENABLE_PURE_MODE DSE_EBA_ISSUE_NCPCA_CERT DSE_EBA_REVOKE_NCPCA_CERT	Modification des données de configuration associées à un service eDirectory.	Cet événement est signalé en cas de modification des données de configuration. Par exemple, toute modification apportée à la configuration EBA déclenche cet événement.

Exemples d'événements de gestion de service ou d'application

Les sections suivantes présentent des exemples d'événements liés à la gestion des services ou des applications.

- « Activer le service » page 928
- « Désactiver le service » page 928
- « Invoquer le service » page 928

- « Terminer le service » page 928
- « Modifier la configuration du service » page 929

Activer le service

Cliquez sur **Activer le service** pour générer un événement lorsqu'un service, une opération ou une fonction est activée, comme illustré dans l'exemple suivant :


```
Mar 07 10:03:15 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "1100.1.2.194:0"}},"Target" : {"Data" : {"Module State" : "Loaded","Name" :
"libxdasauditds.so","Version" : "2"}},"Action" : {"Event" : {"Id" :
"0.0.4.5","Name" : "ENABLE_SERVICE","CorrelationID" :
"eDirectory#4294967295#","SubEvent" : "DSE_CHANGE_MODULE_STATE"},"Time" :
{"Offset" : 1488861195},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome"
: "0"}}
```


Désactiver le service

Cliquez sur **Désactiver le service** pour générer un événement lorsqu'une opération, une fonction ou un service est désactivé, comme illustré dans l'exemple suivant :


```
Mar 10 11:00:07 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"Module State" : "Unloading","Name" : "libsnmpinst.so","Version" :
"2"}},"Action" : {"Event" : {"Id" : "0.0.4.4","Name" :
"DISABLE_SERVICE","CorrelationID" : "eDirectory#4294967295#","SubEvent" :
"DSE_CHANGE_MODULE_STATE"},"Time" : {"Offset" : 1489123807},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Invoquer le service

Cliquez sur **Invoquer le service** pour générer un événement lorsqu'un service de sécurité pertinent est invoqué, comme illustré dans l'exemple suivant :


```
Mar 03 14:41:44 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.5.0","Name" : "INVOKE_SERVICE","CorrelationID" :
"eDirectory#0#","SubEvent" : "DSE_SYNC_PART_START"},"Time" : {"Offset" :
1488532304},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Terminer le service

Cliquez sur **Terminer le service** pour générer un événement de fin d'un service, comme illustré dans l'exemple suivant :

```
Mar 03 14:41:44 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "LNX-TREE-BUILD101","Name" : "CN=SLES12-194-
12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr" : "100.1.2.194","SysName" :
"SLES12-194-12"}},"Initiator" : {"Account" : {"Domain" : "LNX-TREE-
BUILD101","Name" : "CN=SLES12-194-12,OU=novell,OU=co,O=in"},"Entity" : {"SysAddr"
: "100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.5.1","Name" : "TERMINATE_SERVICE","CorrelationID" :
"eDirectory#0#","SubEvent" : "DSE_SYNC_PART_END"},"Time" : {"Offset" :
1488532304},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Modifier la configuration du service

Cliquez sur **Modifier la configuration du service** pour générer un événement signalé lors de la modification des données de configuration, comme illustré dans l'exemple suivant :


```
Mar 16 21:07:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" :
"100.1.2.194:40159"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.4.2","Name" : "MODIFY_SERVICE_CONFIG","CorrelationID" :
"eDirectory#34#","SubEvent" : "DSE_SYNC_PARTITION"},"Time" : {"Offset" :
1489678666},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Événements opérationnels

Très rarement générés, les événements opérationnels sont considérés comme importants. Par exemple, l'arrêt d'un serveur essentiel pour l'entreprise est exceptionnel, car cette opération est impossible sans avoir obtenu l'autorisation d'une personne.

Tableau H-7 *Taxinomie des événements opérationnels*

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Utilisation
Démarrer le système	0.0.8.0	DSE_AGENT_OPEN_LOCAL DSE_RELOAD_DS	Démarrer un système	Cet événement est signalé lorsqu'un serveur, un système ou une application essentielle démarre.
Arrêter le système	0.0.8.1	DSE_AGENT_CLOSE_LOCAL	Arrêter un système	Cet événement est signalé lorsqu'un serveur, un système ou une application essentielle s'arrête.
Sauvegarder la zone de stockage de données	0.0.8.4	DSE_BACKUP_ENTRY	Sauvegarder la zone de stockage de données	Cet événement est signalé lorsqu'un serveur, un système ou une application essentielle sauvegarde une zone de stockage de données importante.

Nom de l'événement	Identificateur de l'événement	Événement eDir correspondant	Description	Utilisation
Récupérer la zone de stockage de données	0.0.8.5	DSE_RESTORE_ENTRY	Récupérer la zone de stockage de données	Cet événement est signalé lorsqu'un serveur, un système ou une application essentielle restaure une zone de stockage de données importante.
Opérations internes	0.1.0.3.0.0	DSE_CRC_FAILURE DSE_DELETE_SUBTREE DSE_DELETE_UNUSED_EXTREF DSE_DSA_BAD_VERB DSE_LOST_ENTRY DSE_NEW_SCHEMA_EPOCH DSE_NO_REPLICA_PTR DSE_PURGE_ENTRY_FAIL DSE_EBA_ISSUE_CRL	Événement relatif au fonctionnement d'un service ou d'une application.	Utilisé pour la consignation des événements générés par des opérations internes d'eDirectory.
Modifier le contexte du processus	0.0.4.3	DSE_PARTITION_STATE_CHG DSE_LDAP_MODLDAPSERVER DSE_PART_STATE_CHG_REQ DSE_REPAIR_TIME_STAMPS DSE_RESET_DS_COUNTERS DSE_SET_NEW_MASTER DSE_SYNTHETIC_TIME DSE_SPLIT_DONE DSE_SPLIT_PARTITION DSE_JOIN_PARTITIONS DSE_ABORT_PARTITION_OP DSE_LOW_LEVEL_JOIN	Modifier un contexte de traitement	Cet événement est signalé en cas de modification de tout attribut d'un contexte de processus. Par exemple, la création d'une partition déclenche cet événement.

Exemples d'événements exceptionnels

Les sections suivantes présentent des exemples pour les événements exceptionnels.

- « Démarrer le système » page 931
- « Arrêter le système » page 931
- « Sauvegarder le stockage de données » page 931
- « Récupérer la zone de stockage de données » page 931

- « Opérations internes » page 932
- « Modifier le contexte du processus » page 932

Démarrer le système

Cliquez sur **Démarrer le système** pour générer un événement lorsqu'un serveur, un système ou une application essentielle démarre, comme illustré dans l'exemple suivant :


```
Mar 13 11:20:24 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.8.0","Name" :
"START_SYSTEM","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_AGENT_OPEN_LOCAL"},"Time" : {"Offset" : 1489384224},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Arrêter le système

Cliquez sur **Arrêter le système** pour générer un événement lorsqu'un serveur, un système ou une application essentielle s'arrête, comme illustré dans l'exemple suivant :


```
Mar 13 11:16:23 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.8.1","Name" :
"SHUTDOWN_SYSTEM","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_AGENT_CLOSE_LOCAL"},"Time" : {"Offset" : 1489383983},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Sauvegarder le stockage de données

Cliquez sur **Sauvegarder le stockage de données** pour générer un événement lorsqu'un serveur, un système ou une application essentielle sauvegarde une zone de stockage de données, comme illustré dans l'exemple suivant :


```
Mar 14 13:03:29 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:13018"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.8.4","Name" : "BACKUP_DATA_STORE","CorrelationID" :
"eDirectory#43#","SubEvent" : "DSE_BACKUP_ENTRY"},"Time" : {"Offset" :
1489476809},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Récupérer la zone de stockage de données

Cliquez sur **Récupérer le stockage de données** pour générer un événement lorsqu'un serveur, un système ou une application essentielle récupère une zone de stockage de données, comme illustré dans l'exemple suivant :

```
Mar 14 14:16:02 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Name" :
"CN=admin,O=novell","Id" : "32872"},"Entity" : {"SysAddr" :
"100.1.2.194:10203"}},"Target" : {"Data" : {"Name" : "OU=users,O=novell","Version"
: "2"}},"Action" : {"Event" : {"Id" : "0.0.8.5","Name" :
"RECOVER_DATA_STORE","CorrelationID" : "eDirectory#36#bd5cb85b-0f9f-4268-a221-
5bb85cbd9f0f","SubEvent" : "DSE_RESTORE_ENTRY"},"Time" : {"Offset" :
1489481162},"Log" : {"Severity" : 7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Opérations internes

Cliquez sur **Opérations internes** pour générer cet événement lorsque des événements de consignation sont générés par les opérations internes d'eDirectory, comme illustré dans l'exemple suivant :


```
Mar 15 13:45:13 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "VLV_MEM","Name" : "CN=stdir-vm-53,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "stdir-vm-
53.labs.blr.novell.com"}},"Initiator" : {"Account" : {"Domain" : "VLV_MEM","Name" :
"CN=stdir-vm-53,O=novell"},"Entity" : {"SysAddr" : "100.1.2.194:0"}},"Target" :
{"Data" : {"ValidityEnd" : "03/16/2017 01:45:13 PM","ValidityStart" : "03/15/2017
01:45:13 PM","Version" : "2"}},"Action" : {"Event" : {"Id" : "0.0.12.2","Name" :
"INTERNAL_OPERATIONS","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_EBA_ISSUE_CRL"},"Time" : {"Offset" : 1489565713},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```


Modifier le contexte du processus

Cliquez sur **Modifier le contexte du processus** pour générer un événement en cas de modification d'attributs d'un contexte de processus, comme illustré dans l'exemple suivant :


```
Mar 16 21:07:46 eDirectory : INFO {"Source" : "eDirectory#DS","Observer" :
{"Account" : {"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" :
{"SysAddr" : "100.1.2.194","SysName" : "SLE12-142"}},"Initiator" : {"Account" :
{"Domain" : "TREEUPGRADE","Name" : "CN=SLE12-142,O=novell"},"Entity" : {"SysAddr" :
"100.1.2.194:0"}},"Target" : {"Data" : {"Version" : "2"}},"Action" : {"Event" :
{"Id" : "0.0.5.3","Name" : "MODIFY_PROCESS_CONTEXT","CorrelationID" :
"eDirectory#0#042b517b-41c4-4c9b-b5b5-7b512b04c441","SubEvent" :
"DSE_PARTITION_STATE_CHG"},"Time" : {"Offset" : 1489678666},"Log" : {"Severity" :
7},"Outcome" : "0","ExtendedOutcome" : "0"}}
```

Assignation d'événements eDirectory à des événements CEF

Cette section contient les informations suivantes :

- « Assignation d'événements eDirectory à des événements CEF » page 933
- « Événements CEF » page 938

Assignation d'événements eDirectory à des événements CEF

Le Tableau I-1 répertorie les événements internes eDirectory assignés aux événements CEF correspondants. Pour plus d'informations sur les événements eDirectory et leur description, reportez-vous à la page des services eDirectory. Pour plus d'informations sur les événements CEF, reportez-vous à la section « Événements CEF » page 938.

Tableau I-1 *Événements CEF assignés à des événements eDirectory*

Catégorie d'événement	Événement CEF	Événement eDirectory
Sécurité	CONNECTION Pour obtenir un exemple de cet événement, reportez-vous à la section « Connexion » page 938.	DSE_CONNECTION
Sécurité	LOGIN Pour obtenir un exemple de cet événement, reportez-vous à la section « Connexion » page 939.	DSE_LOGIN_EX DSE_NMAS_LOG_SRVR_BEGIN_LOGIN DSE_NMAS_LOG_FINISH_LOGIN_STATUS DSE_NMAS_LOG_SASL_MECHANISM_RESULT DSE_EBA_REQ_BA_MATERIAL
Sécurité	LOGOUT Pour obtenir un exemple de cet événement, reportez-vous à la section « Déconnexion » page 939.	DSE_LOGOUT
Sécurité	ADD_MEMBER Pour obtenir un exemple de cet événement, reportez-vous à la section « Ajout d'un membre » page 939.	DSE_ADD_VALUE

Catégorie d'événement	Événement CEF	Événement eDirectory
Sécurité	DELETE_MEMBER Pour obtenir un exemple de cet événement, reportez-vous à la section « Supprimer le membre » page 940.	DSE_DELETE_VALUE
Sécurité	INTRUDER_DETECTED Pour obtenir un exemple de cet événement, reportez-vous à la section « Intrusion détectée » page 940.	DSE_ADD_VALUE
Sécurité	ACCOUNT_UNLOCK Pour obtenir un exemple de cet événement, reportez-vous à la section « Déverrouillage du compte » page 940.	DSE_DELETE_VALUE
Sécurité	LOGIN_DISABLED Pour obtenir un exemple de cet événement, reportez-vous à la section « Connexion désactivée » page 940.	DSE_ADD_VALUE
Sécurité	LOGIN_ENABLED Pour obtenir un exemple de cet événement, reportez-vous à la section « Connexion activée » page 941.	DSE_DELETE_VALUE
Sécurité	ACL_CHANGED Pour obtenir un exemple de cet événement, reportez-vous à la section « ACL modifiée » page 941.	DSE_ADD_VALUE DSE_DELETE_VALUE
Sécurité	CHANGE_SECURITY_EQUALS Pour obtenir un exemple de cet événement, reportez-vous à la section « Changer les équivalents de sécurité » page 941.	DSE_ADD_VALUE DSE_DELETE_VALUE
Sécurité	VERIFY_PASSWORD Pour obtenir un exemple de cet événement, reportez-vous à la section « Vérifier le mot de passe » page 942.	DSE_VERIFY_PASS
Sécurité	AUDIT_CONFIG Pour obtenir un exemple de cet événement, reportez-vous à la section « Configuration de l'audit » page 942.	DSE_ADD_VALUE DSE_DELETE_VALUE

Catégorie d'événement	Événement CEF	Événement eDirectory
Sécurité	CHANGE_PASSWORD Pour obtenir un exemple de cet événement, reportez-vous à la section « Changer le mot de passe » page 942.	DSE_CHGPASS DSE_NMAS_LOG_SET_PWD DSE_NMAS_LOG_SET_DIST_PWD DSDSE_NMAS_LOG_DELETE_PWD DSE_NMAS_LOG_DELETE_DIST_PWD DSE_NMAS_LOG_CHANGE_PWD DSE_NMAS_LOG_DELETE_ALL_LOGIN_SECRET DSE_NMAS_LOG_SET_LOGIN_SECRET DSE_NMAS_LOG_DELETE_LOGIN_SECRET
Sécurité	CHANGE_LOGIN_CONFIG Pour obtenir un exemple de cet événement, reportez-vous à la section « Changer la configuration de la connexion » page 942.	DSE_NMAS_LOG_SET_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_LOGIN_CONFIG DSE_NMAS_LOG_DELETE_ALL_LOGIN_CONFIG
Sécurité	QUERY_CREDENTIALS Pour obtenir un exemple de cet événement, reportez-vous à la section « Références de requête » page 943.	DSE_NMAS_LOG_GET_PWD_HISTORY DSE_NMAS_LOG_GET_PWD DSE_NMAS_LOG_GET_LOGIN_CONFIG DSE_NMAS_LOG_CHECK_PWD_SYNTAX_POLICY DSE_NMAS_LOG_GET_ALL_LOGIN_SECRET DSE_NMAS_LOG_GET_PWD_STATUS DSE_NMAS_LOG_GET_ALL_LOGIN_CONFIG DSE_NMAS_LOG_GET_DIST_PWD DSE_NMAS_LOG_GET_PWD_HISTORY
Sécurité	IMPERSONATE Pour obtenir un exemple de cet événement, reportez-vous à la section « Emprunter l'identité » page 943.	DSE_IMPERSONATE
Sécurité	AUTHENTICATE Pour obtenir un exemple de cet événement, reportez-vous à la section « Authentification » page 943.	DSE_AUTHENTICATE
Objets	CREATE_OBJECT Pour obtenir un exemple de cet événement, reportez-vous à la section « Créer un objet » page 944.	DSE_CREATE_ENTRY DSE_ADD_ENTRY

Catégorie d'événement	Événement CEF	Événement eDirectory
Objets	DELETE_OBJECT Pour obtenir un exemple de cet événement, reportez-vous à la section « Supprimer l'objet » page 944.	DSE_REMOVE_ENTRY
Objets	RENAME_OBJECT Pour obtenir un exemple de cet événement, reportez-vous à la section « Renommer l'objet » page 944	DSE_RENAME_ENTRY
Objets	MOVE_OBJECT Pour obtenir un exemple de cet événement, reportez-vous à la section « Déplacer l'objet » page 945.	DSE_MOVE_SOURCE_ENTRY DSE_MOVE_DEST_ENTRY
Objets	DSA_READ Pour obtenir un exemple de cet événement, reportez-vous à la section « DSU lu » page 945.	DSE_DSA_READ
Objets	SEARCH Pour obtenir un exemple de cet événement, reportez-vous à la section « Rechercher » page 945.	DSE_SEARCH
Attributs	READ_ATTRIBUTE Pour obtenir un exemple de cet événement, reportez-vous à la section « Lire l'attribut » page 946.	DSE_READ_ATTR
Attributs	DELETE_ATTRIBUTE Pour obtenir un exemple de cet événement, reportez-vous à la section « Supprimer l'attribut » page 946.	DSE_DELETE_ATTRIBUTE
Attributs	ADD_VALUE Pour obtenir un exemple de cet événement, reportez-vous à la section « Ajouter une valeur » page 946.	DSE_ADD_VALUE
Attributs	DELETE_VALUE	DSE_DELETE_VALUE
Attributs	COMPARE_ATTRIBUTE_VALUE Pour obtenir un exemple de cet événement, reportez-vous à la section « Comparer la valeur de l'attribut » page 947.	DSE_COMPARE_ATTR_VALUE
LDAP	LDAP_BIND LDAP_UNBIND	DSE_LDAP_BIND DSE_LDAP_UNBIND

Catégorie d'événement	Événement CEF	Événement eDirectory
	LDAP_CONNECTION	DSE_LDAP_CONNECTION
	LDAP_SEARCH	DSE_LDAP_SEARCH
	LDAP_ADD	DSE_LDAP_ADD
	LDAP_COMPARE	DSE_LDAP_COMPARE
	LDAP_MODIFY	DSE_LDAP_MODIFY
	LDAP_DELETE	DSE_LDAP_DELETE
	LDAP_MODIFY_DN	DSE_LDAP_MODDN
	LDAP_ABANDON	DSE_LDAP_ABANDON
	LDAP_EXTENDED_OPERATION	DSE_LDAP_EXTOP
	LDAP_SYSTEM_EXTENDED_OPERATION	DSE_LDAP_SYSEXTOP
	LDAP_PASSWORD_MODIFY	DSE_LDAP_PASSWDMODIFY
	MODIFY_LDAP_SERVER_CONFIGURATION	DSE_LDAP_MODLDAPSERVER
	UNKNOWN_LDAP_OPERATION	DSE_LDAP_UNKNOWNOP
	LDAP_BIND_RESPONSE	DSE_LDAP_BINDRESPONSE
	LDAP_SEARCH_RESPONSE	DSE_LDAP_SEARCHRESPONSE
	LDAP_SEARCH_ENTRY_RESPONSE	DSE_LDAP_SEARCHENTRYRESPONSE
	LDAP_ADD_RESPONSE	DSE_LDAP_ADDRESPONSE
	LDAP_COMPARE_RESPONSE	DSE_LDAP_COMPARERESPONSE
	LDAP_MODIFY_RESPONSE	DSE_LDAP_MODIFYRESPONSE
	LDAP_DELETE_RESPONSE	DSE_LDAP_DELETERESPONSE
	LDAP_MODIFY_DN_RESPONSE	DSE_LDAP_MODDNRESPONSE
	LDAP_EXTENDED_OPERATION_RESPONSE	DSE_LDAP_EXTOP_RESPONSE
EBA	MODIFY_SERVICE_CONFIG	DSE_EBA_ISSUE_NCPCA_CERT
	Pour obtenir un exemple de cet événement, reportez-vous à la section « Modifier la configuration du service » page 947.	DSE_EBA_REVOKE_NCPCA_CERT
		DSE_EBA_MOVE_EBA_CA
		DSE_EBA_ISSUE_CRL
		DSE_EBA_REQ_SERVER_BA_MATERIAL

Événements CEF

Les événements CEF sont classés dans les catégories suivantes :

- « Événements de sécurité » page 938
- « Événements d'objets » page 944
- « Événements d'attributs » page 946
- « Événements EBA » page 947

Événements de sécurité

Les événements de cet ensemble ne sont applicables que dans le cadre d'opérations d'audit de sécurité d'eDirectory. Une opération de sécurité peut accorder/révoquer un accès ou une connexion, mais aussi autoriser/refuser une requête ou une modification de mot de passe. Cet ensemble d'événements aide également à détecter les tentatives d'intrusion sur le système eDirectory.

Exemples d'événements de sécurité :

Cette section inclut des exemples pour les événements de sécurité suivants :

- « Connexion » page 938
- « Connexion » page 939
- « Déconnexion » page 939
- « Ajout d'un membre » page 939
- « Supprimer le membre » page 940
- « Intrusion détectée » page 940
- « Déverrouillage du compte » page 940
- « Connexion désactivée » page 940
- « Connexion activée » page 941
- « ACL modifiée » page 941
- « Changer les équivalents de sécurité » page 941
- « Vérifier le mot de passe » page 942
- « Configuration de l'audit » page 942
- « Changer le mot de passe » page 942
- « Changer la configuration de la connexion » page 942
- « Références de requête » page 943
- « Emprunter l'identité » page 943
- « Authentification » page 943

REMARQUE : les exemples contenus dans les sections suivantes sont uniquement fournis à titre de référence.

Connexion

Cliquez sur **Connexion** pour générer un événement lors de la création d'un canal de communication entre les composants du système, comme illustré dans l'exemple suivant :

```
Oct 31 17:00:22 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035E|CONNECTION|0|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 31 2017 17:00:22 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.164 spt=23017 duser=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
cn1Label=Connection ID cn1=246358976 cn2Label=Created(1)/Terminated(0) cn2=1
cs1Label=Client Address cs1=164.99.179.164:23017 cs2Label=Module cs2=LDAP Server
cs3Label=Tree Name cs3=TEST-CEF-AGN cs4Label=Correlation ID
cs4=eDirectory#4294967295# flexString2Label=SubEvent flexString2=DSE_CONNECTION
cat=Security reason=0 outcome=Success
```

Connexion

Cliquez sur **Connexion** pour générer un événement lors de la création d'une session. Par exemple, une connexion au système eDirectory.

```
Oct 31 17:00:22 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035C|LOGIN|1|dvc=164.99.179.194 dvchost=SLES12SP2-
194 rt=Oct 31 2017 17:00:22 dtz=IST sourceServiceName=CN\=SLES12SP2-
194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS src=164.99.179.164 spt=59737
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=admin,OU\=novell,OU\=co,O\=in
cs1Label=Client Address cs1=164.99.179.164:59737 cs2Label=Class Name cs2=User
cs3Label=Tree Name cs3=TEST-CEF-AGN cs4Label=Correlation ID cs4=nmas#262183#
cs6Label=Server Name cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
flexString1Label=Login Method flexString1=0 flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_FINISH_LOGIN_STATUS flexNumber2Label=Grouping
flexNumber2=386 cat=Security reason=0 outcome=Success
```

Déconnexion

Cliquez sur **Déconnexion** pour générer un événement lors de l'arrêt d'une session existante. Par exemple, une déconnexion du système eDirectory.

```
Jan 09 18:34:15 eDirectory
CEF:0|NetIQ|eDirectory|9.1|CEF0B0303|LOGOUT|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 03 2017 13:10:32 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.44.5 spt=53738 suser=[Public] duser=CN\=SLES12SP2-
194,OU\=server,OU\=co,O\=in cs1Label=Client Address cs1=164.99.44.5 cs2Label=Class
Name cs2=User cs3Label=Tree Name cs3=TEST-CEF-NOV3 cs4Label=Correlation ID
cs4=eDirectory#17# cs6Label=Object DN cs6=CN\=admin,OU\=novell,OU\=co,O\=in
flexString2Label=SubEvent flexString2=DSE_LOGOUT flexNumber2Label=Grouping
flexNumber2=127 cat=Security reason=0 outcome=Success
```

Ajout d'un membre

Cliquez sur **Ajouter un membre** pour générer un événement lors de l'ajout d'un utilisateur au groupe, comme illustré dans l'exemple suivant :

```
Jan 09 18:34:15 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0336|ADD_MEMBER|1|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:34:15 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=grp1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=Group cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#bc560efc-53d4-4ad9-
85b4-fc0e56bcd453 cs6Label=Member DN cs6=CN\=lynx-user,OU\=lnx-
users,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent flexString2=DSE_ADD_VALUE
flexNumber2Label=Grouping flexNumber2=3676 cat=Security reason=0 outcome=Success
```

Supprimer le membre

Cliquez sur **Supprimer le membre** pour générer un événement lors de la suppression d'un utilisateur du groupe, comme illustré dans l'exemple suivant :

```
Jan 09 18:35:06 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0337|DELETE_MEMBER|1|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:35:06 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=grp1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=Group cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#9136617f-4412-48da-
bf33-7f6136911244 cs6Label=Member DN cs6=CN\=lynx-user,OU\=lnx-
users,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_DELETE_VALUE flexNumber2Label=Grouping flexNumber2=3687
cat=Security reason=0 outcome=Success
```

Intrusion détectée

Cliquez sur **Intrus détecté** pour générer un événement lors de la détection d'un intrus, comme illustré dans l'exemple suivant :

```
Jan 09 18:35:06 eDirectory
CEF:0|NetIQ|eDirectory|9.1|CEF0B0357|INTRUDER_DETECTED|5|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 17 2017 19:50:20 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=0 suser=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
duser=CN\=raghu,OU\=lens,OU\=QA,OU\=HD,OU\=DSLR,OU\=SLR,OU\=digital,OU\=camera,O\=
sony,L\=tokyo,dc\=co,C\=jp cs1Label=Intruder Address cs1=TCP: 164.99.179.164:33584
cs2Label=Reset Time cs2=10/17/17 19:52:20 cs3Label=Tree Name cs3=TEST-CEF222
cs4Label=Correlation ID cs4=eDirectory#0#349e5670-0b80-4c99-b7f0-70569e34800b
cs6Label=Class cs6=User flexString2Label=SubEvent flexString2=DSE_ADD_VALUE
flexNumber2Label=Grouping flexNumber2=102 cat=Security reason=0 outcome=Success
```

Déverrouillage du compte

Cliquez sur **Déverrouillage du compte** pour générer un événement lors du déverrouillage d'un compte verrouillé, comme illustré dans l'exemple suivant :

```
Jan 09 19:10:32 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B035F|ACCOUNT_UNLOCK|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 19:10:32 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.156 spt=0 suser=CN\=SLES12-SP3-156,OU\=lnx-
server,OU\=server,OU\=co,O\=in duser=CN\=rr,OU\=lnx-users,OU\=novell,OU\=co,O\=in
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=NEW-TREE-9th
cs4Label=Correlation ID cs4=eDirectory#0#ad3a0226-764e-488c-b90a-26023aad4e76
flexString2Label=SubEvent flexString2=DSE_DELETE_VALUE flexNumber2Label=Grouping
flexNumber2=122 cat=Security reason=0 outcome=Success
```

Connexion désactivée

Cliquez sur **Connexion désactivée** pour générer un événement lors de la désactivation d'un compte utilisateur, comme illustré dans l'exemple suivant :

```
Jan 09 18:18:48 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0356|LOGIN_DISABLED|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:18:48 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=lynx-user1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#f04b6deb-df9b-4f4b-
a8e8-eb6d4bf09bdf flexString2Label=SubEvent flexString2=DSE_ADD_VALUE
flexNumber2Label=Grouping flexNumber2=100 cat=Security reason=0 outcome=Success
```

Connexion activée

Cliquez sur **Connexion activée** pour générer un événement lors de l'activation d'un compte utilisateur désactivé, comme illustré dans l'exemple suivant :

```
Jan 09 18:18:56 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0355|LOGIN_ENABLED|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:18:56 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=54936
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=lynx-user1,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User cs3Label=Tree Name
cs3=NEW-TREE-9th cs4Label=Correlation ID cs4=eDirectory#14#f99f0883-251e-424e-
a724-83089ff91e25 flexString2Label=SubEvent flexString2=DSE_DELETE_VALUE
flexNumber2Label=Grouping flexNumber2=107 cat=Security reason=0 outcome=Success
```

ACL modifiée

Cliquez sur **ACL modifiée** pour générer un événement en cas de modification d'une ACL sur un objet, comme illustré dans l'exemple suivant :

```
Jan 09 18:04:56 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0354|ACL_CHANGED|3|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:04:56 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.158 spt=52120
suser=CN\=admin,OU\=novell,OU\=co,O\=in duser=CN\=lynx-user,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cn1Label=ACL Added cn1=1 cs1Label=Value cs1=Entry
ID: .CN\=lynx-user.OU\=lnx-users.OU\=novell.OU\=co.O\=in.T\=NEW-TREE-9th.,
Attribute ID: [All Attributes Rights], Privileges: Attribute Read cs2Label=Class
Name cs2=User cs3Label=Tree Name cs3=NEW-TREE-9th cs4Label=Correlation ID
cs4=eDirectory#18#c4f344f7-db17-4366-8a19-f744f3c417db cs6Label=Trustee
cs6=CN\=lynx-user,OU\=lnx-users,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping flexNumber2=83 cat=Security
reason=0 outcome=Success
```

Changer les équivalents de sécurité

Cliquez sur **Changer les équivalents de sécurité** pour générer un événement en cas de modification des équivalents de sécurité sur un objet, comme illustré dans l'exemple suivant :

```
Jan 09 18:29:38 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0341|CHANGE_SECURITY_EQUALS|3|dvc=164.99.179.
156 dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:29:38 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.156 spt=0 suser=CN\=SLES12-SP3-156,OU\=lnx-
server,OU\=server,OU\=co,O\=in duser=CN\=raghu,OU\=lnx-
users,OU\=novell,OU\=co,O\=in cn1Label=Add/Remove cn1=1 cs2Label=Class Name
cs2=User cs3Label=Tree Name cs3=NEW-TREE-9th cs4Label=Correlation ID
cs4=eDirectory#0#6d1355d0-0401-4858-8475-d055136d0104 cs6Label=Equivalent DN
cs6=CN\=grp,OU\=novell,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping flexNumber2=3639 cat=Security
reason=0 outcome=Success
```

Vérifier le mot de passe

Cliquez sur **Vérifier le mot de passe** pour générer un événement lors de la vérification du mot de passe d'un compte.

Configuration de l'audit

Cliquez sur **Configuration de l'audit** pour générer un événement lors de toute modification des paramètres qui contrôlent le service d'audit, comme illustré dans l'exemple suivant :

```
Jan 09 18:27:12 eDirectory
CEF:0|eDirectory|eDirectory|9.1|CEF0B0006|AUDIT_CONFIG|2|dvc=164.99.179.156
dvchost=SLES12-SP3-156.labs.blr.novell.com rt=Jan 09 2018 18:27:12 dtz=IST
sourceServiceName=CN\=SLES12-SP3-156,OU\=lnx-server,OU\=server,OU\=co,O\=in
sproc=eDirectory#DS src=164.99.179.160 spt=54980 suser=CN\=srv-
160,OU\=server,OU\=co,O\=in duser=CN\=SLES12-SP3-156,OU\=lnx-
server,OU\=server,OU\=co,O\=in cs1Label=Attribute Value cs1=cefEvents\=ACL_CHANGED
$$QUERY_CREDENTIALS cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name cs3=NEW-
TREE-9th cs4Label=Correlation ID cs4=eDirectory#16#8dcd3ede-baf8-4e71-9f1e-
de3ecd8df8ba cs6Label=Attribute Name cs6=cefConfiguration
flexString2Label=SubEvent flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping
flexNumber2=3631 cat=Security reason=0 outcome=Success
```

Changer le mot de passe

Cliquez sur **Changer le mot de passe** pour générer un événement lors du changement de mot de passe d'un compte, comme illustré dans l'exemple suivant :

```
Oct 31 17:06:11 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0290064|CHANGE_PASSWORD|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Oct 31 2017 17:06:11 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=raghu,novell,co,in cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TEST-
CEF-AGN cs4Label=Correlation ID cs4=nmas#0# cs6Label=Server Name
cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_SET_LOGIN_SECRET flexNumber2Label=Grouping
flexNumber2=405 cat=Security reason=0 outcome=Success
```

Changer la configuration de la connexion

Cliquez sur **Changer la configuration de la connexion** pour générer un événement lors d'un changement de configuration de la connexion du compte, comme illustré dans l'exemple suivant :

```
Nov 02 10:21:00 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0290061|CHANGE_LOGIN_CONFIG|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:21:00 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=raghu,novell,co,in cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TEST-
CEF-AGN cs4Label=Correlation ID cs4=nmas#0# cs6Label=Server Name
cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_SET_LOGIN_CONFIG flexNumber2Label=Grouping
flexNumber2=2034 cat=Security reason=0 outcome=Success
```

Références de requête

Cliquez sur **Références de requête** pour générer un événement lors d'une requête d'obtention des références d'un compte en particulier, comme illustré dans l'exemple suivant :

```
Nov 02 10:21:00 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0290062|QUERY_CREDENTIALS|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:21:00 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#NMAS
src=164.99.179.194 spt=0 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=raghu,novell,co,in cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TEST-
CEF-AGN cs4Label=Correlation ID cs4=nmas#0# cs6Label=Server Name
cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent
flexString2=DSE_NMAS_LOG_GET_LOGIN_CONFIG flexNumber2Label=Grouping
flexNumber2=2035 cat=Security reason=0 outcome=Success
```

Emprunter l'identité

Cliquez sur **Emprunter l'identité** pour générer un événement en cas d'emprunt d'identité pour un compte, comme illustré dans l'exemple suivant :

```
Nov 02 10:29:38 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0231|IMPERSONATE|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:29:38 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=56451 suser=CN\=admin,OU\=novell,OU\=co,O\=in
duser=CN\=raghu,OU\=novell,OU\=co,O\=in cs3Label=Tree Name cs3=TEST-CEF-AGN
cs4Label=Correlation ID cs4=eDirectory#10# cs6=CN\=SLES12SP2-
194,OU\=server,OU\=co,O\=in flexString2Label=SubEvent flexString2=DSE_IMPERSONATE
flexNumber2Label=Grouping flexNumber2=2048 cat=Security reason=0 outcome=Success
```

Authentification

Cliquez sur **Authentifier** pour générer un événement lorsqu'un utilisateur s'authentifie pour ouvrir une session, comme illustré dans l'exemple suivant :

```
Nov 02 10:32:39 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B035D|AUTHENTICATE|1|dvc=164.99.179.194
dvchost=SLES12SP2-194 rt=Nov 02 2017 10:32:39 dtz=IST
sourceServiceName=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in sproc=eDirectory#DS
src=164.99.179.194 spt=0 suser=CN\=impuser,OU\=novell,OU\=co,O\=in
duser=CN\=impuser,OU\=novell,OU\=co,O\=in cs2Label=Class Name cs2=User
cs3Label=Tree Name cs3=TEST-CEF-AGN cs4Label=Correlation ID cs4=eDirectory#12#
cs6Label=Server Name cs6=CN\=SLES12SP2-194,OU\=server,OU\=co,O\=in
flexString2Label=SubEvent flexString2=DSE_AUTHENTICATE flexNumber2Label=Grouping
flexNumber2=2058 cat=Security reason=0 outcome=Success
```

Événements d'objets

Cet ensemble d'événements s'applique aux opérations associées à l'objet Audit d'eDirectory. Une opération de type objet peut créer, supprimer, renommer, déplacer ou interroger des objets.

Exemples d'événements d'objets :

Cette section fournit des exemples pour les événements d'objets suivants :

- « Créer un objet » page 944
- « Supprimer l'objet » page 944
- « Renommer l'objet » page 944
- « Déplacer l'objet » page 945
- « DSU lu » page 945
- « Rechercher » page 945

REMARQUE : les exemples contenus dans les sections suivantes sont uniquement fournis à titre de référence.

Créer un objet

Cliquez sur **Créer un objet** pour générer un événement lors de la création d'un objet dans l'arborescence eDirectory, comme illustré dans l'exemple suivant :

```
Oct 23 23:57:19 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0001|CREATE_OBJECT|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 23 2017 23:57:19 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=52362 suser=CN\=Admin,O\=novell duser=CN\=user001,O\=novell
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TREE910W cs4Label=Correlation
ID cs4=eDirectory#17#dc0fee11-5cd9-47d4-b981-cdb8ecd47e07
flexString2Label=SubEvent flexString2=DSE_CREATE_ENTRY flexNumber2Label=Grouping
flexNumber2=677768 cat=Objects reason=0 outcome=Success
```

Supprimer l'objet

Cliquez sur **Supprimer l'objet** pour générer un événement lors de la suppression d'un objet de l'arborescence eDirectory, comme illustré dans l'exemple suivant :

```
Oct 24 00:02:35 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0309|DELETE_OBJECT|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 24 2017 00:02:35 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=52362 suser=CN\=Admin,O\=novell duser=CN\=user001,O\=novell
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TREE910W cs4Label=Correlation
ID cs4=eDirectory#17#2b97f69d-2984-4f96-a83c-0b6c828bc462
flexString2Label=SubEvent flexString2=DSE_REMOVE_ENTRY flexNumber2Label=Grouping
flexNumber2=677993 cat=Objects reason=0 outcome=Success
```

Renommer l'objet

Cliquez sur **Renommer l'objet** pour générer un événement lorsqu'un objet est renommé, comme illustré dans l'exemple suivant :

```
Oct 24 02:06:23 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0003|RENAME_OBJECT|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 24 2017 02:06:23 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=55434 suser=CN\=Admin,O\=novell duser=CN\=u1,O\=novell
cs2Label=Class Name cs2=User cs3Label=Tree Name cs3=TREE910W cs4Label=Correlation
ID cs4=eDirectory#17#28250918-af9c-4098-b56a-5757e456102a cs6Label=New Object DN
cs6=CN\=u1changed,O\=novell flexString2Label=SubEvent flexString2=DSE_RENAME_ENTRY
flexNumber2Label=Grouping flexNumber2=683314 cat=Objects reason=0 outcome=Success
```

Déplacer l'objet

Cliquez sur **Déplacer l'objet** pour générer un événement lors du déplacement d'un objet, comme illustré dans l'exemple suivant :

```
Oct 24 02:18:57 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0004|MOVE_OBJECT|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:18:57 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.58 spt=55434 suser=CN\=Admin,O\=novell
duser=CN\=u1changed,O\=novell cs2Label=Class Name cs2=User cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#17#28789395-394f-49d5-bb4e-
b95410b0f9b5 cs6Label=New DN cs6=CN\=u1changed,OU\=org,O\=novell
flexString2Label=SubEvent flexString2=DSE_MOVE_SOURCE_ENTRY
flexNumber2Label=Grouping flexNumber2=683861 cat=Objects reason=0 outcome=Success
```

DSU lu

Cliquez sur **DSU lu** pour générer un événement lors de la lecture d'un objet, comme illustré dans l'exemple suivant :

```
Oct 24 02:36:27 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0230|DSA_READ|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:36:27 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=20928 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=CN\=WIN-
37D8M9SKD2U-NDS,O\=novell cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#1# flexString2Label=SubEvent
flexString2=DSE_DSA_READ cat=Objects reason=0 outcome=Success
```

Rechercher

Cliquez sur **Rechercher** pour générer un événement lorsqu'une requête est effectuée pour une opération de recherche, comme illustré dans l'exemple suivant :

```
Oct 24 02:36:29 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B033C|SEARCH|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:36:29 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=21184 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell
duser=CN\=Security cn1Label=Scope cn1=2 cn2Label=Nodes To Search cn2=100
cs2Label=Class Name cs2=SAS:Security cs3Label=Tree Name cs3=TREE910W
cs4Label=Correlation ID cs4=eDirectory#2# flexString2Label=SubEvent
flexString2=DSE_SEARCH flexNumber2Label=Grouping flexNumber2=684639 cat=Objects
reason=0 outcome=Success
```

Événements d'attributs

Cet ensemble d'événements s'applique aux opérations associées à l'attribut d'audit d'eDirectory. Une opération d'attribut peut créer, supprimer, renommer, déplacer ou rechercher un attribut.

Exemples d'événements d'attributs :

Cette section fournit des exemples pour les événements d'attributs suivants :

- « Lire l'attribut » page 946
- « Supprimer l'attribut » page 946
- « Ajouter une valeur » page 946
- « Supprimer la valeur » page 947
- « Comparer la valeur de l'attribut » page 947

REMARQUE : les exemples contenus dans les sections suivantes sont uniquement fournis à titre de référence.

Lire l'attribut

Cliquez sur **Lire l'attribut** pour générer un événement lors de la lecture d'un attribut sur un objet, comme illustré dans l'exemple suivant :

```
Oct 26 11:38:35 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0323|READ_ATTRIBUTE|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 25 2017 23:08:35 dtz=India Standard Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=18369 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=CN\=WIN-
37D8M9SKD2U-NDS,O\=novell cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#1# cs6Label=Attribute Name
cs6=cefConfiguration flexString2Label=SubEvent flexString2=DSE_READ_ATTR
cat=Attributes reason=0 outcome=Success
```

Supprimer l'attribut

Cliquez sur **Supprimer l'attribut** pour générer un événement lors de la suppression d'un attribut d'un objet, comme illustré dans l'exemple suivant :

```
Oct 24 22:54:36 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0009|DELETE_ATTRIBUTE|0|dvc=164.99.179.60
dvchost=WIN-37D8M9SKD2U rt=Oct 24 2017 22:54:36 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=21184 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=CN\=WIN-
37D8M9SKD2U-NDS,O\=novell cs2Label=Class Name cs2=NCP Server cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#2#a9ea8944-6a78-4a69-9c11-
727635aa79e8 cs6Label=Attribute Name cs6=Network Address flexString2Label=SubEvent
flexString2=DSE_DELETE_ATTRIBUTE flexNumber2Label=Grouping flexNumber2=736694
cat=Attributes reason=0 outcome=Success
```

Ajouter une valeur

Cliquez sur **Ajouter une valeur** pour générer un événement lors de l'ajout d'une valeur à un attribut, comme illustré dans l'exemple suivant :

```
Oct 24 02:38:12 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0006|ADD_VALUE|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:38:12 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=0 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=.[Pseudo
Server] cs1Label=Attribute Value cs1=720575940530274304 cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#0#f9787bd7-0541-47ca-9391-
5a4bada90f02 cs6Label=Attribute Name cs6=treeReferral flexString2Label=SubEvent
flexString2=DSE_ADD_VALUE flexNumber2Label=Grouping flexNumber2=684713
cat=Attributes reason=0 outcome=Success
```

Supprimer la valeur

Cliquez sur **Supprimer la valeur** pour générer un événement lorsqu'une valeur est supprimée d'un attribut, comme illustré dans l'exemple suivant :

```
Oct 24 02:38:12 NetIQ
CEF:0|NetIQ|eDirectory|9.1|CEF0B0007|DELETE_VALUE|0|dvc=164.99.179.60 dvchost=WIN-
37D8M9SKD2U rt=Oct 24 2017 02:38:12 dtz=Pacific Daylight Time
sourceServiceName=CN\=WIN-37D8M9SKD2U-NDS,O\=novell sproc=eDirectory#DS
src=164.99.179.60 spt=0 suser=CN\=WIN-37D8M9SKD2U-NDS,O\=novell duser=.[Pseudo
Server] cs1Label=Attribute Value cs1=720575940530274304 cs3Label=Tree Name
cs3=TREE910W cs4Label=Correlation ID cs4=eDirectory#0#1c411e7f-9657-474e-8e8e-
80fc92921f96 cs6Label=Attribute Name cs6=localReferral flexString2Label=SubEvent
flexString2=DSE_DELETE_VALUE flexNumber2Label=Grouping flexNumber2=684714
cat=Attributes reason=0 outcome=Success
```

Comparer la valeur de l'attribut

Cliquez sur **Comparer la valeur de l'attribut** pour générer un événement lors de la comparaison d'une valeur d'attribut, comme illustré dans l'exemple suivant :

Événements EBA

Cet ensemble d'événements s'applique à l'audit des opérations associées à l'authentification EBA d'eDirectory. Les opérations associées à l'authentification EBA sont, entre autres, l'activation et la désactivation d'EBA, l'ajout ou la suppression d'un serveur, le déplacement d'EBACA d'un serveur à un autre, voire `ndslogin`.

Exemples d'événements EBA :

Cette section fournit des exemples pour les événements EBA suivants :

- « Modifier la configuration du service » page 947

REMARQUE : les exemples contenus dans les sections suivantes sont uniquement fournis à titre de référence.

Modifier la configuration du service

Cliquez sur **Modifier la configuration du service** pour générer un événement lorsque l'arborescence eDirectory contient des modifications liées à l'authentification EBA, comme indiqué dans l'exemple suivant :

```
Sep 17 16:34:56 eDirectory
CEF:0|eDirectory|eDirectory|9.2|CEF0B0503|MODIFY_SERVICE_CONFIG|1|dvc=164.99.179.2
16 dvchost=SLESSP1-216 rt=Sep 17 2019 16:34:56 dtz=IST
sourceServiceName=CN\=SLESSP1-216,O\=novell sproc=eDirectory#DS src=164.99.179.216
spt=0 cs1Label=CertAuthOldSvrAddress cs1=164.99.179.216
cs2Label=CertAuthNewSvrAddress cs2=164.99.179.216 cs3Label=Tree Name cs3=TREE216
cs4Label=Correlation ID cs4=eDirectory#4294967295# cs6Label=Server Name
cs6=CN\=SLESSP1-216,O\=novell flexString2Label=SubEvent
flexString2=DSE_EBA_MOVE_EBA_CA flexNumber2Label=Grouping flexNumber2=205
cat=Security reason=0 outcome=Success
```

J Dépannage

- « Dépannage des problèmes liés à XDAS » page 949
- « Dépannage du protocole SNMP » page 951
- « Dépannage d'iMonitor » page 954
- « Dépanner iManager » page 956
- « Dépannage des notices nécrologiques » page 956
- « Migration vers NetIQ eDirectory » page 960
- « Résolution des problèmes du schéma » page 966
- « Dépannage DSRepair » page 966
- « Dépannage de la réplication » page 967
- « Dépannage du clonage de DIB » page 967
- « Dépannage des services d'infrastructure de clés publiques de NetIQ » page 968
- « Utilitaires de dépannage sous Linux » page 973
- « Dépannage de NMAS » page 974
- « Accès à HTTPSTK lorsque les services Annuaire ne sont pas chargés » page 977
- « Dépannage du codage des données » page 978
- « eDirectory Management Toolbox » page 981
- « Dépannage de SASL-GSSAPI » page 983
- « Gestion de la consignation des erreurs dans eDirectory » page 984
- « Divers » page 988
- « Dépannage d'IPV6 » page 995
- « Dépannage EBA » page 996

Dépannage des problèmes liés à XDAS

Les informations suivantes sont utiles dans le cadre de l'installation de Novell XDAS :

Erreur lors de l'initialisation du module XDAS

Cause possible : Vous ne pouvez pas vous connecter à l'adresse IP du serveur ou au numéro de port mentionné dans le fichier `xdasconfig.properties` lorsque vous initialisez le module XDAS. Vous obtenez le message suivant :

```
log4cxx: Could not instantiate TCP Socket to <IP>. All logging
will FAIL.

log4cxx: IO Exception : status code = 111
```

Action : Pour éviter ce problème :

1. Vérifiez si l'adresse IP du serveur ou le numéro de port spécifié dans le fichier `xdasconfig.properties` est correct.
2. Vérifiez si le serveur à distance est accessible et accepte la connexion sur le port indiqué.
3. Rechargez le module xdasauditds.

La connexion TCP est perdue

Cause possible : Si le serveur à distance n'est pas accessible ou n'accepte pas de connexion sur le port indiqué, le message d'erreur suivant s'affiche :

```
log4cxx: Detected problem with TCP connection to <IP>. All logging
will FAIL.
```

```
log4cxx: IO Exception : status code = 32
```

Action : Pour contourner ce problème :

1. Vérifiez si le serveur à distance est accessible et accepte la connexion sur le port indiqué.
2. Rechargez le module xdasauditds.

Problème de fichier de certificat SSL

Cause possible : Le fichier de certificat SSL n'est pas valide ou pas présent à l'emplacement indiqué dans le fichier `xdasconfig.properties`. L'erreur suivante s'affiche :

```
log4cxx: could not load verify locations for SSL
```

Action : Pour éviter ce problème :

1. Indiquez le chemin absolu vers un fichier de certificat valide.
2. Rechargez le module xdasauditds.

La connexion réseau avec le serveur à distance est perdue

Source : L'erreur suivante s'affiche :

```
log4cxx: SSL write failed for <IP>. All logging will FAIL.
```

Action : Pour éviter ce problème :

1. Vérifiez si le serveur à distance est accessible et accepte la connexion sur le port indiqué.
2. Rechargez le module xdasauditds.

Échec de la connexion SSL

Cause possible : La connexion SSL échoue, car le processus de reconnaissance mutuelle TLS/SSL échoue ou le système enregistre un échec de connexion. Le message d'erreur suivant s'affiche :

```
log4cxx: SSL Connect Failed to <IP>
```

Action : Pour éviter ce problème :

1. Vérifiez si le serveur à distance est accessible et écoute sur le port indiqué.
2. Vérifiez si le certificat est valide.
3. Rechargez le module xdasauditds.

Dépannage du protocole SNMP

Les trappes peuvent ne pas être générées comme prévu

Des trappes sont envoyées seulement si la requête verbale correspondante est reçue par le serveur. Si ce n'est pas le cas, aucun envoi n'est effectué. Par exemple, l'envoi de `ndsDeleteAttribute` s'effectue uniquement si la requête `ndsRemoveEntry` (numéro de trappe 108) est envoyée. Une application peut néanmoins toujours lire les listes de contrôle d'accès et décider de vérifier si l'utilisateur dispose de droits suffisants pour exécuter l'opération de suppression. Dans ce cas, la trappe `ndsDeleteAttribute` ne sera pas générée. Vous pouvez cependant utiliser iMonitor pour afficher les statistiques du verbe sur un serveur particulier.

Pour obtenir les trappes de toutes les occurrences, attribuez la valeur zéro à l'intervalle de temps.

Vous pouvez spécifier que les trappes sont seulement envoyées en cas d'échec. Vous pouvez spécifier que les trappes sont envoyées dans tous les cas.

ndssnmpsa doit être redémarré lors du redémarrage de l'agent maître

Pour redémarrer ndssnmpsa, vous devez d'abord l'arrêter.

Pour arrêter ndssnmpsa, entrez la commande suivante :

Linux : `/etc/init.d/ndssnmpsa stop`

Pour démarrer ndssnmpsa, entrez la commande suivante :

Linux : `/etc/init.d/ndssnmpsa start`

Objet Groupe SNMP

Si l'installation de l'objet Groupe SNMP échoue, vous pouvez remédier au problème en exécutant la commande suivante sur la console du serveur :

```
ndsconfig add -m snmp
```

Erreur de création d'objet SNMP sous Windows Server

Pour résoudre une éventuelle erreur de création d'objet Groupe SNMP lors de l'installation d'eDirectory sur un serveur dont la plate-forme Windows est prise en charge, vous devez créer manuellement l'objet Groupe SNMP. Pour plus d'informations sur la procédure de création manuelle d'un objet SNMP, reportez-vous au Chapitre 18, « Prise en charge du protocole SNMP pour NetIQ eDirectory », page 521.

Composant eDirectory pour l'initialisation de SNMP. Error code : -255ou Échec de l'initialisation. Error code : -255

Vous avez peut-être omis de spécifier `nom_hôte:port` ou `adresse_IP:port` comme paramètre dans la commande `SERVER` du fichier de configuration SNMP d'eDirectory.

Le fichier de configuration SNMP eDirectory est `ndssnmp.cfg`. Il réside dans les répertoires suivants :

- Linux : `/etc/opt/novell/eDirectory/conf/ndssnmp/`
- Windows : *`répertoire_installation`*`\SNMP\`

Statistiques SNMP LDAP non signalées

Lorsque la liaison anonyme est désactivée, les statistiques SNMP LDAP ne sont pas signalées.

Pour résoudre ce problème :

1. Autorisez la liaison anonyme.
2. Lancez le sous-agent.
3. Désactivez/refusez la liaison anonyme.

Erreur de segmentation lors de l'accès au sous-agent

Lorsqu'un utilisateur essaie de lancer le sous-agent (`ndssnmpsa`) à l'aide d'un mot de passe eDirectory incorrect, une erreur de segmentation se produit.

Pour éviter cette erreur, veillez à utiliser le mot de passe eDirectory correct lors du lancement du sous-agent.

Problèmes liés à après la mise à niveau 8.7.3 vers eDirectory 9.0

Après avoir mis à niveau eDirectory 8.7.3 vers la version 9.0, il se peut que vous obteniez le message d'erreur suivant :

```
%%% Attempting to restart the NetIQ eDirectory SNMP subagent (ndssnmpsa)...
Starting NDS SNMP Subagent ...
Initialization failure. Error code : -255
Please Wait...
Done

%%% Unable to start ndssnmpsa... Please try starting it manually...
```

Cette erreur se produit parce que dans la version 9.0, eDirectory n'écoute pas sur l'hôte local. Dans les versions antérieures, l'`hôte local SERVER` était défini par défaut dans le fichier `ndssnmp.cfg`.

Pour résoudre cette erreur, vous devez éditer manuellement le fichier `ndssnmp.cfg` et inclure le nom d'hôte du serveur eDirectory devant être surveillé.

Par exemple, entrez ce qui suit dans le fichier `ndssnmp.cfg` :

```
SERVER test-server
```

test-server est le nom d'hôte sur lequel eDirectory est exécuté sur le port NCP par défaut (à savoir, le port 524). Si eDirectory est exécuté sur un autre port (par exemple : 1 524), l'entrée doit avoir la syntaxe suivante :

```
SERVER test-server:1524
```

Erreurs au démarrage du sous-agent NDS

Le démarrage du sous-agent peut échouer et afficher le message suivant :

```
Unable to load library: libnetsnmp.so
```

Pour résoudre cette erreur, exportez la variable d'environnement SNMP_MAJOR_VERSION avec le numéro de la version principale de la bibliothèque net-snmp (`libnetsnmp.so`). Exemple : Vous pouvez utiliser la commande suivante :

```
export  SNMP_MAJOR_VERSION=10
```

Redémarrage de ndssnmpsa

Lors du redémarrage de l'agent principal sous Linux, ndssnmpsa doit également être redémarré.

Pour redémarrer ndssnmpsa, vous devez d'abord l'arrêter.

Pour arrêter ndssnmpsa, saisissez la commande suivante :

```
/etc/init.d/ndssnmpsa stop
```

Pour démarrer ndssnmpsa, entrez la commande suivante :

```
/etc/init.d/ndssnmpsa start
```

Compilation de edir.mib

Le fichier MIB eDirectory (`<répertoire_racine_installation_eDirectory>\snmp\edir.mib`) sous Windows est compilé avec quelques erreurs et avertissements sur HP-OpenView. Vous pouvez ignorer ces erreurs.

Modification du fichier de configuration SNMP

Si LDAP n'est pas configuré pour s'exécuter en mode Texte clair, le nom du fichier de certificat de racine approuvée doit être indiqué dans le fichier de configuration SNMP (par exemple, SSLKEY `C:\Novell\nds\trust.der`) avant le lancement du sous-agent SNMP d'eDirectory.

ndssnmp.cfg se trouve dans le répertoire `C:\novell\nds\snmp` sous Windows.

Utilisation de SNMP après l'installation d'une nouvelle arborescence

Lors de l'installation initiale 9.0 (création d'une arborescence), si le service SNMP de Windows est installé sur le serveur et que ce service comporte un ou plusieurs services dépendants, eDirectory ne parvient pas à fermer le service SNMP. Dans ce cas, SNMP n'est pas prêt à l'emploi après l'installation d'eDirectory.

Suivez ces étapes pour redémarrer le service SNMP :

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services**.
2. Cliquez avec le bouton droit de la souris sur **Service SNMP** dans la **liste des noms**, puis cliquez sur **Arrêter**.
3. Cliquez sur **Oui pour tout**.
4. Cliquez avec le bouton droit de la souris sur **Service SNMP** dans la **liste des noms**, puis cliquez sur **Démarrer**.

Désinstallation de SNMP pendant la désinstallation

Si le service SNMP de Windows est installé sur un serveur et que ce service comporte un ou plusieurs services dépendants, le programme de désinstallation d'eDirectory ne supprime pas tous les fichiers SNMP du dossier `C:\novell\nds`. Toutefois, les autres processus de désinstallation

s'exécutent correctement, notamment la suppression des entrées de registre SNMP et le processus d'annulation de la configuration qu'exécute l'agent SNMP de NetIQ à l'aide de DS et du service SNMP.

Pour effectuer la désinstallation :

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services**.
2. Cliquez avec le bouton droit de la souris sur **Service SNMP** dans la **liste des noms**, puis cliquez sur **Arrêter**.
3. Cliquez sur **Oui pour tout**.
4. Cliquez avec le bouton droit de la souris sur **Service SNMP** dans la **liste des noms**, puis cliquez sur **Démarrer**.
5. Supprimez manuellement les fichiers SNMP restant dans le dossier `C:\novell\nds`.

L'installation d'eDirectory arrête SNMP sous Windows 2012

SNMP cesse de fonctionner après l'installation d'eDirectory et affiche le message d'erreur suivant :

`SNMP subagent error -672` (Erreur du sous-agent SNMP -672)

Solution :

1. Installez et configurez le service SNMP après l'installation d'eDirectory.
2. Exécutez le fichier `dssnmpsupport.exe` sur votre serveur eDirectory.

REMARQUE : appliquez le fichier `dssnmpsupport.exe` uniquement si le `service MpsSvc` est en cours d'exécution sur le serveur eDirectory.

Dépannage d'iMonitor

Recherche d'objets contenant des caractères double octet dans iMonitor

Lorsque vous utilisez iMonitor pour rechercher des objets dans une arborescence eDirectory, le lien hypertexte entre un objet dont le nom contient des caractères à double octet et ses propriétés peut ne pas fonctionner correctement.

Vérification de l'état de santé de l'agent dans une arborescence à serveur unique

Dans iMonitor, la fonction de vérification de l'état de santé de l'agent affiche une icône d'avertissement dans la colonne Résultats si vous l'exécutez sur une arborescence à serveur unique, en raison de l'état Données périssables. N'en déduisez pas que l'arborescence se trouve dans un état critique ni que la vérification de l'état de santé ne fonctionne pas correctement. L'état Données périssables indique la quantité de données qui n'ont pas encore été synchronisées sur une réplique au moins. Une arborescence à serveur unique, de par sa nature, laisse toujours peser un risque d'incident majeur sur les données du fait qu'elles ne sont répliquées dans aucun autre emplacement. La perte du disque dur signifie, dans ce cas, la perte des données.

Si vous ne souhaitez pas afficher les avertissements relatifs aux données périssables ou au nombre de répliques lisibles dans l'arborescence à serveur unique, vous pouvez désactiver ces vérifications de l'état de santé en modifiant les entrées suivantes du fichier `ndsimonhealth.ini` :

`perishable_data-active: OFF`

et

`ring_readable-Min_Marginal: 1` ou `ring_readable-active: OFF`

Vous désactivez ainsi les avertissements relatifs au nombre de répliques lisibles et aux données périssables.

Le rapport d'iMonitor ne contient pas les heures d'enregistrement

La fonction Rapports personnalisés d'iMonitor place l'URL spécifiée par l'utilisateur dans le rapport enregistré (le fichier HTML enregistré) lors de la création du rapport personnalisé. En d'autres termes, lorsque vous ouvrez un rapport personnalisé enregistré qui a été exécuté, vous accédez aux données courantes et non aux données collectées via l'URL durant l'exécution de ce rapport. Ce problème sera résolu dans une version ultérieure d'iMonitor.

Tampons horaires de création et de modification

Étant donné que les plates-formes Linux ne gèrent pas l'heure de création d'un fichier, iMonitor affiche la même valeur pour les heures de création et de modification.

Disposition de l'écran Exécuter le rapport non alignée sur iMonitor

Les cadres de navigation et d'assistant apparaissent en double sous Linux.

Pour résoudre ce problème, rafraîchissez la page.

iMonitor affiche l'erreur -672

- **Linux :** iMonitor affiche l'erreur -672 si l'outil dsdump s'exécute parallèlement à iMonitor. Pour résoudre ce problème, quittez l'outil dsdump avant de démarrer iMonitor.
- **Windows :** iMonitor affiche l'erreur -672 si l'outil dsbrowse ou dsedit s'exécute parallèlement à iMonitor. Pour résoudre ce problème, quittez l'outil dsbrowse ou dsedit avant de démarrer iMonitor.

iMonitor affiche l'erreur -702

Si vous assignez des droits ACL d'une entrée de groupe à un objet Utilisateur, iMonitor affiche un message d'erreur lors de la validation de l'entrée après la mise à niveau du serveur eDirectory.

Vous devez mettre à jour manuellement la valeur de `ValidACLFlags` dans le fichier `ndsimonhealth.conf` et redémarrer le serveur eDirectory.

Tampons horaire affichés au format hexadécimal

Si vous définissez un attribut de syntaxe d'heure dont la valeur est antérieure au 1er janvier 1970, iMonitor affiche le tampon horaire de l'attribut au format hexadécimal au lieu du format de date/heure standard. iMonitor affiche tous les attributs avec des valeurs ultérieures au 1er janvier 1970 au format de date/heure.

Problème de configuration de Trace dans iMonitor dans Internet Explorer 11

La configuration de Trace dans iMonitor ne fonctionne pas dans Internet Explorer 10.

Pour contourner ce problème, lancez Internet Explorer 10 en mode compatibilité et ajoutez l'adresse iMonitor à la liste des sites de confiance, puis redémarrez le navigateur.

Dépanner iManager

Échec des opérations LDAP après la création d'un groupe LDAP à l'aide de la fonction de création rapide

La fonction de création rapide crée uniquement un objet Groupe LDAP avec des attributs factices que vous pouvez modifier ultérieurement. Comme la création est réalisée avec la version 11 au lieu de la version 12, toutes les opérations LDAP échouent, car aucun serveur LDAP ne peut être associé en raison de l'incompatibilité des versions.

Pour éviter ce problème, après avoir créé le groupe LDAP à l'aide de la fonction de création rapide, remplacez le numéro de version de l'objet Groupe LDAP par 12.

Dépannage des notices nécrologiques

Les notices nécrologiques servent d'attributs opérationnels que eDirectory place sur les objets afin de garantir l'intégrité référentielle pendant les opérations de suppression, de déplacement, de changement de nom et de restauration. Par exemple, si le groupe A comprend le membre Utilisateur B et que ce membre est supprimé, l'annuaire supprime automatiquement la référence à cet utilisateur du groupe A. Dans eDirectory 9.0, les notices nécrologiques générées par les opérations de suppression, de déplacement et de changement de nom sont optimisées par défaut.

REMARQUE : Les objets qui possèdent des notices nécrologiques sont pris en considération à chaque synchronisation sortante d'un agent, ainsi que par le processus de notice nécrologique qui est planifié pour s'exécuter à la fin d'un cycle de synchronisation entrante.

Les notices nécrologiques se classent en trois grandes catégories :

- Les notices nécrologiques primaires incluent les types Mort (0001), Restauré (0000), Déplacé (0002), Nouveau RDN (0005) et Nouveau RDN de l'arborescence (0008).
- Les notices nécrologiques secondaires sont généralement associées à une notice primaire et représentent les agents et les partitions qui doivent être avertis de l'opération spécifiée dans la notice primaire. Elles incluent les types Lien en amont (0006), Utilisé par (000C) et Déplacer l'arborescence (000a).
- Les notices nécrologiques de suivi incluent Non déplaçable (0003), Ancien RDN (0004) et Ancien RDN de l'arborescence (0007).

Les notices nécrologiques, hormis celles de la dernière catégorie, doivent passer par une succession d'états de synchronisation :

- État initial ou émis (0)
- Notifié (1)
- OK pour la purge (2)
- Purgeable (4)

Ces états sont enregistrés dans le champ Drapeaux de l'attribut de notice nécrologique. Pour que la notice nécrologique puisse passer à l'état suivant, l'état actuel doit avoir été synchronisé pour toutes les répliques de l'objet réel. Pour déterminer si un état de notice nécrologique a été communiqué à toutes les répliques de l'anneau, un vecteur est calculé à partir du vecteur de transition. Dans eDirectory 8.6 (ou version ultérieure), un vecteur de notice nécrologique non stocké est utilisé. Les

versions précédentes utilisaient le vecteur de purge. Si le tampon horaire de modification de la notice nécrologique est antérieur au vecteur endommagé, le serveur responsable de cette notice peut la faire passer à l'état suivant.

Dans le cas d'une notice nécrologique secondaire de type Lien en amont, l'agent qui contient la réplique maîtresse de l'objet associé à cette notice prend en charge le passage aux états suivants. Dans le cas d'une notice nécrologique secondaire de type Utilisé par, cette tâche incombe à l'agent de réplique qui a créé cette notice, et ce tant que la réplique existe. Si la réplique vient à disparaître, l'agent qui contient la réplique maîtresse de cette partition se chargera de faire passer la notice Utilisé par aux états suivants. Dans le cas d'une notice nécrologique de type Déplacer l'arborescence, ce passage aux états suivants est assuré par la réplique maîtresse de la partition racine.

Pour que les notices nécrologiques primaires puissent passer à leur état suivant, toutes les notices secondaires doivent d'abord être passées par tous leurs états successifs. Lorsque la notice nécrologique primaire a atteint son dernier état et que celui-ci est synchronisé pour tous les serveurs de l'anneau, il ne reste plus que l'enveloppe d'objet, c'est-à-dire un objet dépourvu d'attributs, qui peut ensuite être purgé du système par le processus de purge. Les notices nécrologiques de suivi sont supprimées dès que la notice primaire est prête à être supprimée ou, dans le cas de `Inhibit_move`, dès qu'elle est passée à l'état `OBF_NOTIFIED` dans la réplique maîtresse.

La réplique chargée du traitement des notices nécrologiques effectue ce traitement dans un processus d'arrière-plan (le processus Notice nécrologique) qui est planifié pour chaque partition après qu'une partition donnée a achevé un cycle de synchronisation entrante. S'il n'existe pas d'autre réplique de la partition, le processus de réplication sortante reste planifié en fonction de l'intervalle de pulsation. Le processus de réplication sortante démarre alors le processus de notice nécrologique. Ce dernier ne peut pas être planifié manuellement et n'a pas besoin de l'être. Lors de la synchronisation, les vecteurs de transition sont mis à jour, ce qui a pour effet de faire avancer les vecteurs de purge et de notice nécrologique. À mesure que ces vecteurs progressent, les états de notice nécrologique sont également autorisés à avancer. Ceci, combiné à la planification automatique effectuée durant la synchronisation entrante, complète le cycle de traitement des notices nécrologiques. L'élément essentiel du processus Notice nécrologique est donc la synchronisation des objets.

Pour un objet en cours de suppression, une fois que toutes les notices associées à une notice primaire de type Mort sont passées au dernier état (Purgeable) et que cet état a été synchronisé pour toutes les répliques, un nouveau processus est chargé de supprimer de la base de données l'enveloppe d'entrée résiduelle. Le processus de purge s'exécute automatiquement pour supprimer ces enveloppes. Pour planifier manuellement le processus de purge et modifier son intervalle automatique, reportez-vous à la section « Affichage de l'activité de l'agent » page 254.

Résolution des problèmes de notices nécrologiques orphelines

Pendant que vous examinez les objets Notice nécrologique, parcourez l'anneau de répliques et comparez les différentes notices présentes sur cet anneau.

- Si toutes les répliques ne possèdent pas de copie de la notice nécrologique et que tous les attributs ne sont pas qualifiés pour une purge, l'objet n'est pas cohérent dans l'ensemble de l'anneau de répliques, ce qui indique un problème de notice orpheline.
- Si l'objet existe dans toutes les répliques et qu'il est cohérent, son état est peut-être bloqué à cause d'erreurs de synchronisation ou parce que le processus de notice nécrologique détecte des erreurs.

Pour éviter ce problème :

- **Méthode préconisée :** si eDirectory 8.6 (ou une version ultérieure) est installé sur l'un des serveurs de l'anneau de répliques, accédez à l'objet correspondant dans iMonitor et sélectionnez Envoyer une unique entrée. Vous effectuez ainsi un envoi non expert à toutes les autres répliques.
- **Méthode beaucoup moins recommandée :** si tous les serveurs de l'anneau de répliques qui possèdent une copie de la notice nécrologique orpheline sont antérieurs à eDirectory 8.6, chargez DSBrowse avec l'option -a, affichez l'objet, puis associez un tampon horaire à l'entrée. L'objet, tel qu'il existe sur ce serveur, devient ainsi la copie experte. Toutefois, nous déconseillons cette dernière méthode qui est contraire aux bonnes pratiques.

Résolution des problèmes de notices nécrologiques orphelines dans les références externes

Si la notice concerne un objet qui n'est pas stocké sur ce serveur (autrement dit, l'objet est une référence externe) :

- Vérifiez que l'objet réel possède une notice nécrologique équivalente. Si tel n'est pas le cas, la notice est orpheline.
- Si l'objet réel possède une notice équivalente, remédiez aux problèmes liés à cet objet avant d'essayer de résoudre ceux qui concernent la notice dans la partition de `référence externe`.

Pour éviter ce problème :

- **Méthode la moins recommandée :** exécutez DSRepair avec l'option de tampon horaire sélectionnée.
- **Méthode la moins recommandée :** déplacez une réplique réelle vers le serveur, attendez qu'elle soit active puis que la notice nécrologique soit traitée. Une fois la notice nécrologique traitée, vous pouvez supprimer la réplique si vous le souhaitez.

Résolution des problèmes de synchronisation avec les notices nécrologiques

Pour vérifier que les notices nécrologiques sont correctement synchronisées :

- Pour détecter et corriger les éventuelles erreurs de synchronisation, utilisez la page Synchronisation de l'agent d'iMonitor.
- Les notices nécrologiques changent d'état une fois que tous les agents qui contiennent une copie de l'anneau de répliques ont été avertis de ce changement d'état. Il existe différentes manières de s'assurer que chaque réplique a vu les données :

  Pendant que vous parcourez les entrées qui possèdent des notices nécrologiques, cliquez sur le lien Synchronisation des entrées. La page qui s'ouvre affiche tous les attributs qui n'ont pas été synchronisés pour toutes les répliques.

  Recherchez le plus ancien tampon horaire pour n'importe quelle valeur d'attribut de notice nécrologique. La différence entre cette heure et l'heure actuelle doit être supérieure à l'intervalle affiché dans le champ Delta d'anneau maximal de la page Synchronisation de partition.

  Évaluez le vecteur de transition.

Recherche des erreurs de notices nécrologiques

Consultez État du processus de l'agent : Notices nécrologiques pour rechercher les éventuelles erreurs.

- Problèmes les plus fréquemment rencontrés dans l'état des processus de l'agent : les notices nécrologiques comprennent les erreurs

  -625, -622, -634 et –635, qui sont des problèmes de communication. Pour plus d'informations, reportez-vous à Rapport d'informations sur le serveur.

  -601 et -603, qui indiquent que des serveurs n'ont pas été correctement supprimés ou que l'objet Serveur a peut-être une classe de base inconnue.
- Les erreurs affichées dans cette page ne sont pas fatales. À la prochaine exécution du processus de notice nécrologique pour cette partition, l'opération fera l'objet d'une nouvelle tentative. Remédiez aux problèmes affichés dans cette page, puis attendez la nouvelle tentative.

Précédentes méthodes

Dans le passé, plusieurs méthodes ont été employées pour remédier au blocage des notices nécrologiques. Certaines impliquaient des opérations de partition onéreuses ou l'utilisation de fonctions qui ne faisaient l'objet d'aucune documentation et pouvaient provoquer des problèmes dans le futur.

La première consiste à changer la réplique qui contient le maître. Cette méthode fonctionnait dans certains cas, puisque le maître est l'agent chargé de faire passer les notices nécrologiques Lien en amont par leurs différents états. Lorsque la réplique est incohérente et que le maître ne contient pas l'objet supprimé, le remplacement des maîtres par un agent contenant l'entrée supprimée avec ses notices nécrologiques permet au nouvel agent de faire passer les notices par leurs différents états successifs pour finalement les purger. L'envoi d'une unique entrée est un moyen beaucoup moins dangereux de résoudre les problèmes de notices nécrologiques bloquées à cause d'une réplique incohérente.

La deuxième méthode consiste à exécuter DSRepair avec certains paramètres afin de supprimer toutes les notices nécrologiques. (Il existe une application tierce qui répare toutes les notices nécrologiques bloquées en lançant DSRepair.) Nous ne recommandons pas cette méthode. L'utilisation de ces paramètres supprime toutes les notices nécrologiques de l'agent, y compris celles qui ne sont pas bloquées, avec le risque de provoquer de nouvelles incohérences et davantage de blocages de notices nécrologiques. Comme il ne s'agit pas d'une opération distribuée, vous devez exécuter DSRepair sur tous les serveurs qui contiennent des notices nécrologiques bloquées, ce qui augmente le risque de supprimer prématurément les notices nécrologiques d'un de ces serveurs pour une autre partition. En supprimant prématurément des notices nécrologiques, vous risquez de créer d'autres notices orphelines et de provoquer des problèmes qui ne seront pas détectés avant plusieurs années, lorsque vous modifierez les types de réplique, ajouterez des répliques ou effectuerez d'autres opérations de partitionnement.

La troisième méthode consiste à rendre les objets experts soit en utilisant DSBrowse en mode avancé et en associant un tampon horaire à l'entrée, soit en exécutant DSRepair avec le paramètre -0T. Cette méthode rend l'entrée experte et celle-ci se synchronise avec toutes les autres répliques. Procédez avec la plus grande prudence car vous risquez de perdre des données modifiées sur d'autres serveurs. Nous recommandons d'employer rarement cette méthode de suppression des notices nécrologiques.

Migration vers NetIQ eDirectory

Migration du schéma Sun ONE vers NetIQ eDirectory

Pour migrer le schéma Sun ONE vers NetIQ eDirectory, exécutez les étapes suivantes :

Étape 1 : Exécutez l'opération de mise à jour du cache de schéma.

Vous pouvez enregistrer les erreurs qui se sont produites lors de la comparaison du schéma dans un fichier d'erreurs à l'aide de la commande suivante :

`ice -e` *`LDIF error file name`* `-C -a -SLDAP -s` *`Sun ONE server`* `-p` *`Sun ONE port`* `-DLDAP -s` *`eDirectory server`* `-p` *`eDirectory port`*

Par exemple :

```
ice -e err.ldf -C -a -SLDAP -s sun_srv1 -p sun_port1 -DLDAP -s edir_srv2 -p
edir_port2
```

Les éventuelles erreurs rencontrées lors de la comparaison du schéma sont inscrites dans le fichier d'erreurs (`err.ldf` dans l'exemple). Il n'est pas nécessaire de vous connecter pour exécuter cette opération, sauf si l'un des serveurs requiert une authentification afin de lire le DSE racine. Microsoft Active Directory requiert une authentification pour lire le DSE racine.

Étape 2 : Corrigez le fichier d'erreurs LDIF afin d'éliminer les erreurs.

- Sun ONE détermine publiquement certaines définitions de schéma qui ne le sont pas dans eDirectory. Les attributs tels que `objectClasses`, `attributeTypes`, `ldapSyntaxes` et `subschemSubentry` sont pris en compte. Ces définitions existent de façon interne et sont d'une importance capitale pour le schéma ; elles ne peuvent donc pas être modifiées. Les opérations qui tentent de les modifier génèrent le message d'erreur suivant :

  ```
  LDAP error : 53 (DSA is unwilling to perform)
  ```

  Tous les enregistrements qui contiennent des références à ces définitions produisent l'erreur suivante :

  ```
  LDAP error : 16 : ( No such attribute )
  ```

  Par conséquent, les enregistrements qui contiennent des références à ces objets ou qui tentent de modifier ces définitions doivent être commentés dans le fichier d'erreurs LDIF (`err.ldf` dans l'exemple).
- Certaines définitions d'attributs objectClasses dans Sun ONE ne possèdent pas d'attributs d'assignation de nom. L'ajout de ces attributs objectClasses produit l'erreur suivante dans eDirectory :

  ```
  LDAP error : 80 (NDS error: ambiguous naming (-651)
  ```

  Cette erreur se produit car Sun ONE n'utilise pas la même méthode de détermination des règles d'assignation de nom que eDirectory.

  Pour y remédier, utilisez l'*une* des trois options suivantes :

  Option 1 :

  Ajoutez un attribut d'assignation de nom valable à chaque définition objectClasses en cause.

  Par exemple :

  Pour ajouter l'attribut d'assignation de nom `[ cn ]` à la classe d'objet `netscapeMachineData`, modifiez l'entrée (*en italique* dans l'exemple ci-dessous) dans le fichier `err.ldf` comme suit afin d'inclure le drapeau `X-NDS_NAMING` :

```
dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
    DESC 'iPlanet defined objectclass' SUP top STRUCTURAL MAY c'n '    X-
NDS_NAMING 'cn' )-
```

Option 2 :

Affectez la valeur AUXILIARY ou ABSTRACT à chaque définition objectClasses en cause.

Par exemple :

Pour modifier la définition de la classe d'objet `netscapeMachineData` et affecter la valeur AUXILIARY à la place de STRUCTURAL, modifiez l'entrée du fichier `err.ldf` (en *italique* dans l'exemple ci-dessous) :

```
dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
   DESC 'iPlanet defined objectclass' SUP top AUXILIARY )-
```

Pour modifier la définition de la classe d'objet `netscapeMachineData` et affecter la valeur ABSTRACT à la place de STRUCTURAL, modifiez l'entrée du fichier `err.ldf` (*en italique* dans l'exemple ci-dessous) :

```
dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
   DESC 'iPlanet defined objectclass' SUP top ABSTRACT )-
```

Option 3 :

)-Ajoutez cn à la définition de `Top` dans eDirectory, afin de générer un attribut d'assignation de nom éventuel pour chaque objectClasses.

Il existe deux façons différentes d'ajouter `cn` à `Top` :

- **Méthode 1 :**

  Créez un fichier de la manière suivante et donnez-lui le nom `topsch.ldf`.

  ```
  version : 1

  dn:cn=schema

  changetype :modify

  delete : objectclasses

  objectclasses : ( 2.5.6.0 NAME 'top' STRUCTURAL )

  -

  add:objectclasses

  objectclasses : (2.5.6.0 NAME 'top' STRUCTURAL MAY cn)
  ```

  Utilisez la ligne de commande d'importation, de conversion et d'exportation NetIQ suivante :

  ```
  ice -SLDIF -f LDIF_file_name -DLDAP -s eDirectory_server -p eDirectory_port
  -d eDirectory_Admin_DN -w eDirectory_password
  ```

  Par exemple :

  ```
  ice -SLDIF -f topsch.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
  cn=admin,o=org -w pwd1
  ```

- **Méthode 2 :**

  1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches**  .

2. Cliquez sur **Schéma** > **Ajouter un attribut**.
3. Dans la liste **Classes disponibles**, sélectionnez **Haut**, puis cliquez sur **OK**.
4. Double-cliquez sur **CN** dans la liste **Attributs facultatifs disponibles**.
5. Cliquez sur **OK**.

- Certaines définitions objectClass contiennent `userPassword` dans leur liste d'attributs obligatoires. L'ajout de ces définitions objectClasses à eDirectory produit l'erreur suivante :

  ```
  LDAP error : 16 (No such attribute)
  ```

  Pour corriger cette erreur, modifiez la définition objectClass afin d'hériter de la nouvelle classe d'objet de `ndsLoginProperties` et supprimez l'attribut `userPassword` de la liste des attributs obligatoires.

  Par exemple :

  Une classe d'objet contenant `userPassword` dans la liste d'attributs obligatoires :

  ```
  version : 1
  dn: cn=schemaz
  changetype: modify
  add: objectClasses
  objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
   Standard LDAP objectClass' SUP top STRUCTURAL MUST userPassword )
  ```

  doit être modifiée comme suit (prêtez attention à la modification dans la dernière ligne) :

  ```
  version : 1
  dn: cn=schema
  changetype: modify
  add: objectClasses
  objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
   Standard LDAP objectClass' SUP (ndsLoginProperties $ top) STRUCTURAL)
  ```

Étape 3 : Importez le fichier LDIF.

Utilisez la commande d'importation, de conversion et d'exportation NetIQ suivante pour importer le fichier LDIF de comparaison de schéma modifié (`err.ldf` dans l'exemple) :

```
ice -e error_file -SLDIF -f modified_LDIF_file -DLDAP -s eDirectory_server -p
eDirectory_port -d eDirectory_Admin_DN -w eDirectory_password
```

Par exemple :

```
ice -e errors.ldf -SLDIF -f err.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

Migration du schéma Active Directory vers NetIQ eDirectory via l'utilitaire ICE

Lors de la migration du schéma de Active Directory vers NetIQ eDirectory via l'utilitaire ICE pour la classe d'objet `Computer`, l'erreur `-651` (concernant une ambiguïté dans les noms) s'affiche.

Pour résoudre ce problème, procédez comme suit :

Étape 1 : Exécutez l'opération de mise à jour du cache de schéma.

Lors de la migration du schéma de Active Directory vers NetIQ eDirectory via l'utilitaire ICE, vérifiez que vous avez fourni l'option de journal d'erreurs (`-e`) de l'utilitaire ICE comme suit :

```
ice -e error_file -S ldap -s Active_Directory_server -p Active_Directory_port -d
Active_Directory_full_admin_context -w Active_Directory_password -D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

Par exemple :

```
ice -e err.ldf -S ldap -s activesrv1 -p activeport1 -d cn=admin,o=company -w
activepwd -D ldap -s edirsrv2 -p edirport2 -d cn=admin,o=company -w edirpwd
```

Étape 2 : Corrigez le fichier d'erreurs LDIF afin d'éliminer les erreurs.

L'entrée qui a échoué figure dans le fichier `err.ldf` comme indiqué ci-dessous :

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP (device $
 user ) STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $
 local PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netboot MirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )

-
```

Modifiez cette entrée dans le fichier d'erreur (`err.ldf` dans l'exemple ci-dessous) pour supprimer la classe d'objet `user` de la liste des classes d'objet supérieures dans la définition de la classe d'objet `Computer` :

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP device
 STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $ local
 PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netbootMirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )
```

Étape 3 : Importez le fichier LDIF.

Maintenant, importez l'entrée modifiée en utilisant la commande ICE suivante :

```
ice -S ldif -f LDIF_file -D ldap -s Novell_eDirectory_server -p port_number -d
full_admin_context -w password
```

Par exemple :

```
ice -S ldif -f err.ldf -D ldap -s edirsrv1 -p edirport1 -d cn=admin,o=company -w
pwd1
```

Migration de OpenLDAP vers NetIQ eDirectory

Les données migrées depuis un serveur OpenLDAP comportent parfois des mots de passe MD5, ce qui peut provoquer une interruption des applications si les méthodes NMAS appropriées ne sont pas installées. Pour NetIQ eDirectory, la méthode NMAS SimplePassword doit être installée à l'aide de la commande suivante :

```
nmasinst -addmethod contexte_admin nom_arborescence fichier_configuration -h
nom_hôte:port-w mot_de_passe
```

Par exemple : `nmasinst -addmethod admin.novell eDir-Tree /Linux/eDirectory/nmas/NmasMethods/Novell/SimplePassword/config.txt -h eDir_srv:524 -w secret`

Migration du schéma OpenLDAP vers eDirectory

Pour migrer le schéma OpenLDAP vers eDirectory, procédez comme suit :

Étape 1 : Exécutez l'opération de mise à jour du cache de schéma.

Vous pouvez enregistrer les erreurs qui se sont produites lors de la comparaison du schéma dans un fichier d'erreurs à l'aide de la commande suivante :

```
ice -e error_file -C -a -S ldap -s OpenLDAP_server -p Open_LDAP_port - D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

Par exemple :

```
ice -e err.ldf -C -a -SLDAP -s open_srv1 -p open_port1 -DLDAP -s edir_srv2 -p
edir_port2 -d cn=admin,o=novell -w secret
```

Les éventuelles erreurs rencontrées lors de la comparaison du schéma sont inscrites dans le fichier d'erreurs (`err.ldf` dans l'exemple).

Étape 2 : Corrigez le fichier d'erreurs LDIF afin d'éliminer les erreurs.

Open LDAP détermine publiquement certaines définitions de schéma, dont les attributs tels que `objectClasses`, `attributeTypes`, `ldapSyntaxes` et `subschemSubentry`. Ces définitions existent de façon interne et sont d'une importance capitale pour le schéma ; elles ne peuvent donc pas être modifiées. Les opérations qui tentent de les modifier génèrent le message d'erreur suivant :

```
LDAP error : 53 (DSA is unwilling to perform)
```

Tous les enregistrements qui contiennent des références à ces définitions produisent l'erreur suivante :

```
LDAP error : 16 ( No such attribute )
```

Par conséquent, les enregistrements qui contiennent des références à ces objets ou qui tentent de modifier ces définitions doivent être commentés dans le fichier d'erreurs LDIF (`err.ldf` dans l'exemple).

Migration des données Open LDAP vers NetIQ eDirectory

Exécutez la commande suivante pour migrer les données :

```
ice -e error_data.ldif -SLDAP -s OpenLDAP_server -p OpenLDAP_port  -d admin_context
-w password -t -b dc=blr,dc=novell,dc=com -F objectclass=* -DLDAP -d  admin_context
-w password  -l  -F
```

Par exemple :

```
ice -e err_data.ldif -SLDAP -s open_srv1 -p open_port1  -d
cn=administrator,dc=blr,dc=novell,dc=com -w secret1 -t -b dc=blr,dc=novell,dc=com
-F objectclass=* -DLDAP -d cn=admin,o=novell -w secret2 -l -F
```

La migration de certains objets peut également échouer en raison de références en aval et de dépendances internes entre les objets, mais cela n'implique pas nécessairement l'interruption des applications.

Compatibilité de PAM avec NetIQ eDirectory après la migration

Après une migration de OpenLDAP vers eDirectory, vous devez effectuer certaines modifications pour que PAM fonctionne avec eDirectory.

Modifications dans le fichier /etc/ldap.conf

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
  binddn cn=admin,o=acme
  ...
# The credentials to bind with.
# Optional: default is no credential.
  bindpw secret
  ...
# The search scope.
  scope sub
  ...
# Filter to AND with uid=%s
  pam_filter objectclass=inetorgperson
  ...
# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
  pam_password nds
  ...
  ssl off
  ...
```

Modifications des données de l'annuaire

Ces modifications ne concernent que le scénario pour lequel les objets Utilisateur dans OpenLDAP ont CRYPT comme algorithme de codage de mot de passe.

À l'aide d'iManager, ajoutez l'attribut suivant avec la valeur spécifiée dans le conteneur renfermant tous les objets Utilisateur :

Attribut : `sasDefaultLoginSequence`

Valeur : Simple Password

Résolution des problèmes du schéma

Cette section comprend des informations permettant de dépanner le schéma.

Résolution des problèmes du schéma

Lorsqu'une classe auxiliaire est dissociée d'un objet, la valeur n'est pas supprimée immédiatement, mais elle est marquée comme étant absente. La classe auxiliaire est associée à l'entrée jusqu'à ce que le processus DRL nettoie ces valeurs lors de la validation proprement dite de l'objet.

Le processus en arrière-plan DRL étant fort consommateur de ressources, les autres opérations sont lentes lors de ce nettoyage. La durée du processus de nettoyage dépend du nombre d'objets réels et de références externes dans le système. Étant donné que ce processus utilise une grande quantité de mémoire et une capacité importante du processeur, vous ne devez pas l'exécuter régulièrement. Par défaut, le processus en arrière-plan Backlinker s'exécute 50 minutes après le démarrage de ndsd, puis toutes les 13 heures.

La suppression d'une classe auxiliaire d'une entrée peut prendre entre 0 et 13 heures, auxquelles s'ajoute la durée nécessaire au traitement de cette entrée dans le système.

Pour contourner ce problème, supprimez l'entrée de la classe auxiliaire en déclenchant le processus Backlinker par l'intermédiaire de DSTrace ou d'iMonitor.

REMARQUE : Lorsque l'objet est supprimé, les valeurs sont immédiatement purgées, car cette suppression est gérée par d'autres processus en arrière-plan.

Dépannage de l'assignation de syntaxe LDAP

Certaines syntaxes DS ne sont pas assignées de manière unique aux syntaxes LDAP. Ce problème se produit dans eDirectory 9.1 et versions antérieures.

Ce problème a été résolu dans eDirectory 9.1 SP1. Si vous souhaitez rétablir l'assignation précédente, affectez une valeur à la variable d'environnement `NDSD_NLDAP_PRE911_SCHEMA`.

Dépannage DSRepair

Exécution de DSRepair sur une DIB montée sur NFS sous Linux

Les erreurs –732 ou –6009 peuvent apparaître lorsque vous essayez d'exécuter les opérations ndsrepair (DSRepair) sur une DIB montée sur NFS sur des systèmes Linux.

L'exécution de DSRepair avec l'option -R se bloque

Après avoir activé les attributs codés sur les attributs indexés, si vous exécutez ndsrepair (DSRepair) avec l'option `-R`, un blocage se produit.

Dépannage de la réplication

eDirectory met à votre disposition les services Annuaire performants de NetIQ, ainsi que la tolérance aux pannes inhérente à la réplication. La réplication vous permet de conserver des copies de tout ou partie de la base de données eDirectory, sur plusieurs serveurs en même temps.

Configuration de la réplication codée via iManager

Vous ne pouvez pas configurer la réplication codée via iManager si l'un des serveurs de l'anneau de répliques est arrêté.

Échec de la fusion d'arborescences à l'aide de la réplication chiffrée

Lorsque la réplication codée est activée, la fusion d'arborescences échoue. Avant d'effectuer ce type d'opération, veillez donc à désactiver la réplication codée pour chaque arborescence. Si des serveurs EBA sont activés sur les arborescences, la fusion des arborescences peut réussir. Toutefois, une fois la fusion terminée, l'arborescence devient instable et la réplication ne se fait pas correctement, ce qui provoque des échecs lors des authentifications.

Résolution des problèmes de répliques eDirectory

Vous devez toujours conserver plusieurs répliques des partitions eDirectory. Ainsi, si une réplique est altérée ou perdue en raison d'une défaillance de disque dur, vous pouvez la supprimer à l'aide de NetIQ iManager et la remplacer par une autre, issue de la réplique intacte.

Pour plus d'informations sur la suppression de répliques, reportez-vous à la section Gestion des répliques du *Guide d'administration de NetIQ eDirectory 9.0*.

Dépannage du clonage de DIB

Erreurs -601 et -603 entraînant l'échec du clonage de la DIB

Si les attributs et la réplication codés sont activés au niveau de l'arborescence, le clonage de la DIB échoue avec les erreurs suivantes :

- Clone DIB on target server fails with the -601 error while configuring SAS (Échec du clonage de la DIB sur le serveur cible avec l'erreur -601 lors de la configuration SAS)
- After Clone DIB, the newly created clone object fails with the -603 error (Après le clonage de la DIB, le nouvel objet Clone échoue avec l'erreur -603)

Pour éviter ces problèmes, désactivez les attributs et la réplication codés.

Échec possible du clonage de la DIB immédiatement après le chargement en bloc hors ligne

Si vous tentez de cloner un serveur immédiatement après un chargement en bloc hors ligne, l'opération peut échouer si le chargement en bloc a été effectué avec l'option de désactivation des index.

Cela ne pose toutefois pas problème si le clonage de la DIB est initié quelques heures après la fin du chargement en bloc.

Problème au niveau du clonage lorsque la fonction de réplication codée est activée

Pour effectuer une opération de clonage avec la fonction de réplication codée activée sur le serveur source, modifiez la stratégie ER pour exclure temporairement le serveur cloné. Ceci peut être changé une fois la configuration du serveur cloné effectuée.

Dépannage des services d'infrastructure de clés publiques de NetIQ

Non-fonctionnement des opérations PKI

Si les opérations d'infrastructure de clés publiques (Public Key Infrastructure, PKI) dans iManager ne fonctionnent pas, cela peut provenir du fait que les services PKI de NetIQ ne sont pas en cours d'exécution sur l'hôte Linux. Pour démarrer les services PKI, entrez la commande `npki -1`.

Si vous ne pouvez pas créer de certificats, vous devez vous assurer que le module NICI est correctement installé. Reportez-vous à la section « Initialisation du module NICI sur le serveur » du *Guide d'administration de NetIQ eDirectory*. Pour vérifier si le module NICI est initialisé, reportez-vous à la section « Vérification de l'installation et de l'initialisation de NICI sur le serveur » du *Guide d'administration de NetIQ eDirectory*.

La suppression de la configuration d'un serveur eDirectory qui fonctionne comme serveur de clés d'arborescence dans une arborescence multiserveur, après que les objets eDirectory existants ont été déplacés vers un serveur différent, échoue et renvoie le code d'erreur correspondant à une réplique décisive.

Pour terminer l'opération, vous devez remplacer l'attribut DN du serveur de clés dans l'objet W0, sous le conteneur Sécurité > KAP, par un autre serveur de l'arborescence ayant téléchargé la clé d'arborescence à partir de ce serveur.

1. Dans NetIQ iManager, cliquez sur le bouton **Rôles et tâches** .
2. Cliquez sur **Administration eDirectory** > **Modifier un objet**.
3. Indiquez le nom et le contexte de l'objet W0 (il s'agit en général de W0.KAP.Security), puis cliquez sur **OK**.
4. Dans la colonne **Attributs définis**, sélectionnez **NDSPKI:SD Key Server DN**, puis cliquez sur **Éditer**.
5. Spécifiez le nom et le contexte d'un autre serveur dans le champ **DN du serveur de clés du domaine de sécurité**, puis cliquez sur **OK**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Lors de la désinstallation du serveur eDirectory contenant l'objet Autorité de certification (CA), les objets KMO créés sur ce serveur sont déplacés vers un autre serveur de l'arborescence et rendus non valides.

Vous devez recréer les objets CA et KMO pour l'arborescence. Pour plus d'informations, reportez-vous aux sections « Création d'un objet Autorité de certification organisationnelle » et « Création d'un objet Certificat de serveur » du *Guide d'administration de NetIQ eDirectory*.

Il est recommandé de ne pas désinstaller le serveur eDirectory sur lequel l'objet Autorité de certification de l'arborescence a été créé.

Utilisation de PKIDiag

PKIDiag est un utilitaire conçu pour diagnostiquer et corriger les objets Serveur de certificats. PKIDiag peut être utilisé pour effectuer les tâches suivantes :

- Renommer ou déplacer des objets relatifs à des serveurs afin qu'ils respectent l'assignation de nom et le schéma d'endiguement appropriés si un serveur a été déplacé.
- Créer les objets requis s'ils n'existent pas.
- Accorder les droits nécessaires entre les objets.
- Lier les objets s'ils ne le sont pas.
- Créer les certificats SSL CertificateIP et SSL CertificateDNS s'ils n'existent pas.
- Corriger les certificats SSL CertificateIP et SSL CertificateDNS s'ils présentent un nom incorrect ou sont périmés ou proches de l'expiration.

La fonctionnalité PKIDiag est utilisée par deux autres processus, la vérification automatique de l'état de santé du serveur et la tâche de création d'un certificat par défaut dans iManager.

La vérification automatique de l'état de santé du serveur est exécutée chaque fois qu'un serveur est redémarré ou que DSREPAIR est exécuté. Vous utilisez le processus de création d'un certificat par défaut pour remplacer les certificats par défaut créés lors de l'installation de Certificate Server. Pour plus d'informations, reportez-vous à la section « Création d'objets Certificat de serveur par défaut » page 735.

Reportez-vous au document TID #3640106 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3640106&sliceId=SAL_Public&dialogID=2494290&stateId=1%200%202492620) pour plus d'informations sur PKIDiag et son utilisation.

Message d'attente de la synchronisation des serveurs

Il arrive qu'après la création du certificat de l'utilisateur, le client ne parvienne pas à rafraîchir la vue afin d'inclure le nouveau certificat. Une boîte de dialogue apparaît alors avec un message indiquant que le système attend la synchronisation des serveurs. À ce stade, le certificat de l'utilisateur a été créé, mais les serveurs concernés par la création n'ont pas encore été synchronisés. Vous pouvez fermer la boîte de dialogue sans incidence sur la création du certificat de l'utilisateur.

Erreur lors de la réutilisation de surnoms de certificat

Si une erreur se produit au cours de la création d'un certificat utilisateur, essayez d'utiliser un surnom différent pour le certificat. Le surnom spécifié n'est peut-être pas disponible pour une réutilisation.

Erreur -1426 lors de l'exportation d'une clé privée d'un utilisateur

Tous les serveurs comportant des répliques de la partition dans laquelle réside l'objet Utilisateur doivent disposer du même niveau de cryptographie (NICI américaine/internationale ou NICI restreinte à l'importation). Si ce n'est pas le cas, un message d'erreur -1426 peut s'afficher lorsque vous exportez la clé privée de l'utilisateur si la taille de cette dernière est trop élevée.

Pour exporter la clé privée de l'utilisateur après une erreur -1426, vous devez mettre à niveau la cryptographie sur les serveurs comportant des répliques de la partition ou supprimer la réplique des serveurs disposant d'une cryptographie exportable.

Le serveur utilise un certificat SSL CertificateIP ayant expiré

eDirectory 9.0 ne prend pas en charge le certificat SSL CertificateIP. Si vous effectuez la mise à niveau vers eDirectory 9.0 à partir d'une version antérieure, le certificat SSL CertificateIP reste associé au serveur. Lorsque les certificats dans votre environnement expirent, le certificat SSL CertificateIP ne se renouvelle pas automatiquement.

Une fois la mise à niveau vers eDirectory 9.0 effectuée, vous pouvez commencer à utiliser le certificat SSL CertificateDNS au lieu du certificat SSL CertificateIP quand vous le voulez.

Autorités de certification externes

Certaines autorités de certification tierces telles que VeriSign utilisent une autorité de certification intermédiaire pour signer les certificats de serveur. Pour importer ces certificats dans un objet Certificat de serveur, le certificat de serveur ainsi que l'autorité de certification intermédiaire et le certificat de racine approuvée doivent figurer dans un seul fichier au format PKCS#7 (`.p7b`). Si votre autorité de certification ne peut pas fournir ce type de fichier, vous pouvez en créer un vous-même en suivant la procédure ci-dessous sur une machine cliente avec Internet Explorer 5.5 ou version ultérieure.

1. Importez le certificat du serveur dans Internet Explorer. Pour ce faire, double-cliquez sur le fichier ou accédez à **Fichier** > **Ouvrir** et sélectionnez le nom de fichier.
2. Si le certificat de l'autorité de certification externe n'est pas déjà répertorié comme autorité de certification approuvée dans Internet Explorer, importez les autorités de certification intermédiaires ainsi que l'autorité de certification de niveau de la racine de la même manière.
3. Dans Internet Explorer, sélectionnez **Outils** > **Options Internet**. Sélectionnez l'onglet **Contenu**, puis le bouton **Certificats**.
4. Sous l'onglet **Personnel**, recherchez le certificat du serveur. Sélectionnez-le, puis cliquez sur **Exporter**.
5. Acceptez les valeurs par défaut dans l'assistant jusqu'à ce que vous arriviez à la page Format du fichier d'exportation, puis sélectionnez le format Standard de syntaxe de message cryptographique - Certificats PKCS#7 (.p7b).
6. Continuez la procédure dans l'assistant.

   Le fichier PKCS#7 peut désormais être importé dans l'objet Certificat de serveur.

Déplacement d'un serveur

Si un objet Serveur est déplacé, les objets LDAP, Service SAS et Certificat du serveur (les objets KMO, « Key Material Object », ou objets Matériel clé) de ce serveur doivent également être déplacés. Notez toutefois que la vérification automatique de l'état de santé du serveur déplacera ces objets pour vous la prochaine fois que vous redémarrez le serveur.

Prise en charge de DNS

Si DNS est configuré pour le serveur, le nom de l'objet par défaut pour un certificat de serveur sera :

.CN=<*nom_DNS_serveur*>.O=<*nom_arborescence*>

Dans le cas contraire, le nom de l'objet par défaut est le nom distinctif complet du serveur. Vous pouvez modifier le nom de l'objet par défaut en sélectionnant Personnalisé au cours du processus de création du certificat.

Suppression d'un serveur

Lorsque vous supprimez un serveur d'eDirectory™ et le réinstallez dans le même contexte sous le même nom, la réinstallation ne se déroule correctement que si vous supprimez également l'objet Service SAS qui représente le serveur supprimé (s'il existe).

Le processus doit se dérouler comme suit :

1. Déterminez si les certificats par défaut doivent être sauvegardés. Si c'est le cas, sauvegardez-les.
2. Supprimez les certificats par défaut.
3. Supprimez l'objet SAS.

Par exemple, pour un serveur nommé mon_serveur, il peut exister un objet SAS nommé Service SAS – mon_serveur dans le même conteneur que le serveur. Vous devez supprimer manuellement cet objet SAS (via iManager) après avoir supprimé le serveur de l'arborescence, mais avant de le réinstaller.

en présence d'un serveur de CA organisationnelle ou de clés SD, vous devez effectuer des opérations supplémentaires. Ces opérations sont décrites dans le document TID #3623407 (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3623407&sliceId=SAL_Public&dialogID=2494325&stateId=1%200%202492660).

Les certificats de serveur par défaut créés pour le serveur doivent également être supprimés, de manière à être recréés lors de la réinsertion du serveur.

Il s'agit des certificats SSL Certificate IP – mon_serveur et SSL Certificate DNS – mon_serveur. Vous devez faire preuve de vigilance lors de la suppression de ces certificats. Si des données ont été codées à l'aide de l'un de ces certificats, il convient de les récupérer avant de supprimer les certificats.

Limitations des noms d'objet des autorités de certification

Les certificats de serveur contenant un caractère @ dans leur nom d'objet peuvent entraîner un échec des connexions SSL. Contactez le support technique pour résoudre le problème.

Vitesse de validation des certificats

Le processus de validation des certificats comprend plusieurs vérifications des données contenues dans le certificat, ainsi que des données dans la chaîne de certificats. Une chaîne de certificats est constituée d'un certificat d'autorité de certification racine et, éventuellement, des certificats des autorités de certification intermédiaires.

La validation des informations contenues dans un certificat et sa chaîne de certificats associée ne nécessite pas beaucoup de temps. Toutefois, l'opération peut être un peu plus longue dans les cas suivants :

- Si le certificat a été signé par une autorité de certification externe et si un ou plusieurs des certificats ont une extension de point de distribution CRL.

  Afin de valider le certificat, la CRL de chaque certificat applicable dans la chaîne doit être récupérée. La CRL doit alors être examinée pour déterminer si le certificat a été révoqué.

Si les CRL sont volumineuses ou si le serveur utilisant le point de distribution CRL est occupé, la validation du certificat peut prendre un certain temps. Pour accélérer l'opération, vous pouvez prendre l'une des mesures suivantes (ou les deux) :

- Augmentez la vitesse de la connexion utilisée pour vérifier l'état de révocation du certificat.
- Contactez le fournisseur de l'autorité de certification.

- Si un ou plusieurs certificats comportent une extension AIA OCSP. Si le répondeur OCSP est occupé, la validation peut nécessiter beaucoup de temps.
- Si vous validez un certificat utilisateur.

  Pour les certificats de serveur, toute la chaîne de certificats est stockée avec le certificat du serveur dans l'objet Matériel clé. Par conséquent, lorsqu'un certificat de serveur est validé, le client peut obtenir tous les certificats nécessaires en lisant simplement un seul objet. Il en va autrement pour les certificats utilisateur. Seul le certificat utilisateur proprement dit est stocké dans l'objet Utilisateur. Par conséquent, le client doit récupérer la chaîne de certificats à partir d'autres objets stockés dans le conteneur de sécurité afin de valider le certificat utilisateur.

  Afin de valider un certificat utilisateur signé par l'autorité de certification organisationnelle, le client doit lire l'objet de cette dernière, afin de récupérer le certificat de l'autorité de certification. Afin de valider un certificat utilisateur signé par une autorité de certification externe, le client doit lire le conteneur de racines approuvées dans le conteneur de sécurité pour composer une chaîne de certificats qui correspond au certificat utilisateur. Dans ce cas, pour que la validation du certificat utilisateur réussisse, un administrateur doit avoir déjà importé les certificats des autorités de certification externes dans le conteneur de racines approuvées.

  Le temps nécessaire à la validation d'un certificat utilisateur peut être réduit en supprimant du conteneur de racines approuvées les certificats ayant expiré qui ne sont plus approuvés.

Validation de certificats après la suppression de l'autorité de certification organisationnelle

Si vous supprimez l'autorité de certification organisationnelle (à un moment autre que lors d'une procédure de sauvegarde et de restauration), vous devez exporter le certificat auto-signé et créer une nouvelle racine approuvée dans le conteneur de racines approuvées. Si vous ne le faites pas, vous rencontrerez le comportement suivant lors de la validation de ces certificats :

- Les certificats utilisateur signés par l'autorité de certification supprimée ne sont pas valides. Cela est dû au fait que le certificat de l'autorité de certification qui a signé le certificat utilisateur est introuvable dans l'objet Autorité de certification organisationnelle ou dans le conteneur de racines approuvées. Si vous souhaitez que ces certificats utilisateur restent valides, vous devez ajouter le certificat auto-signé de l'ancienne autorité de certification dans le conteneur de racines approuvées.
- Les certificats de serveur signés par l'autorité de certification supprimée restent valides. Cela est dû au fait que le certificat de l'autorité de certification est stocké dans l'objet Matériel clé, avec le certificat de serveur.

  Si vous avez supprimé l'autorité de certification organisationnelle parce que la clé a été compromise ou en raison d'une faille de sécurité, vous devez révoquer immédiatement tous les certificats utilisateur et de serveur signés par cette autorité. Si vous ne pouvez pas les révoquer, vous devez les supprimer et créer de nouveaux certificats pour les remplacer. Vous devez également demander à tous les utilisateurs susceptibles d'avoir importé le certificat de votre autorité de certification organisationnelle dans leur navigateur de le supprimer.

Changement de nom du conteneur de sécurité

Vous ne pouvez pas renommer le conteneur de sécurité.

eDirectory ne peut pas valider les certificats après la recréation de l'autorité de certification de l'arborescence

eDirectory ne parvient pas à valider les certificats après la recréation de l'autorité de certification lors de la mise à niveau d'eDirectory vers la dernière version ou lors de son installation dans un emplacement personnalisé.

Pour résoudre ce problème, si le chemin d'installation d'eDirectory est différent de `C:\NetIQ\eDirectory` (sous Windows) ou `/var/opt/novell/eDirectory` (sous Linux), vous devez spécifier le chemin d'accès au fichier CRL correct conformément au chemin d'installation d'eDirectory lorsque vous recréez l'autorité de certification de l'arborescence ou lors de la création de l'objet CRL. Vous devez choisir l'option Personnalisé dans le plug-in iManager lors de la recréation de l'autorité de certification à partir de l'Assistant Configurer l'autorité de certification et spécifier le chemin d'accès au fichier CRL correct pour éviter toute erreur. Par exemple, eDirectory installe par défaut les fichiers CRL dans le chemin `C:\NetIQ\eDirectory\htdoc\crl\`. Si vous installez eDirectory dans un emplacement personnalisé (`C:\`*`emplacement_personnalisé`*`\eDirectory\`), veillez à mettre à jour le chemin d'accès au fichier CRL lors de la recréation de l'autorité de certification de l'arborescence. Par exemple, `C:\`*`emplacement_personnalisé`*`\eDirectory\htdoc\crl\`.

REMARQUE : si une version antérieure d'eDirectory a été installée dans l'emplacement par défaut (`C:\Novell\NDS\`), vous devez appliquer la solution décrite ci-dessus lorsque vous recréez l'autorité de certification de l'arborescence après une mise à niveau vers la dernière version.

Utilitaires de dépannage sous Linux

Utilitaire d'importation, de conversion et d'exportation NetIQ

Si un serveur LDAP est rafraîchi ou déchargé pendant qu'une opération de l'utilitaire d'importation/de conversion/d'exportation NetIQ est en cours, le message `Timeout de l'opération LBURP` s'affiche. Le serveur est rétabli ultérieurement, lorsque le délai de l'opération LBURP expire.

Utilitaire ndsmerge

Les serveurs PKI sont inactifs après une opération de fusion. Ils doivent être redémarrés à l'aide de la commande `npki -l`.

Les opérations de fusion peuvent échouer sur des versions différentes du produit. Si votre serveur exécute une ancienne version des NDS ou d'eDirectory, mettez-le à jour vers la dernière version d'eDirectory, puis reprenez l'opération de fusion.

La fusion de deux arborescences échoue si des conteneurs subordonnés possédant le même nom figurent dans les arborescences source et cible. Renommez l'un des conteneurs, puis continuez la fusion.

Pendant l'opération de greffage, le message d'erreur `-611 endiguement non autorisé` peut s'afficher. Modifiez le schéma en exécutant `ndsrepair`. Exécutez `ndsrepair -S` et sélectionnez **Améliorations de schéma facultatives**.

Si vous essayez d'effectuer une sauvegarde incrémentielle avant d'effectuer une sauvegarde complète, l'opération de sauvegarde échoue.

Utilitaire DSTrace

Si vous avez activé l'écran DSTrace, un message d'erreur peut apparaître, indiquant qu'un objet primaire n'est pas valide pour le lien de référence. Vous pouvez ignorer ce message si eDirectory fonctionne correctement.

Utilitaire ndsbackup

Lors de la sauvegarde d'eDirectory, le message `Erreur NDS : Échec de la connexion au serveur NDS.` peut s'afficher. Cela peut être dû au fait que eDirectory écoute sur un port différent du port par défaut 524. Dans la ligne de commande, entrez le numéro de port sur lequel eDirectory a été configuré. Par exemple, si eDirectory a été configuré sur le numéro de port 1524, entrez ce qui suit :

```
ndsbackup sR 164.99.148.82:1524
```

Lorsque vous sauvegardez les données, eDirectory peut afficher un message `NDS Error: Requires a Password` (Erreur NDS : mot de passe requis). En effet, le serveur contient peut-être des attributs marqués pour le chiffrement et il se peut que vous n'ayez pas utilisé l'option -E pour chiffrer ou déchiffrer les données de sauvegarde.

Si vous essayez d'effectuer une sauvegarde incrémentielle avant d'effectuer une sauvegarde complète, l'opération de sauvegarde échoue.

Erreur -786 lors de l'exécution de DSRepair

Lorsque vous utilisez DSRepair, vous devez disposer dans la partition spécifique de votre machine sur laquelle s'exécute DSRepair d'un espace disponible correspondant au triple de la taille du fichier DIB.

Les utilitaires d'eDirectory impliquent que les utilisateurs s'authentifient à l'aide d'un mot de passe NDS

Si le mot de passe universel est utilisé, il doit être synchronisé avec le `mot de passe NDS` afin que tous les outils de ligne de commande d'eDirectory puissent s'authentifier.

Dépannage de NMAS

Codes d'erreur NMAS

Une liste complète des codes d'erreur NMAS est disponible dans le NDK de NMAS.

Problèmes liés aux méthodes de connexion et aux séquences

- Pour que les produits utilisent correctement les méthodes de connexion NMAS, au moins un serveur NMAS de la partition eDirectory doit contenir une réplique Lecture/écriture des objets Utilisateur qui emploieront NMAS.
- Toutes les méthodes de connexion ou de post-connexion n'utilisent pas le champ de mot de passe initial lorsqu'elles sont activées. Si vous êtes invité à entrer un mot de passe, vous pouvez ignorer le champ de mot de passe et fermez l'invite.
- Il est impossible d'utiliser deux méthodes avec mot de passe (méthodes simple et NDS, par exemple) dans une séquence de type AND si le client Novell est configuré pour afficher le champ de mot de passe (ce qui correspond à la configuration par défaut).

Problèmes d'administration

- Vous devez accorder des droits explicites aux utilisateurs avec authentification modulée. Les droits hérités ne sont pas valides. Par exemple, le droit Superviseur est défini pour un administrateur dans le conteneur [Root]. Les droits de l'administrateur ne sont pas définis dans l'objet Volume. Par conséquent, si l'administrateur change le libellé de sécurité du volume Connecté, il ne pourra pas disposer des droits appropriés. Il doit assigner des droits explicites au volume, aux répertoires ou aux fichiers du volume.
- Si le mot de passe universel est activé et que vous essayez de définir le mot de passe simple, un message d'erreur -1697 est renvoyé.
- Les utilitaires d'eDirectory tels que DSBackup (ndsbackup), DSRepair (ndsrepair) et DSMerge (ndsmerge) fonctionnent avec des mots de passe NDS, mais pas avec des mots de passe simples NMAS. eDirectory 9.0 utilise le mot de passe universel.

  Pour plus d'informations sur le mot de passe universel, reportez-vous au *NetIQ Password Management 3.3.2 Administration Guide* (https://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html) (Guide d'administration de NetIQ Password Management 3.3.2).
- Si vous cliquez sur **OK** ou basculez entre des onglets pendant la création ou le changement de nom d'un libellé, cela crée ou renomme toujours le libellé, même si vous répondez **Non** au message vous invitant à **enregistrer les modifications apportées aux libellés**. Vous devez cliquer sur le bouton **Annuler** pour ignorer les modifications. Une fois un libellé créé, il ne peut pas être supprimé. Vous pouvez cependant le renommer avec un nom encore inutilisé, tel que `Inutilisé_x`.
- Lorsque vous utilisez les fonctions d'audit XDAS pour NMAS, le format DN des événements suivants n'est pas généré dans la notation LDAP.
  - 00290035 - Résultat du mécanisme SASL
  - 00290061 - Définition de la configuration de la connexion
  - 00290062 - Obtention de la configuration de la connexion
  - 00290064 - Définition du secret de connexion

  REMARQUE : l'ID (par exemple, 00290035 ou 00290061) correspond à l'ID d'événement NMAS comme indiqué dans le fichier `lsc`. L'ID d'événement NMAS fait partie du champ `subEvent` dans le format XDAS.

Connexion impossible sous Linux quelle que soit la méthode utilisée

Après avoir installé et configuré NMAS, redémarrez le serveur eDirectory.

Si vous réinstallez une méthode après avoir désinstallé une instance antérieure de cette méthode, redémarrez le serveur eDirectory.

L'utilisateur ajouté à l'aide de l'utilitaire ICE ne parvient pas à se connecter avec un mot de passe simple on Linux

Lorsque vous ajoutez des utilisateurs avec des mots de passe simples via l'utilitaire d'importation, de conversion et d'exportation NetIQ, utilisez l'option `-l`.

SLP_NETWORK_ERROR(-23) Se produit sur des machines Windows

La requête SLP (Service Location Protocol) renvoie l'erreur -23 SLP_NETWORK_ERROR sur les machines virtuelles ayant une adresse DHCP ou sur les machines physiques ou virtuelles dans lesquelles le protocole SLP n'est pas diffusé.

Vous pouvez éviter cette erreur SLP en configurant l'agent Annuaire de votre réseau de l'une des manières suivantes :

1. Copiez le fichier `C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf` dans le répertoire `c:\Windows\`.
2. Ouvrez le fichier `slp.conf` à l'aide d'un éditeur de texte et modifiez la ligne suivante :

   ```
   ;net.slp.DAAddresses = myDay1,myDa2,myDa3
   ```

   par

   ```
   net.slp.DAAddresses = <Give your DA Address>
   ```

3. Enregistrez les modifications, puis fermez le fichier.

OU

1. Copiez le fichier `C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf` dans le répertoire `c:\Windows\`.
2. Ouvrez le fichier `slp.conf` à l'aide d'un éditeur de texte et modifiez la ligne suivante :

   ```
   ;net.slp.isDA = true
   ```

   par

   ```
   net.slp.isDA = true
   ```

3. Enregistrez les modifications, puis fermez le fichier.

Le chemin d'installation qui apparaît dans le champ Chemin d'installation lors de l'installation d'eDirectory sous Windows est incorrect

Lorsque vous installez eDirectory, si, au lieu d'accepter l'emplacement par défaut pour l'installation, vous cliquez sur l'icône **Parcourir** pour sélectionner un autre emplacement, puis fermez la boîte de dialogue Parcourir sans sélectionner de dossier, le chemin d'installation qui apparaît dans le champ **Chemin d'installation** est incorrect. Ce problème se produit uniquement lors de l'installation d'eDirectory sous Windows Server 2012 Édition Standard (64 bits) et Windows Server 2012 R2 (64 bits).

Pour résoudre ce problème, remplacez manuellement le chemin d'accès par l'emplacement souhaité.

L'ajout d'un serveur n'aboutit pas si le protocole SLP n'est pas configuré correctement sous Windows.

L'installation d'eDirectory échoue lors de l'ajout d'un serveur à une arborescence (où vous devez parcourir votre arborescence actuelle), si SLPD est déjà installé et en cours d'exécution. Windows affiche le message *launch.exe died*.

Pour installer correctement eDirectory, effectuez les opérations suivantes sans redémarrer le système :

1. Arrêtez le protocole SLP (Service Location Protocol).
2. Supprimez le fichier `C:\Windows\slp.conf`.
3. Supprimez le dossier `C:\Windows\System32\Novell\eDir\OpenSLP`.

4 Supprimez la valeur RegKeys du service SLPD de `Registry HKLM\SYSTEM\CurrentControlSet\Services\slpd`.

5 Exécutez à nouveau le programme d'installation avec le rôle d'administrateur.

Accès à HTTPSTK lorsque les services Annuaire ne sont pas chargés

Vous pouvez définir un utilisateur Admin préconfiguré qui permet d'accéder à HTTPSTK (HTTP Protocol Stack - pile de protocoles HTTP) lorsque DS n'est pas chargé. L'utilisateur admin préconfiguré, sadmin, a des droits équivalents sur l'objet Utilisateur eDirectory admin. Si l'état du serveur ne permet pas à eDirectory de fonctionner correctement, vous pouvez vous connecter au serveur avec l'identité de cet utilisateur et effectuer toutes les tâches requises de diagnostic et de débogage qui ne requièrent pas eDirectory.

Définition du mot de passe sadmin sous Windows

Utilisez la page du gestionnaire à distance DHOST (accessible via l'URL `/dhost` ou à partir de la page racine) pour définir le mot de passe sadmin. Si vous voulez définir ou modifier le mot de passe sadmin, `dhost.exe` doit être en cours d'exécution sur le serveur eDirectory.

1 Ouvrez un navigateur Web.

2 Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   par exemple :

   `http://MyServer:80/dhost`

   Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

   `http://137.65.135.150:80/dhost`

3 Entrez un nom d'utilisateur, un contexte et un mot de passe.

4 Cliquez sur **Serveur HTTP**, puis entrez un mot de passe sadmin.

5 Vérifiez le mot de passe que vous venez d'entrer, puis cliquez sur **Soumettre**.

Définition du mot de passe sadmin sous Linux

Pour définir le mot de passe sadmin sous Linux, vous pouvez utiliser la page de gestion à distance DHost ou l'utilitaire ndsconfig.

Utilisation de la page de gestion à distance de DHost

Accédez à la page du gestionnaire distant de DHost via l'URL `/dhost` ou à partir de la page racine, et définissez le mot de passe sadmin. Si vous voulez définir ou modifier le mot de passe sadmin, le serveur eDirectory doit être en cours d'exécution.

1 Ouvrez un navigateur Web.

2 Dans le champ de l'adresse URL, saisissez :

   `http://nom.serveur:port/dhost`

   par exemple :

   `http://MyServer:80/dhost`

Vous pouvez également utiliser l'adresse IP du serveur pour accéder à DHost iConsole. Par exemple :

```
http://137.65.135.150:80/dhost
```

3 Entrez un nom d'utilisateur, un contexte et un mot de passe.

4 Cliquez sur **Serveur HTTP**, puis entrez un mot de passe sadmin.

5 Vérifiez le mot de passe que vous venez d'entrer, puis cliquez sur **Soumettre**.

Utilisation de ndsconfig

L'utilitaire ndsconfig permet de définir le mot de passe sadmin. Si vous voulez définir ou modifier ce mot de passe, ndsd doit être en cours d'exécution sur le serveur eDirectory.

Entrez la commande suivante sur la console du serveur : :

```
ndsconfig set http.server.sadmin-pwd=mot_de_passe
```

où *mot de passe* représente le nouveau mot de passe sadmin.

Pour plus d'informations sur l'utilisation de l'utilitaire ndsconfig, reportez-vous à la section « Paramètres de l'utilitaire ndsconfig » du *Guide d'installation de NetIQ eDirectory* .

Dépannage du codage des données

NetIQ eDirectory 9.0 permet de chiffrer certaines données sensibles lors de leur stockage sur le disque et lorsque le client y accède. Ce chapitre fournit des informations sur les erreurs susceptibles de se produire lors de l'utilisation des fonctions de réplication et des attributs chiffrés dans eDirectory 9.0.

Pour plus d'informations sur les autres messages d'erreur dans eDirectory, reportez-vous au site Web des codes d'erreur de NetIQ (http://www.novell.com/documentation/nwec/).

-6090 0xFFFFE836 ERR_ER_DISABLED

Le processus de synchronisation des répliques eDirectory a tenté de démarrer la réplication codée avec le serveur eDirectory cible, alors que le processus de réplication codée des répliques est désactivé sur ce serveur.

Cause possible

La réplication codée est désactivée sur le serveur eDirectory cible.

Opération

Activez la réplication codée sur le serveur eDirectory cible.

-6089 0xFFFFE837 ERR_REQUIRE_SECURE_ACCESS

Une application (accès du client) a tenté d'accéder à un attribut codé par le biais d'un canal en texte clair.

Source

eDirectory ou NDS.

Cause possible

Les attributs codés sont configurés de manière à n'être accessibles que par le biais d'un canal sécurisé. L'application essaie toutefois d'y accéder via un canal en texte clair.

Opération

L'application doit accéder aux attributs codés par le biais d'un canal sécurisé, tel qu'un canal sécurisé LDAP ou HTTP.

Cause possible

Si cette erreur se produit lors de la réplication, cela signifie qu'un ou plusieurs serveurs de l'anneau de répliques ont des attributs marqués pour le chiffrement et sont configurés de manière à n'être accessibles que par le biais d'un canal sécurisé.

Opération

Changez la configuration de la règle d'attributs codés pour que ces derniers soient accessibles via des canaux non sécurisés. Pour plus d'informations, reportez-vous au Chapitre 11, « Chiffrement des données dans eDirectory », page 315.

Cause possible

Si cette erreur se produit lorsque la réplication codée est configurée au niveau de la partition ou entre les répliques de cette dernière, cela signifie que l'anneau de répliques contient des serveurs dotés d'une version d'eDirectory antérieure à 9.0.

Opération

Mettez à niveau tous les serveurs de l'anneau de répliques vers une version compatible avec eDirectory 9.0.

-666 FFFFFD66 INCOMPATIBLE NDS VERSION

Texte à insérer ici

Cause possible

Si la réplication codée est activée au niveau de la partition et que vous essayez d'ajouter une réplique de cette partition à un serveur eDirectory, cela signifie que la version eDirectory de ce dernier n'est pas compatible avec celle du serveur source.

Opération

Mettez à niveau le serveur vers une version compatible d'eDirectory.

Cause possible

Si la partition parent inclut des serveurs dotés d'une version d'eDirectory antérieure à 9.0 (anneau avec différentes versions) et si la réplication codée est activée pour la partition enfant, les opérations de fusion et/ou de jonction de partitions ne sont pas autorisées et l'erreur ERR_INCOMPATIBLE_DS_VERSION est renvoyée.

Cela s'explique par le fait que, d'une part, la partition enfant contient des données sensibles pour lesquelles la réplication codée est activée au niveau de la partition et que, d'autre part, la partition parent inclut un ou plusieurs serveurs dotés d'une version d'eDirectory antérieure à 9.0. La réplication codée étant uniquement activée entre les serveurs eDirectory 9.0, lors d'opérations de fusion, les données sensibles sont exposées pendant la réplication vers les serveurs dotés de versions antérieures à eDirectory 9.0.

Opération

1. Mettez à niveau le serveur vers une version compatible d'eDirectory.

   OU

2. Désactivez la réplication codée pour la partition parent ou enfant.

   REMARQUE : Si vous désactivez la réplication codée, la réplication s'effectuera en texte clair.

Problème de doublons d'algorithmes de chiffrement

Si vous ajoutez un attribut pour le chiffrement à l'aide de LDIF, n'associez pas deux algorithmes à un même attribut.

Par exemple, si vous désignez *title* comme un attribut codé avec les algorithmes de codage AES et DES, l'algorithme à considérer en fin de compte n'est pas clairement défini. À chaque exécution du contrôleur de connectivité (limber), l'attribut title bascule entre AES et DES. C'est comme si la configuration était modifiée.

Pour éviter ce type de scénario, nous vous recommandons de ne pas assigner deux algorithmes à un même attribut.

Cela ne se produit pas si vous marquez les attributs pour le chiffrement à l'aide d'iManager.

Chiffrement des attributs de flux

Les attributs de flux peuvent être présents sous forme de données en texte clair. Cela s'explique par le fait que eDirectory 9.0 ne code pas les attributs de flux.

Configuration de la réplication codée via iManager

Vous ne pouvez pas configurer la réplication codée via iManager si l'un des serveurs de l'anneau de répliques est arrêté.

Affichage/modification d'attributs codés via iManager

Si un attribut d'un objet est codé, vous ne pouvez pas afficher ni modifier l'objet à l'aide d'iManager.

Pour éviter ce problème, vous pouvez afficher ou modifier l'attribut codé via un canal sécurisé grâce à l'une des méthodes suivantes :

- LDAP : la requête LDAP doit être envoyée via un canal sécurisé, ce qui signifie qu'il faut utiliser le certificat de racine approuvée du serveur.
- ICE : l'objet peut être modifié à l'aide de scripts LDIF. Dans ce cas, ICE doit utiliser un canal sécurisé.
- Utilisez iManager 2.5 FP2, iManager 2.6 ou une version ultérieure.

REMARQUE : nous vous recommandons d'utiliser iManager 2.6 ou une version ultérieure pour afficher ou modifier les attributs codés.

Vous pouvez également désactiver l'option imposant l'utilisation d'un canal sécurisé pour afficher ou modifier les attributs codés en désactivant l'attribut `requireSecure` dans la règle d'attributs codés. L'objet et les attributs codés deviennent alors accessibles par tous les clients via un canal en texte clair. Une fois cette opération effectuée, iManager pourra accéder à l'objet.

Échec de la fusion d'arborescences avec la réplication codée activée

Lorsque la réplication codée est activée, la fusion d'arborescences échoue. Avant d'effectuer ce type d'opération, veillez donc à désactiver la réplication codée pour chaque arborescence.

Le contrôleur de connectivité (limber) affiche l'erreur -603

Le contrôleur de connectivité (limber) affiche l'erreur -603 si le serveur dispose uniquement d'une réplique de référence subordonnée de la partition de stratégie d'attributs codés.

Pour éviter ce problème, effectuez l'une des opérations suivantes :

- Attribuez un accès en lecture à l'objet Serveur NCP. Pour ce faire, utilisez iManager pour ajouter un ayant droit à la racine de l'arborescence et accorder un accès en lecture à l'objet Serveur NCP. Dans les attributs, spécifiez `attrEncryptionDefinition` et `attrEncryptionRequiresSecure`.
- Attribuez un accès public en lecture aux attributs suivants via LDAP ou ndssch :
  - `attrEncryptionDefinition`
  - `attrEncryptionRequiresSecure`

eDirectory Management Toolbox

L'outil eMBox (NetIQ eDirectory Management Toolbox) permet d'accéder à tous les utilitaires de l'interface dorsale d'eDirectory, à distance comme sur le serveur.

eMBox, combiné à NetIQ iManager, fournit un accès via le Web à des utilitaires tels que DSRepair, DSMerge, Service Manager, ainsi qu'à l'utilitaire de sauvegarde et de restauration.

IMPORTANT : pour pouvoir exécuter les tâches eMBox, les services basés sur le rôle doivent être configurés via iManager pour l'arborescence à administrer.

Toutes les fonctions sont accessibles, sur le serveur local ou à distance, via un client à ligne de commande. Grâce au client eMBox, vous pouvez effectuer des tâches pour plusieurs serveurs à partir d'un seul serveur ou poste de travail. Pour exécuter tous les outils eMTools (eDirectory Management Tools), tels que Backup, DSRepair, DSMerge, Schema Operations et eDirectory Service Manager, eMBox doit être chargé et en cours d'exécution sur le serveur eDirectory.

Impossible d'arrêter les services eMTool

Lors de l'exécution de la commande `serviceStop -n{service}`, dans laquelle *{service}* correspond à l'un des services (`libsasl.so`, `libncpengine.so`, `libhttpstk.so` ou `libdsloader.so`), l'erreur suivante se produit :

```
Service {service} could not be stopped, Error : -660
```

Il ne s'agit pas d'une erreur. Vous ne pouvez pas arrêter ces processus (plus particulièrement `libsasl.so`, `libncpengine.so`, `libhttpstk.so` et `libdsloader.so`), car d'autres modules en dépendent.

La restauration génère l'erreur -6020

Si vous avez repositionné les journaux dans un emplacement par défaut pendant une opération de restauration à l'aide de DSBK ou d'un client eMBox, l'erreur -6020 s'affiche. Pour éviter cette erreur, vous devez indiquer le paramètre `-s` dans la commande `restore`.

Suppression d'un objet déplacé

La suppression d'un objet déplacé peut échouer (erreur -637) dans une arborescence contenant plusieurs serveurs.

Problème de déplacement de groupe dynamique

Le déplacement d'un objet Groupe dynamique comportant `dynamicgroup` dans l'attribut `Object Class` vers un autre conteneur bloque la fonction de groupe dynamique. Une fois l'objet déplacé, les requêtes et les recherches sur les membres dynamiques ne fonctionnent pas.

Problème lors de la réparation des adresses réseau par l'intermédiaire de

Lors de la réparation des adresses réseau par l'intermédiaire de eMBox, les erreurs suivantes surviennent car eMBox n'est pas mis à jour avec les correctifs récents destinés à la réparation :

```
ERREUR : adresse réseau introuvable pour ce serveur - Erreur : 11004
```

```
ERREUR : reconnexion impossible. Erreur : 11004
```

Affichage des pages du manuel en français

Pour afficher les pages du manuel français sous Red Hat Linux, exportez l'élément suivant :

```
export MANPATH=/opt/novell/man/frutf8:/opt/novell/eDirectory/man/frutf8
```

Suppression d'un objet déplacé

La suppression d'un objet déplacé peut échouer (erreur -637) dans une arborescence contenant plusieurs serveurs.

eDirectory ne génère pas d'événement de déconnexion en raison des limites de sa partie client

eDirectory ne génère pas d'événement de déconnexion lorsque vous vous déconnectez d'iManager. Il s'agit d'une limitation technique du client faisant partie d'eDirectory.

Des applications d'audit peuvent utiliser des API NWDS pour recevoir des événements de déconnexion. Les applications qui utilisent LDAP peuvent toutefois surveiller les événements de déconnexion à l'aide des événements d'annulation de liaison.

Problèmes générés par la valeur de TERM lors de l'exécution de DSTrace

Les balises TIME et TAGS s'affichent comme activées (soulignées) bien qu'elles ne le soient pas par défaut. Si la valeur de TERM est définie sur VT100 ou xterm à partir d'un terminal Linux, ces balises s'affichent comme si elles étaient activées (soulignées). Ce problème ne survient avec aucun autre terme, par exemple dtterm.

eMBox ne gère pas les caractères double octet

eMBox ne gère pas les caractères double octet pour la configuration d'un répertoire de transaction individuelle par l'intermédiaire du client eMBox et d'iManager. Cette opération peut toutefois être exécutée via DSBK.

Dépannage de SASL-GSSAPI

Cette section traite des messages d'erreur consignés par le mécanisme d'authentification SASL-GSSAPI.

Problème lié à la présence de plusieurs objets Utilisateur

La liaison LDAP avec GSSAPI SASL échoue si le même principal Kerberos est associé à plusieurs objets Utilisateur eDirectory.

ID d'autorisation

Le fichier RFC 2222 prévoit la prise en charge d'un ID d'autorisation envoyé par l'utilisateur et le client. Cela n'est toutefois pas compatible avec la méthode SASL GSSAPI.

Fichier journal

Les messages d'erreur sont enregistrés dans le fichier `ndsd.log` dans les installations Linux.

Messages d'erreur

Message d'erreur	Problème
SASL-GSSAPI : Reading Object user_FDN FAILED eDirectory error code (La lecture de l'objet FDN_utilisateur a échoué code_erreur_eDirectory)	cette erreur est générée dans eDirectory. Les noms de principaux Kerberos ne sont pas associés à l'objet Utilisateur (`userdn`).
SASL-GSSAPI : Reading Object Realm_FDN FAILED eDirectory error code (La lecture de l'objet FDN_domaine a échoué code_erreur_eDirectory)	cette erreur est générée dans eDirectory. L'objet `Domaine` n'existe pas.
SASL-GSSAPI : Mémoire insuffisante	mémoire insuffisante pour exécuter l'opération.
SASL-GSSAPI: Invalid Input (Entrée non valide)	L'entrée du client est défectueuse ou non valide.
SASL-GSSAPI : NMAS error NMAS error code (Erreur NMAS code_erreur_NMAS)	cette erreur interne est générée dans NMAS.
SASL-GSS : Invalid LDAP service principal name *LDAP_service_principal_name* (Nom de principal de service LDAP nom_principal_service_LDAP non valide)	le nom de principal de service LDAP n'est pas valide.
SASL-GSS : Reading LDAP service principal key from eDirectory failed (La lecture de la clé de principal de service LDAP d'eDirectory a échoué)	**Cause :** l'objet Principal de service LDAP n'est pas créé. **Cause :** la clé maîtresse de l'objet Domaine est modifiée. **Cause :** l'objet Principal de service LDAP est introuvable dans la sous-arborescence du domaine auquel il appartient.

Message d'erreur	Problème
SASL-GSS : Creating GSS context failed (La création du contexte GSS a échoué)	**Cause :** l'heure n'est pas synchronisée entre le client, le KDC et les serveurs eDirectory. **Cause :** la clé du principal de service LDAP a été modifiée dans la base de données Kerberos, mais n'a pas été mise à jour dans eDirectory. **Cause :** le type de chiffrement n'est pas pris en charge.
SASL GSSAPI: Invalid user FDN = *user_FDN* (Nom de domaine complet utilisateur incorrect = FDN_utilisateur)	Le FDN de l'utilisateur fourni par le client n'est pas valide.
SASL-GSSAPI : No user DN is associated with principal *client_principal_name* (Aucun DN utilisateur associé au principal nom_principal_client)	Un objet `Utilisateur` de la sous-arborescence n'est pas associé au nom de principal Kerberos.
SASL-GSSAPI : More than one user DN is associated with principal *client_principal_name* (Plusieurs DN utilisateur sont associés au principal nom_principal_client)	Plusieurs objets `Utilisateur` de la sous-arborescence sont associés au même principal.
ldap_simple_bind_s : Références non valides major = 1, minor =0	**Cause :** Ce problème peut s'expliquer par le fait que la version du principal de service LDAP sur le serveur KDC ne correspond pas à celle du serveur eDirectory. En effet, à chaque extraction de la clé de principal de service LDAP vers le fichier keytab, le numéro de version de la clé est incrémenté. **Opération :** Procédez comme suit: 1. Mettez à jour la clé sur le serveur eDirectory afin de synchroniser les numéros de version. 2. Détruisez les tickets au niveau du client. 3. Obtenez de nouveau le TGT pour le principal. 4. Exécutez l'opération de liaison LDAP `sasl`.

Gestion de la consignation des erreurs dans eDirectory

La consignation des erreurs démarre automatiquement pendant l'installation d'eDirectory.

Niveaux de gravité des messages

Tous les messages sont associés à un niveau de gravité qui permet de déterminer leur caractère critique.

Message d'erreur	Description
Fatal: Un message fatal indique un problème important, comme la perte de données ou de fonctionnalité.	**Exemples :** ◆ Si le serveur eDirectory ne parvient pas à charger des modules système comme NCPEngine et DSLoader pendant le chargement de modules, une erreur fatale est signalée et consignée. ◆ Si le serveur eDirectory ne parvient pas à établir une connexion sur le port sécurisé 636, une erreur fatale est signalée et consignée.
Avertissement : Message qui n'est pas nécessairement grave, mais qui peut engendrer un problème ultérieurement.	**Exemples :** ◆ Échecs de connexion entre deux serveurs quelconques de l'arborescence, engendrant l'ajout d'un serveur dans un cache d'adresses erronées. Le serveur peut quitter cet état spécifique après réinitialisation du cache d'adresses erronées. ◆ Si l'application client LDAP établit une liaison et met fin à la connexion sans annuler la liaison, le serveur LDAP consigne un avertissement avec le message correspondant. ◆ Si le serveur eDirectory a utilisé tous les descripteurs de fichier et a atteint la limite Seuil, il ne peut pas traiter les requêtes entrantes ni y répondre, ce qui entraîne un échec de l'application.
Erreur : Message qui peut être dû à une opération non valide, mais qui ne cause aucun problème.	**Exemples :** ◆ Lorsqu'une application client tente d'ajouter un objet pour lequel les attributs ne sont pas définis dans le schéma, le serveur eDirectory signale l'erreur ERR_NO_SUCH_ATTRIBUTE. ◆ Lorsqu'un utilisateur tente de se connecter avec un mot de passe non valide, le serveur eDirectory renvoie l'erreur ERR_FAILED_AUTHENTICATION.
Informations : Message qui décrit l'aboutissement d'une opération ou d'un événement dans le serveur eDirectory.	**Exemples :** ◆ Lorsque le chargement/déchargement d'un module aboutit, il peut s'avérer approprié de consigner un message d'information concernant l'opération. ◆ Si la configuration du cache de base de données est modifiée, un message d'information devrait être consigné lors de la réussite de l'enregistrement de cette configuration.

Message d'erreur	Description
Débogage : Message contenant des informations qui aideront les développeurs à déboguer un programme.	**Exemples :** Lors d'une recherche de groupe dynamique, le message affiche tous les membres de ce groupe avec des informations sur l'ID d'entrée, l'ID de partition et le DN des membres. Ces informations contribuent à déterminer si tous les membres sont renvoyés au niveau eDirectory.

Configuration de la consignation des erreurs

Définition du niveau de gravité sous Linux : Afin de configurer les paramètres de consignation des erreurs pour les messages côté serveur, vous pouvez utiliser les paramètres `n4u.server.log-levels` et `n4u.server.log-file` du fichier de configuration `/etc/opt/novell/eDirectory/conf/nds.conf`.

Les niveaux de gravité disponibles sont `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` et `LogDbg` (par ordre décroissant de gravité). Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section « Niveaux de gravité des messages » page 984.

Le niveau de gravité par défaut est `LogFatal`. Dès lors, seuls les messages dont le niveau de gravité est fatal seront consignés.

Pour définir le niveau de gravité, utilisez le paramètre `n4u.server.log-levels` dans le fichier `nds.conf` comme suit :

```
n4u.server.log-levels=niveau_gravité
```

Par exemple :

- Pour définir la gravité sur le niveau `LogInfo` et les niveaux supérieurs, entrez la commande suivante :

  ```
  n4u.server.log-levels=LogInfo
  ```

  Avec cette configuration, les messages de niveaux de gravité `LogInfo` et supérieurs (c'est-à-dire `LogFatal`, `LogWarn` et `LogErr`) sont consignés dans le fichier journal.
- Pour définir la gravité sur le niveau `LogWarn` et les niveaux supérieurs, entrez la commande suivante :

  ```
  n4u.server.log-levels=LogWarn
  ```

  Avec cette configuration, les messages de niveaux de gravité `LogWarn` et supérieurs (`LogFatal`) sont consignés dans le fichier journal.
- Pour définir la gravité sur le niveau `LogDbg` et les niveaux supérieurs, entrez la commande suivante :

  ```
  n4u.server.log-levels=LogDbg
  ```

  Avec cette configuration, les messages du niveau de gravité `LogDbg` sont consignés dans le fichier journal.

  REMARQUE : vous devez affecter la valeur true à la variable d'environnement `NDSD_EVENT_DISK_CACHE` lors de la définition du niveau de consignation `LogDbg` (`n4u.server.log-levels`).

Spécification du nom du fichier journal sous Linux : pour spécifier l'emplacement du fichier journal où les messages sont consignés, utilisez le paramètre `n4u.server.log-file` dans le fichier `nds.conf`. Par défaut, les messages sont consignés dans le fichier `ndsd.log`.

Par exemple, pour consigner les messages dans le fichier `/tmp/edir.log`, entrez la commande suivante :

```
n4u.server.log-file=/tmp/edir.log
```

Pour consigner les messages dans le journal système, utilisez le paramètre `n4u.server.log-file` comme suit :

```
n4u.server.log-file=syslog
```

Définition du niveau de gravité sous Windows

Les niveaux de gravité disponibles sont `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` et `LogDbg` (par ordre décroissant de gravité). Pour plus d'informations sur les niveaux de gravité, reportez-vous à la section « Niveaux de gravité des messages » page 984.

Pour définir le niveau de gravité, procédez comme suit :

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**
2. Dans l'onglet **Services**, sélectionnez **dhlog.dlm**.
3. Entrez le niveau de consignation dans la zone **Paramètres de démarrage**.

   Par exemple, pour définir la consignation sur le niveau `LogErr` et les niveaux supérieurs, entrez la commande suivante :

   ```
   LogLevels=LogErr
   ```

4. Cliquez sur **Configurer**
5. Dans l'onglet **Configuration ACS**, cliquez sur le signe plus de **DHostLogger**.

   Le paramètre `LogLevel` est actualisé avec la valeur configurée.

   REMARQUE : la gravité du niveau de trace ne fonctionne pas sous Windows.

Indication du nom et du chemin du fichier journal sous Windows

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**
2. Dans l'onglet **Services**, sélectionnez **dhlog.dlm**.
3. Entrez le chemin du fichier journal dans la zone **Paramètres de démarrage** comme suit :

   `LogFile=`*`file_path`*

   Par exemple, pour définir le chemin du fichier journal sur `/tmp/Err.log`, entrez la commande suivante dans la zone Paramètres de démarrage :

   ```
   LogFile=/tmp/Err.log
   ```

4. Cliquez sur **Configurer**
5. Dans l'onglet **Configuration ACS**, cliquez sur le signe plus de **DHostLogger**.

   Le paramètre `LogFile` est actualisé avec la valeur configurée.

Indication de la taille du fichier journal sous Windows

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** > **NetIQ eDirectory Services**
2. Dans l'onglet **Services**, sélectionnez **dhlog.dlm**.

3 Entrez le chemin du fichier journal dans la zone **Paramètres de démarrage** comme suit :

   `LogSize=size`

   La taille du fichier par défaut est de 1 Mo.

4 Cliquez sur **Configurer**

5 Dans l'onglet **Configuration ACS**, cliquez sur le signe plus de **DHostLogger**.

   Le paramètre `LogSize` est actualisé avec la valeur configurée.

Divers

Sauvegarde d'un conteneur

Lors de l'exécution de l'utilitaire ndsbackup pour sauvegarder un conteneur renfermant un grand nombre d'objets (de l'ordre d'un million), il se peut que vous deviez attendre un certain temps pour obtenir la liste des objets du conteneur et démarrer leur sauvegarde individuelle.

Connexions eDirectory répétées

Des connexions eDirectory répétées peuvent consumer la mémoire disponible. Pour résoudre ce problème, désactivez l'attribut Login Update (Mise à jour de la connexion) à l'aide d'iMonitor.

Activation des statistiques Event System

Les statistiques relatives à l'heure sont conservées pour chaque événement généré et sont consommées dans eDirectory. Ces informations sont utiles pour la résolution des problèmes de consommation d'événements. Ces statistiques ne sont pas nécessaires au fonctionnement normal de l'annuaire ; elles sont par conséquent désactivées pour des raisons de performances. Les statistiques des événements peuvent être activées lors de l'exécution à l'aide des paramètres de configuration avancés d'iMonitor.

Pour afficher les statistiques des événements, définissez le paramètre `ENABLE_EVENT_STATISTICS`e t redémarrez le serveur. Il s'agit d'un paramètre de configuration permanente.

Suivi des problèmes de mémoire endommagée sous Linux

Sur les plates-formes Linux, eDirectory utilise Google malloc (`libtcmalloc`) en tant qu'allocateur de mémoire par défaut.

Pour suivre les problèmes de mémoire endommagée, définissez la variable d'environnement `MALLOC_CHECK_` dans le script de démarrage ndsd. Le script de démarrage recherche cette variable. Si elle est définie, la variable système malloc par défaut est utilisée ; dans le cas contraire, la variable `libtcmalloc` est chargée.

Paramètres MALLOC_CHECK dans ndsd

- Si le paramètre `MALLOC_CHECK_` est défini sur 0, toute détection de segment de mémoire altéré est ignorée en mode silencieux.
- Si le paramètre `MALLOC_CHECK_` est défini sur 2, la commande d'abandon est appelée immédiatement.

  Cela permet d'identifier la cause réelle de l'altération de la mémoire dès les premières phases du processus (cette altération est plus compliquée à identifier dans les phases ultérieures).

Connexion TCP non terminée après une déconnexion anormale

Il arrive parfois que le serveur OES Linux ne parvienne pas à détecter un hôte client qui s'est terminé brusquement en raison d'une défaillance du poste de travail ou d'une panne de courant. Toutefois, la connexion reste active pendant le timeout par défaut (environ 12 à 15 minutes) avant la désactivation de la connexion. Si vous avez défini les connexions simultanées sur 1, il est recommandé de mettre fin à la connexion manuellement ou de patienter pendant toute la durée du timeout avant d'établir une nouvelle connexion. Cette situation se produit lorsque le processus Watchdog ne parvient pas à terminer la connexion correctement. Par conséquent, si les connexions simultanées sont définies sur 1 et que la connexion n'est pas arrêtée par le processus Watchdog, les utilisateurs ne peuvent pas se connecter. Le noyau Linux fournit trois paramètres qui permettent de modifier le mode de fonctionnement des sondes `keepalive` du côté serveur. Utilisez ces paramètres pour mettre en œuvre une solution de contournement au niveau TCP.

Ces paramètres sont disponibles dans le répertoire `/proc/sys/net/ipv4/`.

- `tcp_keepalive_time` : détermine la fréquence d'envoi des paquets TCP `keepalive` afin de maintenir la connexion si elle n'est pas utilisée actuellement. Cette valeur n'est utilisée que lorsque le paramètre `keepalive` est activé.

  Le paramètre `tcp_keepalive_time` utilise une valeur d'entier en secondes. La valeur par défaut est de 7 200 secondes, soit 2 heures. Ce processus convient à la plupart des hôtes et ne nécessite pas de nombreuses ressources réseau. Si vous définissez ce paramètre sur une valeur faible, il utilise des ressources réseau pour un trafic inutile.
- `tcp_keepalive_probes` : détermine la fréquence d'envoi des sondes TCP `keepalive` avant qu'une connexion soit considérée comme étant interrompue.

  Le paramètre `tcp_keepalive_probes` utilise une valeur d'entier inférieure à 50 (recommandation), en fonction des valeurs `tcp_keepalive_time` et `tcp_keepalive_interval`. La valeur par défaut consiste à définir 9 sondes avant que l'application soit informée de l'interruption de la connexion.
- `tcp_keepalive_intvl` : détermine la durée de réponse pour chaque sonde `keepalive`. Cette valeur est importante pour calculer la durée qui doit s'écouler avant que la sonde `keepalive` considère la connexion comme terminée.

  Le paramètre `tcp_keepalive_intvl` utilise une valeur d'entier, la valeur par défaut étant de 75 secondes. Par conséquent, le processus global incluant 9 sondes de 75 secondes prend environ 11 minutes. Les valeurs par défaut des variables `tcp_keepalive_probes` et `tcp_keepalive_intvl` permettent d'évaluer la durée par défaut avant que la connexion soit considérée comme ayant abouti à un timeout en raison des sondes `keepalive`.

Modifiez ces trois paramètres de manière à ce qu'ils résolvent le problème sans pour autant générer de grandes quantités de trafic supplémentaire. Par exemple, vous pouvez effectuer la modification suivante (avec une durée de détection de 3 minutes) :

- `tcp_keepalive_time set -120`
- `tcp_keepalive_probes - 3`
- `tcp_keepalive_intvl - 20`

REMARQUE : Soyez prudent lorsque vous modifiez les valeurs de ces paramètres et évitez de choisir des connexions déjà valides.

Les paramètres prennent effet dès que les fichiers sont modifiés. Vous devez redémarrer tous les services. Toutefois, les paramètres ne sont valides que pour la session en cours. Une fois que le serveur est redémarré, les paramètres reprennent leur valeur par défaut.

Pour que le paramétrage soit permanent (même après un redémarrage), effectuez les opérations suivantes :

Ajoutez les entrées suivantes dans `/etc/sysctl.conf`.

- net.ipv4.tcp_keepalive_time=120
- net.ipv4.tcp_keepalive_probes=3
- net.ipv4.tcp_keepalive_intvl=20

Nous vous recommandons d'utiliser ces paramètres que si tous les clients et serveurs sont connectés par l'intermédiaire d'un réseau local.

L'erreur NDS, échec du système (-632) se produit lors d'une recherche ldapsearch d'objets Utilisateur

Importez les objets Utilisateur avec le mot de passe simple, puis activez le mot de passe universel du conteneur dans lequel les objets Utilisateur sont importés. Arrêtez le serveur DS et définissez l'environnement comme suit : `NDSD_TRY_NMASLOGIN_FIRST=tree`. Redémarrez ensuite le serveur DS. Lorsque vous effectuez une recherche ldapsearch des objets Utilisateur importés avec le mot de passe simple, l'erreur suivante s'affiche :

```
ldap_bind: Unknown error,  additional info: NDS error: system failure (-632)
```

Pour la résoudre, définissez la connexion par mot de passe simple comme séquence de connexion par défaut pour le conteneur dans lequel les objets Utilisateur sont importés avant de rechercher ces derniers via ldapsearch.

Lorsque LDAP demande à NMAS de connecter un utilisateur, NMAS utilise la séquence de connexion par défaut. Si vous ne spécifiez pas de séquence de connexion par défaut pour ces utilisateurs, NMAS utilisera la séquence NDS. Si ces utilisateurs n'ont pas reçu de mot de passe NDS lorsque vous les avez importés, la séquence NDS ne fonctionnera pas. Si vous activez le mot de passe universel et que l'utilisateur se connecte avec le mot de passe simple, ce dernier sera synchronisé avec le mot de passe NDS et le mot de passe universel.

Désactivation de SecretStore on Linux

Un administrateur eDirectory peut désactiver SecretStore sous Linux à l'aide des processus suivants :

1. Accédez au répertoire `nds-modules`, puis renommez ou déplacez les modules SecretStore suivants :

   ```
   libsss.so
   libssncp.so
   libssldp.so
   ```

2. Redémarrez le serveur.

Désactivation de SecretStore sous Windows

Un administrateur eDirectory peut désactiver SecretStore sous Windows à l'aide des processus suivants :

1. Accédez au répertoire `novell\nds`, puis renommez ou déplacez les modules SecretStore suivants :

   ```
   lsss.dll
   sss.dlm
   ```

```
ssncp.dlm
ssldp.dlm
```

2 Redémarrez le serveur.

Emplacement du fichier de configuration dsbk

Le fichier `dsbk.conf` est situé dans le répertoire `/etc` et non à l'emplacement réservé à l'instance spécifique de eDirectory.

Échec d'ouverture du fichier de consignation des erreurs par ldif2dib lorsque le chemin du répertoire de la DIB est personnalisé

Ldif2dib ne parvient pas à ouvrir le fichier de consignation par défaut `ldif2dib.log` lorsque le répertoire `dib` a été déplacé vers un emplacement personnalisé.

Pour éviter ce problème, indiquez explicitement l'emplacement du fichier de consignation à l'aide du paramètre `-b`.

Échec de démarrage de ndsd après un crash système

Dans certains cas, les services eDirectory (`ndsd`) ne redémarrent pas après un crash système ou une panne d'alimentation. Pour redémarrer eDirectory, procédez comme suit :

1 Supprimez le fichier`/var/opt/novell/eDirectory/data/ndsd.pid`.

2 Entrez la commande `/etc/init.d/ndsd start`.

N'exécutez pas DSTrace avec toutes les balises activées sur les ordinateurs Linux

Lorsque toutes les balises sont activées, veillez à ne pas exécuter DSTrace sur les éléments suivants :

- **Un système chargé en mode journal :** il à tendance à augmenter la mémoire ndsd.
- **Des serveurs en mode en ligne :** il bloque ndsd.

Non-compatibilité RFC de LDAP pour les requêtes de recherche anonymes

Si un client effectue une opération de recherche non authentifiée alors que les liaisons anonymes sont désactivées, le serveur LDAP répond avec le résultat de liaison indiquant une authentification inappropriée (`operationsError`), au lieu du résultat de la recherche.

Dépannage des ports à l'aide des instances personnalisées d'eDirectory 9.0

Dans eDirectory 9.0, si vous configurez une nouvelle instance dans un emplacement personnalisé alors que le serveur d'instance par défaut est arrêté, elle utilise les ports de l'instance par défaut. L'instance par défaut ne répond pas, car ses ports sont affectés à l'instance dans l'emplacement personnalisé.

Suivez la procédure présentée à la section « Dépannage des ports à l'aide des instances personnalisées de eDirectory 8.8 » avant de redémarrer l'hôte.

Redémarrage de l'hôte

Seule l'instance par défaut créée à l'aide des fichiers binaires d'instance par défaut se lance au redémarrage.

Vous pouvez définir les chemins et utiliser ndsmanage pour exécuter les autres instances.

ndsd n'écoute pas sur l'adresse de boucle d'un port NCP donné

En présence de plusieurs instances d'eDirectory, la seconde instance et les suivantes essaient d'écouter sur le port par défaut 524 au lieu du port NCP™ de l'adresse de boucle.

Pour résoudre ce problème, définissez le paramètre n4u.server.tcp-port de la seconde instance sur le port sur lequel elle est censée écouter. Le paramètre n4u.server.tcp-port se trouve dans le fichier `nds.conf`.

IMPORTANT : toutes les instances d'eDirectory doivent être opérationnelles avant de procéder à la mise à niveau vers eDirectory 9.0.

OID de transaction LDAP

Dans le cadre de la prise en charge des transactions LDAP, les attributs `supportedGroupingTypes` et `transactionGroupingType` sont identiques (`2.16.840.1.113719.1.27.103.7`).

Erreurs -5871 et -5875 dans la trace LDAP

Les erreurs -5871 et -5875 dans la trace LDAP sont généralement provoquées par le fait que la fermeture du client LDAP est forcée, sans annulation de la liaison. Par conséquent, ces erreurs ne sont pas préoccupantes et peuvent être ignorées. Pour plus d'informations sur ces erreurs, reportez-au site Web des codes d'erreur NetIQ (http://www.novell.com/documentation/nwec/).

NDSCons génère une erreur -625 si une arborescence est renommée

Si vous renommez l'arborescence sur le serveur primaire et arrêtez l'hôte DHost sur le serveur secondaire, l'utilitaire NDSCons génère sur le serveur secondaire un message d'erreur -625 indiquant un échec du transport, tandis que l'hôte DHost continue à fonctionner sur le serveur primaire et le serveur secondaire. L'erreur se produit car NDSCons s'exécutait sur le serveur secondaire lorsque l'arborescence a été renommée sur le serveur primaire. NDSCons fonctionne correctement si vous le fermez, puis le redémarrez.

REMARQUE : il n'est pas possible de renommer l'arborescence, car cette opération n'est pas prise en charge si EBA est activé sur des serveurs dans l'arborescence.

L'écoute sur plusieurs cartes réseau ralentit les performances ldapsearch

Pour éviter ce problème :

Désactivez dans le fichier de configuration les cartes réseau qui ralentissent les performances ldapsearch.

ou

Activez l'évaluation du renvoi avancé (ARC) à l'aide de la commande `set NDSTRACE =!ARC1` dans DSTrace.

Impossible de limiter le nombre d'utilisateurs simultanés sur les plates-formes Linux

Vous ne pouvez pas limiter le nombre de connexions simultanées sur les plates-formes Linux. Pour revenir au comportement antérieur (vérification stricte sur la base du port), définissez le paramètre suivant dans le fichier `nds.conf`.

```
n4u.server.mask-port-number=0
```

Échec de l'arrêt de ndsd lié au protocole SLP

Si aucun agent Annuaire SLP n'est configuré sur votre réseau, la recherche de services qui utilisent le protocole SLP peut prendre plus de temps. Lors de l'arrêt d'eDirectory, ndsd essaie d'effectuer des opérations à l'aide du protocole SLP. Ces tentatives peuvent être plus longues que le délai normal autorisé par le script d'initialisation, ce qui entraîne un arrêt forcé.

Pour résoudre ce problème :

1. Créez un fichier vide avec le nom `hosts.nds` dans le répertoire de configuration. Le répertoire de configuration d'un serveur peut être obtenu en exécutant la commande suivante : `ndsconfig get n4u.server.confdir`
2. Définissez une variable d'environnement NDS_USESLP sur 0 en spécifiant les informations suivantes : export NDS_USESLP=0 in `/opt/novell/eDirectory/sbin/pre_ndsd_start`
3. Redémarrez eDirectory.

Redémarrage du module NLDAP sous Windows

Après avoir arrêté NLDAP, vous devez redémarrer le serveur pour charger ce processus.

SecretStore sur LDAP

La fonctionnalité SecretStore de NetIQ ne fonctionne pas sur LDAP. Pour résoudre ce problème, vous devez rafraîchir LDAP via iManager.

Impossible de modifier la phrase secrète après le déverrouillage de SecretStore

SecretStore se verrouille si vous tentez de récupérer un mot de passe oublié en vous connectant avec des références utilisateur et une phrase secrète erronée. Vous pouvez déverrouiller SecretStore à l'aide de droits d'administrateur, et le client NetIQ SecureLogin vous permet de vous connecter sans phrase secrète. Si vous tentez de modifier la phrase secrète, la connexion échoue et génère une erreur.

Réinitialisation des références de l'utilisateur lors de leur modification via SecretStore

Lorsque vous essayez d'enregistrer les nouvelles références dans SecretStore à l'aide du plug-in iManager, une colonne de références vierge s'affiche car iManager n'est pas parvenu à enregistrer les modifications.

Vous ne pouvez modifier les références à l'aide du plug-in iManager de SecretStore que si vous êtes connecté en tant qu'utilisateur et non en tant qu'administrateur.

La création d'un ensemble de références différent avec le même nom d'utilisateur remplace l'ensemble de références précédent

Lorsque vous enregistrez un autre ensemble de références, SecretStore ne parvient pas à conserver le premier ensemble et seul le dernier ensemble de références est visible.

Vous ne pouvez modifier les références à l'aide du plug-in iManager de SecretStore que si vous êtes connecté en tant qu'utilisateur et non en tant qu'administrateur.

Le serveur HTTP utilise le certificat SSL CertificateIP même après son expiration

Si vous effectuez la mise à niveau vers eDirectory 9.0 à partir d'une version antérieure, le serveur HTTP continue d'utiliser le certificat SSL CertificateIP même après son expiration. Cela est dû au fait qu'eDirectory 8.8 SP8 ne conserve pas le certificat SSL CertificateIP et n'en réémet pas même si le certificat SSL CertificateIP arrive à expiration ou est supprimé.

Par conséquent, si le certificat SSL CertificateIP arrive à expiration ou est supprimé, vous devez en créer un manuellement à l'aide du plug-in iManager ou utiliser à la place le certificat SSL CertificateDNS.

eDirectory contient deux fichiers binaires ldapsearch différents

Il existe deux ensembles d'outils LDAP (`ldapadd`, `ldapconfig`, `ldapdelete`, `ldapmodify`, `ldapmodrdn` et `ldapsearch`) sur un système SLES (ainsi que le RPM openldap2-client) équipé d'eDirectory : l'un dans le dossier `/usr/bin`, installé par le système d'exploitation SLES, et l'autre dans le dossier `/opt/novell/eDirectory/bin`, installé par eDirectory.

Bien que les fonctionnalités de base des deux ensembles d'outils LDAP soient identiques, chacun de ces ensembles ajoute ses propres fonctionnalités. Selon les paramètres de chemin d'accès dans la variable d'environnement `PATH`, l'ensemble d'outils en cours d'utilisation peut être différent et donc les fonctionnalités disponibles peuvent également varier.

ldapsearch ne renvoie aucun résultat

ldapsearch ne renvoie aucun résultat lorsque l'utilisateur de liaison de dispose pas des droits de lecture pour tous les attributs qui font partie du filtre de recherche.

Pour résoudre ce problème, assurez-vous que l'utilisateur de liaison possède des droits de lecture pour tous les attributs qui font partie du filtre de recherche.

L'affichage de la liste virtuelle affiche un message d'erreur avec eDirectory 9.1

L'affichage de la liste virtuelle (VLV) affiche un message d'erreur avec eDirectory 9.1 lorsque toutes les répliques de partition ne sont pas présentes sur le serveur eDirectory sur lequel VLV est exécuté.

Vérifiez que toutes les répliques de partition sont présentes sur le serveur eDirectory sur lequel VLV est exécuté.

eDirectory ne démarre pas après le déplacement de datadir vers un nouvel emplacement

Si vous déplacez `datadir` vers un nouvel emplacement après avoir configuré eDirectory sur SLES 12 ou version ultérieure, procédez comme suit :

- Mettez à jour le nouvel emplacement du fichier `ndsd.pid` dans le fichier de service qui se trouve dans l'emplacement `/usr/lib/systemd/system/`.

Par exemple, si le fichier `nds.conf` se trouve dans `/etc/opt/novell/eDirectory`, un exemple de fichier de service est créé comme ci-dessous :

`/usr/lib/systemd/system/ndsdtmpl-etc-opt-novell-eDirectory-conf-ds.conf@.service`.

- Rechargez le daemon à l'aide de la commande `systemctl daemon-reload`.
- Redémarrez le serveur eDirectory.

Échec de l'installation d'eDirectory en raison d'une stratégie d'exécution restreinte

L'installation d'eDirectory échoue lorsque la stratégie d'exécution Windows est restreinte pour PowerShell.

Pour résoudre ce problème, définissez la stratégie d'exécution Windows sur RemoteSigned pour PowerShell.

Dépannage d'IPV6

La recherche sécurisée OpenLDAP échoue avec IPv6

La recherche sécurisée OpenLDAP échoue avec IPv6 si le certificat associé au serveur LDAP comporte une adresse IPv6 dans le champ **Autre nom de l'objet**.

Le plug-in ICE ne fonctionne pas pour les adresses IPV6

Il ne parvient pas à se connecter au serveur demandé si iManager n'écoute que l'adresse IPv4 avec l'erreur suivante :

```
Unable to connect to the requested server. Verify the name/address and port.
```

Pour configurer IPv6 pour que iManager fonctionne avec eDirectory, vous devez activer IPv6 à l'aide des étapes suivantes :

1. Définissez les propriétés suivantes dans le fichier `catalina.properties` et redémarrez Tomcat.

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

   Notez que `java.net.preferIPv4Stack` s'applique à iManager pour qu'il fonctionne avec eDirectory et que `java.net.preferIPv4Addresses` s'applique aux navigateurs pour qu'ils fonctionnent avec iManager.
2. Accédez à **Options LDAP > Afficher les serveurs LDAP > Connexions > Serveur LDAP,**, puis ajoutez des interfaces LDAP pour les adresses IPv6 avec des numéros de port.

   ```
   ldap://[xx::xx]:389
   ldaps://[xx::xx]:636
   ```
3. Configurez RBS (Role-Based Services), puis déconnectez-vous et reconnectez-vous.

Modules d'écoute pour les adresses IPv6 non spécifiées sous Linux et Windows

Un module d'écoute pour une adresse IPv6 non spécifiée accepte les connexions IPv4 et IPv6 sous Linux. En raison de ce comportement, Linux ne vous autorise pas à démarrer simultanément sur un même port des modules d'écoute IPv4 et IPv6 non spécifiés. Par conséquent, si un module d'écoute est déjà configuré pour une adresse IPv6 non spécifiée, celui de l'adresse IPv4 non spécifiée ne parvient pas à démarrer. Linux utilise une adresse non spécifiée pour les modules d'écoute LDAP.

Sous Windows, un module d'écoute IPv6 non spécifié n'accepte que les connexions IPv6. Par conséquent, vous devez configurer un module d'écoute IPv4 distinct pour qu'il accepte à la fois les connexions IPv4 et les connexions IPv6.

Par défaut, les modules d'écoute IPv4 et IPv6 sont configurés pour ldapInterfaces. En fonction de la plate-forme, la commande ldapInterfaces démarre les modules d'écoute requis.

Dépannage EBA

La connexion EBA échoue si le DN utilisateur contient un attribut sans OID

La connexion EBA échoue lorsque le DN utilisateur contient un attribut sans OID.

Pour résoudre ce problème, vous devez ajouter l'OID à l'attribut DN utilisateur dans le schéma.