
Directory and Resource Administrator

Guide de l'administrateur

Juillet 2018

Mentions légales

© Copyright 2007 – 2018 Micro Focus ou l'une de ses sociétés affiliées.

Les seules garanties pour les produits et services de Micro Focus et de ses filiales et concédants de licence (« Micro Focus ») sont énoncées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucun élément du présent document ne doit être interprété comme constituant une garantie supplémentaire. Micro Focus ne pourra pas être tenu responsable des erreurs techniques ou éditoriales ou des omissions contenues dans le présent document. Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

À propos de ce guide 7

1 Mise en route 9

1.1	Qu'est-ce que Directory and Resource Administrator ?	9
1.2	Présentation des composants de Directory and Resource Administrator (DRA)	10
1.2.1	Serveur d'administration DRA	10
1.2.2	Console de délégation et de configuration	11
1.2.3	Console de gestion des comptes et des ressources	11
1.2.4	Console Web	11
1.2.5	Composants de création de rapports	12
1.2.6	Moteur de workflow	12
1.2.7	Architecture du produit	13

2 Installation et mise à niveau du produit 15

2.1	Planification du déploiement	15
2.1.1	Recommandations relatives à la ressource testée	15
2.1.2	Provisioning de ressources d'environnement virtuel	15
2.1.3	Ports et protocoles requis	16
2.1.4	Plates-formes prises en charge	19
2.1.5	Configuration requise pour le serveur d'administration DRA	20
2.1.6	Configuration requise de la console Web et des extensions DRA	24
2.1.7	Configuration requise pour la création de rapports	25
2.1.8	Exigences de licence	26
2.2	Installation du produit	26
2.2.1	Installation du serveur d'administration DRA	27
2.2.2	Installation de clients DRA	28
2.2.3	Installation des extensions REST DRA	29
2.2.4	Installation du serveur de workflow	30
2.2.5	Installation de DRA Reporting	30
2.3	Mise à jour de produit	31
2.3.1	Planification d'une mise à niveau DRA	32
2.3.2	Tâches préalables à la mise à niveau	32
2.3.3	Mise à niveau du serveur d'administration DRA	35
2.3.4	Mise à niveau des extensions REST DRA	38
2.3.5	Mise à niveau de DRA Reporting	39

3 Configuration des composants et processus 41

3.1	Configuration initiale	41
3.1.1	Liste de contrôle de la configuration	41
3.1.2	Installation ou mise à niveau de licences	41
3.1.3	Configuration des fonctions et des serveurs DRA	42
3.1.4	Configuration du client de délégation et de configuration	57
3.1.5	Configuration du client Web	57
3.2	Connexion aux systèmes gérés	65
3.2.1	Gestion des domaines Active Directory	66
3.2.2	Connexion aux dossiers publics	69
3.2.3	Activation de la prise en charge de Microsoft Exchange	71
3.2.4	Activation d'Exchange Online et de Skype Entreprise Online	72
3.2.5	Ajout d'un locataire Office 365	72

4 Modèle de délégation 75

4.1	Présentation du modèle de délégation dynamique	75
4.1.1	Contrôles du modèle de délégation	75
4.1.2	Mode de traitement des requêtes par DRA	76

4.1.3	Exemples de la façon dont DRA traite les assignations de délégation	76
4.2	Instances Active Views	79
4.2.1	Instances Active Views intégrées	80
4.2.2	Implémentation d'une instance Active Views personnalisée	81
4.3	Rôles	83
4.3.1	Rôles intégrés	83
4.3.2	Création de rôles personnalisés	91
4.4	Pouvoirs	91
4.4.1	Pouvoirs intégrés	91
4.4.2	Implémentation de pouvoirs personnalisés	92
4.4.3	Extension des pouvoirs	93
4.5	Assignations de délégations	94
5	Stratégie et automatisation des processus	95
5.1	Présentation de la stratégie DRA	95
5.1.1	Application des stratégies par le serveur d'administration	95
5.1.2	Stratégies intégrées	96
5.1.3	Implémentation d'une stratégie personnalisée	100
5.1.4	Restriction des groupes de sécurité intégrés natifs	100
5.1.5	Gestion des stratégies	102
5.1.6	Stratégie du client de délégation et de configuration	113
5.2	Automatisation de déclencheurs préalables ou postérieurs à une tâche	115
5.2.1	Automatisation des processus par le serveur d'administration	115
5.2.2	Implémentation d'un déclencheur d'automatisation	116
5.3	Workflow automatisé	117
6	Audit et création de rapports	119
6.1	Audit des activités	119
6.1.1	Journal natif des événements Windows	119
6.1.2	Présentation des archives de journaux	121
6.2	Création de rapports	124
6.2.1	Gestion de la collecte des données pour la création de rapports	124
6.2.2	Rapports intégrés	125
7	Fonctions supplémentaires	129
7.1	Assignations temporaires à des groupes	129
7.2	Groupes dynamiques DRA	130
7.3	Fonctionnement de l'horodatage des événements	130
7.3.1	Événement AD DS	131
7.3.2	Opérations prises en charge	131
7.4	Mot de passe de récupération BitLocker	132
7.4.1	Affichage et copie d'un mot de passe de récupération BitLocker	132
7.4.2	Recherche d'un mot de passe de récupération	133
7.5	Analyseur ActiveView	133
7.5.1	Démarrage d'une collecte de données Active Views	133
7.5.2	Génération d'un rapport de l'analyseur	134
7.5.3	Purge des données analysées	134
7.6	Corbeille	134
7.6.1	Assignation de pouvoirs concernant la corbeille	135
7.6.2	Utilisation de la corbeille	135
8	Personnalisation des clients	137
8.1	Client de délégation et de configuration et client ARM	137

8.1.1	Personnalisation de pages de propriétés	137
8.1.2	Outils personnalisés	143
8.1.3	Personnalisation de l'interface utilisateur	146
8.2	Client Web	147
8.2.1	Personnalisation de pages de propriétés	147
8.2.2	Personnalisation des formulaires de workflow	148
8.2.3	Personnalisation de l'image de marque de l'interface utilisateur	151

9 Outils et utilitaires **153**

9.1	Utilitaire de diagnostic	153
9.2	Utilitaire des objets supprimés	153
9.2.1	Autorisations requises pour l'utilitaire des objets supprimés	154
9.2.2	Syntaxe de l'utilitaire des objets supprimés	154
9.2.3	Options de l'utilitaire des objets supprimés	154
9.2.4	Exemples pour l'utilitaire des objets supprimés	155
9.3	Utilitaire de contrôle de l'état de santé	156
9.4	Utilitaire de la corbeille	156
9.4.1	Autorisations requises pour l'utilitaire de la corbeille	157
9.4.2	Syntaxe de l'utilitaire de la corbeille	157
9.4.3	Options de l'utilitaire de la corbeille	157
9.4.4	Exemples pour l'utilitaire de la corbeille	157

À propos de ce guide

Le *Guide de l'administrateur* fournit des informations conceptuelles concernant le produit Directory and Resource Administrator (DRA). Il définit la terminologie ainsi que différents concepts associés. Il fournit également des procédures détaillées pour de nombreuses tâches de configuration et opérationnelles.

Public

Ce guide fournit des informations qui permettront aux utilisateurs de comprendre les concepts de l'administration et de mettre en œuvre un modèle d'administration sécurisé et distribué.

Documentation supplémentaire

Ce guide fait partie de la documentation consacrée à Directory and Resource Administrator. Pour obtenir une liste complète des publications relatives à cette version, visitez le [site Web de la documentation \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Contactez 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

Contactez 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 pour améliorer la documentation, cliquez sur **comment on this topic** (Ajouter un commentaire sur cette rubrique) situé en bas de chaque page dans la version HTML de la 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

Les communautés NetIQ et la communauté en ligne de NetIQ sont 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, les communautés NetIQ vous aident 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 Mise en route

Avant d'installer et de configurer l'ensemble des composants de Directory and Resource Administrator™ (DRA), vous devez comprendre les principes de base du fonctionnement de DRA au sein de votre entreprise et le rôle des composants DRA dans l'architecture du produit.

1.1 Qu'est-ce que Directory and Resource Administrator ?

Directory and Resource Administrator fournit une administration sécurisée et efficace des identités à privilèges au sein de Microsoft Active Directory (AD). DRA effectue une délégation granulaire du « privilège minimal » afin que les administrateurs et les utilisateurs reçoivent uniquement les autorisations nécessaires dans le cadre de leurs responsabilités spécifiques. DRA veille également au respect des stratégies, fournit des audits et des rapports détaillés sur les activités, mais simplifie aussi la réalisation des tâches répétitives grâce à l'automatisation des processus informatiques. Chacune de ces fonctionnalités contribue à protéger les environnements Active Directory et Exchange de vos clients contre le risque de réaffectation de privilèges, les erreurs, les activités malveillantes et la non-conformité réglementaire, tout en réduisant la charge de travail de l'administrateur en accordant des fonctionnalités en self-service aux utilisateurs, aux responsables de l'entreprise et au personnel du service d'assistance.

DRA étend également les puissantes fonctions de Microsoft Exchange pour assurer une gestion transparente des objets Exchange. Par le biais d'une interface utilisateur unique et commune, DRA fournit une administration basée sur des stratégies pour la gestion des boîtes aux lettres, des dossiers publics et des listes de distribution dans votre environnement Microsoft Exchange.

DRA propose les solutions dont vous avez besoin pour contrôler et gérer vos environnements Active Directory, Microsoft Windows, Microsoft Exchange et Microsoft Office 365.

- ♦ **Prise en charge d'Active Directory, Office 365, Exchange et Skype Entreprise** : assure la gestion administrative d'Active Directory, d'Exchange Server sur site, de Skype Entreprise sur site, d'Exchange Online et de Skype Entreprise Online.
- ♦ **Contrôles granulaires de l'accès aux privilèges utilisateur et administrateur** : la technologie brevetée ActiveView délègue uniquement les privilèges nécessaires à l'exécution de responsabilités spécifiques et empêche la réaffectation des privilèges.
- ♦ **Console Web personnalisable** : une approche intuitive permet à du personnel sans formation technique de réaliser facilement et en toute sécurité des tâches administratives au moyen d'un accès limité et d'un minimum de fonctionnalités (assignées).
- ♦ **Audit approfondi des activités et création de rapports** : fournit un enregistrement d'audit complet de toutes les activités réalisées avec le produit. Stocke en toute sécurité les données à long terme et démontre aux auditeurs (par exemple, PCI DSS, FISMA, HIPAA et NERC CIP) que des processus sont en place pour contrôler l'accès à Active Directory.
- ♦ **Automatisation des processus informatiques** : automatise les workflows pour des tâches aussi diverses que le provisioning et le déprovisioning, les actions des utilisateurs et des boîtes aux lettres, l'application de stratégies et les tâches en self-service contrôlées. Renforce l'efficacité de l'entreprise et réduit les tâches administratives manuelles et répétitives.

- ♦ **Intégrité opérationnelle** : empêche les modifications malintentionnées ou incorrectes qui affectent les performances et la disponibilité des systèmes et services en fournissant un contrôle d'accès granulaire aux administrateurs et en gérant l'accès aux systèmes et aux ressources.
- ♦ **Application des processus** : préserve l'intégrité des processus de gestion des modifications clés qui vous aident à améliorer la productivité, réduire les erreurs, gagner du temps et augmenter l'efficacité de l'administration.
- ♦ **Intégration avec Change Guardian** : permet d'améliorer l'audit des événements générés dans Active Directory en dehors de DRA et de l'automatisation du workflow.

1.2 Présentation des composants de Directory and Resource Administrator (DRA)

Les composants de DRA que vous utiliserez systématiquement pour gérer les accès privilégiés incluent les serveurs primaire et secondaires, les consoles de l'administrateur, les composants de création de rapports et le moteur de workflow Aegis permettant d'automatiser les processus de workflow.

Le tableau suivant identifie les interfaces utilisateur et les serveurs d'administration habituellement utilisés par chaque type d'utilisateur de DRA :

Type d'utilisateur de DRA	Interfaces utilisateur	Serveur d'administration
Administrateur DRA (Personne en charge de la configuration du produit)	Console de délégation et de configuration	Serveur primaire
	DRA Reporting Center Setup (NRC) CLI (<i>facultatif</i>) Fournisseur ADSI DRA(<i>facultatif</i>)	Serveur secondaire
Administrateur occasionnel du service d'assistance	Console de gestion des comptes et des ressources	Serveur secondaire
Administrateur occasionnel du service d'assistance	Console Web	Tout serveur DRA sur lequel le service REST DRA est installé

1.2.1 Serveur d'administration DRA

Le serveur d'administration DRA stocke les données de configuration (environnementales, accès délégué et stratégie), exécute les tâches de l'opérateur et d'automatisation et audite l'activité de l'ensemble du système. Tout en prenant en charge plusieurs clients au niveau de la console et de l'API, le serveur est conçu pour offrir une haute disponibilité pour la redondance et l'isolement géographique via un modèle d'évolutivité d'ensemble multi-maître (MMS, Multi-Master Set). Dans ce modèle, chaque environnement DRA nécessite un serveur d'administration DRA primaire qui se synchronise avec un certain nombre de serveurs d'administration DRA secondaires supplémentaires.

Nous recommandons vivement de ne pas installer les serveurs d'administration sur les contrôleurs de domaine Active Directory. Pour chaque domaine géré par DRA, assurez-vous qu'il existe au moins un contrôleur de domaine sur le même site que le serveur d'administration. Par défaut, le serveur d'administration accède au contrôleur de domaine le plus proche pour toutes les opérations de lecture et d'écriture. Lors de l'exécution de tâches spécifiques à un site, telles que les

réinitialisations de mots de passe, vous pouvez spécifier un contrôleur de domaine spécifique du site pour traiter l'opération. Il est conseillé d'envisager de consacrer un serveur d'administration secondaire à la création de rapports, au traitement par lots et aux workloads automatisés.

1.2.2 Console de délégation et de configuration

La console de délégation et de configuration est une interface utilisateur à installer qui permet aux administrateurs système d'accéder aux fonctions de configuration et d'administration de DRA.

- ♦ **Delegation Management (Gestion de la délégation)** : permet de spécifier et d'assigner de façon granulaire l'accès aux ressources et tâches gérées aux assistants administrateur.
- ♦ **Policy and Automation Management (Gestion des stratégies et de l'automatisation)** : permet de définir et d'appliquer une stratégie pour garantir la conformité aux normes et conventions applicables à l'environnement.
- ♦ **Configuration Management (Gestion de la configuration)** : permet de mettre à jour les paramètres et les options système DRA, d'ajouter des personnalisations et de configurer les services gérés (Active Directory, Exchange, Office 365, etc.).

1.2.3 Console de gestion des comptes et des ressources

La console de gestion des comptes et des ressources est une interface utilisateur à installer permettant aux assistants administrateur de DRA d'afficher et de gérer les objets délégués des domaines et des services connectés.

1.2.4 Console Web

La console Web est une interface utilisateur Web qui fournit un accès rapide et simple aux assistants administrateur pour afficher et gérer les objets délégués des domaines et des services connectés. Les administrateurs peuvent personnaliser l'apparence et l'utilisation de la console Web afin d'inclure l'image de marque de l'entreprise ainsi que des propriétés d'objet personnalisées.

L'administrateur DRA peut également créer et modifier des formulaires de workflow automatisés pour déclencher le cas échéant des tâches de routine automatisées.

L'historique des modifications unifiées est une autre fonction de la console Web qui permet l'intégration avec les serveurs d'historique des modifications afin d'auditer les modifications apportées aux objets Active Directory en dehors de DRA. Les options des rapports de l'historique des modifications incluent :

- ♦ Modifications apportées à...
- ♦ Modifications apportées par...
- ♦ Boîte aux lettres créée par...
- ♦ Utilisateur, groupe et adresse électronique du contact créés par...
- ♦ Utilisateur, groupe et adresse électronique du contact supprimés par...
- ♦ Attribut virtuel créé par...
- ♦ Objets déplacés par...

1.2.5 Composants de création de rapports

DRA Reporting fournit des modèles intégrés et personnalisables pour la gestion de DRA et des détails sur les domaines et les systèmes gérés par DRA :

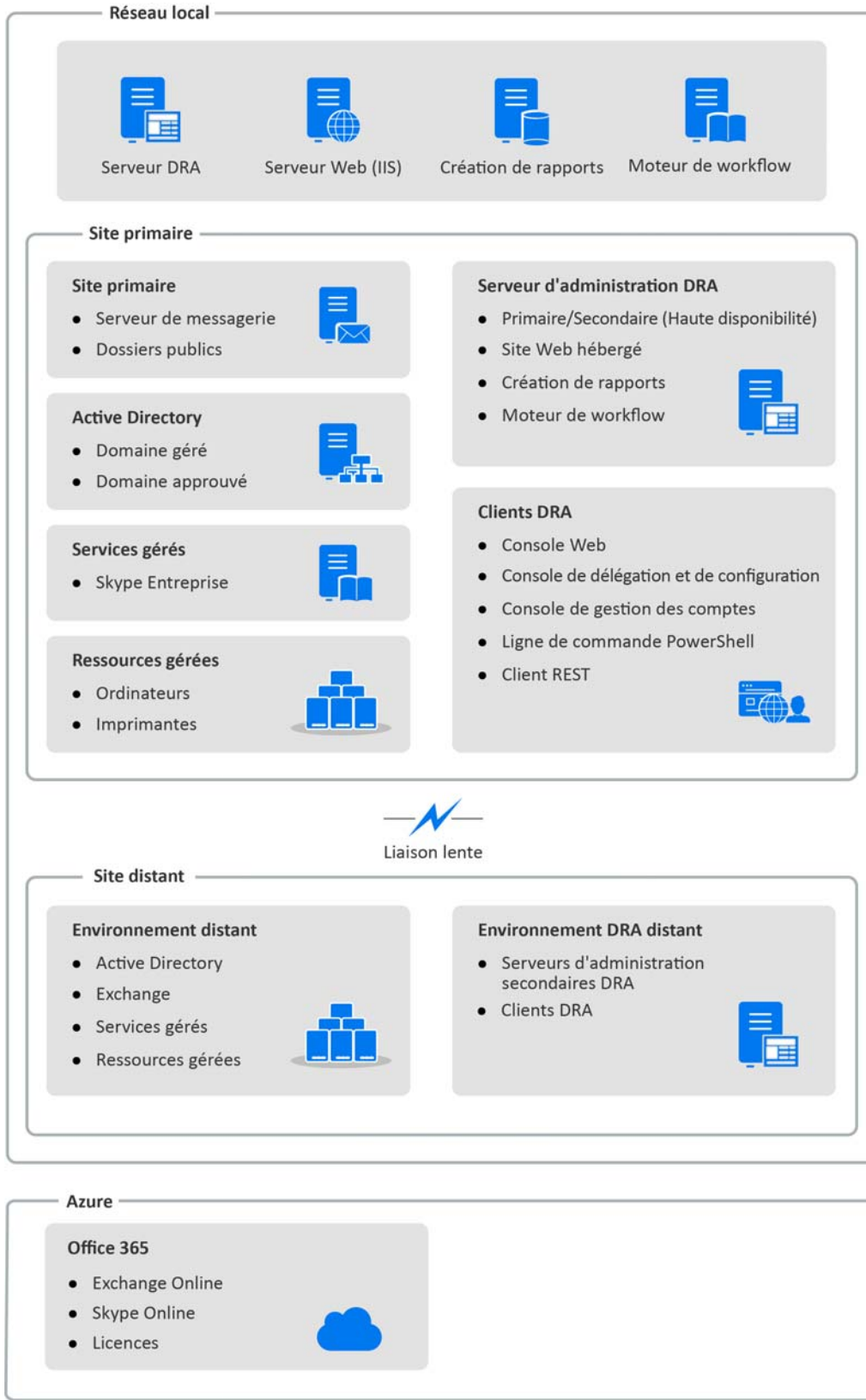
- ♦ Rapports sur les ressources pour les objets Active Directory
- ♦ Rapports sur les données d'objet Active Directory
- ♦ Rapports récapitulatifs Active Directory
- ♦ Rapports sur la configuration de DRA
- ♦ Rapports sur la configuration d'Exchange
- ♦ Rapports sur Office 365 Exchange Online
- ♦ Rapports détaillés sur les tendances d'activité (par mois, domaine et pic)
- ♦ Rapports d'activité DRA récapitulatifs

Les rapports DRA peuvent être planifiés et publiés via SQL Server Reporting Services pour être facilement distribués aux participants.

1.2.6 Moteur de workflow

DRA s'intègre au moteur de workflow Aegis pour automatiser les tâches de workflow via la console Web dans laquelle les assistants administrateur peuvent configurer le serveur de workflow et exécuter des formulaires d'automatisation de workflow personnalisés, puis afficher l'état de ces workflows. Pour plus d'informations sur le moteur de workflow, reportez-vous au [site de documentation DRA \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

1.2.7 Architecture du produit



2 Installation et mise à niveau du produit

Ce chapitre décrit la configuration matérielle et logicielle requise de même que les exigences de compte pour Directory and Resource Administrator. Il vous guide ensuite tout au long de la procédure d'installation en fournissant une liste de contrôle pour chaque composant de l'installation.

2.1 Planification du déploiement

Lorsque vous planifiez le déploiement de Directory and Resource Administrator, utilisez cette section pour évaluer la compatibilité de votre environnement matériel et logiciel et noter les ports et protocoles requis que vous devrez configurer pour le déploiement.

2.1.1 Recommandations relatives à la ressource testée

Cette section fournit des informations au sujet du dimensionnement recommandé pour notre ressource de base. Vos résultats peuvent varier en fonction du matériel disponible, de l'environnement spécifique, du type spécifique de données traitées, mais aussi d'autres facteurs. Des configurations matérielles plus puissantes et étendues pourront probablement gérer des charges plus importantes. Pour toute question, veuillez consulter les services NetIQ Consulting.

Exécution dans un environnement avec environ un million d'objets Active Directory :

Composant	UC	Mémoire	Stockage
Serveur d'administration DRA	4 UC (x64)/cœurs 2 GHz	16 Go	100 Go
Console Web DRA	2 UC (x64)/cœurs 2 GHz	8 Go	100 Go
DRA Reporting	4 UC (x64)/cœurs 2 GHz	16 Go	100 Go
Serveur de workflow DRA	4 UC (x64)/cœurs 2 GHz	16 Go	100 Go

2.1.2 Provisioning de ressources d'environnement virtuel

DRA conserve les segments de mémoire importants actifs pendant de longues périodes. Prenez en compte les recommandations suivantes lors du provisioning de ressources pour un environnement virtuel :

- ♦ Allouez l'espace de stockage en tant que « Thick Provisioned » (Provisioning lourd).
- ♦ Définissez la réservation de mémoire sur Reserve All Guest Memory(All Locked) [Réserver toute la mémoire invité(entièrement verrouillée)]
- ♦ Assurez-vous que le fichier de pagination est suffisamment volumineux pour permettre une éventuelle réallocation de la mémoire en ballon sur la couche virtuelle.

2.1.3 Ports et protocoles requis

Les ports et protocoles pour la communication DRA sont mentionnés dans cette section.

- ♦ Les ports configurables sont indiqués par un astérisque *
- ♦ Les ports nécessitant un certificat sont indiqués par deux astérisques **

Serveurs d'administration DRA

Protocole et port	Sens	Destination	Utilisation
TCP 135	Bidirectionnel	Serveurs d'administration DRA	Mappeur de nœud d'extrémité, exigence de base pour la communication DRA ; permet aux serveurs d'administration de se localiser l'un l'autre dans MMS
TCP 445	Bidirectionnel	Serveurs d'administration DRA	Réplication du modèle de délégation ; réplication de fichiers lors de la synchronisation MMS (SMB)
Plage de ports TCP dynamique *	Bidirectionnel	Contrôleurs de domaine Microsoft Active Directory	Par défaut, DRA assigne des ports dynamiquement à partir de la plage de ports TCP comprise entre 1 024 et 65 535. Vous pouvez, toutefois, configurer cette plage à l'aide des services de composants. Pour plus d'informations, reportez-vous à l'article Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Utilisation du modèle COM distribué avec des pare-feu (DCOM))
TCP 50000 *	Bidirectionnel	Serveurs d'administration DRA	Réplication d'attributs et communication ADAM avec le serveur DRA. (LDAP)
TCP 50001 *	Bidirectionnel	Serveurs d'administration DRA	Réplication d'attributs SSL (ADAM)
TCP/UDP 389	Sortant	Contrôleurs de domaine Microsoft Active Directory	Gestion des objets Active Directory (LDAP)
	Sortant	Serveur Microsoft Exchange	Gestion des boîtes aux lettres (LDAP)
TCP/UDP 53	Sortant	Contrôleurs de domaine Microsoft Active Directory	Résolution de noms
TCP/UDP 88	Sortant	Contrôleurs de domaine Microsoft Active Directory	Permet l'authentification du serveur DRA auprès des contrôleurs de domaine (Kerberos)
TCP 80	Sortant	Serveur Microsoft Exchange	Requis pour tous les serveurs Exchange locaux 2010 à 2013 (HTTP)
	Sortant	Microsoft Office 365	Accès PowerShell à distance (HTTP)
TCP 443	Sortant	Microsoft Office 365, Change Guardian	Accès à l'API graphique et intégration à Change Guardian (HTTPS)

Protocole et port	Sens	Destination	Utilisation
TCP 443, 5986, 5985	Sortant	Microsoft PowerShell	Applets de commande natives PowerShell (HTTPS) et communication à distance PowerShell
TCP 8092 * **	Sortant	Serveur de workflow	État du workflow et déclenchement (HTTPS)
TCP 50101 *	Entrant	Client DRA	Cliquez avec le bouton droit sur le rapport Historique des modifications dans le rapport d'audit de l'interface utilisateur. Peut être configuré lors de l'installation.
TCP 8989	Localhost	Service d'archivage des journaux	Communication avec l'archivage des journaux (ouverture via le pare-feu non requise)
TCP 50102	Bidirectionnel	Service core DRA	Service d'archivage des journaux
TCP 50103	Localhost	Service de cache DRA	Communication avec le service de cache sur le serveur DRA (ouverture via le pare-feu non requise)
TCP 1433	Sortant	Microsoft SQL Server	Collecte des données de création de rapports
UDP 1434	Sortant	Microsoft SQL Server	Le service de navigateur SQL Server utilise ce port pour identifier le port de l'instance nommée.
TCP 8443	Bidirectionnel	Serveur Change Guardian	Historique des modifications unifiées

Serveur REST DRA

Protocole et port	Sens	Destination	Utilisation
TCP 8755 * **	Entrant	Serveur IIS, applets de commande PowerShell DRA	Exécution des activités de workflow basées sur REST DRA (ActivityBroker)
TCP 11192 * **	Sortant	Service hôte DRA	Pour la communication entre le service REST DRA et le service d'administration DRA
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Découverte automatique à l'aide de SCP (Service Connection Point)
TCP 443	Sortant	Contrôleurs de domaine Microsoft AD	Découverte automatique à l'aide de SCP (Service Connection Point)

Console Web (IIS)

Protocole et port	Sens	Destination	Utilisation
TCP 8755 * **	Sortant	Service REST DRA	Pour la communication entre la console Web DRA, le PowerShell DRA et le service hôte DRA
TCP 443	Entrant	Navigateur client	Ouverture d'un site Web DRA
TCP 443 **	Sortant	Serveur d'authentification avancée	Authentification avancée

Console de délégation et d'administration DRA

Protocole et port	Sens	Destination	Utilisation
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Détection automatique à l'aide de SCP
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de workflow de l'adaptateur DRA. Par défaut, DCOM assigne dynamiquement des ports à partir de la plage de ports TCP 1 024 à 65 535. Vous pouvez, toutefois, configurer cette plage à l'aide des services de composants. Pour plus d'informations, reportez-vous à l'article Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Utilisation du modèle COM distribué avec des pare-feu (DCOM))
TCP 50102	Sortant	Service core DRA	Génération du rapport de l'historique des modifications

Serveur de workflow

Protocole et port	Sens	Destination	Utilisation
TCP 8755	Sortant	Serveurs d'administration DRA	Exécution des activités de workflow basées sur REST DRA (ActivityBroker)

Protocole et port	Sens	Destination	Utilisation
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de workflow de l'adaptateur DRA. Par défaut, DCOM assigne dynamiquement des ports à partir de la plage de ports TCP 1 024 à 65 535. Vous pouvez, toutefois, configurer cette plage à l'aide des services de composants. Pour plus d'informations, reportez-vous à l'article Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM) (Utilisation du modèle COM distribué avec des pare-feu (DCOM))
TCP 1433	Sortant	Microsoft SQL Server	Stockage des données de workflow
TCP 8091	Entrant	Console des opérations et console de configuration	API de workflow BSL (TCP)
TCP 8092 **	Entrant	Serveurs d'administration DRA	API de workflow BSL (HTTP) et (HTTPS)
TCP 2219	Localhost	Fournisseur d'espace de noms	Utilisé par le fournisseur d'espaces de noms pour exécuter des adaptateurs
TCP 9900	Localhost	Correlation Engine	Utilisé par l'instance Correlation Engine pour communiquer avec le moteur de workflow et le fournisseur d'espaces de noms
TCP 10117	Localhost	Fournisseur d'espace de noms de gestion des ressources	Utilisé par le fournisseur d'espace de noms de gestion des ressources

2.1.4 Plates-formes prises en charge

Pour obtenir les informations les plus récentes sur les plates-formes logicielles prises en charge, reportez-vous à la page Directory and Resource Administrator sur le site Web de NetIQ : <https://www.netiq.com/support>

Système géré	Conditions préalables
Active Directory	<ul style="list-style-type: none"> ◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	<ul style="list-style-type: none"> ◆ Microsoft Exchange 2010 SP3 (à l'exception des dossiers publics) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online

Système géré	Conditions préalables
Microsoft Office 365	<ul style="list-style-type: none"> ◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Module Windows Azure Active Directory pour Windows PowerShell https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype Entreprise Online, module Windows PowerShell https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype Entreprise	<ul style="list-style-type: none"> ◆ Microsoft Skype Entreprise 2015
Historique des modifications	<ul style="list-style-type: none"> ◆ Change Guardian 5.0, 5.1
Navigateurs Web	<ul style="list-style-type: none"> ◆ Microsoft Internet Explorer 11, Edge ◆ Google Chrome ◆ Mozilla Firefox
Automatisation des workflows	<ul style="list-style-type: none"> ◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2

2.1.5 Configuration requise pour le serveur d'administration DRA

DRA requiert la configuration de serveur suivante pour les logiciels et les comptes :

Configuration logicielle requise

Composant	Conditions préalables
Cible d'installation	Système d'exploitation du serveur d'administration de NetIQ :
Système d'exploitation	<ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 est uniquement pris en charge à des fins de mise à niveau. <p>REMARQUE : Le serveur doit également être membre d'un domaine natif Microsoft Windows Server pris en charge.</p> <p>Interfaces Windows DRA :</p> <ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1 (x86 et x64), 10 (x86 et x64)
Programme d'installation	<ul style="list-style-type: none"> ◆ Microsoft .Net Framework 4.5.2 et versions ultérieures

Composant	Conditions préalables
Serveur d'administration	<p>Directory and Resource Administrator :</p> <ul style="list-style-type: none"> ◆ Microsoft .Net Framework 4.5.2 et versions ultérieures ◆ L'un des suivants : <ul style="list-style-type: none"> ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Packages (x64 et x86) ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 et x86) ◆ Microsoft Message Queuing ◆ Rôles Microsoft Active Directory Lightweight Directory Services ◆ Service d'accès à distance au registre démarré <p>Microsoft Office 365/Exchange Online Administration :</p> <ul style="list-style-type: none"> ◆ Module Windows Azure Active Directory pour Windows PowerShell ◆ Assistant de connexion Microsoft Online Services pour professionnels de l'informatique ◆ Skype Entreprise Online, module Windows PowerShell <p>Pour plus d'informations, reportez-vous à la section Plates-formes prises en charge.</p>
Composants Web hérités	<p>Serveur Web :</p> <ul style="list-style-type: none"> ◆ Microsoft Internet Information Services (IIS) Versions 8.0, 8.5, 10 <p>Composants Microsoft IIS :</p> <ul style="list-style-type: none"> ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Service de rôle de sécurité Microsoft IIS <p>Interfaces Windows DRA :</p> <ul style="list-style-type: none"> ◆ Microsoft .Net Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)

Configuration requise pour les comptes

Compte	Description	Autorisations
Groupe AD LDS	Le compte de service DRA doit être ajouté à ce groupe pour l'accès à AD LDS.	◆ Groupe de sécurité locale de domaine

Compte	Description	Autorisations
Compte de service DRA	Autorisations requises pour exécuter le service d'administration NetIQ	<ul style="list-style-type: none"> ◆ Autorisations de type « Utilisateurs du modèle COM distribué » ◆ Membre du groupe d'administrateurs AD LDS ◆ Groupe d'opérateurs de compte ◆ Groupes d'archivage de journaux (OnePointOp ConfigAdms et OnePointOp) <p>REMARQUE : pour plus d'informations sur la configuration de comptes d'accès aux domaines à privilège minimal, reportez-vous à la section : Comptes d'accès DRA à privilège minimal.</p>
Administrateur DRA	Compte utilisateur ou groupe provisionné pour le rôle intégré d'administrateur DRA	<ul style="list-style-type: none"> ◆ Groupe de sécurité locale du domaine ou compte utilisateur du domaine ◆ Membre du domaine géré ou d'un domaine approuvé <ul style="list-style-type: none"> ◆ Si vous indiquez un compte à partir d'un domaine approuvé, vérifiez que l'ordinateur du serveur d'administration peut s'authentifier auprès de ce compte.
Comptes d'assistant administrateur DRA	Comptes qui recevront des pouvoirs par le biais de DRA.	<ul style="list-style-type: none"> ◆ Ajoutez tous les comptes d'assistant administrateur de DRA au groupe « Utilisateurs du modèle COM distribué » afin qu'ils puissent se connecter au serveur DRA à partir de clients distants. <p>REMARQUE : DRA peut être configuré pour effectuer cette gestion à votre place pendant l'installation.</p>

Comptes d'accès DRA à privilège minimal

Vous trouverez ci-dessous les autorisations et privilèges requis pour les comptes spécifiés et les commandes de configuration à exécuter.

Compte d'accès au domaine : Assignez les autorisations Active Directory suivantes au compte d'accès au domaine :

- ◆ Contrôle TOTAL sur les objets Domaine intégré
- ◆ Contrôle TOTAL sur les objets Ordinateur
- ◆ Contrôle TOTAL sur les objets Contact
- ◆ Contrôle TOTAL sur les objets Conteneur
- ◆ Contrôle TOTAL sur les groupes de distribution dynamique
- ◆ Contrôle TOTAL sur les objets Groupe

- ♦ Contrôle TOTAL sur les objets Inetorgperson
- ♦ Contrôle TOTAL sur les objets MsExchSystemObjectContainer
- ♦ Contrôle TOTAL sur les objets Unité organisationnelle
- ♦ Contrôle TOTAL sur les objets Imprimante
- ♦ Contrôle TOTAL sur les dossiers publics
- ♦ Contrôle TOTAL sur les objets Utilisateur

Indiquez les privilèges suivants avec une étendue de type « Cet objet et tous les objets enfants » dans le compte d'accès au domaine :

- ♦ Autoriser la création d'objets Ordinateur
- ♦ Autoriser la création d'objets Contact
- ♦ Autoriser la création d'un conteneur
- ♦ Autoriser la création d'objets Groupe
- ♦ Autoriser la création d'objets MsExchDynamicDistiributionList
- ♦ Autoriser la création d'objets Unité organisationnelle
- ♦ Autoriser la création de dossiers publics
- ♦ Autoriser la création d'un point de connexion de service
- ♦ Autoriser la création d'objets Utilisateur
- ♦ Autoriser la suppression d'objets Ordinateur
- ♦ Autoriser la suppression d'objets Contact
- ♦ Autoriser la suppression d'un conteneur
- ♦ Autoriser la suppression d'objets Groupe
- ♦ Autoriser la suppression d'objets InetOrgPerson
- ♦ Autoriser la suppression d'objets MsExchDynamicDistiributionList
- ♦ Autoriser la suppression d'objets Unité organisationnelle
- ♦ Autoriser la suppression de dossiers publics
- ♦ Autoriser la suppression d'un point de connexion de service
- ♦ Autoriser la suppression d'objets Utilisateur

Compte d'accès au locataire Office 365 : assignez les autorisations Active Directory suivantes au compte d'accès au locataire Office 365 :

- ♦ Administrateur de la gestion des utilisateurs dans Office 365
- ♦ Gestion des destinataires dans Exchange Online

Compte d'accès Exchange : assignez le rôle **Gestion de l'organisation** au compte d'accès Exchange pour gérer Exchange 2010.

Compte d'accès à Skype : assurez-vous que ce compte est employé par un utilisateur Skype et qu'il est membre d'au moins un des éléments suivants :

- ♦ Rôle CSAdministrator
- ♦ Rôles CSUserAdministrator et CSArchiving

Compte d'accès aux dossiers publics : assignez les autorisations Active Directory suivantes au compte d'accès aux dossiers publics :

- ♦ Gestion des dossiers publics
- ♦ Dossiers publics de messagerie

Opérations postérieures à l'installation de DRA :

- ♦ Exécutez la commande suivante pour déléguer l'autorisation sur le « Conteneur d'objets supprimés » à partir du dossier d'installation DRA (Remarque : la commande doit être exécutée par un administrateur de domaine) :

```
DraDelObjsUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<Nom Compte>
```

- ♦ Exécutez la commande suivante pour déléguer l'autorisation sur le « NetIQReceyleBin OU » à partir du dossier d'installation DRA (Remarque : cette opération ne peut être effectuée qu'après avoir ajouté les domaines respectifs à gérer par DRA) :

```
DraRecycleBinUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<Nom Compte>
```

- ♦ Ajoutez le compte de remplacement de privilège minimal au groupe « Administrateurs locaux » sur chaque ordinateur sur lequel DRA gère des ressources telles que des imprimantes, des services, un journal des événements, des périphériques, etc.
- ♦ Accordez au compte de remplacement de privilège minimal une « Autorisation complète » sur les dossiers de partage ou les dossiers DFS pour lesquels les répertoires privés sont provisionnés.
- ♦ Ajoutez le compte de remplacement de privilège minimal au rôle « Gestion de l'organisation » pour gérer des objets Exchange.

2.1.6 Configuration requise de la console Web et des extensions DRA

La configuration requise pour la console Web et les extensions REST est la suivante :

Configuration logicielle requise

Composant	Conditions préalables
Cible d'installation	Système d'exploitation : <ul style="list-style-type: none">♦ Microsoft Windows Server 2016, Microsoft Windows 10, avec Microsoft IIS 10♦ Microsoft Windows Server 2012, 2012 R2 avec Microsoft IIS 8.0, 8.5
Service hôte DRA	<ul style="list-style-type: none">♦ Microsoft .Net Framework 4.5.2♦ Serveur d'administration DRA
Service et nœud d'extrémité REST DRA	<ul style="list-style-type: none">♦ Microsoft .Net Framework 4.5.2
Extensions PowerShell	<ul style="list-style-type: none">♦ Microsoft .Net Framework 4.5.2♦ PowerShell 4.0

Composant	Conditions préalables
Console Web DRA	<p>Serveur Web :</p> <ul style="list-style-type: none"> ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft Internet Information Services WCF (Activation) <p>Composants Microsoft IIS :</p> <ul style="list-style-type: none"> ◆ Serveur Web <ul style="list-style-type: none"> ◆ Fonctionnalités HTTP communes <ul style="list-style-type: none"> ◆ Contenu statique ◆ Document par défaut ◆ Navigateur de répertoires ◆ Erreurs HTTP ◆ Développement d'applications <ul style="list-style-type: none"> ◆ ASP ◆ Santé et diagnostics <ul style="list-style-type: none"> ◆ Consignation HTTP ◆ Moniteur de requête ◆ Sécurité <ul style="list-style-type: none"> ◆ Authentification de base ◆ Performances <ul style="list-style-type: none"> ◆ Compression de contenu statique ◆ Outils de gestion du serveur Web

2.1.7 Configuration requise pour la création de rapports

La configuration requise pour DRA Reporting est la suivante :

Configuration logicielle requise

Composant	Conditions préalables
Cible d'installation	<p>Système d'exploitation :</p> <ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012, 2012 R2, 2016

Composant	Conditions préalables
NetIQ Reporting Center (v3.2)	<p>Base de données :</p> <ul style="list-style-type: none"> ◆ Microsoft SQL Server 2012, 2014, 2016 ◆ Microsoft SQL Server Reporting Services <p>Serveur Web :</p> <ul style="list-style-type: none"> ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Composants Microsoft IIS : <ul style="list-style-type: none"> ◆ ASP .NET 4.0 <p>Microsoft .NET Framework 3.5:</p> <p>Tout serveur d'administration DRA qui se connecte à DRA Reporting nécessite également .NET Framework 3.5.</p> <p>REMARQUE : Lorsque vous installez NetIQ Reporting Center (NRC) sur un ordinateur SQL Server, vous devrez peut-être installer .NET Framework 3.5 manuellement avant d'installer NRC.</p>
DRA Reporting	<p>Base de données :</p> <ul style="list-style-type: none"> ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

2.1.8 Exigences de licence

Votre licence détermine les produits et les fonctions que vous pouvez utiliser. DRA exige qu'une clé de licence soit installée avec le serveur d'administration.

Après avoir installé le serveur d'administration, vous pouvez faire appel à l'utilitaire de contrôle de l'état de santé pour installer une clé de licence d'évaluation (TrialLicense.lic) qui permet de gérer un nombre illimité de comptes utilisateur et de boîtes aux lettres pendant 30 jours.

Reportez-vous au contrat de licence utilisateur final (CLUF) pour plus d'informations concernant la définition de la licence et les restrictions qui y sont associées.

2.2 Installation du produit

Ce chapitre vous guide tout au long de l'installation de Directory and Resource Administrator. Pour plus d'informations sur la planification de votre installation ou de la mise à niveau, reportez-vous à la section [Planification du déploiement](#).

- ◆ [Section 2.2.1, « Installation du serveur d'administration DRA », page 27](#)
- ◆ [Section 2.2.2, « Installation de clients DRA », page 28](#)
- ◆ [Section 2.2.3, « Installation des extensions REST DRA », page 29](#)
- ◆ [Section 2.2.4, « Installation du serveur de workflow », page 30](#)
- ◆ [Section 2.2.5, « Installation de DRA Reporting », page 30](#)

2.2.1 Installation du serveur d'administration DRA

Vous pouvez installer le serveur d'administration DRA en tant que nœud primaire ou secondaire dans votre environnement. La configuration requise pour les serveurs d'administration primaire et secondaires est identique, sachant toutefois que chaque déploiement DRA doit inclure un serveur d'administration primaire.

Liste de contrôle pour une installation interactive

Étape	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour effectuer l'installation à l'aide d'un compte disposant de privilèges d'administration locaux.
Copie et exécution du kit d'installation d'administration NetIQ	Exécutez le kit d'installation DRA (NetIQAdminInstallationKit.msi) pour extraire le support d'installation DRA dans le système de fichiers local. REMARQUE : le kit d'installation installe .NET Framework sur le serveur cible, le cas échéant.
Exécution de l'installation de DRA	Lancez l'installation de DRA. REMARQUE : pour exécuter l'installation ultérieurement, accédez à l'emplacement auquel le support d'installation a été extrait et exécutez Setup.exe.
Sélection du composant du serveur d'administration NetIQ et de la cible d'installation	Choisissez les composants à installer et acceptez l'emplacement d'installation par défaut C:\Program Files (x86)\NetIQ\DRA ou spécifiez un autre emplacement d'installation. Options des composants : Serveur d'administration NetIQ <ul style="list-style-type: none">◆ Kit de ressources d'archivage des journaux◆ SDK DRA NetIQ Composant Web hérité Interfaces utilisateur <ul style="list-style-type: none">◆ Gestion des comptes et des ressources◆ Fournisseur ADSI DRA◆ Interface de ligne de commande◆ Délégation et configuration
Vérification des conditions préalables	La boîte de dialogue Prérequisites (Conditions préalables) affiche la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guide pour remplir les conditions préalables requises éventuellement manquantes pour que l'installation se déroule correctement.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final.

Étape	Détails
Sélection du mode de fonctionnement du serveur	<p>Sélectionnez Primary (Primaire) pour installer le premier serveur d'administration DRA dans un MMS (il n'y aura qu'un seul serveur primaire par déploiement) ou Secondary (Secondaire) pour joindre un nouveau serveur d'administration DRA à un MMS existant.</p> <p>Pour plus d'informations à propos du MMS, reportez-vous à la section Configuration du MMS.</p>
Indication des comptes d'installation et des informations d'identification	<ul style="list-style-type: none"> ◆ Compte de service DRA ◆ Groupe LDS AD ◆ Administrateur DRA <p>Pour plus d'informations, reportez-vous à la section Configuration requise pour le serveur d'administration DRA.</p>
Configuration des autorisations DCOM	Activez DRA afin de configurer l'accès « DCOM » pour les utilisateurs authentifiés.
Configuration des ports	Pour plus d'informations sur les ports par défaut, reportez-vous à la section Ports et protocoles requis .
Indication de l'emplacement de stockage	Indiquez l'emplacement du fichier local à utiliser par DRA pour stocker les données d'audit et de cache.
Vérification de la configuration de l'installation	Vous pouvez vérifier la configuration sur la page de résumé de l'installation avant de cliquer sur Installer pour procéder à l'installation.
Vérification de post-installation	Une fois l'installation effectuée, le vérificateur de l'état de santé s'exécute pour vérifier l'installation et mettre à jour la licence du produit.

2.2.2 Installation de clients DRA

Vous pouvez installer des consoles et des clients de ligne de commande DRA spécifiques en exécutant le fichier DRAInstall.msi avec le paquetage .mst correspondant sur la cible d'installation :

NetIQDRAUserConsole.mst	Installe la console de gestion des comptes et des ressources
NetIQDRACLI.mst	Installe l'interface de ligne de commande
NetIQDRAADSI.mst	Installe le fournisseur DRA ADSI
NetIQDRAClients.mst	Installe toutes les interfaces utilisateur DRA

Pour déployer des clients DRA spécifiques sur plusieurs ordinateurs de votre entreprise, configurez un objet Stratégie de groupe pour installer le paquetage .MST spécifique.

- 1 Lancez Utilisateurs et ordinateurs Active Directory et créez un objet Stratégie de groupe.
- 2 Ajoutez le paquetage DRAInstall.msi à cet objet Stratégie de groupe.
- 3 Vérifiez que cet objet Stratégie de groupe comporte une des propriétés suivantes :
 - ◆ Chaque compte utilisateur du groupe dispose d'autorisations Utilisateur avec pouvoir pour l'ordinateur approprié.
 - ◆ Activez le paramètre de stratégie Toujours installer avec des droits élevés.

- 4 Ajoutez le fichier .mst de l'interface utilisateur, tel que NetIQDRAUserConsole.mst, à cet objet Stratégie de groupe.
- 5 Distribuez votre stratégie de groupe.

REMARQUE : pour plus d'informations sur la stratégie de groupe, reportez-vous à l'aide de Microsoft Windows. Pour tester et déployer facilement et en toute sécurité les stratégies de groupe dans votre entreprise, utilisez l'*administrateur de stratégie de groupe*.

2.2.3 Installation des extensions REST DRA

Le paquetage d'extensions REST DRA comporte quatre fonctions :

- ♦ **Service hôte DRA NetIQ** : passerelle utilisée pour communiquer avec le service d'administration DRA. Ce service doit s'exécuter sur un ordinateur sur lequel le service d'administration DRA est installé.
- ♦ **Service et nœuds d'extrémité REST DRA** : fournit les interfaces RESTful qui permettent à la console Web DRA et aux clients non-DRA de demander des opérations DRA. Ce service doit s'exécuter sur un ordinateur sur lequel une console DRA ou le service d'administration DRA est installé.
- ♦ **Extensions PowerShell** : fournit un module PowerShell qui permet aux clients non-DRA de demander des opérations DRA à l'aide des applets de commande PowerShell.
- ♦ **Console Web DRA** : interface du client Web principalement utilisée par les assistants administrateur, mais qui inclut également des options de personnalisation.

Étape	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour effectuer l'installation à l'aide d'un compte disposant de privilèges d'administration locaux.
Installation du certificat SSL	S'il n'est pas déjà installé sur le serveur Windows, un certificat SSL doit être installé avant d'exécuter l'installation.
Copie et exécution du kit d'installation d'administration NetIQ	Copiez le kit d'installation DRA <code>NetIQAdminInstallationKit.msi</code> sur le serveur cible et exécutez-le en double-cliquant sur le fichier ou en l'appelant à partir de la ligne de commande. Le kit d'installation extrait le support d'installation DRA dans le système de fichiers local vers un emplacement personnalisable.
Exécution du programme d'installation des extensions REST DRA	Une fois que le kit d'installation DRA a terminé l'extraction du support d'installation, il vous invite à lancer l'installation de DRA. Accédez à l'emplacement auquel le support d'installation a été extrait, cliquez avec le bouton droit sur le fichier <code>DRARESTExtensionsInstaller.exe</code> , puis sélectionnez Exécuter en tant qu'administrateur .
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final.
Sélection de composants et Indication de l'emplacement cible de l'installation	Dans la boîte de dialogue Select Components (Sélectionner les composants), installez toutes les options : DRA Host Service (service hôte DRA), DRA REST Endpoints and service (nœuds d'extrémité et service REST DRA), PowerShell Extensions (extensions PowerShell) et DRA Web Console (console Web DRA). Acceptez l'emplacement d'installation par défaut <code>C:\Program Files (x86)\NetIQ\DRA Extensions</code> ou indiquez un autre emplacement pour l'installation.

Étape	Détails
Vérification des conditions préalables	La boîte de dialogue Prerequisites (Conditions préalables) affiche la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guide pour remplir les conditions préalables requises éventuellement manquantes pour que l'installation se déroule correctement.
Spécification du compte de service à exécuter en tant que	Par défaut, le compte de service existant du serveur DRA est affiché. Indiquez le mot de passe du compte de service. Pour plus d'informations sur la configuration d'un compte de service pour le serveur d'administration DRA, reportez-vous à la section Configuration requise pour le serveur d'administration DRA .
Spécification du certificat SSL du service REST	Sélectionnez le certificat SSL que vous utiliserez pour le service REST et indiquez les ports de service REST et Hôte.
Spécification du certificat SSL de la console Web	Indiquez le certificat SSL que vous utiliserez pour la connexion HTTPS.
Vérification de la configuration de l'installation	Vous pouvez vérifier la configuration sur la page de résumé de l'installation avant de cliquer sur Installer pour procéder à l'installation.

2.2.4 Installation du serveur de workflow

Pour plus d'informations sur l'installation du serveur de workflow, reportez-vous au [Workflow Automation Administrator Guide](#) (Guide de l'administrateur d'automatisation de workflow).

2.2.5 Installation de DRA Reporting

DRA Reporting vous demande d'installer deux fichiers exécutables à partir du kit d'installation NetIQ DRA : `NRCSetup.exe` et `DRAReportingSetup.exe`.

Étapes	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour effectuer l'installation à l'aide d'un compte disposant de privilèges d'administration locaux. Veillez à ce que ce compte possède des privilèges d'administrateur local et de domaine, mais aussi des privilèges d'administrateur système sur le serveur SQL.
Copie et exécution du kit d'installation d'administration NetIQ	Copiez le kit d'installation DRA <code>NetIQAdminINStallationKit.msi</code> sur le serveur cible et exécutez-le en double-cliquant sur le fichier ou en l'appelant à partir de la ligne de commande. Le kit d'installation extrait le support d'installation DRA dans le système de fichiers local vers un emplacement personnalisable. De plus, le kit d'installation installe .NET Framework sur le serveur cible si nécessaire pour remplir la condition préalable du programme d'installation du produit DRA.
Exécution du fichier d'installation de NetIQ Reporting Center (NRC)	Une fois que le kit d'installation DRA a terminé l'extraction du support d'installation, accédez à l'emplacement auquel le support d'installation a été extrait et exécutez le fichier <code>NRCSetup.exe</code> .
Sélection du composant NetIQ Reporting Center	Dans la boîte de dialogue Select Components (Sélectionner les composants), utilisez le composant par défaut « NetIQ Reporting Center » pour installer les quatre composants NRC.

Étapes	Détails
Indication de l'emplacement cible de l'installation	Acceptez l'emplacement d'installation par défaut C:\Program Files (x86)\NetIQ\Reporting Center ou indiquez un autre emplacement d'installation.
Vérification des conditions préalables et installation	La boîte de dialogue Prerequisites (Conditions préalables) affiche la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guide pour remplir les conditions préalables requises éventuellement manquantes pour que l'installation se déroule correctement. IMPORTANT : .NET Framework 3.5 doit être installé manuellement sur le serveur de création de rapports avant l'installation de NRC.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final.
Installation de la base de données de configuration	Utilisez les valeurs par défaut de la boîte de dialogue Configuration Database Installation - SQL Server Logon (Installation de la base de données de configuration - Connexion à SQL Server) ou fournissez l'authentification SQL pour terminer l'installation de NRC. Si vous avez utilisé l'instance par défaut pour l'installation de SQL Server, le champ Instance doit rester vide.
Exécution de l'installation de DRA Reporting	Accédez à l'emplacement auquel le support d'installation a été extrait et exécutez DRAReportingSetup.exe pour installer le composant de gestion permettant l'intégration de DRA Reporting.
Acceptation du contrat de licence CLUF	Acceptez les termes du contrat de licence utilisateur final pour terminer l'exécution de l'installation.

2.3 Mise à jour de produit

Ce chapitre présente une procédure qui vous aide à mettre à niveau ou à migrer un environnement distribué par phases contrôlées.

Ce chapitre suppose que votre environnement contienne plusieurs serveurs d'administration, certains serveurs étant situés sur des sites distants. Cette configuration est appelée ensemble multi-maître (MMS, Multi-Master Set). Un MMS comprend un serveur d'administration primaire et un ou plusieurs serveurs d'administration secondaires associés. Pour plus d'informations sur le fonctionnement d'un MMS, reportez-vous à la section [Configuration du MMS](#).

- ♦ [Section 2.3.1, « Planification d'une mise à niveau DRA », page 32](#)
- ♦ [Section 2.3.2, « Tâches préalables à la mise à niveau », page 32](#)
- ♦ [Section 2.3.3, « Mise à niveau du serveur d'administration DRA », page 35](#)
- ♦ [Section 2.3.4, « Mise à niveau des extensions REST DRA », page 38](#)
- ♦ [Section 2.3.5, « Mise à niveau de DRA Reporting », page 39](#)

2.3.1 Planification d'une mise à niveau DRA

Exécutez le kit `NetIQAdminInstallationKit.msi` pour extraire le support d'installation de DRA, puis installez et exécutez l'utilitaire de contrôle de l'état de santé.

Assurez-vous de planifier votre déploiement de DRA avant d'entamer la procédure de mise à niveau. Lorsque vous planifiez votre déploiement, tenez compte des instructions suivantes :

- ♦ Testez la procédure de mise à niveau dans votre environnement de test avant de déployer la mise à niveau dans votre environnement de production. Les tests vous permettent d'identifier et de résoudre les problèmes inattendus sans entraver les tâches quotidiennes des responsables administratifs.
- ♦ Reportez-vous à [Ports et protocoles requis](#).
- ♦ Déterminez le nombre d'assistants administrateur qui s'appuient sur chaque MMS. Si la plupart de vos assistants administrateur s'appuient sur des serveurs ou des ensembles de serveurs spécifiques, commencez par mettre à niveau ces serveurs durant les heures creuses.
- ♦ Déterminez les assistants administrateur qui ont besoin de la console de délégation et de configuration. Vous pouvez obtenir cette information de l'une des façons suivantes :
 - ♦ Passez en revue les assistants administrateur associés aux groupes d'assistants administrateur intégrés.
 - ♦ Passez en revue les assistants administrateur associés à la technologie ActiveViews intégrée.
 - ♦ Utilisez DRA Reporting pour générer des rapports sur le modèle de sécurité, tels que les rapports ActiveView Assistant Admin Details (Détails des assistants administrateur ActiveView) et Groupes d'assistants administrateur.

Informez ces assistants administrateur de vos plans de mise à niveau des interfaces utilisateur.

- ♦ Déterminez les assistants administrateur qui doivent se connecter au serveur d'administration primaire. Ces assistants administrateur doivent mettre à niveau leurs ordinateurs client une fois que vous avez mis à niveau le serveur d'administration primaire.

Informez ces assistants administrateur de vos plans de mise à niveau des serveurs d'administration et des interfaces utilisateur.

- ♦ Déterminez si vous devez implémenter des modifications de délégation, de configuration ou de stratégie avant de commencer la procédure de mise à niveau. Selon votre environnement, cette décision peut être prise au cas par cas.
- ♦ Coordonnez la mise à niveau de vos ordinateurs client et de vos serveurs d'administration pour assurer un temps hors service minimal. Sachez que DRA ne prend pas en charge l'exécution des versions antérieures de DRA avec la version actuelle de DRA sur le même serveur d'administration ou ordinateur client.

2.3.2 Tâches préalables à la mise à niveau

Avant d'installer les mises à niveau, effectuez au préalable les étapes suivantes pour préparer chaque ensemble de serveurs à la mise à niveau.

Étapes	Détails
Sauvegarde de l'instance AD LDS	Ouvrez l'utilitaire de contrôle de l'état de santé et procédez à la vérification de la sauvegarde de l'instance AD LDS pour créer une sauvegarde de votre instance AD LDS actuelle.

Étapes	Détails
Création d'un plan de déploiement	Créez un plan de déploiement pour la mise à niveau des serveurs d'administration et des interfaces utilisateur (ordinateurs client des assistants administrateur). Pour plus d'informations, reportez-vous à la section Planification d'une mise à niveau DRA .
Allocation d'un serveur secondaire pour l'exécution d'une version antérieure de DRA	<i>Facultatif</i> : allouez un serveur d'administration secondaire à l'exécution d'une version antérieure de DRA lors de la mise à niveau d'un site.
Introduction des modifications nécessaires pour ce MMS	Apportez les modifications nécessaires aux paramètres de délégation, de configuration ou de stratégie pour ce MMS. Utilisez le serveur d'administration primaire pour modifier ces paramètres.
Synchronisation des MMS	Synchronisez les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.
Sauvegarde du registre du serveur primaire	Sauvegardez le registre à partir du serveur d'administration primaire. La sauvegarde de vos anciens paramètres de registre permet de récupérer facilement votre configuration précédente et ses paramètres de sécurité.

REMARQUE : si vous devez restaurer l'instance AD LDS, procédez comme suit :

- 1 Arrêtez l'instance AD LDS en cours dans Gestion de l'ordinateur > Services. L'intitulé sera différent : `NetIQDRASecureStoragexxxxx`.
- 2 Remplacez le fichier **adamnts.dit** actuel par le fichier **adamnts.dit** de sauvegarde comme indiqué ci-dessous :
 - ♦ Emplacement du fichier actuel : `%ProgramData%/NetIQ/DRA/<NomInstanceDRA>/data/`
 - ♦ Emplacement du fichier de sauvegarde : `%ProgramData%/NetIQ/ADLDS/`
- 3 Redémarrez l'instance AD LDS.

Allocation d'un serveur d'administration local pour l'exécution d'une version antérieure de DRA

L'allocation d'un ou plusieurs serveurs d'administration secondaires pour exécuter localement une version antérieure de DRA sur un site pendant la mise à niveau peut aider à réduire le temps hors service et les connexions coûteuses vers des sites distants. Cette étape est facultative et permet aux assistants administrateur d'utiliser une version antérieure de DRA tout au long de la procédure de mise à niveau, jusqu'à ce que vous soyez certain que votre déploiement est terminé.

Envisagez cette option si vous êtes concerné par une ou plusieurs des exigences de mise à niveau suivantes :

- ♦ Vous souhaitez un minimum de temps hors service, voire aucun.
- ♦ Vous devez prendre en charge un grand nombre d'assistants administrateur sans pouvoir mettre immédiatement à niveau tous les ordinateurs client.
- ♦ Vous voulez continuer à prendre en charge l'accès à une version antérieure de DRA après la mise à niveau du serveur d'administration primaire.
- ♦ Votre environnement inclut un MMS qui s'étend sur plusieurs sites.

Vous pouvez installer un nouveau serveur d'administration secondaire ou désigner un serveur secondaire existant exécutant une version antérieure de DRA. Si vous avez l'intention de mettre à niveau ce serveur, il doit être le dernier serveur que vous mettez à niveau. Dans le cas contraire, désinstallez complètement DRA de ce serveur lorsque vous avez terminé votre mise à niveau.

Configuration d'un nouveau serveur secondaire

L'installation d'un nouveau serveur d'administration secondaire sur un site local peut vous aider à éviter les connexions coûteuses à des sites distants et garantit que vos assistants administrateur peuvent continuer à utiliser une version antérieure de DRA sans interruption. Si votre environnement comporte un MMS qui s'étend sur plusieurs sites, vous devriez envisager cette option. Par exemple, si votre MMS se compose d'un serveur d'administration primaire sur votre site de Paris et d'un serveur d'administration secondaire sur votre site de Tokyo, envisagez d'installer un serveur secondaire sur le site de Paris et de l'ajouter au MMS correspondant. Ce serveur supplémentaire permet aux assistants administrateur du site de Paris d'utiliser une version antérieure de DRA jusqu'à ce que la mise à niveau soit terminée.

Utilisation d'un serveur secondaire existant

Vous pouvez utiliser un serveur d'administration secondaire existant en tant que serveur dédié pour une version antérieure de DRA. Si vous ne prévoyez pas de mettre à niveau un serveur d'administration secondaire sur un site donné, vous devez envisager cette option. Si vous ne pouvez pas dédier un serveur secondaire existant, envisagez d'installer un nouveau serveur d'administration pour ce faire. L'allocation d'un ou plusieurs serveurs secondaires pour l'exécution d'une version antérieure de DRA permet à vos assistants administrateur de continuer à utiliser une version antérieure de DRA sans interruption jusqu'à la fin de la mise à niveau. Le recours à cette option est idéal dans les environnements étendus qui utilisent un modèle d'administration centralisée.

Synchronisation de votre ensemble de serveurs utilisant une version antérieure de DRA

Avant de sauvegarder le registre de la version antérieure de DRA ou d'entamer la procédure de mise à niveau, assurez-vous de synchroniser les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.

REMARQUE : vérifiez que vous avez apporté toutes les modifications nécessaires aux paramètres de délégation, de configuration ou de stratégie de ce MMS. Utilisez le serveur d'administration primaire pour modifier ces paramètres. Une fois le serveur d'administration primaire mis à niveau, vous ne pouvez pas synchroniser les paramètres de délégation, de configuration ou de stratégie avec les serveurs d'administration exécutant des versions antérieures de DRA.

Pour synchroniser votre ensemble de serveurs existant :

- 1 Connectez-vous au serveur d'administration primaire en tant qu'administrateur intégré.
- 2 Démarrez l'interface MMC.
- 3 Dans le panneau de gauche, développez **Gestion de la configuration**.
- 4 Cliquez sur **Serveurs d'administration**.
- 5 Dans le volet de droite, sélectionnez le serveur d'administration primaire approprié pour cet ensemble de serveurs.
- 6 Cliquez sur **Propriétés**.

- 7 Sous l'onglet Planification de la synchronisation, cliquez sur **Rafraîchir maintenant**.
- 8 Vérifiez la réussite de la synchronisation et la disponibilité de tous les serveurs d'administration secondaires.

Sauvegarde du registre du serveur d'administration

La sauvegarde du registre du serveur d'administration garantit que vous pouvez revenir à vos configurations précédentes. Par exemple, si vous devez désinstaller complètement la version actuelle de DRA et utiliser la version précédente, le fait de disposer d'une sauvegarde de vos paramètres de registre précédents vous permet de récupérer facilement vos paramètres de configuration et de sécurité.

Cependant, soyez prudent lorsque vous modifiez votre registre. En cas d'erreur dans votre registre, le serveur d'administration peut ne pas fonctionner comme prévu. Si une erreur se produit pendant la procédure de mise à niveau, vous pouvez utiliser la sauvegarde de vos paramètres de registre pour le restaurer. Pour plus d'informations, reportez-vous à *l'aide de l'Éditeur du Registre*.

IMPORTANT : la version du serveur DRA, le nom du système d'exploitation Windows de même que la configuration du domaine géré doivent être parfaitement identiques lors de la restauration du registre.

IMPORTANT : avant la mise à niveau, sauvegardez le système d'exploitation Windows de la machine qui héberge DRA ou créez une image instantanée de la machine virtuelle.

Pour sauvegarder le registre du serveur d'administration :

- 1 Exécutez `regedit.exe`.
- 2 Cliquez avec le bouton droit sur le nœud
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint`, et sélectionnez **Exporter**.
- 3 Indiquez le nom et l'emplacement du fichier dans lequel enregistrer la clé de registre, puis cliquez sur **Enregistrer**.

2.3.3 Mise à niveau du serveur d'administration DRA

La liste de contrôle suivante vous guide tout au long de la procédure de mise à niveau. Réeffectuez cette procédure pour mettre à niveau chaque ensemble de serveurs de votre environnement. Si vous ne l'avez pas encore fait, employez l'utilitaire de contrôle de l'état de santé pour créer une sauvegarde de votre instance AD LDS actuelle.

Vous pouvez répartir cette procédure de mise à niveau en plusieurs phases, en mettant à jour un MMS à la fois. Cette procédure de mise à niveau vous permet également d'inclure temporairement des serveurs secondaires exécutant une version antérieure de DRA et des serveurs secondaires exécutant la version actuelle de DRA dans le même MMS. DRA prend en charge la synchronisation entre les serveurs d'administration exécutant une version antérieure de DRA et les serveurs exécutant la version actuelle de DRA. Cependant, sachez que DRA ne prend pas en charge l'exécution d'une version antérieure de DRA avec la version actuelle sur le même serveur d'administration ou ordinateur client.

Dans DRA 9.2 ou version ultérieure, la configuration du serveur d'automatisation du workflow est stockée dans AD LDS au lieu du registre. Lors de la mise à jour de DRA 9.1 ou version antérieure vers DRA 9.2 ou version ultérieure, la configuration du registre est automatiquement déplacée vers AD LDS et répliquée sur l'ensemble des serveurs secondaires.

AVERTISSEMENT : ne mettez pas à niveau vos serveurs d'administration secondaires tant que vous n'avez pas mis à niveau le serveur d'administration primaire de ce MMS.

Étapes	Détails
Exécution de l'utilitaire de contrôle de l'état de santé	Installez l'utilitaire de contrôle de l'état de santé DRA en mode autonome et exécutez-le à l'aide d'un compte de service. Résolvez tous les problèmes.
Exécution d'une mise à niveau test	Effectuez une mise à niveau test dans votre environnement de test afin d'identifier les problèmes potentiels et de minimiser les temps hors service en production.
Ordre de la mise à niveau	Déterminez l'ordre dans lequel vous souhaitez mettre à niveau vos ensembles de serveurs.
Préparation de chaque MMS pour la mise à niveau	Préparez chaque MMS pour la mise à niveau. Pour plus d'informations, reportez-vous aux Tâches préalables à la mise à niveau .
Mise à niveau du serveur primaire	Mettez à niveau le serveur d'administration primaire dans le MMS approprié.
Installation d'un nouveau serveur secondaire	<i>(Facultatif)</i> Pour réduire les temps hors service sur les sites distants, installez un serveur d'administration secondaire local exécutant la version de DRA la plus récente.
Déploiement des interfaces utilisateur	Déployez les interfaces utilisateur auprès de vos assistants administrateur.
Mise à niveau des serveurs secondaires	Mettez à niveau les serveurs d'administration secondaires du MMS.
Mise à niveau de DRA Reporting	Mettez à niveau DRA Reporting.
Mise à niveau des extensions REST	Exécutez le programme d'installation des extensions REST DRA.
Exécution de l'utilitaire de contrôle de l'état de santé	Exécutez l'utilitaire de contrôle de l'état de santé qui a été installé dans le cadre de la mise à niveau. Résolvez tous les problèmes.

Mise à niveau du serveur d'administration primaire

Après avoir préparé votre MMS, mettez à niveau le serveur d'administration primaire. Ne mettez pas à niveau les interfaces utilisateur sur les ordinateurs client des assistants administrateur tant que vous n'avez pas terminé la mise à niveau du serveur d'administration primaire. Pour plus d'informations, reportez-vous à la section [Déploiement des interfaces utilisateur DRA](#).

REMARQUE : pour des considérations plus détaillées sur les mises à niveau, reportez-vous aux *Directory and Resource Administrator Release Notes* (Notes de version de Directory and Resource Administrator).

Avant de procéder à la mise à niveau, informez vos assistants administrateur de la date et heure auxquelles vous prévoyez de démarrer cette procédure. Si vous avez alloué un serveur d'administration secondaire pour l'exécution d'une version antérieure de DRA, spécifiez également ce serveur afin que les assistants administrateur puissent continuer à utiliser la version précédente de DRA pendant la mise à niveau.

REMARQUE : une fois que vous avez mis à niveau le serveur d'administration primaire, vous ne pouvez pas synchroniser les paramètres de délégation, de configuration ou de stratégie de ce serveur avec les serveurs d'administration secondaires exécutant une version antérieure de DRA.

Installation d'un serveur d'administration secondaire local pour la version actuelle de DRA

L'installation d'un nouveau serveur d'administration secondaire pour exécuter la version actuelle de DRA sur un site local peut vous aider à réduire les connexions coûteuses aux sites distants tout en réduisant les temps hors service globaux et en permettant un déploiement plus rapide des interfaces utilisateur. Cette étape est facultative et permet aux assistants administrateur d'utiliser à la fois la version actuelle de DRA et une version antérieure de DRA tout au long de la procédure de mise à niveau, jusqu'à ce que vous soyez certain que votre déploiement est terminé.

Envisagez cette option si vous êtes concerné par une ou plusieurs des exigences de mise à niveau suivantes :

- ◆ Vous souhaitez un minimum de temps hors service, voire aucun.
- ◆ Vous devez prendre en charge un grand nombre d'assistants administrateur sans pouvoir mettre immédiatement à niveau tous les ordinateurs client.
- ◆ Vous voulez continuer à prendre en charge l'accès à une version antérieure de DRA après la mise à niveau du serveur d'administration primaire.
- ◆ Votre environnement inclut un MMS qui s'étend sur plusieurs sites.

Par exemple, si votre MMS se compose d'un serveur d'administration primaire sur votre site de Paris et d'un serveur d'administration secondaire sur votre site de Tokyo, envisagez d'installer un serveur secondaire sur le site de Tokyo et de l'ajouter au MMS correspondant. Ce serveur supplémentaire équilibre mieux la charge d'administration quotidienne sur le site de Tokyo et permet aux assistants administrateur de l'un ou l'autre site d'utiliser une version antérieure de DRA ainsi que la version actuelle de DRA jusqu'à la fin de la mise à niveau. En outre, vos assistants administrateur ne subissent aucun temps hors service puisque vous pouvez déployer immédiatement les interfaces utilisateur DRA actuelles. Pour plus d'informations sur la mise à niveau des interfaces utilisateur, reportez-vous à la section [Déploiement des interfaces utilisateur DRA](#).

Déploiement des interfaces utilisateur DRA

En général, vous devez déployer les interfaces utilisateur DRA actuelles après la mise à niveau du serveur d'administration primaire et d'un serveur d'administration secondaire. Toutefois, pour les assistants administrateur qui doivent utiliser le serveur d'administration primaire, assurez-vous d'abord de mettre à niveau leurs ordinateurs client en installant la console de délégation et de configuration. Pour plus d'informations, reportez-vous à la section [Planification d'une mise à niveau DRA](#).

Si vous effectuez souvent un traitement par lots via l'interface de ligne de commande ou le fournisseur ADSI ou si vous générez fréquemment des rapports, envisagez d'installer ces interfaces utilisateur sur un serveur d'administration secondaire dédié pour conserver un équilibre de charge approprié sur le MMS.

Vous pouvez autoriser vos assistants administrateur à installer les interfaces utilisateur DRA ou déployer ces interfaces au moyen d'une stratégie de groupe. Vous pouvez également déployer facilement et rapidement la console Web pour plusieurs assistants administrateur.

REMARQUE : vous ne pouvez toutefois pas exécuter plusieurs versions des composants DRA côte à côte sur le même serveur DRA. Si vous prévoyez de mettre à niveau progressivement les ordinateurs client des assistants administrateur, envisagez de déployer la console Web pour garantir un accès immédiat à un serveur d'administration exécutant la version actuelle de DRA.

Mise à niveau des serveurs d'administration secondaires

Lors de la mise à niveau des serveurs d'administration secondaires, vous pouvez mettre à niveau chaque serveur en fonction de vos besoins d'administration. Étudiez également la planification de la mise à niveau et le déploiement de l'interface utilisateur DRA. Pour plus d'informations, reportez-vous à la section [Déploiement des interfaces utilisateur DRA](#).

Par exemple, un plan de mise à niveau standard peut comprendre les étapes suivantes :

- 1 Mettez à niveau un serveur d'administration secondaire.
- 2 Demandez aux assistants administrateur qui utilisent ce serveur d'installer les interfaces utilisateur appropriées, telles que la console de gestion des comptes et des ressources.
- 3 Répétez les étapes 1 et 2 ci-dessus jusqu'à la mise à niveau complète du MMS.

Avant de procéder à la mise à niveau, informez vos assistants administrateur de la date et heure auxquelles vous prévoyez de démarrer cette procédure. Si vous avez alloué un serveur d'administration secondaire pour l'exécution d'une version antérieure de DRA, spécifiez également ce serveur afin que les assistants administrateur puissent continuer à utiliser la version précédente de DRA pendant la mise à niveau. Lorsque vous avez terminé la procédure de mise à niveau pour ce MMS et que tous les ordinateurs client des assistants administrateur exécutent des interfaces utilisateur mises à niveau, placez hors ligne tous les serveurs restants qui utilisent une version antérieure de DRA.

2.3.4 Mise à niveau des extensions REST DRA

Pour mettre à niveau la console Web et les extensions REST vers Directory and Resource Administrator 9.2, vous devez utiliser DRA 9.0.1 ou une version ultérieure. Pour plus d'informations sur la configuration requise, reportez-vous à la section [Configuration requise de la console Web et des extensions DRA](#).

Pour mettre à niveau la console Web et les extensions DRA :

- 1 Après avoir téléchargé le kit d'installation DRA, accédez à l'emplacement auquel le support d'installation a été extrait, cliquez avec le bouton droit sur le fichier `DRARESTExtensionsInstaller.exe`, puis sélectionnez **Exécuter en tant qu'administrateur**.
- 2 Suivez les instructions de l'Assistant d'installation jusqu'à ce que l'installation soit terminée, puis cliquez sur **Terminer**.

Pour plus d'informations sur les étapes de l'Assistant d'installation, reportez-vous aux étapes d'une nouvelle installation : [Installation des extensions REST DRA](#).

Mise à jour du contenu personnalisé

Lorsque vous effectuez une mise à niveau vers une version plus récente de DRA, vous souhaitez conserver toutes les personnalisations que vous avez effectuées pour la console Web sur le serveur Web. Pour vous faciliter la tâche, DRA dispose d'un utilitaire de mise à niveau des personnalisations intégré au programme d'installation des extensions REST DRA. Cet utilitaire s'exécute

automatiquement lorsque vous exécutez le fichier exécutable `DRARESTExtensionsInstaller.exe` pour mettre à niveau des extensions REST sur le serveur Web. Vous pouvez également réexécuter manuellement l'utilitaire à partir du répertoire d'installation de DRA après l'installation.

Une partie de la procédure de l'utilitaire de mise à niveau des personnalisations consiste à sauvegarder vos personnalisations avant le démarrage de la mise à niveau. Au cours de la procédure de mise à niveau, l'utilitaire crée un fichier journal de toutes les modifications apportées en raison de la mise à niveau et inclut également un avertissement relatif aux éléments de personnalisation qui ne peuvent pas être mis à jour automatiquement.

Nous recommandons de consulter le journal après la mise à niveau. Si nécessaire, vous pouvez restaurer l'état initial des personnalisations antérieures de la mise à niveau en les copiant à partir du dossier de sauvegarde. Vous pouvez définir le chemin du dossier pour les personnalisations mises à niveau lorsque l'utilitaire de mise à niveau des personnalisations s'ouvre ou vous pouvez utiliser le chemin par défaut, qui est renseigné automatiquement.

Les chemins par défaut pour les personnalisations mises à niveau et la sauvegarde des personnalisations sont fournis ci-dessous :

- ♦ Chemin par défaut du dossier personnalisé :
`C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom`
- ♦ Dossier de sauvegarde par défaut :
`$CustomFolderPath\custom_upgrade_${VERSIONFROM}_to_${VERSIONTO}_backup`

2.3.5 Mise à niveau de DRA Reporting

Avant de mettre à niveau DRA Reporting, assurez-vous que votre environnement répond à la configuration minimale requise pour NRC 3.2. Pour plus d'informations sur la configuration requise pour l'installation et les considérations de mises à niveau du produit, reportez-vous au *NetIQ Reporting Center Reporting Guide* (Guide de création de rapports de NetIQ Reporting Center).

Étapes	Détails
Désactivation de la prise en charge de DRA Reporting	Pour vous assurer que les collecteurs de création de rapports ne s'exécutent pas pendant la procédure de mise à niveau, désactivez la prise en charge de DRA Reporting dans la fenêtre Reporting Service Configuration (Configuration du service de création de rapports) de la console de délégation et de configuration.
Connexion au serveur d'instance SQL avec les informations d'identification applicables	Connectez-vous au serveur Microsoft Windows sur lequel vous avez installé l'instance SQL pour les bases de données de création de rapports avec un compte d'administrateur. Assurez-vous que ce compte dispose des privilèges d'administrateur local ainsi que des privilèges d'administrateur système sur SQL Server.
Lancement du programme d'installation de DRA Reporting	Exécutez le fichier exécutable <code>DRAReportingSetup.exe</code> à partir du kit d'installation et suivez les instructions de l'Assistant d'installation.
Exécution du programme d'installation de NRC	<i>Conditionnel</i> : si votre service Web NRC est installé sur un autre ordinateur, connectez-vous à l'ordinateur sur lequel le service Web est installé et exécutez <code>NRCSetup.exe</code> pour mettre à niveau le service Web NRC. REMARQUE : si la base de données de configuration a été installée sur un serveur distinct, elle devra d'abord être mise à niveau.

Étapes	Détails
Exécution du programme d'installation de NRC sur les ordinateurs client	Exécutez <code>NRCSetup.exe</code> sur tous les ordinateurs client NRC.
Activation de la prise en charge de DRA Reporting	Sur votre serveur d'administration primaire, activez la création de rapports dans la console de délégation et de configuration.

Si votre environnement utilise l'intégration SSRS, vous devez redéployer vos rapports. Pour plus d'informations sur le redéploiement des rapports, reportez-vous au [NetIQ Reporting Center Reporting Guide](#) (Guide de la création de rapports de NetIQ Reporting Center) sur le site Web de documentation.

3 Configuration des composants et processus

Ce chapitre fournit des informations pour la première configuration de DRA, y compris des serveurs et de leur personnalisation, des consoles et de leur personnalisation, d'Office 365, de l'administration des dossiers publics et de la connexion aux serveurs.

3.1 Configuration initiale

Cette section décrit les étapes de configuration requises si vous installez Directory and Resource Administrator pour la première fois.

3.1.1 Liste de contrôle de la configuration

Utilisez la liste de contrôle suivante pour vous aider à configurer DRA dans le cadre d'une première utilisation.

Étapes	Détails
Installation d'une licence DRA	Employez l'utilitaire de contrôle de l'état de santé pour appliquer une licence DRA. Pour plus d'informations sur les licences DRA, reportez-vous à la section Exigences de licence .
Configuration des fonctions et des serveurs DRA	Configurez le MMS, les exceptions de clonage, la réplication des fichiers, l'horodatage des événements, le caching, AD LDS, les groupes dynamiques, la corbeille, la création de rapports, l'historique des modifications unifiées et le serveur de workflow.
Configuration du client de délégation et de configuration	Configurez la manière dont les éléments sont accessibles et affichés dans le client de délégation et de configuration.
Configuration du client Web	Configurez la déconnexion automatique, les certificats, les connexions serveur et les composants d'authentification.

3.1.2 Installation ou mise à niveau de licences

DRA nécessite un fichier de clé de licence. Ce fichier contient vos informations de licence et est installé sur le serveur d'administration. Après avoir installé le serveur d'administration, employez l'utilitaire de contrôle de l'état de santé pour installer le fichier de clé de licence d'évaluation (`TrialLicense.lic`) fourni par NetIQ Corporation.

Pour mettre à niveau une licence d'évaluation ou une licence existante, ouvrez la Console de délégation et de configuration et accédez à **Configuration-Management** (Gestion de la configuration) > **Update License** (Mettre à jour la licence). Lorsque vous mettez à niveau votre licence, mettez à niveau le fichier de licence sur chaque serveur d'administration.

Vous pouvez afficher votre licence de produit via la console de délégation et de configuration ou la console de gestion des comptes et des ressources. Pour afficher votre licence de produit, accédez au menu **File** (Fichier) > **DRA Properties** (Propriétés DRA) > **License** (Licence).

3.1.3 Configuration des fonctions et des serveurs DRA

Afin de gérer l'accès à privilège minimal pour les tâches Active Directory à l'aide de DRA, de nombreux composants et processus doivent être configurés. Il s'agit notamment de configurations de composants généraux et clients. Cette section fournit des informations concernant les composants et processus généraux nécessitant une configuration pour DRA.

Configuration du MMS

Un environnement MMS utilise plusieurs serveurs d'administration pour gérer le même ensemble de domaines et de serveurs membres. Un MMS comprend un serveur d'administration primaire et plusieurs serveurs d'administration secondaires.

Le mode par défaut pour le serveur d'administration est Primaire. Lorsque vous ajoutez des serveurs secondaires à votre environnement MMS, n'oubliez pas qu'un serveur d'administration secondaire ne peut appartenir qu'à un seul ensemble de serveurs.

Pour vous assurer que tous les serveurs de l'ensemble gèrent les mêmes données, synchronisez régulièrement les serveurs secondaires avec le serveur d'administration primaire. Pour simplifier la maintenance, utilisez le même compte de service pour tous les serveurs d'administration de la forêt du domaine.

IMPORTANT

- ♦ Lorsque vous installez le serveur secondaire, sélectionnez **Secondary Administration Server** (Serveur d'administration secondaire) dans le programme d'installation.
- ♦ La version DRA du nouveau serveur secondaire doit être identique à celle du serveur DRA primaire, de sorte que toutes les fonctionnalités qui sont disponibles sur le serveur primaire le soient également sur le serveur secondaire.

Ajout d'un serveur d'administration secondaire

Vous pouvez ajouter un serveur d'administration secondaire à un MMS existant dans le client de délégation et de configuration. Pour ajouter un serveur secondaire, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

REMARQUE : pour que l'ajout d'un serveur secondaire réussisse, vous devez d'abord installer le produit Directory and Resource Administrator sur l'ordinateur du serveur d'administration. Pour plus d'informations, reportez-vous à la section [Installation du serveur d'administration DRA](#).

Pour ajouter un serveur d'administration secondaire, cliquez avec le bouton droit sur **Administration Server** (Serveur d'administration) sur le noeud Configuration Management, puis sélectionnez **Add Secondary Server** (Ajouter un serveur secondaire).

Promotion d'un serveur d'administration secondaire

Vous pouvez promouvoir un serveur d'administration secondaire au rang de serveur d'administration primaire. Lorsque vous promouvez un serveur d'administration secondaire au rang de serveur d'administration primaire, le serveur d'administration primaire existant devient un serveur d'administration secondaire au sein de l'ensemble de serveurs. Pour promouvoir un serveur d'administration secondaire, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines. Avant de promouvoir un serveur d'administration secondaire, synchronisez le MMS de sorte qu'il présente la configuration la plus récente.

Pour plus d'informations sur la synchronisation du MMS, reportez-vous à la section [Planification de la synchronisation](#).

REMARQUE : un serveur primaire qui vient d'être promu peut se connecter uniquement aux serveurs secondaires qui étaient disponibles lors du processus de promotion. Si un serveur secondaire est devenu indisponible au cours du processus de promotion, contactez le support technique.

Pour promouvoir un serveur d'administration secondaire :

- 1 Accédez au noeud **Configuration Management > Administration Servers** (Serveurs d'administration).
- 2 Dans le volet de droite, sélectionnez le serveur d'administration secondaire à promouvoir.
- 3 Dans le menu Tâches, cliquez sur **Advanced** (Avancé) > **Promote Server** (Promouvoir un serveur).

IMPORTANT : lorsque le compte de service du serveur secondaire est différent de celui du serveur primaire ou lorsque le serveur secondaire est installé dans un domaine différent de celui du serveur primaire (domaines approuvés/non approuvés) et que vous promouvez le serveur secondaire, veillez à déléguer les rôles suivants avant de promouvoir le serveur secondaire : **Audit All Objects** (Auditer tous les objets), **Configure Servers and Domains** (Configurer les serveurs et les domaines) et **Generate UI Reports** (Générer les rapports de l'interface utilisateur). Vérifiez ensuite que les synchronisations MMS ont réussi.

Rétrogradation d'un serveur d'administration primaire

Vous pouvez rétrograder un serveur d'administration primaire au rang de serveur d'administration secondaire. Pour rétrograder un serveur d'administration primaire, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

Pour rétrograder un serveur d'administration primaire :

- 1 Accédez au noeud **Configuration Management > Serveurs d'administration**.
- 2 Dans le volet de droite, sélectionnez le serveur d'administration primaire à rétrograder.
- 3 Dans le menu Tâches, cliquez sur **Advanced** (Avancé) > **Demote Server** (Rétrograder un serveur).
- 4 Spécifiez l'ordinateur à désigner comme nouveau serveur d'administration primaire, puis cliquez sur **OK**.

Planification de la synchronisation

La synchronisation permet de garantir que tous les serveurs d'administration du MMS utilisent les mêmes données de configuration. Bien que vous puissiez synchroniser manuellement les serveurs à tout moment, la planification par défaut est définie pour synchroniser le MMS toutes les 4 heures. Vous pouvez modifier cette planification afin de l'adapter aux besoins de votre entreprise.

Pour modifier la planification de la synchronisation ou pour synchroniser manuellement les serveurs MMS, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

Pour accéder à la planification de la synchronisation ou pour effectuer des synchronisations manuelles, accédez à **Configuration Management > Serveurs d'administration** et utilisez le menu **Tâches** ou cliquez avec le bouton droit sur un serveur sélectionné. La planification de la synchronisation figure dans les propriétés du serveur sélectionné.

Présentation des options de synchronisation

La synchronisation des serveurs MMS peut s'effectuer essentiellement selon quatre options différentes :

- ◆ Sélectionnez le serveur primaire et synchronisez tous les serveurs secondaires avec l'option Synchronize All Servers (Synchroniser tous les serveurs).
- ◆ Sélectionnez un serveur secondaire et synchronisez uniquement ce serveur.
- ◆ Configurez la planification de la synchronisation pour les serveurs primaires et secondaires indépendamment.
- ◆ Configurez la planification de la synchronisation de tous les serveurs. Cette option est activée lorsque le paramètre suivant est sélectionné dans la planification de la synchronisation du serveur primaire :

Configure secondary Administration servers when refreshing the primary Administration server (Configurer les serveurs d'administration secondaires lors du rafraîchissement du serveur d'administration primaire)

REMARQUE : si vous désélectionnez cette option, les fichiers de configuration sont copiés sur les serveurs secondaires selon la planification primaire, mais ils ne sont pas chargés par le serveur secondaire à ce moment-là ; ils sont chargés en fonction de la planification configurée sur le serveur secondaire. Cela est utile si les serveurs se trouvent dans des fuseaux horaires différents. Par exemple, vous pouvez configurer tous les serveurs pour qu'ils rafraîchissent leur configuration en pleine nuit, même si cela implique des heures différentes en raison des fuseaux horaires.

Gestion des exceptions de clonage

Les exceptions de clonage permettent de définir des propriétés d'utilisateurs, de groupes, de contacts et d'ordinateurs qui ne sont pas copiées en cas de clonage de l'un de ces objets.

Vous pouvez gérer les exceptions de clonage pour autant que vous disposiez des pouvoirs appropriés. Le rôle Gérer les exceptions de clonage octroie des pouvoirs pour afficher, créer et supprimer des exceptions de clonage.

Pour afficher ou supprimer une exception de clonage existante ou pour en créer une, accédez à **Configuration Management > Clone Exceptions** (Exceptions de clonage) > **Tasks** (Tâches) ou cliquez avec le bouton droit.

Réplication des fichiers

Lorsque vous créez des outils personnalisés, il se peut qu'avant d'exécuter ces derniers, vous deviez installer, sur l'ordinateur client DRA, des fichiers d'accompagnement utilisés par ces outils. Vous pouvez utiliser les fonctions de réplication de fichiers DRA pour répliquer rapidement et facilement les fichiers d'accompagnement des outils personnalisés à partir du serveur d'administration primaire vers les serveurs d'administration secondaires dans le MMS ainsi que vers les ordinateurs client DRA. La réplication des fichiers vous permet également de répliquer les scripts de déclenchement du serveur primaire vers les serveurs secondaires.

Vous pouvez utiliser des outils personnalisés et la réplication des fichiers ensemble pour vous assurer que les ordinateurs client DRA peuvent bien accéder aux fichiers des outils personnalisés. DRA réplique les fichiers des outils personnalisés sur les serveurs d'administration secondaires pour que les ordinateurs client DRA se connectant aux serveurs d'administration secondaires puissent accéder à ces outils.

DRA réplique les fichiers des outils personnalisés présents sur le serveur d'administration primaire vers les serveurs d'administration secondaires au cours du processus de synchronisation MMS. DRA télécharge les fichiers des outils personnalisés sur les ordinateurs client DRA lorsque ces derniers se connectent aux serveurs d'administration.

REMARQUE : DRA télécharge les fichiers des outils personnalisés à l'emplacement suivant sur les ordinateurs client DRA :

`{répertoire_installation_DRA}\{ID_MMS}\Download`

La valeur MMSID correspond à l'identification du MMS à partir duquel DRA télécharge les fichiers des outils personnalisés.

Téléchargement des fichiers des outils personnalisés pour la réplication

Lorsque vous téléchargez des fichiers sur le serveur d'administration primaire, vous spécifiez les fichiers que vous souhaitez télécharger et répliquer entre le serveur d'administration primaire et tous les serveurs d'administration secondaires dans l'ensemble MMS. DRA permet de télécharger des fichiers de bibliothèque, des fichiers de script et des fichiers exécutables.

Le rôle Répliquer les fichiers permet de répliquer les fichiers à partir du serveur d'administration primaire vers les serveurs d'administration secondaires dans le MMS ainsi que vers les ordinateurs client DRA. Le rôle Répliquer les fichiers comporte les pouvoirs suivants :

- ♦ **Supprimer les fichiers du serveur** : ce pouvoir permet à DRA de supprimer les fichiers qui n'existent plus sur le serveur d'administration primaire, sur les serveurs d'administration secondaires et sur les ordinateurs client DRA.
- ♦ **Définir les informations de fichier** : ce pouvoir permet à DRA de mettre à jour les informations des fichiers sur les serveurs d'administration secondaires.
- ♦ **Télécharger les fichiers sur le serveur** : ce pouvoir permet à DRA de télécharger les fichiers de l'ordinateur client DRA vers le serveur d'administration primaire.

REMARQUE : vous ne pouvez télécharger qu'un seul fichier à la fois pour la réplication à l'aide de l'interface utilisateur Réplication des fichiers au niveau de la console de délégation et de configuration.

Pour télécharger un fichier d'outil personnalisé sur le serveur d'administration primaire :

- 1 Accédez à **Configuration Management > File Replication** (Réplication des fichiers).

- 2 Dans le menu Tâches, cliquez sur **Upload File** (Télécharger le fichier).
- 3 Pour rechercher et sélectionner le fichier à télécharger, cliquez sur **Browse** (Parcourir).
- 4 Si vous souhaitez télécharger le fichier sélectionné sur tous les ordinateurs client DRA, cochez la case **Download to all client computer** (Télécharger sur tous les ordinateurs client).
- 5 Si vous souhaitez enregistrer une bibliothèque COM, cochez la case **Register COM library** (Enregistrer une bibliothèque COM).
- 6 Cliquez sur **OK**.

REMARQUE

- ♦ DRA télécharge les fichiers de script ou d'accompagnement qui doivent être répliqués sur d'autres serveurs d'administration secondaires dans le répertoire `{répertoire_installation_DRA}\FileTransfer\Replicate` sur le serveur d'administration primaire. Le dossier `{répertoire_installation_DRA}\FileTransfer\Replicate` est également référencé sous la forme `{chemin_fichiers_répliqués_DRA}`.
 - ♦ DRA télécharge les fichiers de script ou d'accompagnement qui doivent être répliqués sur des ordinateurs client DRA dans le répertoire `{répertoire_installation_DRA}\FileTransfer\Download` sur le serveur d'administration primaire.
 - ♦ Le fichier d'outil personnalisé téléchargé sur le serveur d'administration primaire est distribué vers les serveurs d'administration secondaires lors de la synchronisation planifiée suivante ou lors de la synchronisation manuelle.
-

Réplication de plusieurs fichiers entre les serveurs d'administration

Si vous disposez de plusieurs fichiers à télécharger et à répliquer entre le serveur d'administration primaire et des serveurs d'administration secondaires dans votre MMS, vous pouvez télécharger manuellement ces fichiers pour la réplication en les copiant dans le répertoire de réplication du serveur d'administration primaire, qui se trouve à l'emplacement suivant :

```
{DRAInstallDir}\FileTransfer\Replicate
```

Le répertoire de réplication est créé lors de l'installation de DRA.

Le serveur d'administration identifie automatiquement les fichiers dans le répertoire de réplication et les réplique entre les serveurs d'administration au cours de la synchronisation planifiée suivante. Après la synchronisation, DRA affiche les fichiers téléchargés dans la fenêtre File Replication (Réplication des fichiers) de la console de délégation et de configuration.

REMARQUE : si vous souhaitez répliquer les fichiers qui contiennent les bibliothèques COM devant être enregistrées, vous ne pouvez pas copier manuellement les fichiers dans le répertoire de réplication du serveur d'administration. Vous devez utiliser la console de délégation et de configuration pour télécharger chaque fichier et enregistrer la bibliothèque COM.

Réplication de plusieurs fichiers sur les ordinateurs client DRA

Si vous avez plusieurs fichiers à répliquer entre le serveur d'administration primaire et les ordinateurs client DRA, vous pouvez copier ces fichiers dans le répertoire de réplication du client sur le serveur d'administration primaire, qui se trouve à l'emplacement suivant :

```
{DRAInstallDir}\FileTransfer\Download
```

Le répertoire de réplication du client est créé lors de l'installation de DRA.

Le serveur d'administration identifie automatiquement les fichiers dans le dossier `Download` et les réplique sur les serveurs d'administration secondaires au cours de la synchronisation planifiée suivante. Après la synchronisation, DRA affiche les fichiers téléchargés dans la fenêtre de réplication des fichiers de la console de délégation et de configuration. DRA télécharge les fichiers répliqués sur les ordinateurs client DRA la première fois que ceux-ci se connectent aux serveurs d'administration après la réplication.

REMARQUE : si vous souhaitez répliquer les fichiers qui contiennent les bibliothèques COM devant être enregistrées, vous ne pouvez pas copier les fichiers dans le répertoire de téléchargement du serveur d'administration. Vous devez utiliser la console de délégation et de configuration pour télécharger chaque fichier et enregistrer la bibliothèque COM.

Horodatage des événements

Lorsque l'audit AD Domain Services est activé, les événements DRA sont consignés comme ayant été générés par le compte de service DRA ou le compte d'accès au domaine s'il est configuré. L'horodatage des événements améliore encore cette fonction en générant un événement AD DS supplémentaire qui identifie l'assistant administrateur ayant effectué l'opération.

Pour que ces événements soient générés, vous devez configurer l'audit AD DS et activer l'horodatage des événements sur le serveur d'administration DRA. Lorsque l'horodatage des événements est activé, vous pouvez consulter les modifications apportées dans les rapports d'événements Change Guardian par les assistants administrateur.

- ♦ Pour configurer l'audit AD DS, reportez-vous au document [AD DS auditing \(https://technet.microsoft.com/en-us/library/cc731607\(v=ws.10\).aspx\)](https://technet.microsoft.com/en-us/library/cc731607(v=ws.10).aspx) (Audit AD DS).
- ♦ Pour configurer l'intégration de Change Guardian, reportez-vous à la section [Configuration des serveurs de l'historique des modifications unifiées \(UCH\)](#).
- ♦ Pour activer l'horodatage des événements, ouvrez la console de délégation et de configuration en tant qu'administrateur DRA et procédez comme suit :

1. Accédez à **Configuration Management > Update Administration Server Options** (Mettre à jour les options de serveur d'administration) > **Event Stamping** (Horodatage des événements).
2. Sélectionnez un type d'objet, puis cliquez sur **Update** (Mettre à jour).
3. Sélectionnez un attribut à utiliser pour l'horodatage des événements de ce type d'objet.

DRA prend actuellement en charge l'horodatage des événements pour les utilisateurs, les groupes, les contacts, les ordinateurs et les unités organisationnelles.

DRA requiert également que les attributs existent dans le schéma AD pour chacun de vos domaines gérés. C'est un point important à prendre en compte si vous ajoutez des domaines gérés après la configuration de l'horodatage des événements. Si vous devez ajouter un domaine géré qui ne contient pas un attribut sélectionné, les opérations à partir de ce domaine ne seront pas auditées avec les données d'horodatage des événements.

Étant donné que DRA va modifier ces attributs, vous devez sélectionner des attributs qui ne sont pas utilisés par DRA ni par une quelconque autre application dans votre environnement.

Pour plus d'informations sur l'horodatage des événements, reportez-vous à la section [Fonctionnement de l'horodatage des événements](#).

Activation de plusieurs gestionnaires pour les groupes

Lorsque vous activez la prise en charge de plusieurs gestionnaires pour gérer un groupe, un des deux attributs par défaut est utilisé pour enregistrer les gestionnaires du groupe. En cas d'exécution de Microsoft Exchange, l'attribut est `msExchCoManagedByLink`. Si le système n'exécute pas Microsoft Exchange, l'attribut par défaut est `nonSecurityMember`. Cette dernière option peut être modifiée. Toutefois, il est recommandé de contacter le support technique afin de déterminer un attribut approprié si vous avez besoin de modifier ce paramètre.

Pour activer la prise en charge de plusieurs gestionnaire pour les groupes :

- 1 Dans le panneau de gauche, cliquez sur **Configuration Management**.
- 2 Sous Common Tasks (Tâches courantes) dans le volet de droite, cliquez sur **Update Administration Server Options** (Mettre à jour les options de serveur d'administration).
- 3 Sous l'onglet Enable Support for Group Multiple Managers (Activer la prise en charge de plusieurs gestionnaires pour les groupes), cochez la case **Enable support for group's multiple managers** (Activer la prise en charge de plusieurs gestionnaires pour le groupe).

Communications chiffrées

Cette fonction vous permet d'activer ou de désactiver l'utilisation de communications chiffrées entre, d'une part, les clients de délégation et de configuration et ARM et, d'autre part, le serveur d'administration. Par défaut, DRA chiffre les mots de passe des comptes. Cette fonctionnalité ne chiffre pas les communications PowerShell ou des clients Web, lesquelles sont traitées séparément par des certificats de serveur.

L'utilisation de communications chiffrées peut affecter les performances. Par défaut, la communication chiffrée est désactivée. Si vous activez cette option, les données sont chiffrées pendant la communication entre les interfaces utilisateur et le serveur d'administration. DRA utilise le chiffrement standard Microsoft pour les appels de procédure distante (Remote Procedure Call, RPC).

Pour activer les communications chiffrées, accédez à **Configuration Management > Update Administration Server Options** (Mettre à jour les options de serveur d'administration) > onglet **General** (Général), puis cochez la case **Encrypted Communications** (Communications chiffrées).

REMARQUE : pour chiffrer toutes les communications entre les interfaces utilisateur et le serveur d'administration, vous devez disposer des pouvoirs appropriés, tels que ceux du rôle Configurer les serveurs et les domaines.

Définition d'attributs virtuels

L'utilisation d'attributs virtuels permet de créer des propriétés et de les associer à des utilisateurs, des groupes, des groupes de distribution dynamique, des contacts, des ordinateurs et des unités organisationnelles. Grâce aux attributs virtuels, vous pouvez créer des propriétés sans avoir à étendre le schéma Active Directory.

Les attributs virtuels vous permettent d'ajouter des propriétés aux objets dans Active Directory (AD). Vous pouvez créer, activer, désactiver, associer ou dissocier des attributs virtuels uniquement sur le serveur d'administration primaire. DRA stocke les attributs virtuels que vous créez dans AD LDS. DRA réplique les attributs virtuels présents sur le serveur d'administration primaire vers les serveurs d'administration secondaires au cours du processus de synchronisation MMS.

Vous pouvez gérer les attributs virtuels pour autant que vous disposiez des pouvoirs appropriés. Le rôle *Manage Virtual Attributes* (Gérer les attributs virtuels) octroie des pouvoirs pour créer, activer, associer, dissocier, désactiver et afficher des attributs virtuels.

Création d'attributs virtuels

Vous devez disposer du pouvoir *Create Virtual Attributes* (Créer des attributs virtuels) pour créer des attributs virtuels et du pouvoir *View Virtual Attributes* (Afficher les attributs virtuels) pour consulter ces derniers.

Pour créer un attribut virtuel, accédez au noeud **Configuration Management > Virtual Attributes** (Attributs virtuels) > **Managed Attributes** (Attributs gérés), puis cliquez sur **New Virtual Attribute** (Nouvel attribut virtuel) dans le menu Tasks (Tâches).

Association d'attributs virtuels à des objets

Vous pouvez associer uniquement des attributs virtuels activés à des objets Active Directory. Une fois l'attribut virtuel associé à un objet, cet attribut est disponible en tant que partie intégrante des propriétés de l'objet.

Pour exposer les attributs virtuels via les interfaces utilisateur DRA, vous devez créer une page de propriétés personnalisée.

Pour associer un attribut virtuel à un objet, accédez au noeud **Configuration Management > Virtual Attributes** (Attributs virtuels) > **Managed Attributes** (Attributs gérés), cliquez avec le bouton droit sur l'attribut virtuel à utiliser et sélectionnez **Associate** (Associer) > (type d'objet).

REMARQUE

- ♦ Vous ne pouvez associer les attributs virtuels qu'avec des utilisateurs, des groupes, des groupes de distribution dynamique, des ordinateurs, des contacts et des unités organisationnelles.
 - ♦ Lorsque vous associez un attribut virtuel à un objet, DRA crée automatiquement les deux pouvoirs personnalisés par défaut. Les assistants administrateur doivent disposer de ces pouvoirs personnalisés pour gérer l'attribut virtuel.
-

Dissociation des attributs virtuels

Vous pouvez dissocier des attributs virtuels des objets Active Directory. Tout nouvel objet que vous créez n'affiche pas l'attribut virtuel dissocié parmi les propriétés de l'objet.

Pour dissocier un attribut virtuel d'un objet Active Directory, accédez au noeud **Configuration Management > Virtual Attributes** (Attributs virtuels) > **Managed Classes** (Classes gérées) > (type d'objet). Cliquez avec le bouton droit sur l'attribut virtuel et sélectionnez **Disassociate** (Dissocier).

Désactivation des attributs virtuels

Vous pouvez désactiver des attributs virtuels s'ils ne sont associés à aucun objet Active Directory. Lorsque vous désactivez un attribut virtuel, les administrateurs ne peuvent pas l'afficher ni l'associer à un objet.

Pour désactiver un attribut virtuel, accédez à **Configuration Management > Attributs gérés**. Cliquez avec le bouton droit sur l'attribut souhaité dans le volet de la liste, puis sélectionnez **Disable** (Désactiver).

Configuration du caching

Le serveur d'administration crée et gère un **cache des comptes** qui contient des parties de l'annuaire Active Directory pour les domaines gérés. DRA utilise le cache des comptes pour améliorer les performances lors de la gestion des comptes utilisateur, des groupes, des contacts et des comptes d'ordinateur.

Pour planifier une heure de rafraîchissement du cache ou pour afficher l'état du cache, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

REMARQUE : pour effectuer des rafraîchissements incrémentiels du cache des comptes dans les domaines qui contiennent des sous-arborescences gérées, vérifiez que le compte de service bénéficie d'un accès en lecture au conteneur Objets supprimés, ainsi qu'à tous les objets dans le domaine de la sous-arborescence. Vous pouvez employer l'utilitaire des objets supprimés pour vérifier et déléguer les autorisations appropriées.

Rafraîchissements complets et incrémentiels

Un rafraîchissement incrémentiel du cache des comptes met à jour uniquement les données qui ont changé depuis le dernier rafraîchissement. Le rafraîchissement incrémentiel offre une méthode rationalisée pour suivre les changements au sein de votre annuaire Active Directory. Le rafraîchissement incrémentiel permet de mettre à jour rapidement le cache des comptes en perturbant le moins possible l'activité de l'entreprise.

IMPORTANT : Microsoft Server limite le nombre d'utilisateurs simultanés connectés à la session WinRM/WinRS à cinq et le nombre de shells par utilisateur à cinq également. Veillez donc à ce que le compte utilisateur en question soit limité à cinq shells pour les serveurs DRA secondaires.

Un rafraîchissement incrémentiel met à jour les données suivantes :

- ♦ Les objets nouveaux et clonés
- ♦ Les objets supprimés et déplacés
- ♦ Les adhésions aux groupes
- ♦ Toutes les propriétés d'objet mises en cache pour les objets modifiés

Un rafraîchissement complet du cache des comptes reconstruit le cache des comptes de DRA pour le domaine spécifié.

REMARQUE : pendant l'exécution d'un rafraîchissement complet du cache des comptes, le domaine n'est pas disponible pour les utilisateurs DRA.

Exécution d'un rafraîchissement complet du cache des comptes

Pour rafraîchir le cache des comptes, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré « Configurer les serveurs et les domaines ».

Pour effectuer un rafraîchissement complet immédiat du cache des comptes :

- 1 Accédez à **Configuration Management > Managed Domains** (Domaines gérés).
- 2 Cliquez avec le bouton droit sur le domaine souhaité, puis sélectionnez **Propriétés** (Propriétés).
- 3 Cliquez sur **Refresh Now** (Rafraîchir maintenant) sous l'onglet **Full refresh** (Rafraîchissement complet).

Fréquences planifiées par défaut

La fréquence à laquelle vous devez rafraîchir le cache des comptes dépend de la fréquence des changements au sein de votre entreprise. Le rafraîchissement incrémentiel permet de mettre à jour le cache des comptes souvent, pour vous assurer que DRA dispose des dernières informations concernant Active Directory.

Par défaut, le serveur d'administration effectue un rafraîchissement incrémentiel du cache des comptes selon les fréquences suivantes :

Type de domaine	Fréquence de rafraîchissement planifiée par défaut
Domaines gérés	Toutes les 5 minutes
Domaines approuvés	Toutes les heures

Vous ne pouvez pas planifier un rafraîchissement complet du cache des comptes (Full Accounts Cache Refresh, FACR). Toutefois, DRA exécute automatiquement un FACR dans les circonstances suivantes :

- ♦ après avoir configuré un domaine géré pour la première fois ;
- ♦ après avoir mis à niveau DRA vers une nouvelle version complète à partir d'une version précédente ;
- ♦ après avoir installé un Service Pack DRA.

L'exécution d'un rafraîchissement complet du cache des comptes peut nécessiter plusieurs minutes.

Considérations

Vous devez régulièrement rafraîchir le cache des comptes pour que DRA dispose bien des informations les plus récentes. Avant d'effectuer ou de planifier un rafraîchissement du cache des comptes, passez en revue les points suivants :

- ♦ Pour effectuer un rafraîchissement incrémentiel du cache des comptes, le compte d'accès ou de service du serveur d'administration doit être autorisé à accéder aux objets supprimés dans l'annuaire Active Directory du domaine approuvé ou géré.
- ♦ Lorsque DRA effectue un rafraîchissement du cache des comptes, le serveur d'administration n'inclut pas les groupes de sécurité locaux des domaines approuvés. Par conséquent, DRA ne vous permet pas d'ajouter un groupe de sécurité local du domaine approuvé à un groupe local sur le serveur membre géré.
- ♦ Si vous omettez un domaine approuvé dans le cadre d'un rafraîchissement du cache des comptes, le serveur d'administration ignore également ce domaine lors du rafraîchissement de la configuration des domaines.
- ♦ Si vous incluez un domaine approuvé précédemment ignoré dans le rafraîchissement du cache des comptes, effectuez un rafraîchissement complet du cache des comptes pour le domaine géré. Ainsi, le cache des comptes sur le serveur d'administration du domaine géré reflète correctement les données d'adhésion des groupes de vos domaines gérés et approuvés.
- ♦ Si vous définissez l'intervalle de rafraîchissement incrémentiel du cache des comptes sur **Jamais**, le serveur d'administration exécute uniquement des rafraîchissements complets du cache des comptes. Un rafraîchissement complet du cache des comptes peut prendre un certain temps au cours duquel vous ne pouvez pas gérer les objets de ce domaine.
- ♦ DRA ne peut pas déterminer automatiquement lorsque des modifications sont effectuées via d'autres outils, tels que Microsoft Directory Services. Les opérations réalisées en dehors de DRA peuvent nuire à la précision des informations mises en cache. Par exemple, si vous utilisez

un autre outil pour ajouter une boîte aux lettres à un compte utilisateur, vous ne pouvez pas utiliser Exchange pour gérer cette boîte aux lettres tant que vous n'avez pas mis à jour le cache des comptes.

- ♦ L'exécution d'un rafraîchissement complet du cache des comptes supprime les statistiques de dernière connexion tenues à jour dans le cache. Le serveur d'administration collecte alors les dernières informations de connexion auprès de tous les contrôleurs de domaine.

Activation de la collecte des imprimantes Active Directory

La collecte des imprimantes AD est désactivée par défaut. Pour l'activer, accédez à **Configuration Management > Update Administration Server Options** (Mettre à jour les options de serveur d'administration) > onglet **General** (Général), puis cochez la case **Collect Printers** (Collecter les imprimantes).

AD LDS

Vous pouvez configurer le rafraîchissement de nettoyage AD LDS afin qu'il s'exécute selon une planification pour des domaines spécifiques. Le paramètre par défaut est « Jamais ». Vous pouvez également afficher l'état de nettoyage et consulter des informations spécifiques relatives à la configuration AD LDS (ADAM).

Pour configurer la planification ou afficher l'état du nettoyage d'AD LDS, cliquez avec le bouton droit sur le domaine souhaité sur le noeud **Gestion des comptes et des ressources > Tous mes objets gérés**, puis sélectionnez respectivement **Properties** (Propriétés) > **Adlds Cleanup Refresh Schedule** (Planification du rafraîchissement de nettoyage d'AD LDS) ou **Adlds Cleanup status** (État du nettoyage d'AD LDS).

Pour afficher les informations de configuration d'AD LDS (ADAM), accédez à **Configuration Management > Update Server Options** (Mettre à jour les options de serveur) > **ADAM Configuration** (Configuration ADAM).

Groupe dynamique

Un groupe dynamique est un groupe dont l'adhésion change en fonction d'un ensemble défini de critères que vous configurez dans les propriétés du groupe. Dans les propriétés du domaine, vous pouvez configurer le rafraîchissement de groupe dynamique à exécuter selon une planification pour des domaines spécifiques. Le paramètre par défaut est « Jamais ». Vous pouvez également afficher l'état de rafraîchissement.

Pour configurer la planification ou afficher l'état de rafraîchissement de groupe dynamique, cliquez avec le bouton droit sur le domaine souhaité sur le noeud **Gestion des comptes et des ressources > Tous mes objets gérés**, puis sélectionnez respectivement **Properties** (Propriétés) > **Dynamic group refresh** (Rafraîchissement de groupe dynamique) ou **Dynamic group status** (État du groupe dynamique).

Pour plus d'informations sur les groupes dynamiques, reportez-vous à la section [Groupes dynamiques DRA](#).

Configuration de la corbeille

Vous pouvez activer ou désactiver la corbeille pour chaque domaine Microsoft Windows ou pour des objets au sein de chaque domaine, et configurer quand et comment vous voulez que le nettoyage de la corbeille se produise.

Pour plus d'informations sur l'utilisation de la corbeille, reportez-vous à la section [Corbeille](#).

Activation de la corbeille

Vous pouvez activer la corbeille pour des domaines spécifiques de Microsoft Windows et pour des objets au sein de ces domaines. Par défaut, DRA active la corbeille pour chaque domaine qu'il gère et pour tous les objets du domaine. Pour activer la corbeille, vous devez être un membre du groupe Administrateurs DRA ou Administrateurs de configuration DRA.

Si votre environnement comprend la configuration suivante, employez l'utilitaire de la corbeille pour activer cette fonction :

- ♦ DRA gère une sous-arborescence de ce domaine.
- ♦ Le compte d'accès ou de service du serveur d'administration n'est pas autorisé à créer le conteneur Corbeille, à déplacer des comptes vers ce conteneur ni à modifier les comptes qu'il contient.

Vous pouvez également employer l'utilitaire de la corbeille afin de vérifier les autorisations du compte d'accès ou de service du serveur d'administration sur le conteneur Corbeille.

Pour activer la corbeille, cliquez avec le bouton droit sur le domaine souhaité sur le noeud **Corbeille**, puis sélectionnez **Enable Recycle Bin** (Activer la corbeille).

Désactivation de la corbeille

Vous pouvez désactiver la corbeille pour des domaines spécifiques de Microsoft Windows et pour des objets au sein de ces domaines. Si une corbeille désactivée contient des comptes, vous ne pouvez pas afficher, supprimer définitivement ni restaurer ces comptes.

Pour désactiver la corbeille, vous devez être un membre du groupe Administrateurs DRA ou Administrateurs de configuration DRA.

Pour désactiver la corbeille, cliquez avec le bouton droit sur le domaine souhaité sur le noeud **Corbeille**, puis sélectionnez **Disable Recycle Bin** (Désactiver la corbeille).

Configuration des objets Corbeille et de leur nettoyage

Par défaut, la corbeille est nettoyée tous les jours. Vous pouvez modifier cette configuration afin de nettoyer la corbeille du domaine tous les x jours. Lors du nettoyage planifié, la corbeille supprime les objets qui ont une ancienneté supérieure au nombre de jours que vous avez configuré pour chaque type d'objet. Le paramètre par défaut pour chaque type consiste à supprimer les objets ayant plus d'un jour. Pour personnaliser le comportement de nettoyage de la corbeille, désactivez-le, réactivez-le, puis définissez l'ancienneté des objets à supprimer pour chaque type d'objet.

Pour configurer le nettoyage de la corbeille, sélectionnez le domaine souhaité au niveau de la console de délégation et de configuration, puis accédez à **Tâches > Propriétés > onglet Corbeille**.

Configuration de la création de rapports

Les sections suivantes fournissent des informations conceptuelles à propos des rapports de gestion DRA et des collecteurs de rapports que vous pouvez activer. Pour atteindre l'assistant dans lequel vous pouvez configurer les collecteurs, accédez à **Configuration Management > Update Reporting Service Configuration** (Mettre à jour la configuration du service de création de rapports).

Configuration du collecteur Active Directory

Le collecteur Active Directory recueille un ensemble défini d'attributs à partir d'Active Directory pour chaque utilisateur, groupe, contact, ordinateur, unité organisationnelle et groupe de distribution dynamique gérés dans DRA. Ces attributs sont stockés dans la base de données de création de rapports et sont utilisés pour générer des rapports au niveau de la console de création de rapports.

Vous pouvez configurer le collecteur Active Directory pour spécifier les attributs qui sont collectés et stockés dans la base de données de création de rapports. Vous pouvez également configurer le serveur d'administration DRA sur lequel le collecteur s'exécutera.

Configuration du collecteur DRA

Le collecteur DRA recueille des informations sur votre configuration DRA et enregistre ces informations dans la base de données de création de rapports, laquelle permet de générer des rapports au niveau de la console de création de rapports.

Pour activer le collecteur DRA, vous devez spécifier sur quel serveur d'administration DRA il s'exécutera. Il est recommandé de planifier le collecteur DRA pour qu'il s'exécute après une exécution réussie du collecteur Active Directory et pendant les heures auxquelles le serveur est moins chargé ou en dehors des heures de travail normales.

Configuration du collecteur de locataire Office 365

Le collecteur de locataire Office 365 recueille des informations sur les utilisateurs gérés qui sont synchronisés dans Office 365 et enregistre ces informations dans la base de données de création de rapports, laquelle permet de générer des rapports au niveau de la console de création de rapports.

Pour activer le collecteur Office 365, vous devez spécifier sur quel serveur d'administration DRA il s'exécutera.

REMARQUE : le locataire Office 365 ne peut réussir une collecte qu'une fois que le collecteur Active Directory du domaine correspondant a lui-même exécuté une collecte avec succès.

Configuration du collecteur de rapports de gestion

Le collecteur de rapports de gestion collecte des informations d'audit DRA et les enregistre dans la base de données de création de rapports, laquelle permet de générer des rapports au niveau de la console de création de rapports. Lorsque vous activez le collecteur, vous pouvez configurer la fréquence à laquelle les données sont mises à jour dans la base de données pour les requêtes exécutées dans l'outil DRA Reporting.

Cette configuration implique que le compte de service DRA dispose de l'autorisation **sysadmin** dans SQL Server sur le serveur de création de rapports. Les options configurables sont définies ci-après :

- ♦ **Audit Export Data Interval** (Intervalle d'exportation des données d'audit) : il s'agit de l'intervalle selon lequel les données d'audit du journal de trace de DRA (LAS) sont exportées vers la base de données « SMCubeDepot » dans SQL Server.
- ♦ **Management Report Summarization Interval** (Intervalle de résumé de rapport de gestion) : il s'agit de l'intervalle selon lequel les données d'audit de la base de données SMCubeDepot sont injectées dans la base de données DRA Reporting où elles peuvent être interrogées par l'outil DRA Reporting.

Collecte des statistiques de dernière connexion

Vous pouvez configurer DRA pour qu'il collecte les statistiques de dernière connexion auprès de tous les contrôleurs de domaine dans le domaine géré. Pour activer et planifier la collecte des statistiques de dernière connexion, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

Par défaut, la fonction de collecte des statistiques de dernière connexion est désactivée. Si vous souhaitez collecter les données des statistiques de dernière connexion, vous devez activer cette fonction. Une fois que vous avez activé la collecte des statistiques de dernière connexion, vous pouvez afficher ces informations pour un utilisateur particulier ou consulter l'état de collecte de ces dernières.

Pour recueillir les statistiques de dernière connexion :

- 1 Accédez à **Configuration Management > Domaines gérés**.
- 2 Cliquez avec le bouton droit sur le domaine souhaité, puis sélectionnez **Propriétés**.
- 3 Cliquez sur l'onglet **Last logon schedule** (Planification dernière connexion) pour configurer la collecte des statistiques de dernière connexion.

Historique des modifications unifiées

Par défaut, la fonction Historique des modifications unifiées (Unified Change History, UCH) permet de générer des rapports concernant les modifications apportées par DRA.

Délégation des pouvoirs d'historique des modifications unifiées

Pour gérer l'historique des modifications unifiées, assignez le rôle Administration du serveur d'historique des modifications unifiées ou les pouvoirs applicables ci-dessous aux assistants administrateur :

- ♦ Supprimer la configuration du serveur d'historique des modifications unifiées
- ♦ Définir les informations de configuration de l'historique des modifications unifiées
- ♦ Afficher les informations de configuration de l'historique des modifications unifiées

Pour déléguer des pouvoir UCH :

- 1 Cliquez sur **Pouvoirs** sur le noeud Gestion de la délégation, puis utilisez la fonction de recherche d'objets pour rechercher et sélectionner les objets UCH souhaités.
- 2 Cliquez avec le bouton droit sur l'un des pouvoirs UCH sélectionnés et choisissez **Delegate Roles and Powers** (Déléguer des rôles et des pouvoirs).
- 3 Recherchez l'utilisateur, le groupe ou le groupe AA spécifique auquel vous souhaitez déléguer des pouvoirs.
- 4 Utilisez le **sélecteur d'objet** pour rechercher et ajouter les objets souhaités, puis cliquez sur **Roles and Powers** (Rôles et pouvoirs) dans l'assistant.
- 5 Cliquez sur **Active Views** et utilisez le **sélecteur d'objet** pour rechercher et ajouter les objets souhaités.
- 6 Cliquez sur **Next** (Suivant), puis sur **Finish** (Terminer) pour finaliser le processus de délégation.

Configuration des serveurs de l'historique des modifications unifiées (UCH)

Pour configurer des serveurs UCH :

- 1 Lancez la console Web et connectez-vous avec des informations d'identification d'assistant administrateur.
- 2 Accédez à **Administration > Intégrations > Historique des modifications unifiées**, puis cliquez sur l'icône **Ajouter**.
- 3 Indiquez le nom du serveur UCH ou l'adresse IP, le numéro de port, le type de serveur et l'accès aux détails du compte dans la configuration Historique des modifications unifiée.
- 4 Testez la connexion serveur, puis cliquez sur **OK** pour enregistrer la configuration.
- 5 Ajoutez des serveurs supplémentaires selon vos besoins.

Serveur de workflow

Pour utiliser l'automatisation de workflow dans DRA, vous devez installer le moteur de workflow sur un serveur Windows, puis configurer le serveur d'automatisation de workflow via la console Web.

Pour configurer le serveur d'automatisation de workflow, connectez-vous à la console Web et accédez à **Administration > Intégrations > Automatisation de workflow**.

Pour plus d'informations sur l'installation du moteur de workflow, reportez-vous au [Workflow Automation Administrator Guide](#) (Guide de l'administrateur d'automatisation de workflow).

3.1.4 Configuration du client de délégation et de configuration

Le client de délégation et de configuration permet d'accéder aux tâches de configuration et de délégation, afin de répondre aux besoins de gestion d'entreprise allant de l'administration distribuée à l'application des stratégies. Via la console de délégation et de configuration, vous pouvez définir les configurations de serveur et de modèle de sécurité dont vous avez besoin pour gérer efficacement votre entreprise.

Pour configurer le client de délégation et de configuration :

- 1 Lancez le client de délégation et de configuration et accédez à **Configuration Management > Mettre à jour les options de serveur d'administration**.
- 2 Cliquez sur l'onglet **Client Options** (Options du client) et définissez vos paramètres préférés parmi les options de configuration affichées :
 - ♦ Autoriser les utilisateurs à effectuer des recherches par Active View
 - ♦ Masquer les objets source uniquement dans les listes de la console
 - ♦ Afficher les objets Active Directory avancés
 - ♦ Afficher la commande de sécurité
 - ♦ Afficher la ressource et les boîtes aux lettres partagées lors de la recherche d'utilisateurs
 - ♦ Suffixe UPN d'utilisateur par défaut pour le domaine en cours
 - ♦ Nombre maximal d'éléments pouvant être modifiés simultanément (sélection multiple)
 - ♦ Options de recherche
 - ♦ Option de retour chariot
 - ♦ Unités des limites de capacité de stockage de la boîte aux lettres Exchange

3.1.5 Configuration du client Web

Vous pouvez configurer la console Web pour permettre l'authentification à l'aide de cartes à puce ou l'authentification multicritère, et personnaliser la marque avec votre propre logo et votre propre titre d'application.

Démarrage de la console Web

Vous pouvez lancer la console Web depuis n'importe quel ordinateur, périphérique iOS ou périphérique Android équipé d'un navigateur Web. Pour démarrer la console, entrez l'URL appropriée dans le champ d'adresse du navigateur Web. Par exemple, si vous avez installé le composant Web sur l'ordinateur HOUserver, tapez `https://HOUserver/draclient` dans le champ d'adresse de votre navigateur Web.

REMARQUE : pour afficher les informations de compte et Microsoft Exchange les plus à jour au niveau de la console Web, définissez votre navigateur Web pour qu'il recherche les versions les plus récentes des pages mises en cache à chaque visite.

Déconnexion automatique

Vous pouvez définir un délai d'inactivité à l'issue duquel la console Web se déconnecte automatiquement, ou indiquer qu'elle ne se déconnecte jamais automatiquement.

Pour configurer la déconnexion automatique au niveau de la console Web, accédez à **Administration > Configuration > Déconnexion automatique**.

Connexion au serveur DRA

Vous pouvez configurer une des trois options au niveau de la console Web pour définir les options de connexion au serveur DRA. Une fois la configuration de la connexion définie, elle est la même pour les administrateurs et les assistants administrateur dans le panneau de liste déroulante **Options** lors de la connexion à la console Web.

- ♦ Toujours utiliser l'emplacement par défaut du serveur DRA (**Toujours**)
- ♦ Ne jamais utiliser l'emplacement par défaut du serveur DRA (**Jamais**)
- ♦ Utiliser l'emplacement par défaut du serveur DRA uniquement s'il est sélectionné (**Uniquement si sélectionné**)

Le comportement pour chaque option lors de la connexion est décrit ci-dessous :

Configuration de la connexion	Écran de connexion - Options	Description des options de connexion
Toujours	Aucune	Les configurations d'option sont désactivées.
Jamais	Utiliser la découverte automatique	Recherche un serveur DRA automatiquement ; aucune option de configuration n'est disponible.
	Connecter à un serveur DRA spécifique	L'utilisateur configure le serveur et le port.
	Connecter à un serveur DRA qui gère un domaine spécifique	L'utilisateur spécifie un domaine géré et choisit une option de connexion : <ul style="list-style-type: none">♦ Utiliser la découverte automatique (dans le domaine spécifié)♦ Serveur primaire pour ce domaine♦ Rechercher un serveur DRA (dans le domaine spécifié)
Uniquement si sélectionné	Utiliser la découverte automatique	Recherche un serveur DRA automatiquement ; aucune option de configuration n'est disponible.
	Connecter au serveur DRA par défaut	Le serveur par défaut est sélectionné et la configuration du serveur DRA est désactivée.
	Connecter à un serveur DRA spécifique	L'utilisateur configure le serveur et le port.

Configuration de la connexion	Écran de connexion - Options	Description des options de connexion
	Connecter à un serveur DRA qui gère un domaine spécifique	<p>L'utilisateur spécifie un domaine géré et choisit une option de connexion :</p> <ul style="list-style-type: none"> ◆ Utiliser la découverte automatique (dans le domaine spécifié) ◆ Serveur primaire pour ce domaine ◆ Rechercher un serveur DRA (dans le domaine spécifié)

Pour configurer la connexion au serveur DRA au niveau de la console Web, accédez à [Administration](#) > [Configuration](#) > [Connexion au serveur DRA](#).

Connexion au serveur REST

Pour configurer la connexion au service REST, vous devez définir un emplacement de serveur par défaut et un timeout de connexion (en secondes). Vous pouvez configurer une des trois options au niveau de la console Web pour définir les options de connexion au service REST lors de la connexion. Une fois la configuration de la connexion définie, elle est la même pour les administrateurs et les assistants administrateur dans le panneau de liste déroulante **Options** lors de la connexion à la console Web.

- ◆ Toujours utiliser l'emplacement par défaut du service REST (**Toujours**)
- ◆ Ne jamais utiliser l'emplacement par défaut du service REST (**Jamais**)
- ◆ Utiliser l'emplacement par défaut du service REST uniquement s'il est sélectionné (**Uniquement si sélectionné**)

Le comportement pour chaque option lors de la connexion est décrit ci-dessous :

Configuration de la connexion	Écran de connexion - Options	Description des options de connexion
Toujours	Aucune	Les configurations d'option sont désactivées.
Jamais	Utiliser la découverte automatique	Recherche un serveur REST automatiquement ; aucune option de configuration n'est disponible.
	Connecter à un serveur REST spécifique	L'utilisateur configure le serveur et le port.
	Connecter à un serveur REST dans un domaine spécifique	<p>L'utilisateur spécifie un domaine géré et choisit une option de connexion :</p> <ul style="list-style-type: none"> ◆ Utiliser la découverte automatique (dans le domaine spécifié) ◆ Rechercher un serveur REST (dans le domaine spécifié)
Uniquement si sélectionné	Utiliser la découverte automatique	Recherche un serveur REST automatiquement ; aucune option de configuration n'est disponible.
	Connecter au serveur REST par défaut	Le serveur REST par défaut est sélectionné et la configuration du serveur REST est désactivée.

Configuration de la connexion	Écran de connexion - Options	Description des options de connexion
	Connecter à un serveur REST spécifique	L'utilisateur configure le serveur et le port.
	Connecter à un serveur REST dans un domaine spécifique	L'utilisateur spécifie un domaine géré et choisit une option de connexion : <ul style="list-style-type: none"> ◆ Utiliser la découverte automatique (dans le domaine spécifié) ◆ Rechercher un serveur REST (dans le domaine spécifié)

Pour configurer la connexion au service REST au niveau de la console Web, accédez à **Administration > Configuration > Connexion au service REST**.

Authentification

Cette section contient des informations pour la configuration de l'authentification par carte à puce, de l'authentification Windows et de l'authentification multicritère grâce à l'intégration d'Advanced Authentication.

Authentification par carte à puce

Si vous souhaitez configurer la console Web afin qu'elle accepte un utilisateur sur la base des informations d'identification client présentes sur sa carte à puce, vous devez configurer IIS (Internet Information Services) et le fichier de configuration des services REST.

IMPORTANT : vérifiez que les certificats sur la carte à puce sont également installés dans la banque de certificats racine sur le serveur Web, car IIS doit pouvoir trouver les certificats correspondant à ceux sur la carte.

- 1 Installez les composants de l'authentification sur le serveur Web.
 - 1a Démarrez le gestionnaire de serveur.
 - 1b Cliquez sur **Serveur Web (IIS)**.
 - 1c Accédez à la section Services de rôle et cliquez sur **Ajouter des services de rôle**.
 - 1d Accédez au noeud des services de rôle de sécurité et sélectionnez **Authentification Windows** et **Authentification par mappage de certificat client**.
- 2 Activez l'authentification sur le serveur Web.
 - 2a Démarrez le **gestionnaire IIS**.
 - 2b Sélectionnez votre serveur Web.
 - 2c Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.
 - 2d Activez les options Authentification du certificat client Active Directory et Authentification Windows.
- 3 Configurez le client DRA.
 - 3a Sélectionnez votre client DRA.
 - 3b Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.
 - 3c Activez l'option Authentification Windows et désactivez l'option Authentification anonyme.

- 4 Activez les certificats SSL et client sur le client DRA.
 - 4a Recherchez l'icône **Services SSL** sous la section IIS et double-cliquez dessus.
 - 4b Sélectionnez **Exiger SSL** et sélectionnez **Exiger** sous les certificats client.

SUGGESTION : si l'option est disponible, sélectionnez **Exiger SSL 128 bits**.

- 5 Configurez l'application Web de services REST.
 - 5a Sélectionnez votre application Web de services REST.
 - 5b Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.
 - 5c Activez l'option Authentification Windows et désactivez l'option Authentification anonyme.
- 6 Activez les certificats SSL et client dans l'application Web de services REST.
 - 6a Recherchez l'icône **Services SSL** sous la section IIS et double-cliquez dessus.
 - 6b Sélectionnez **Exiger SSL** et sélectionnez **Exiger** sous les certificats client.

SUGGESTION : si l'option est disponible, sélectionnez **Exiger SSL 128 bits**.

- 7 Configurez le fichier de service Web WCF.
 - 7a Sélectionnez votre application Web de services REST et basculez vers l'affichage du contenu.
 - 7b Localisez le fichier `.svc` et cliquez dessus avec le bouton droit.
 - 7c Sélectionnez **Basculer vers l'affichage des fonctions**.
 - 7d Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.
 - 7e Activez l'option Authentification anonyme et désactivez toutes les autres méthodes d'authentification.
- 8 Modifiez le fichier de configuration des services REST.
 - 8a Utilisez un éditeur de texte pour ouvrir le fichier
`C:\inetpub\wwwroot\DRAClient\rest\web.config`.
 - 8b Localisez la ligne `<authentication mode="None" />` et supprimez-la.
 - 8c Ajoutez les lignes suivantes sous la ligne `<system.serviceModel>` :

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy"> <endpoint address=""
binding="webHttpBinding" bindingConfiguration="webHttpEndpointBinding"
name="webHttpEndpoint" contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </
services>
```
 - 8d Ajoutez les lignes suivantes sous la ligne `<serviceDebug
includeExceptionDetailInFaults="false"/>` :

```
<serviceAuthorization impersonateCallerForAllOperations="true" /> <serviceCredentials>
<clientCertificate> <authentication mapClientCertificateToWindowsAccount="true" /> </
clientCertificate> </serviceCredentials>
```
 - 8e Ajoutez les lignes suivantes **au-dessus** de la ligne `<serviceHostingEnvironment
multipleSiteBindingsEnabled="true" />` :

```
<bindings> <webHttpBinding> <binding name="webHttpEndpointBinding"> <security
mode="Transport"> <transport clientCredentialType="Certificate" /> </security> </binding> </
webHttpBinding> </bindings>
```
- 9 Enregistrez le fichier et redémarrez le serveur IIS.

Authentification Windows

Pour activer l'authentification Windows sur la console Web, vous devez configurer IIS et le fichier de configuration des services REST.

- 1 Ouvrez le gestionnaire IIS.
- 2 Dans le volet Connexions, recherchez l'application Web des services REST et sélectionnez-la.
- 3 Dans le volet de droite, accédez à la section IIS et double-cliquez sur **Authentification**.
- 4 Activez l'option **Authentification Windows** et désactivez toutes les autres méthodes d'authentification.
- 5 Utilisez un éditeur de texte pour ouvrir le fichier
`C:\inetpub\wwwroot\DRAClient\rest\web.config` et localiser la ligne `<authentication mode="None" />`.
- 6 Remplacez "None" par "Windows" et enregistrez le fichier.
- 7 Redémarrez le serveur IIS.

Authentification multicritère avec Advanced Authentication

Advanced Authentication Framework (AAF) est notre premier paquetage qui vous permet d'aller au-delà d'une simple combinaison nom d'utilisateur-mot de passe pour protéger plus efficacement vos informations sensibles grâce à une authentification multicritère.

Pour assurer la sécurité, Advanced Authentication prend en charge les protocoles de communication suivants :

- ♦ TLS 1.2 (valeur par défaut), TLS 1.1, TLS 1.0
- ♦ SSL 3.0

L'authentification multicritère est une méthode de contrôle d'accès à un ordinateur qui exige plusieurs modes d'authentification impliquant des catégories distinctes d'informations d'identification pour vérifier l'identité d'un utilisateur.

Il existe trois types de catégories d'authentification (ou « critères ») :

- ♦ *Connaissance* : cette catégorie exige que vous connaissiez une information spécifique, par exemple un mot de passe ou un code d'activation.
- ♦ *Possession* : cette catégorie exige que vous disposiez d'un périphérique d'authentification tel qu'une carte à puce ou un smartphone.
- ♦ *Caractéristique corporelle* : cette catégorie exige d'utiliser une partie de votre anatomie, telle que vos empreintes digitales, comme méthode de vérification.

Chaque critère d'authentification comporte au moins une méthode d'authentification. Une méthode d'authentification est une technique spécifique que vous pouvez utiliser pour établir l'identité d'un utilisateur, par exemple en employant une empreinte digitale ou un mot de passe.

Vous pouvez considérer qu'un processus d'authentification est fort s'il utilise plusieurs types de méthode d'authentification, par exemple s'il combine un mot de passe et une empreinte digitale.

Advanced Authentication prend en charge les méthodes d'authentification suivantes :

- ♦ Mot de passe LDAP
- ♦ RADIUS (Remote Authentication Dial-In User Service)
- ♦ Smartphone

SUGGESTION : la méthode Smartphone requiert que l'utilisateur télécharge une application iOS ou Android. Pour plus d'informations, reportez-vous au *Advanced Authentication - Smartphone Applications User Guide* (Advanced Authentication - Guide de l'utilisateur d'applications pour smartphone), qui est disponible sur le [site Web de documentation de NetIQ](#).

Utilisez les informations des sections suivantes afin de configurer la console Web pour utiliser l'authentification multicritère.

IMPORTANT : bien que certaines des étapes des sections suivantes interviennent au niveau de la console Web, la majeure partie du processus de configuration de l'authentification multicritère requiert un accès à AAF. Ces procédures supposent que vous avez déjà installé AAF et avez accès à la documentation de l'Aide d'AAF.

Ajout d'espaces de stockage à Advanced Authentication Framework

La première étape de la configuration de la console Web pour pouvoir utiliser l'authentification multicritère consiste à ajouter à AAF tous les domaines Active Directory qui contiennent les administrateurs DRA et les assistants administrateur gérés par DRA. Ces domaines sont appelés des espaces de stockage ; ils contiennent les attributs d'identité des utilisateurs et des groupes à authentifier.

- 1 Connectez-vous au portail d'administration d'AAF avec un nom d'utilisateur et un mot de passe de niveau administrateur.
- 2 Accédez au panneau de gauche, puis cliquez sur **Espaces de stockage**.
- 3 Cliquez sur **Ajouter**.
- 4 Complétez le formulaire.

SUGGESTION : le **type LDAP** est **AD**.

SUGGESTION : entrez un nom d'utilisateur et un mot de passe de niveau administrateur dans les champs correspondants.

- 5 Cliquez sur **Ajouter un serveur** .
- 6 Saisissez l'adresse IP du serveur LDAP dans le champ **Adresse**.
- 7 Cliquez sur **Enregistrer**.
- 8 Répétez les étapes 3 à 7 pour tous les autres espaces de stockage AD gérés par DRA.
- 9 Pour chaque espace de stockage répertorié sur la page Espaces de stockage, cliquez sur **Synchroniser maintenant** afin de le synchroniser avec le serveur AAF.

Création de chaînes d'authentification

Une chaîne d'authentification comporte au moins une méthode d'authentification. Les méthodes dans la chaîne seront appelées dans l'ordre selon lequel elles ont été ajoutées à la chaîne. Pour qu'un utilisateur soit authentifié, il doit réussir toutes les méthodes de la chaîne. Par exemple, vous pouvez créer une chaîne qui contient la méthode Mot de passe LDAP et la méthode SMS. Lorsqu'un utilisateur tente de s'authentifier à l'aide de cette chaîne, il doit d'abord s'authentifier avec son mot de passe LDAP, puis il reçoit, sur son téléphone portable, un SMS contenant un mot de passe à usage unique. Une fois le mot de passe saisi, cela signifie que l'utilisateur a accompli toutes les méthodes de la chaîne. L'authentification réussit. Une chaîne d'authentification peut être assignée à un utilisateur ou à un groupe spécifique.

Pour créer une chaîne d'authentification :

- 1 Connectez-vous au portail d'administration d'AAF avec un nom d'utilisateur et un mot de passe de niveau administrateur.
- 2 Accédez au panneau de gauche, puis cliquez sur **Chaînes**. Le panneau de droite affiche la liste des chaînes actuellement disponibles.
- 3 Cliquez sur **Ajouter**.
- 4 Complétez le formulaire. Tous les champs sont obligatoires.

IMPORTANT : ajoutez les méthodes dans l'ordre selon lequel elles doivent être appelées, autrement dit, si vous souhaitez que l'utilisateur commence par entrer un mot de passe LDAP, ajoutez d'abord le mot de passe LDAP à la chaîne.

IMPORTANT : assurez-vous que le paramètre **Appliquer si utilisé par le propriétaire du noeud d'extrémité** est défini sur **DÉSACTIVÉ**.

- 5 Définissez le paramètre **Est activé** sur **ACTIVÉ**.
- 6 Entrez le nom des rôles ou des groupes qui doivent être soumis à la demande d'authentification dans le champ **Rôles et groupes**.

SUGGESTION : si vous souhaitez que la chaîne s'applique à tous les utilisateurs, tapez **tous les utilisateurs** dans le champ **Rôles et groupes** et sélectionnez **Tous les utilisateurs** dans la liste déroulante résultante.

Tout utilisateur ou groupe que vous sélectionnez sera ajouté sous le champ **Rôles et groupes**.

- 7 Cliquez sur **Enregistrer**.

Création d'événements d'authentification

Un événement d'authentification est déclenché par l'application (dans ce cas, la console Web) qui souhaite authentifier un utilisateur. Au moins une chaîne d'authentification doit être assignée à l'événement afin que lorsque celui-ci est déclenché, les méthodes dans la chaîne qui lui est associée soient appelées pour authentifier l'utilisateur.

Un noeud d'extrémité correspond au périphérique réel, par exemple un ordinateur ou un smartphone, qui exécute le logiciel déclenchant l'événement d'authentification. DRA enregistre le noeud d'extrémité auprès d'AAF une fois l'événement créé.

Vous pouvez utiliser la zone Liste blanche des noeuds d'extrémité pour limiter l'accès à un événement à des noeuds d'extrémité spécifiques, ou vous pouvez autoriser tous les noeuds d'extrémité à accéder à l'événement.

Pour créer un événement d'authentification :

- 1 Connectez-vous au portail d'administration d'AAF avec un nom d'utilisateur et un mot de passe de niveau administrateur.
- 2 Accédez au panneau de gauche, puis cliquez sur **Événements**. Le panneau de droite affiche la liste des événements actuellement disponibles.
- 3 Cliquez sur **Ajouter**.
- 4 Complétez le formulaire. Tous les champs sont obligatoires.

IMPORTANT : assurez-vous que le paramètre **Est activé** est défini sur **ACTIVÉ**.

- 5 Si vous souhaitez limiter l'accès à des noeuds d'extrémité spécifiques, accédez à la section Liste blanche des noeuds d'extrémité et déplacez les noeuds d'extrémité ciblés de la liste *Disponible* vers la liste *Utilisé*.

SUGGESTION : Si la liste *Utilisé* ne contient aucun noeud d'extrémité, l'événement sera disponible pour tous les noeuds d'extrémité.

Activation de la console Web

Une fois que vous avez configuré des chaînes et des événements, vous pouvez vous connecter à la console Web en tant qu'administrateur et activer Advanced Authentication.

Une fois l'authentification activée, tous les utilisateurs devront s'authentifier via AAF avant de se voir accorder l'accès à la console Web.

IMPORTANT : avant d'activer la console Web, vous devez déjà être inscrit dans les méthodes d'authentification que la console Web utilisera pour authentifier les utilisateurs. Reportez-vous au *Advanced Authentication Framework User Guide* (Guide de l'utilisateur d'Advanced Authentication Framework) pour savoir comment vous inscrire dans des méthodes d'authentification.

Pour activer Advanced Authentication, connectez-vous à la console Web et accédez à **Administration > Configuration > Advanced Authentication**. Cochez la case **Activé** et configurez le formulaire conformément aux instructions fournies pour chaque champ.

SUGGESTION : une fois la configuration enregistrée, le noeud d'extrémité est créé dans AAF. Pour l'afficher ou le modifier, connectez-vous au portail d'administration d'AAF avec un nom d'utilisateur et un mot de passe de niveau administrateur, puis cliquez sur **Noeuds d'extrémité** dans le volet gauche.

Étapes finales

- 1 Connectez-vous au portail d'administration d'AAF avec un nom d'utilisateur et un mot de passe de niveau administrateur, puis cliquez sur **Événements** dans le volet gauche.
- 2 Modifiez chacun des événements de la console Web :
 - 2a Ouvrez l'événement pour modification.
 - 2b Accédez à la section Liste blanche des noeuds d'extrémité et déplacez le noeud d'extrémité que vous avez créé lors de la configuration de la console Web de la liste **Disponible** vers la liste **Utilisé**. Vous avez ainsi la garantie que seule la console Web peut utiliser ces événements.
- 3 Cliquez sur **Enregistrer**.

3.2 Connexion aux systèmes gérés

Cette section fournit des informations concernant la connexion et la configuration des systèmes gérés reliés aux domaines et aux composants Microsoft Exchange qui incluent le dossier public, Exchange, Office 365 et Skype Entreprise Online.

3.2.1 Gestion des domaines Active Directory

Vous pouvez ajouter de nouveaux ordinateurs et domaines gérés via le client de délégation et de configuration, après avoir installé le serveur d'administration. Vous pouvez également ajouter des domaines approuvés et des sous-arborescences, et leur configurer des comptes d'accès Exchange et de domaine. Pour ajouter des ordinateurs et des domaines gérés, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

REMARQUE : après avoir ajouté les domaines gérés, vérifiez que les planifications de rafraîchissement du cache des comptes pour ces domaines sont correctes.

Pour ajouter des ordinateurs et des domaines gérés :

- 1 Accédez à **Configuration Management > New Managed Domain** (Nouveau domaine géré).
- 2 Spécifiez le nom du domaine ou de l'ordinateur que vous voulez gérer, puis cliquez sur **Next** (Suivant).
- 3 Sous l'onglet **Access account** (Compte d'accès), spécifiez les informations d'identification de compte que DRA doit utiliser pour accéder à ce domaine ou cet ordinateur. Par défaut, DRA utilise le compte de service du serveur d'administration.
- 4 Passez en revue le résumé, puis cliquez sur **Terminer**.
- 5 Pour commencer à gérer les objets de ce domaine ou de cet ordinateur, rafraîchissez la configuration de domaine.

Spécification de comptes d'accès de domaine

Pour chaque sous-arborescence ou domaine géré, vous pouvez spécifier un compte à utiliser au lieu du compte de service du serveur d'administration pour accéder à ce domaine. Ce compte de remplacement est appelé un compte d'accès. Pour configurer un compte d'accès, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

Afin de spécifier un compte d'accès pour un serveur membre, vous devez être autorisé à gérer le domaine dans lequel le membre de domaine existe. Vous ne pouvez gérer des membres de domaine que s'ils existent dans un domaine géré auquel vous avez accès via le serveur d'administration.

Pour spécifier un compte d'accès :

- 1 Accédez au noeud **Configuration Management > Domaines gérés**.
- 2 Cliquez avec le bouton droit sur le domaine ou la sous-arborescence pour lequel/laquelle vous souhaitez spécifier un compte d'accès, puis cliquez sur **Propriétés**.
- 3 Sous l'onglet **Domain access** (Accès au domaine), cliquez sur **Use the following account to access this domain** (Utiliser le compte suivant pour accéder à ce domaine).
- 4 Spécifiez les informations d'identification de ce compte et confirmez-les, puis cliquez sur **OK**.

Pour plus d'informations sur la configuration de ce compte à privilège minimal, reportez-vous à la section [Comptes d'accès DRA à privilège minimal](#).

Spécification de comptes d'accès Exchange

Pour chaque domaine de DRA, vous pouvez gérer les objets Exchange à l'aide du compte d'accès de domaine DRA ou d'un compte d'accès Exchange distinct. Pour configurer un compte d'accès Exchange, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

IMPORTANT : Microsoft Server limite le nombre d'utilisateurs simultanés connectés à la session WinRM/WinRS à cinq et le nombre de shells par utilisateur à cinq également. Veillez donc à ce que le compte utilisateur en question soit limité à cinq shells pour les serveurs DRA secondaires.

Pour spécifier un compte d'accès Exchange :

- 1 Accédez au noeud **Configuration Management > Domaines gérés**.
- 2 Cliquez avec le bouton droit sur le domaine ou la sous-arborescence pour lequel/laquelle vous souhaitez spécifier un compte d'accès, puis cliquez sur **Propriétés**.
- 3 Sous l'onglet Exchange access (Accès Exchange), cliquez sur **Use the following account to access all Exchange servers** (Utiliser le compte suivant pour accéder à tous les serveurs Exchange).
- 4 Spécifiez les informations d'identification de ce compte et confirmez-les, puis cliquez sur **OK**.

Pour plus d'informations sur la configuration de ce compte à privilège minimal, reportez-vous à la section [Comptes d'accès DRA à privilège minimal](#).

Ajout d'une sous-arborescence gérée

Vous pouvez ajouter des sous-arborescences gérées et manquantes à partir de domaines Microsoft Windows spécifiques après l'installation du serveur d'administration. Pour ajouter une sous-arborescence gérée, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

Pour plus d'informations sur les versions de Microsoft Windows prises en charge, reportez-vous à la section [Configuration requise pour le serveur d'administration DRA](#).

En gérant une sous-arborescence d'un domaine Windows, vous pouvez utiliser DRA pour sécuriser un service ou une division au sein d'un domaine d'entreprise plus vaste.

Par exemple, vous pouvez spécifier la sous-arborescence Houston dans le domaine `SOUTHWEST`, ce qui permet à DRA de gérer en toute sécurité uniquement les objets contenus dans l'unité organisationnelle Houston et ses unités organisationnelles enfants. Cette flexibilité vous permet de gérer une ou plusieurs sous-arborescences sans nécessiter d'autorisations d'administration pour l'intégralité du domaine.

REMARQUE

- ♦ Pour vous assurer que le compte spécifié dispose des autorisations nécessaires pour gérer cette sous-arborescence et effectuer des rafraîchissements incrémentiels du cache des comptes, employez l'utilitaire des objets supprimés afin de vérifier et de déléguer les autorisations appropriées.
 - ♦ après avoir ajouté les sous-arborescences gérées, assurez-vous que les planifications de rafraîchissement du cache des comptes pour les domaines correspondants sont correctes.
-

Pour ajouter une sous-arborescence gérée :

- 1 Accédez à **Configuration Management > Nouveau domaine géré**.
- 2 Sous l'onglet Domain or server (Domaine ou serveur), cliquez sur **Manage a domain** (Gérer un domaine) et spécifiez le domaine de la sous-arborescence à gérer.
- 3 Spécifiez le domaine de la sous-arborescence à gérer.
- 4 Sélectionnez **Manage a subtree of this domain** (Gérer une sous-arborescence de ce domaine), puis cliquez sur **Next** (Suivant).
- 5 Sous l'onglet Subtrees (Sous-arborescences), cliquez sur **Add** (Ajouter) pour spécifier la sous-arborescence à gérer. Vous pouvez spécifier plusieurs sous-arborescences.
- 6 Sous l'onglet Compte d'accès, spécifiez les informations d'identification de compte que DRA doit utiliser pour accéder à cette sous-arborescence. Par défaut, DRA utilise le compte de service du serveur d'administration.
- 7 Passez en revue le résumé, puis cliquez sur **Finish** (Terminer).
- 8 Pour commencer à gérer les objets de cette sous-arborescence, rafraîchissez la configuration de domaine.

Ajout d'un domaine approuvé

Les domaines approuvés activent l'authentification utilisateur sur les systèmes gérés dans l'ensemble de votre environnement géré. Une fois que vous avez ajouté un domaine approuvé, vous pouvez spécifier des comptes d'accès de domaine et Exchange, planifier des rafraîchissements du cache et effectuer d'autres actions dans les propriétés du domaine, comme pour un domaine géré.

Pour ajouter un domaine approuvé :

- 1 Sur le noeud **Configuration Management > Domaines gérés**, sélectionnez le domaine géré auquel un domaine approuvé est associé.
- 2 Cliquez sur **Trusted domains** (Domaines approuvés) dans le volet Details (Détails). Le volet Details (Détails) doit être activé dans le menu View (Afficher).
- 3 Cliquez avec le bouton droit sur le domaine approuvé, puis sélectionnez **Properties** (Propriétés).
- 4 Décochez la case **Ignore this trusted domain** (Ignorer ce domaine approuvé) et appliquez vos modifications.

REMARQUE : l'ajout d'un domaine approuvé lance un rafraîchissement complet du cache des comptes, mais vous en êtes averti par le biais d'une invite de confirmation lorsque vous cliquez sur **Appliquer**.

3.2.2 Connexion aux dossiers publics

DRA vous permet de gérer les dossiers publics Microsoft Exchange. Vous pouvez gérer certaines des propriétés des dossiers publics à l'aide de DRA en configurant des domaines de forêt de dossiers publics et en accordant des pouvoirs aux assistants administrateur.

IMPORTANT : pour gérer l'administration des dossiers publics, vous devez tout d'abord activer la prise en charge de Microsoft Exchange dans DRA et disposer des pouvoirs applicables.

- ♦ Pour plus d'informations sur l'activation de Microsoft Exchange, reportez-vous à la section [Activation de la prise en charge de Microsoft Exchange](#).
- ♦ Pour des informations sur les autorisations de compte, reportez-vous à la section [Comptes d'accès DRA à privilège minimal](#).

Pour configurer la prise en charge des dossiers publics Exchange :

- 1 Cliquez avec le bouton droit sur **Managed Public Folder Forests** (Forêts de dossiers publics gérées) sur le noeud Configuration Management, puis cliquez sur **New Public Folder Forest** (Nouvelle forêt de dossiers publics).
- 2 Cliquez sur **Forest Domain** (Domaine de la forêt), spécifiez la forêt Active Directory qui contient les objets Dossier public, puis cliquez sur **Next** (Suivant).
- 3 Dans **Domain access** (Accès au domaine), spécifiez le compte d'accès :
 - ♦ **Use the Directory and Resource Administrator service account (Utiliser le compte du service Directory and Resource Administrator)** : si vous souhaitez utiliser votre compte de service DRA.
 - ♦ **Use the following account to access this domain (Utiliser le compte suivant pour accéder à ce domaine)** : si vous souhaitez utiliser le compte d'accès au domaine.

IMPORTANT : si vous utilisez le serveur secondaire, l'option **Use the Primary Administration Server domain access account** (Utiliser le compte d'accès au domaine du serveur d'administration primaire) est disponible.

- 4 Dans **Exchange access** (Accès Exchange), spécifiez le compte que DRA doit utiliser pour accéder de manière sécurisée aux serveurs Exchange :
 - ♦ **Use the Domain access account for all Exchange servers (Utiliser le compte d'accès au domaine pour tous les serveurs Exchange)** : si vous souhaitez utiliser le compte d'accès au domaine.
 - ♦ **Use the following account to access all Exchange servers (Utiliser le compte suivant pour accéder à tous les serveurs Exchange)** : si vous souhaitez utiliser le compte d'accès Exchange.

IMPORTANT : si vous utilisez le serveur secondaire, l'option **Use the Primary Administration Server Exchange access account** (Utiliser le compte d'accès Exchange du serveur d'administration primaire) est disponible.

- 5 Dans **Exchange server** (Serveur Exchange), sélectionnez le serveur Exchange que DRA doit utiliser pour la gestion des dossiers publics.
- 6 Dans **Summary** (Résumé), passez en revue les détails du compte et du serveur Exchange, puis cliquez sur **Finish** (Terminer) pour finaliser le processus.

Le serveur DRA exécute un rafraîchissement complet du cache des comptes sur le dossier public. La nouvelle forêt de dossiers publics s'affiche au niveau de la console une fois le rafraîchissement du cache terminé, ce qui peut prendre quelques minutes.

REMARQUE : vous pouvez supprimer un domaine sélectionné de la forêt de dossiers publics à partir du menu **Tâches** ou du menu contextuel.

Affichage et modification des propriétés d'un domaine de dossiers publics

Pour afficher ou modifier les propriétés d'un domaine de dossiers publics :

- 1 Cliquez sur **Managed Public Folder Forests** (Forêts de dossiers publics gérées) sur le noeud Configuration Management pour afficher les dossiers publics.
- 2 Double-cliquez sur le compte Public Folder (Dossier public) à afficher, puis sélectionnez **Properties** (Propriétés).
- 3 Dans les propriétés **Public Folder Forest** (Forêt de dossiers publics), vous pouvez effectuer les actions suivantes :
 - ♦ **General (Général)** : permet d'afficher les détails du compte de dossier public et de mettre à jour le champ **Exchange Server**, qui est utilisé par le serveur DRA pour effectuer les activités Exchange sur le serveur de dossiers publics.
 - ♦ **Statistics (Statistiques)** : permet d'afficher le nombre de dossiers publics et le nombre de dossiers publics de messagerie.
 - ♦ **Incremental Status (État du rafraîchissement incrémentiel)** : permet d'afficher ou de mettre à jour l'état du rafraîchissement incrémentiel du cache des comptes.
 - ♦ **Incremental schedule (Planification incrémentielle)** : permet d'afficher la planification du rafraîchissement incrémentiel du cache et de replanifier un rafraîchissement du cache.
 - ♦ **Full status (État du rafraîchissement complet)** : permet d'afficher l'état du rafraîchissement complet du cache des comptes.
 - ♦ **Full refresh (Rafraîchissement complet)** : permet d'effectuer un rafraîchissement complet du cache des comptes immédiatement.
NetIQ recommande d'effectuer un **rafraîchissement complet** uniquement si les données du cache des dossiers publics sont endommagées.
 - ♦ **Domain access (Accès au domaine)** : permet d'afficher les détails du compte de service DRA ou de remplacer les comptes d'accès.
 - ♦ **Exchange access (Accès Exchange)** : permet d'afficher ou de mettre à jour l'accès sécurisé aux serveurs Exchange.

Délégation des pouvoirs de dossiers publics

Les instances Active Views permettent de définir des pouvoirs et de gérer la délégation de dossiers publics. Vous pouvez spécifier des règles pour ajouter des objets gérés, choisir des domaines et assigner des pouvoirs, puis déléguer ces pouvoirs de dossiers publics aux assistants administrateur.

Pour créer une instance Active Views et déléguer des pouvoirs de dossiers publics :

- 1 Sur le noeud **Gestion de la délégation**, cliquez sur **Active Views**.
- 2 Cliquez sur **Suivant** dans l'**assistant** > **Create ActiveView** (Créer une instance Active Views), sélectionnez la règle requise dans la liste déroulante **Add** (Ajouter), puis choisissez Dossiers publics en tant que type d'objet. Par exemple, pour créer un objet correspondant à une règle, sélectionnez **Objects that match a rule** (Objets qui correspondent à une règle), puis choisissez **Public Folders** (Dossiers publics) en tant que type d'objet.

- 3 Spécifiez la règle Active View que vous voulez ajouter au dossier public, puis cliquez sur **Suivant**.
- 4 Spécifiez le nom de l'instance Active Views, puis cliquez sur **Terminer**.
- 5 Cliquez avec le bouton droit sur **Active Views** et accédez à **Delegate Administration** (Déléguer l'administration) > **Assistant Admins** (Assistants administrateur), puis spécifiez le type d'administrateur dans la liste déroulante **Add** (Ajouter) de l'**assistant**.
- 6 Recherchez l'utilisateur, le groupe ou le groupe AA spécifique auquel vous souhaitez déléguer des pouvoirs.
- 7 Utilisez le **sélecteur d'objet** pour rechercher et ajouter les objets souhaités, puis cliquez sur **Roles and Powers** (Rôles et pouvoirs) dans l'**assistant**.
- 8 Sélectionnez **Rôles** dans la liste déroulante **Ajouter**, puis recherchez le rôle Administration des dossiers publics et ajoutez-le.
- 9 Sélectionnez Pouvoirs dans la liste déroulante **Ajouter**, puis recherchez les pouvoirs supplémentaires à assigner à vos assistants administrateur qui ne font pas partie du rôle Administration des dossiers publics et ajoutez-les.
- 10 Cliquez sur **Suivant**, puis sur **Terminer** pour finaliser le processus de délégation.

Une fois les pouvoirs de dossiers publics délégués, les utilisateurs autorisés sont en mesure de créer, lire, mettre à jour et supprimer des propriétés de dossier public dans les domaines configurés à l'aide de la console Web.

3.2.3 Activation de la prise en charge de Microsoft Exchange

L'activation de la prise en charge de Microsoft Exchange permet d'exploiter les fonctions Exchange, telles que les stratégies Microsoft Exchange, la boîte aux lettres intégrée et la gestion des objets compatibles avec la messagerie. Vous pouvez activer ou désactiver la prise en charge de Microsoft Exchange pour chaque serveur d'administration sur les plates-formes suivantes : Microsoft Exchange Server 2010, Microsoft Exchange Server 2013 et versions ultérieures.

Pour activer la prise en charge de Microsoft Exchange, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation, et votre licence doit prendre en charge le produit Exchange. Pour plus d'informations sur les exigences relatives à Microsoft Exchange, reportez-vous à la section [Plates-formes prises en charge](#).

Pour activer la prise en charge de Microsoft Exchange :

- 1 Accédez à **Gestion des stratégies et de l'automatisation** > **Configure Exchange Policies** (Configurer des stratégies Exchange).
- 2 Sélectionnez **Enable Exchange Policy** Activer la stratégie Exchange, puis cliquez sur **Apply** (Appliquer).
DRA vérifie quelles sont les versions des outils de gestion Exchange installées sur le serveur d'administration et active les options qui vous permettent de sélectionner la prise en charge d'Exchange pour les versions appropriées.
- 3 *Si **Enable Exchange Policy** (Activer la stratégie Exchange) a déjà été sélectionné et que les options qui vous permettent de sélectionner la prise en charge d'Exchange ne sont pas activées, cliquez sur **Refresh** (Rafraîchir) pour que DRA vérifie quelles versions des outils de gestion Exchange sont installées sur le serveur d'administration.*

- 4 Pour activer la prise en charge de l'administration Exchange, sélectionnez les options pour activer le support des versions d'Exchange que vous comptez gérer avec ce serveur d'administration.
- 5 Cliquez sur **OK**.

3.2.4 Activation d'Exchange Online et de Skype Entreprise Online

Pour activer la boîte aux lettres Exchange Online et Skype Entreprise Online sous Office 365, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation. Votre licence doit également prendre en charge le produit Microsoft Exchange.

IMPORTANT : Microsoft Server limite le nombre d'utilisateurs simultanés connectés à la session WinRM/WinRS à cinq et le nombre de shells par utilisateur à cinq également. Veillez donc à ce que le compte utilisateur en question soit limité à cinq shells pour les serveurs DRA secondaires.

Pour activer la prise en charge d'Exchange Online et de Skype Entreprise Online :

- 1 Si ce n'est pas déjà fait, installez les composants Microsoft indiqués ci-dessous :
 - ◆ PowerShell 5.0+
 - ◆ Assistant de connexion Microsoft Online Services pour les professionnels des technologies de l'information RTW
<https://www.microsoft.com/en-us/download/details.aspx?id=41950>
 - ◆ Skype Entreprise Online, module Windows PowerShell
<https://www.microsoft.com/en-us/download/details.aspx?id=39366>
 - ◆ Ouvrez PowerShell et exécutez `Install-Module MSOnline`.

Pour plus d'informations, reportez-vous au document <https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell>.
- 2 Ouvrez la console Gestion des ordinateurs et relancez le **service d'administration de NetIQ**.
- 3 Dans le volet de gauche, cliquez sur **Gestion des stratégies et de l'automatisation**.
- 4 Accédez à **Gestion des stratégies et de l'automatisation** > **Configure Office 365 Politiques** (Configurer des stratégies Office 365), puis cliquez sur **Enable Exchange Online Administration support** (Activer la prise en charge de l'administration d'Exchange Online).

3.2.5 Ajout d'un locataire Office 365

Avant de pouvoir gérer Exchange Online et Skype Entreprise Online, vous devez gérer un ou plusieurs locataires Office 365. Avant de pouvoir gérer les locataires Office 365, vous devez activer la prise en charge d'Exchange Online ou de Skype Entreprise Online.

IMPORTANT : Microsoft Server limite le nombre d'utilisateurs simultanés connectés à la session WinRM/WinRS à cinq et le nombre de shells par utilisateur à cinq également. Veillez donc à ce que le compte utilisateur en question soit limité à cinq shells pour les serveurs DRA secondaires.

Pour plus d'informations sur l'activation d'Exchange Online ou de Skype Entreprise Online, reportez-vous aux sections suivantes :

- ♦ [Activation de la prise en charge de Microsoft Exchange](#)
- ♦ [Activation d'Exchange Online et de Skype Entreprise Online](#)

Avant de configurer DRA pour gérer vos locataires Exchange Online, vous devez créer, sur le portail Office 365, un compte qui dispose des autorisations suivantes :

DRA utilisera ce compte pour effectuer toutes les tâches de gestion d'Exchange Online.

- ♦ Administrateur de la gestion des utilisateurs dans Office 365
- ♦ Gestion des destinataires dans Exchange Online

REMARQUE : ce compte peut être synchronisé avec votre environnement Active Directory ou hébergé dans le cloud Microsoft Office 365. DRA ne nécessite pas que ce compte soit dans Active Directory pour effectuer des tâches de gestion.

Pour plus d'informations sur les autorisations de compte, reportez-vous à la section [Comptes d'accès DRA à privilège minimal](#).

Gestion d'un locataire Office 365 et création d'un principal de service

Une fois que vous avez activé la stratégie en ligne dans DRA, vous pouvez accéder à un nouveau nœud sous Configuration Management, nommé **Office 365 Tenants** (Locataires Office 365) et qui vous permet de gérer les nouveaux locataires Office 365.

Pour ajouter un locataire Office 365, accédez à **Configuration Management > Office 365 Tenants** (Locataires Office 365), puis suivez les instructions de l'assistant, y compris l'ajout d'un compte d'accès de locataire Office 365 et la configuration des planifications de rafraîchissement et de mise à jour.

DRA requiert un principal de service disposant d'autorisations Lecteurs de répertoire afin de collecter des données sur les objets du locataire.

Pour créer le principal de service, vous pouvez soit fournir à DRA les informations d'identification d'un compte utilisateur avec le rôle d'administrateur d'entreprise dans Office 365 afin que DRA crée le principal de service pour vous, soit créer le principal de service en mode hors ligne.

REMARQUE

- ♦ DRA n'enregistre pas les informations d'identification de l'administrateur d'entreprise fournies pour créer le principal de service.
 - ♦ Si vous créez le principal de service en mode hors ligne, vous devez spécifier l'identificateur et le mot de passe du principal de service dans l'assistant.
-

L'ajout d'un locataire Office 365 peut prendre plusieurs minutes. Une fois le locataire ajouté, DRA effectue un rafraîchissement complet du cache des comptes pour le locataire. Lorsque le rafraîchissement du cache est terminé, vous pouvez commencer à gérer vos licences Office 365 et vos boîtes aux lettres pour le locataire.

4 Modèle de délégation

DRA permet aux administrateurs d'implémenter un modèle d'autorisations « privilège minimal » en fournissant un ensemble flexible de contrôles pour l'octroi de pouvoirs granulaires à des objets gérés spécifiques dans l'entreprise. Grâce à ces délégations, les administrateurs peuvent s'assurer que les assistants administrateur reçoivent uniquement les autorisations dont ils ont besoin pour effectuer leurs propres rôles et responsabilités.

4.1 Présentation du modèle de délégation dynamique

DRA permet de gérer l'accès administratif à votre entreprise dans le cadre d'un modèle de délégation. Le modèle de délégation permet de définir un accès à « privilège minimal » pour les assistants administrateur par le biais d'un ensemble dynamique de contrôles qui peuvent s'adapter en fonction de l'évolution de l'entreprise. Le modèle de délégation fournit un contrôle d'accès administratif représentant de manière plus fidèle le fonctionnement de votre entreprise :

- ♦ Des règles d'étendue flexibles permettent aux administrateurs de cibler des autorisations par rapport à des objets gérés spécifiques en fonction des besoins commerciaux plutôt que de la structure de l'entreprise.
- ♦ La délégation basée sur les rôles permet d'octroyer les autorisations de manière cohérente et simplifie le provisioning.
- ♦ L'assignation de privilèges peut être administrée sur l'ensemble des domaines, des locataires cloud et des applications gérées à partir d'un emplacement unique.
- ♦ Les pouvoirs granulaires vous permettent de définir sur mesure l'accès spécifique octroyé aux assistants administrateur.

4.1.1 Contrôles du modèle de délégation

Pour provisionner l'accès via le modèle de délégation, les administrateurs utilisent les contrôles suivants :

- ♦ **Délégation** : les administrateurs provisionnent l'accès aux utilisateurs et groupes en assignant un rôle qui dispose d'autorisations spécifiées dans le contexte d'une instance Active Views qui fournit l'étendue.
- ♦ **Instances Active Views** : une instance Active Views représente une étendue spécifique d'objets gérés qui sont définis par une ou plusieurs règles. Les objets gérés identifiés par chaque règle dans une instance Active Views sont regroupés dans une étendue unifiée.
- ♦ **Règle Active Views** : les règles sont définies par des expressions qui correspondent à un ensemble d'objets gérés en fonction de diverses conditions telles que le type d'objet, l'emplacement, le nom, etc.
- ♦ **Rôles** : un rôle représente un ensemble spécifique de pouvoirs (autorisations) requis pour exécuter une fonction d'administration spécifique. DRA fournit un nombre de rôles intégrés pour des fonctions métier courantes et vous pouvez définir des rôles personnalisés mieux adaptés aux besoins de votre organisation.
- ♦ **Pouvoirs** : un pouvoir définit une autorisation spécifique pour les tâches prises en charge par l'objet géré telles que l'affichage, la modification, la création, la suppression, etc. Les autorisations relatives à la modification d'un objet géré peuvent à leur tour être décomposées en

propriétés spécifiques qui peuvent être éditées. DRA fournit une vaste liste de pouvoirs prédéfinis pour les objets gérés pris en charge et permet de définir des pouvoirs personnalisés pour étendre le provisioning via le modèle de délégation.

4.1.2 Mode de traitement des requêtes par DRA

Lorsque le serveur d'administration reçoit une requête pour une action, telle que le changement d'un mot de passe, il procède comme suit :

1. Il recherche les instances Active Views qui sont configurées pour gérer l'objet cible de l'opération.
2. Il valide les pouvoirs assignés au compte qui demande l'action.
 - a. Il évalue toutes les assignations Active Views qui contiennent l'assistant administrateur demandant l'opération.
 - b. Une fois que cette liste est dressée, il répertorie toutes les instances Active Views qui contiennent l'objet cible et l'assistant administrateur.
 - c. Il compare les pouvoirs avec ceux requis pour effectuer l'opération qui émet la requête.
3. *Si le compte dispose du pouvoir approprié*, le serveur d'administration permet d'effectuer l'action.
Si le compte ne dispose pas du pouvoir approprié, le serveur d'administration renvoie une erreur.
4. Il met à jour Active Directory.

4.1.3 Exemples de la façon dont DRA traite les assignations de délégation

Les exemples ci-après décrivent les scénarios courants qui surviennent dans la façon dont DRA évalue le modèle de délégation lors du traitement d'une requête :

Exemple 1 : modification du mot de passe d'un utilisateur

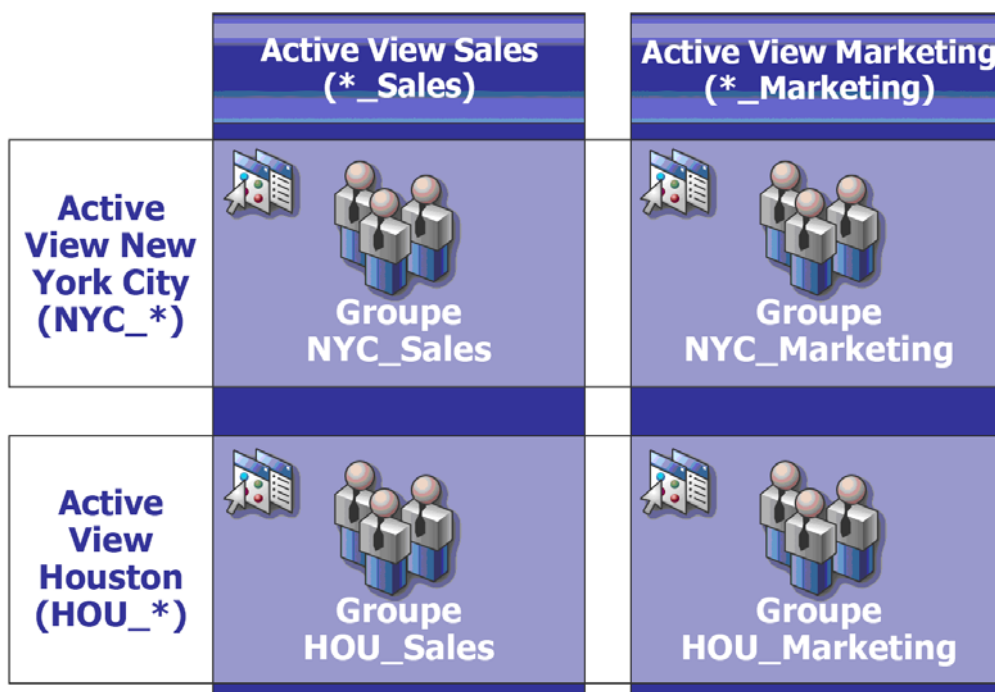
Lorsqu'un assistant administrateur tente de définir un nouveau mot de passe pour le compte utilisateur JSmith, le serveur d'administration recherche toutes les instances Active Views comprenant JSmith. Il recherche toutes les instances Active Views qui indiquent JSmith directement, par le biais d'une règle de caractère joker ou via l'adhésion à un groupe. Si une instance Active Views inclut d'autres instances Active Views, le serveur d'administration recherche également ces instances Active Views supplémentaires. Le serveur d'administration détermine si l'assistant administrateur dispose du pouvoir *Réinitialiser le mot de passe du compte utilisateur* dans l'une de ces instances Active Views. Si l'assistant administrateur possède le pouvoir *Réinitialiser le mot de passe du compte utilisateur*, le serveur d'administration réinitialise le mot de passe de JSmith. S'il ne dispose pas de ce pouvoir, le serveur d'administration refuse la requête.

Exemple 2 : chevauchement d'instances Active Views

Un pouvoir définit les propriétés d'un objet qu'un assistant administrateur peut afficher, modifier ou créer dans votre domaine ou votre sous-arborescence gérée. Plusieurs instances Active Views peuvent inclure le même objet. Cette configuration est désignée sous le terme de **chevauchement d'instances Active Views**.

Lorsque des instances Active Views se chevauchent, vous pouvez accumuler un ensemble de pouvoirs différents pour les mêmes objets. Par exemple, si une instance Active Views vous permet d'ajouter un compte utilisateur à un domaine et qu'une autre instance Active Views vous permet de supprimer un compte utilisateur du même domaine, vous pouvez ajouter ou supprimer des comptes utilisateur dans ce domaine. De cette manière, les pouvoirs dont vous disposez sur un objet donné sont cumulatifs.

Il est important de comprendre comment se chevauchent les instances Active Views et comment vous pouvez obtenir des pouvoirs accrus sur les objets inclus dans ces dernières. Imaginons la configuration Active Views illustrée dans la figure suivante.



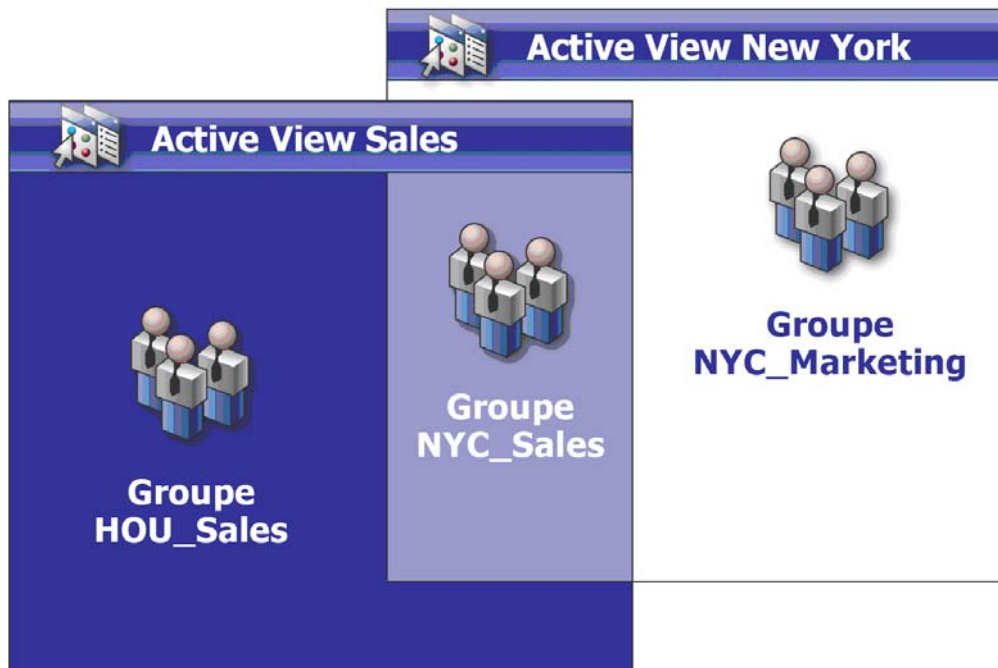
Les onglets blancs identifient les instances Active Views par emplacement : *New York City* et *Houston*. Les onglets noirs identifient les instances Active Views selon leur fonction organisationnelle : *Sales* et *Marketing*. Les cellules affichent les groupes inclus dans chaque instance Active Views.

Le groupe NYC_Sales et le groupe HOU_Sales sont représentés tous les deux dans l'instance Active Views Sales. Si vous disposez de pouvoirs dans l'instance Active Views Sales, vous pouvez gérer tous les membres des groupes NYC_Sales et HOU_Sales. Si vous disposez également de pouvoirs dans l'instance Active Views New York City, ces pouvoirs supplémentaires s'appliquent au groupe NYC_Marketing. De cette manière, les pouvoirs s'accumulent selon les chevauchements des instances Active Views.

Le chevauchement des instances Active Views peut fournir un modèle de délégation souple et puissant. Toutefois, cette fonction peut également avoir des conséquences inattendues. Planifiez soigneusement vos instances Active Views pour être certain que chaque assistant administrateur dispose uniquement des pouvoirs prévus pour chaque compte utilisateur, groupe, unité organisationnelle, contact ou ressource.

Groupes dans plusieurs instances Active Views

Dans cet exemple, le groupe NYC_Sales est représenté dans plusieurs instances Active Views. Les membres du groupe NYC_Sales sont représentés dans l'instance Active Views New York City parce que le nom du groupe correspond à la règle Active View NYC_*. Le groupe est également dans l'instance Active Views Sales, car son nom satisfait à la règle Active View *_Sales. En incluant le même groupe dans plusieurs instances Active Views, vous pouvez autoriser différents assistants administrateur à gérer les mêmes objets différemment.








Utilisation des pouvoirs dans plusieurs instances Active Views

Supposons qu'un assistant administrateur, JSmith, dispose du pouvoir *Modifier les propriétés des utilisateurs généraux* dans l'instance Active Views New York City. Ce premier pouvoir permet à JSmith de modifier toutes les propriétés sous l'onglet Général de la fenêtre des propriétés d'un

utilisateur. JSmith possède le pouvoir *Modifier les propriétés du profil utilisateur* dans l'instance Active Views Sales. Ce deuxième pouvoir permet à JSmith de modifier toutes les propriétés sous l'onglet Profil de la fenêtre des propriétés d'un utilisateur.

La figure suivante indique les pouvoirs que JSmith possède pour chaque groupe.

	Active View Sales (*_Sales)	Active View Marketing (*_Marketing)
Active View New York City (NYC_*)	 !Propriétés générales  !Propriétés du profil Groupe NYC_Sales	 !Propriétés générales Groupe NYC_Marketing
Active View Houston (HOU_*)	 !Propriétés du profil Groupe HOU_Sales	 !Aucun pouvoir Groupe HOU_Marketing

JSmith dispose des pouvoirs suivants :

- ♦ Propriétés générales dans l'instance Active Views NYC_*
- ♦ Propriétés du profil dans l'instance Active Views *_Sales

La délégation de pouvoirs dans ces chevauchements d'instances Active Views permet à JSmith de modifier les propriétés générales et de profil du groupe NYC_Sales. Par conséquent, JSmith dispose de tous les pouvoirs accordés dans toutes les instances Active Views qui représentent le groupe NYC_Sales.

4.2 Instances Active Views

Les instances Active Views permettent d'implémenter un modèle de délégation qui présente les caractéristiques suivantes :

- ♦ est indépendant de votre structure Active Directory ;
- ♦ permet d'assigner des pouvoirs et de définir des stratégies en corrélation avec vos workflows existants ;
- ♦ assure l'automatisation nécessaire pour vous aider à mieux intégrer et personnaliser votre entreprise ;
- ♦ répond de façon dynamique au changement.

Une instance Active Views représente un ensemble d'objets au sein d'un ou de plusieurs domaines gérés. Vous pouvez inclure un objet dans plusieurs instances Active Views. Vous pouvez également inclure de nombreux objets provenant de plusieurs domaines ou unités organisationnelles.

4.2.1 Instances Active Views intégrées

Les instances Active Views intégrées sont celles fournies par défaut par DRA. Ces instances Active Views représentent tous les objets et les paramètres de sécurité actuels. Ainsi, les instances Active Views intégrées fournissent un accès immédiat à tous vos objets et paramètres, ainsi qu'au modèle de délégation par défaut. Vous pouvez utiliser ces instances Active Views pour gérer les objets, tels que les comptes utilisateur et les ressources, ou pour appliquer le modèle de délégation par défaut à votre configuration d'entreprise actuelle.

DRA fournit plusieurs instances Active Views intégrées qui peuvent représenter votre modèle de délégation. Le noeud Active Views intégré contient les instances Active Views suivantes :

All objects (Tous les objets)

Inclut tous les objets de tous les domaines gérés. Cette instance Active Views vous permet de gérer tous les aspects de votre entreprise. Assignez-la à l'administrateur ou à un assistant administrateur (AA) qui a besoin de pouvoirs d'audit sur l'ensemble de l'entreprise.

Objects Current User Manages as Windows Administrator (Objets que l'utilisateur actuel gère en tant qu'administrateur Windows)

Inclut les objets du domaine géré actuel. Cette instance Active Views vous permet de gérer les comptes utilisateur, les groupes, les contacts, les unités organisationnelles et les ressources. Assignez-la aux administrateurs natifs responsables des objets Compte et Ressource dans le domaine géré.

Administration Servers and Managed Domains (Serveurs d'administration et domaines gérés)

Inclut les ordinateurs de serveur d'administration et les domaines gérés. Cette instance Active Views vous permet de gérer la maintenance quotidienne de vos serveurs d'administration. Assignez-la aux assistants administrateur dont les tâches incluent la surveillance de l'état de synchronisation ou le rafraîchissement du cache.

DRA Policies and Automation Triggers (Stratégies DRA et déclencheurs d'automatisation)

Inclut tous les objets Stratégie et Déclencheur d'automatisation de tous les domaines gérés. Cette instance Active Views vous permet de gérer les propriétés et l'étendue des stratégies, ainsi que les propriétés des déclencheurs d'automatisation. Assignez-la aux assistants administrateur responsables de la création et de la maintenance des stratégies de l'entreprise.

DRA Security Objects (Objets de sécurité de DRA)

Inclut tous les objets de sécurité. Cette instance Active Views vous permet de gérer les instances Active Views, les groupes AA et les rôles. Assignez-la aux assistants administrateur responsables de la création et de la maintenance du modèle de sécurité.

SPA Users from All Managed and Trusted Domains (Utilisateurs SPA de tous les domaines gérés et approuvés)

Inclut tous les comptes utilisateur des domaines gérés et approuvés. Cette instance Active View vous permet de gérer les mots de passe utilisateur via Secure Password Administrator (SPA).

Accès aux instances Active Views intégrées

Accédez aux instances Active Views intégrées pour auditer le modèle de délégation par défaut ou pour gérer vos propres paramètres de sécurité.

Pour accéder aux instances Active Views intégrées :

- 1 Accédez à **Gestion de la délégation > Manage ActiveViews** (Gérer les instances Active Views).

- 2 Vérifiez que le champ de recherche est vide, puis cliquez sur **Find Now** (Rechercher maintenant) dans le volet **List items that match my criteria** (Lister les éléments qui répondent à mes critères).
- 3 Sélectionnez l'instance Active Views appropriée.

Utilisation des instances Active Views intégrées

Vous ne pouvez pas supprimer, cloner ni modifier des instances Active Views intégrées. En revanche, vous pouvez les insérer dans votre modèle de délégation existant ou les utiliser pour concevoir votre propre modèle.

Vous pouvez employer des instances Active Views intégrées comme suit :

- ♦ Assignez les différentes instances Active Views intégrées aux groupes AA appropriés. Cette association permet aux membres du groupe AA de gérer l'ensemble d'objets correspondant avec les pouvoirs appropriés.
- ♦ Référez-vous aux associations et règles Active View prédéfinies comme directives pour concevoir et implémenter votre modèle de délégation.

Pour plus d'informations sur la conception d'un modèle de délégation dynamique, reportez-vous à la section [Présentation du modèle de délégation dynamique](#).

4.2.2 Implémentation d'une instance Active Views personnalisée

Une instance Active Views fournit un accès en temps réel à des objets spécifiques au sein d'un ou de plusieurs domaines ou unités organisationnelles. Vous pouvez ajouter ou supprimer des objets d'une instance Active Views sans changer la structure de l'unité organisationnelle ou le domaine sous-jacent.

Vous pouvez envisager une instance Active Views comme un domaine virtuel ou une unité organisationnelle, ou comme le résultat d'une instruction SELECT ou d'une vue de base de données pour une base de données relationnelle. Les instances Active Views peuvent inclure ou exclure n'importe quel ensemble d'objets, contenir d'autres instances Active Views et avoir du contenu qui se chevauche. Les instances Active Views peuvent contenir des objets issus de domaines, d'arborescences et de forêts différents. Vous pouvez configurer les instances Active Views pour répondre à tous les besoins de gestion de l'entreprise.

Les instances Active Views peuvent inclure les types d'objet suivants :

Comptes :

- ♦ Utilisateurs
- ♦ Groupes
- ♦ Ordinateurs
- ♦ Contacts
- ♦ Groupes de distribution dynamiques
- ♦ Imprimantes publiées
- ♦ Travaux d'impression d'imprimantes publiées
- ♦ Boîtes aux lettres de ressources
- ♦ Boîtes aux lettres partagées
- ♦ Dossiers publics

Objets d'annuaire :

- ♦ Unités organisationnelles
- ♦ Domaines
- ♦ Serveurs membres

Objets de délégation :

- ♦ Instances Active Views
- ♦ Auto-administration
- ♦ Subordonnés directs
- ♦ Groupes gérés

Ressources :

- ♦ Utilisateurs connectés
- ♦ Périphériques
- ♦ Journaux d'événements
- ♦ Fichiers ouverts
- ♦ Imprimantes
- ♦ Travaux d'impression
- ♦ Services
- ♦ Partages

Au fur et à mesure de l'évolution de votre entreprise, vos instances Active Views changent pour inclure ou exclure les nouveaux objets. Les instances Active Views vous permettent ainsi de réduire la complexité de votre modèle, de garantir la sécurité requise et de bénéficier de bien plus de souplesse que celle offerte par les autres outils d'organisation de l'entreprise.

Règles Active View

Une instance Active Views peut être constituée de règles qui incluent ou excluent des objets tels que des comptes utilisateur, des groupes, des unités organisationnelles, des contacts, des ressources, des ordinateurs, des boîtes aux lettres de ressources, des boîtes aux lettres partagées, des groupes de distribution dynamique et des instances Active Views. Cette flexibilité rend les instances Active Views dynamiques.

Ces correspondances sont appelées des **caractères joker**. Par exemple, vous pouvez définir une règle pour inclure tous les ordinateurs dont les noms correspondent à `DOM*`. Cette spécification de caractère joker recherche tout compte d'ordinateur dont le nom commence par la chaîne de caractères `DOM`. La correspondance par caractère joker rend l'administration dynamique, car les comptes sont automatiquement inclus lorsqu'ils satisfont à la règle. De cette façon, lorsque vous utilisez des caractères joker, il est inutile de reconfigurer les instances Active Views lorsque votre organisation change.

Un autre exemple consiste à définir les instances Active Views en fonction de l'adhésion au groupe. Vous pouvez définir une règle qui inclut tous les membres des groupes qui commencent par les lettres NYC. Ensuite, chaque membre ajouté à n'importe quel groupe qui correspond à cette règle est automatiquement inclus dans cette instance Active Views. Lorsque votre entreprise change ou se développe, DRA réapplique les règles pour inclure ou exclure les nouveaux objets dans les instances Active Views appropriées.

4.3 Rôles

Cette section comprend une liste avec des descriptions des rôles intégrés à DRA, des explications sur l'utilisation de ces rôles et des informations sur la création et la gestion de rôles personnalisés.

Pour obtenir une description générale des rôles et de leur utilisation, reportez-vous à la section [Contrôles du modèle de délégation](#).

4.3.1 Rôles intégrés

Les rôles AA intégrés fournissent un accès immédiat à un ensemble de pouvoirs couramment utilisés. Vous pouvez étendre votre configuration actuelle de la sécurité à l'aide de ces rôles par défaut pour déléguer des pouvoirs à certains comptes utilisateur ou à d'autres groupes.

Ces rôles contiennent les pouvoirs requis pour effectuer les tâches administratives courantes. Par exemple, le rôle Administration DRA contient tous les pouvoirs requis pour gérer les objets. Toutefois, pour utiliser ces pouvoirs, le rôle doit être associé à un compte utilisateur ou à un groupe AA et à l'instance Active Views gérée.

Étant donné que les rôles intégrés font partie du modèle de délégation par défaut, vous pouvez les utiliser pour déléguer rapidement des pouvoirs et implémenter la sécurité. Ces rôles prédéfinis répondent aux tâches courantes que vous pouvez effectuer via les interfaces utilisateur de DRA. La liste suivante décrit chaque rôle intégré et résume les pouvoirs qui lui sont associés.

Administration des serveurs d'applications

Fournit les pouvoirs requis pour configurer, consulter et supprimer des configurations de serveurs d'applications.

Auditer tous les objets

Fournit tous les pouvoirs requis pour afficher les propriétés des objets, des stratégies et des configurations au sein de votre entreprise. Ce rôle ne permet pas à un assistant administrateur de modifier les propriétés. Assignez ce rôle aux assistants administrateur chargés d'auditer des actions dans l'ensemble de votre entreprise. Permet aux assistants administrateur d'afficher tous les noeuds, excepté le noeud Outils personnalisés.

Auditer un nombre limité de propriétés de ressources et de comptes

Fournit des pouvoirs pour toutes les propriétés d'objet.

Auditer les ressources

Fournit tous les pouvoirs requis pour afficher les propriétés des ressources gérées. Assignez ce rôle aux assistants administrateur chargés de l'audit des objets Ressource.

Auditer les utilisateurs et les groupes

Fournit tous les pouvoirs requis pour afficher les propriétés des comptes utilisateur et des groupes, mais ne permet pas de modifier ces propriétés. Assignez ce rôle aux assistants administrateur chargés de l'audit des propriétés des comptes.

Planificateur intégré - Usage interne uniquement

Fournit les pouvoirs requis pour planifier le moment auquel DRA actualise le cache.

Cloner l'utilisateur avec la boîte aux lettres

Fournit tous les pouvoirs requis pour cloner un compte utilisateur existant, ainsi que sa boîte aux lettres. Assignez ce rôle aux assistants administrateur chargés de la gestion des comptes utilisateur.

REMARQUE : Pour que les assistants administrateur puissent ajouter le nouveau compte utilisateur à un groupe lors de la tâche de clonage, assignez-leur également le rôle Gérer les adhésions aux groupes.

Administration des ordinateurs

Fournit tous les pouvoirs requis pour modifier les propriétés des ordinateurs. Ce rôle permet aux assistants administrateur d'ajouter, de supprimer et d'arrêter des ordinateurs, ainsi que de synchroniser les contrôleurs de domaine. Assignez ce rôle aux assistants administrateur chargés de gérer des ordinateurs dans les instances Active Views.

Configurer les serveurs et les domaines

Fournit tous les pouvoirs requis pour modifier les options des serveurs d'administration et les domaines gérés. Fournit également les pouvoirs nécessaires pour configurer et gérer les locataires Office 365. Assignez ce rôle aux assistants administrateur responsables de la surveillance et de la maintenance des serveurs d'administration.

Administration des contacts

Fournit tous les pouvoirs requis pour créer un contact, modifier ses propriétés ou le supprimer. Assignez ce rôle aux assistants administrateur chargés de la gestion des contacts.

Créer et supprimer des comptes d'ordinateur

Fournit tous les pouvoirs requis pour créer et supprimer un compte d'ordinateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des ordinateurs.

Créer et supprimer des groupes

Fournit tous les pouvoirs requis pour créer et supprimer un groupe. Assignez ce rôle aux assistants administrateur chargés de la gestion des groupes.

Créer et supprimer une boîte aux lettres de ressources

Fournit tous les pouvoirs requis pour créer et supprimer une boîte aux lettres. Assignez ce rôle aux assistants administrateur chargés de la gestion des boîtes aux lettres.

Créer et supprimer des ressources

Fournit tous les pouvoirs requis pour créer et supprimer des partages et des comptes d'ordinateur, et effacer les journaux d'événements. Assignez ce rôle aux assistants administrateur chargés de la gestion des objets Ressource et des journaux d'événements.

Créer et supprimer des comptes utilisateur

Fournit tous les pouvoirs requis pour créer et supprimer un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des comptes utilisateur.

Administration DRA

Fournit tous les pouvoirs à un assistant administrateur. Ce rôle octroie à un utilisateur les autorisations nécessaires pour effectuer toutes les tâches d'administration dans DRA. Il est équivalent aux autorisations d'un administrateur. Un assistant administrateur associé au rôle Administration DRA peut accéder à tous les noeuds de Directory and Resource Administrator.

Administration des groupes dynamiques

Fournit tous les pouvoirs requis pour gérer les groupes dynamiques Active Directory.

Exécuter des requêtes avancées

Fournit tous les pouvoirs requis pour l'exécution de requêtes avancées enregistrées. Assignez ce rôle aux assistants administrateur chargés de l'exécution des requêtes avancées.

Administration des groupes

Fournit tous les pouvoirs requis pour gérer les groupes et les adhésions aux groupes, et pour afficher les propriétés utilisateur correspondantes. Assignez ce rôle aux assistants administrateur chargés de gérer des groupes ou des objets Compte et Ressource qui sont gérés par le biais de groupes.

Administration du service d'assistance

Fournit tous les pouvoirs requis pour afficher les propriétés de compte utilisateur et pour modifier les mots de passe et les propriétés qui y sont associées. Ce rôle permet également aux assistants administrateur d'activer, de désactiver et de déverrouiller des comptes utilisateur. Assignez ce rôle aux assistants administrateur chargés des tâches de service d'assistance visant à assurer que les utilisateurs disposent d'un accès approprié à leur compte.

Administration des boîtes aux lettres

Fournit tous les pouvoirs requis pour gérer les propriétés de boîte aux lettres Microsoft Exchange. Si vous utilisez Microsoft Exchange, assignez ce rôle aux assistants administrateur chargés de gérer les boîtes aux lettres Microsoft Exchange.

Gérer les collecteurs Active Directory, les collecteurs DRA et les collecteurs de création de rapports de gestion

Fournit tous les pouvoirs requis pour gérer les collecteurs Active Directory, les collecteurs DRA, les collecteurs de locataires Office 365 et les collecteurs de création de rapports de gestion pour la collecte de données. Assignez ce rôle aux assistants administrateur chargés de la gestion de la configuration de la création de rapports.

Gérer les collecteurs Active Directory, les collecteurs DRA, les collecteurs de création de rapports de gestion et la configuration de la base de données

Fournit tous les pouvoirs requis pour gérer les collecteurs Active Directory, les collecteurs DRA, les collecteurs de création de rapports de gestion et la configuration de la base de données pour la collecte de données. Assignez ce rôle aux assistants administrateur chargés de la gestion de la création de rapports et de la configuration de la base de données.

Gérer les requêtes avancées

Fournit tous les pouvoirs requis pour créer, gérer et exécuter les requêtes avancées. Assignez ce rôle aux assistants administrateur chargés de la gestion des requêtes avancées.

Gérer et exécuter des outils personnalisés

Fournit tous les pouvoirs requis pour créer, gérer et exécuter des outils personnalisés. Assignez ce rôle aux assistants administrateur chargés de la gestion des outils personnalisés.

Gérer les exceptions de clonage

Fournit tous les pouvoirs requis pour créer et gérer des exceptions de clonage.

Gérer les propriétés des ordinateurs

Fournit tous les pouvoirs requis pour gérer toutes les propriétés d'un compte d'ordinateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des ordinateurs.

Gérer la configuration de la base de données

Fournit tous les pouvoirs requis pour gérer la configuration de la base de données des rapports de gestion. Assignez ce rôle aux assistants administrateur chargés de la gestion de la configuration de la base de données de création de rapports.

Gérer les groupes de distribution dynamique

Fournit tous les pouvoirs requis pour gérer les groupes de distribution dynamique Microsoft Exchange.

Gérer les droits de boîte aux lettres Exchange

Fournit tous les pouvoirs requis pour gérer la sécurité et les droits pour les boîtes aux lettres Microsoft Exchange. Si vous utilisez Microsoft Exchange, assignez ce rôle aux assistants administrateur chargés de gérer les autorisations des boîtes aux lettres Microsoft Exchange.

Gérer les messages électroniques de groupe

Fournit tous les pouvoirs requis pour afficher, activer ou désactiver l'adresse électronique pour un groupe. Assignez ce rôle aux assistants administrateur chargés de gérer des groupes ou des adresses électroniques pour des objets Compte.

Gérer la sécurité de l'adhésion aux groupes

Fournit tous les pouvoirs requis pour désigner qui peut consulter et modifier les adhésions aux groupes Microsoft Windows via Microsoft Outlook.

Gérer l'adhésion aux groupes

Fournit tous les pouvoirs requis pour ajouter et supprimer des comptes utilisateur ou des groupes à partir d'un groupe existant, et pour afficher le groupe principal d'un compte utilisateur ou d'ordinateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des groupes ou des comptes utilisateur.

Gérer les propriétés de groupe

Fournit tous les pouvoirs requis pour gérer toutes les propriétés d'un groupe. Assignez ce rôle aux assistants administrateur chargés de la gestion des groupes.

Gérer les demandes de déplacement de boîte aux lettres

Fournit tous les pouvoirs requis pour gérer les demandes de déplacement de boîte aux lettres.

Gérer les stratégies et les déclencheurs d'automatisation

Fournit tous les pouvoirs requis pour définir des stratégies et des déclencheurs d'automatisation. Assignez ce rôle aux assistants administrateur chargés de la maintenance des stratégies d'entreprise et de l'automatisation des workflows.

Gérer les imprimantes et les travaux d'impression

Fournit tous les pouvoirs requis pour gérer les imprimantes, les files d'attente d'impression et les travaux d'impression. Pour gérer les travaux d'impression associés à un compte utilisateur, le travail d'impression et le compte utilisateur doivent figurer dans la même instance Active Views. Assignez ce rôle aux assistants administrateur chargés de la maintenance des imprimantes et de la gestion des travaux d'impression.

Gérer les propriétés des boîtes aux lettres de ressources

Fournit tous les pouvoirs requis pour gérer toutes les propriétés d'une boîte aux lettres. Assignez ce rôle aux assistants administrateur chargés de la gestion des boîtes aux lettres.

Gérer les ressources des utilisateurs gérés

Fournit tous les pouvoirs requis pour gérer les ressources associées à des comptes utilisateur spécifiques. Les assistants administrateur et les comptes utilisateur doivent être inclus dans la même instance Active Views. Assignez ce rôle aux assistants administrateur chargés de la gestion des objets Ressource.

Gérer le modèle de sécurité

Fournit tous les pouvoirs requis pour définir les règles d'administration, y compris des instances Active Views, des assistants administrateur et des rôles. Assignez ce rôle aux assistants administrateur chargés de l'implémentation et de la maintenance de votre modèle de sécurité.

Gérer les services

Fournit tous les pouvoirs requis pour gérer les services. Assignez ce rôle aux assistants administrateur chargés de la gestion des services.

Gérer les dossiers partagés

Fournit tous les pouvoirs requis pour gérer les dossiers partagés. Assignez ce rôle aux assistants administrateur chargés de la gestion des dossiers partagés.

Gérer les assignations temporaires à des groupes

Fournit tous les pouvoirs requis pour créer et gérer des assignations temporaires à des groupes. Assignez ce rôle aux assistants administrateur chargés de la gestion des groupes.

Gérer la création de rapports de l'interface utilisateur

Fournit tous les pouvoirs requis pour générer et exporter des rapports de détail des activités pour les utilisateurs, les groupes, les contacts, les ordinateurs, les unités organisationnelles, les pouvoirs, les rôles, les instances Active Views, les conteneurs, les imprimantes publiées et les assistants administrateur. Assignez ce rôle aux assistants administrateur chargés de la génération de rapports.

Gérer les propriétés d'accès à distance de l'utilisateur

Fournit tous les pouvoirs requis pour modifier les propriétés d'accès à distance des comptes utilisateur. Assignez ce rôle aux assistants administrateur chargés de gérer les comptes utilisateur ayant un accès à distance à l'entreprise.

Gérer les adresses électroniques des utilisateurs

Fournit tous les pouvoirs requis pour afficher, activer ou désactiver l'adresse électronique d'un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de gérer les comptes utilisateur ou les adresses électroniques pour des objets Compte.

Gérer le mot de passe utilisateur et le déverrouillage de compte

Fournit tous les pouvoirs requis pour réinitialiser le mot de passe, spécifier les paramètres de mot de passe et déverrouiller un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la maintenance des accès aux comptes utilisateur.

Gérer les propriétés utilisateur

Fournit tous les pouvoirs requis pour gérer toutes les propriétés d'un compte utilisateur, y compris les propriétés de boîte aux lettres Microsoft Exchange. Assignez ce rôle aux assistants administrateur chargés de la gestion des comptes utilisateur.

Gérer les attributs virtuels

Fournit tous les pouvoirs requis pour créer et gérer des attributs virtuels. Assignez ce rôle aux assistants administrateur chargés de la gestion des attributs virtuels.

Gérer les propriétés de l'environnement WTS

Fournit tous les pouvoirs requis pour modifier les propriétés d'environnement WTS pour un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la maintenance de l'environnement WTS ou de la gestion des comptes utilisateur.

Gérer les propriétés de contrôle à distance de WTS

Fournit tous les pouvoirs requis pour modifier les propriétés de contrôle à distance de WTS pour un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la maintenance de l'accès WTS ou de la gestion des comptes utilisateur.

Gérer les propriétés de session WTS

Fournit tous les pouvoirs requis pour modifier les propriétés de session WTS pour un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la maintenance des sessions WTS ou de la gestion des comptes utilisateur.

Gérer les propriétés de terminal WTS

Fournit tous les pouvoirs requis pour modifier les propriétés de terminal WTS pour un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la maintenance des propriétés de terminal WTS ou de la gestion des comptes utilisateur.

Administration des unités organisationnelles

Fournit tous les pouvoirs requis pour gérer les unités organisationnelles (Organizational Units, OU). Assignez ce rôle aux assistants administrateur chargés de gérer la structure Active Directory.

Administration du dossier public

Fournit les pouvoirs requis pour créer, modifier, supprimer, activer ou désactiver des messages électroniques et pour afficher les propriétés de votre dossier public. Vous pouvez assigner ce rôle à tous les assistants administrateur chargés de la gestion du dossier public.

Renommer le groupe et modifier la description

Fournit tous les pouvoirs requis pour modifier le nom et la description d'un groupe. Assignez ce rôle aux assistants administrateur chargés de la gestion des groupes.

Renommer l'utilisateur et modifier la description

Fournit tous les pouvoirs requis pour modifier le nom et la description d'un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des comptes utilisateur.

Répliquer les fichiers

Fournit tous les pouvoirs requis pour télécharger, supprimer et modifier des informations sur les fichiers. Assignez ce rôle aux assistants administrateur chargés de la réplication de fichiers à partir du serveur d'administration primaire vers d'autres serveurs d'administration du MMS et sur les ordinateurs client DRA.

Réinitialiser le mot de passe d'administrateur local

Fournit tous les pouvoirs requis pour réinitialiser le mot de passe du compte d'administrateur local et pour afficher le nom de l'administrateur de l'ordinateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des comptes d'administrateur.

Réinitialiser le mot de passe

Fournit tous les pouvoirs requis pour réinitialiser et modifier des mots de passe. Assignez ce rôle aux assistants administrateur chargés de la gestion des mots de passe.

Réinitialiser le mot de passe et déverrouiller le compte à l'aide de SPA

Fournit tous les pouvoirs requis pour utiliser Secure Password Administrator (SPA) afin de réinitialiser des mots de passe et de déverrouiller des comptes utilisateur.

Réinitialiser les propriétés du code PIN de la messagerie unifiée

Fournit tous les pouvoirs requis pour réinitialiser les propriétés du code PIN de la messagerie unifiée pour les comptes utilisateur.

Administration des ressources

Fournit tous les pouvoirs requis pour modifier les propriétés des ressources gérées, y compris les ressources associées à n'importe quel compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de la gestion des objets Ressource.

Administration des boîtes aux lettres de ressources

Fournit tous les pouvoirs requis pour gérer les boîtes aux lettres de ressources.

Auto-administration

Fournit tous les pouvoirs requis pour modifier les propriétés de base, telles que les numéros de téléphone de votre propre compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de gérer leurs propres informations personnelles.

Administration des boîtes aux lettres partagées

Fournit tous les pouvoirs requis pour créer, modifier, supprimer et afficher les propriétés de vos boîtes aux lettres partagées. Assignez ce rôle à tous les assistants administrateur chargés de la gestion des boîtes aux lettres partagées.

Démarrer et arrêter les ressources

Fournit tous les pouvoirs requis pour démarrer, suspendre, reprendre ou arrêter un service, démarrer ou arrêter un périphérique ou une imprimante, arrêter un ordinateur ou synchroniser les contrôleurs de domaine. Fournit également tous les pouvoirs nécessaires pour démarrer, suspendre et reprendre des services, arrêter des périphériques ou des files d'attente d'impression et arrêter des ordinateurs. Assignez ce rôle aux assistants administrateur chargés de la gestion des objets Ressource.

Transformer un utilisateur

Fournit tous les pouvoirs requis pour ajouter un utilisateur à des groupes de compte de modèle, ou pour l'en supprimer, ainsi que les pouvoirs nécessaires pour modifier les propriétés de l'utilisateur lors de sa transformation.

Administration du serveur de l'historique des modifications unifiées

Fournit les pouvoirs requis pour configurer, consulter et supprimer des configurations de serveur de l'historique des modifications unifiées.

Administration des utilisateurs

Fournit tous les pouvoirs requis pour gérer les comptes utilisateur, les boîtes aux lettres Microsoft Exchange associées et les adhésions aux groupes. Assignez ce rôle aux assistants administrateur chargés de la gestion des comptes utilisateur.

Afficher les collecteurs Active Directory, les collecteurs DRA, les collecteurs de création de rapports de gestion et les informations de configuration de base de données

Fournit tous les pouvoirs requis pour afficher les collecteurs Active Directory, les collecteurs DRA, les collecteurs de création de rapports de gestion et les informations de configuration de base de données.

Afficher toutes les propriétés de l'ordinateur

Fournit tous les pouvoirs requis pour afficher les propriétés d'un compte d'ordinateur. Assignez ce rôle aux assistants administrateur chargés de l'audit des ordinateurs.

Afficher toutes les propriétés du groupe

Fournit tous les pouvoirs requis pour afficher les propriétés d'un groupe. Assignez ce rôle aux assistants administrateur chargés de l'audit des groupes.

Afficher toutes les propriétés de boîte aux lettres de ressource

Fournit tous les pouvoirs requis pour afficher les propriétés d'une boîte aux lettres de ressource. Assignez ce rôle aux assistants administrateur chargés de l'audit des boîtes aux lettres de ressources.

Afficher toutes les propriétés de l'utilisateur

Fournit tous les pouvoirs requis pour afficher les propriétés d'un compte utilisateur. Assignez ce rôle aux assistants administrateur chargés de l'audit des comptes utilisateur.

Administration des serveurs d'automatisation de workflow

Fournit les pouvoirs requis pour configurer, consulter et supprimer des configurations de serveurs d'automatisation de workflow.

Administration WTS

Fournit tous les pouvoirs requis pour gérer les propriétés de Windows Terminal Server (WTS) pour les comptes utilisateur dans l'instance Active Views. Si vous utilisez WTS, assignez ce rôle aux assistants administrateur chargés de la maintenance des propriétés WTS des comptes utilisateur.

Accès aux rôles intégrés

Accédez aux rôles intégrés pour auditer le modèle de délégation par défaut ou pour gérer vos propres paramètres de sécurité.

Pour accéder aux rôles intégrés :

- 1 Accédez à **Gestion de la délégation > Manage Roles** (Gérer les rôles).
- 2 Vérifiez que le champ de recherche est vide, puis cliquez sur **Rechercher maintenant** dans le volet **Lister les éléments qui répondent à mes critères**.
- 3 Sélectionnez le rôle approprié.

Utilisation de rôles intégrés

Vous ne pouvez pas supprimer ni modifier les rôles intégrés. En revanche, vous pouvez les insérer dans votre modèle de délégation existant ou les utiliser pour concevoir et implémenter votre propre modèle.

Vous pouvez employer des rôles intégrés comme suit :

- ♦ Associez un rôle intégré à un compte utilisateur ou un groupe AA. Cette association fournit à l'utilisateur ou aux membres du groupe AA les pouvoirs appropriés pour la tâche.
- ♦ Clonez un rôle intégré et utilisez ce clone comme base pour un rôle personnalisé. Vous pouvez ajouter à ce nouveau rôle d'autres pouvoirs ou rôles, tout comme vous pouvez supprimer des pouvoirs inclus initialement dans le rôle intégré.

Pour plus d'informations sur la conception d'un modèle de délégation dynamique, reportez-vous à la section [Présentation du modèle de délégation dynamique](#).

4.3.2 Création de rôles personnalisés

En créant un rôle, vous pouvez rapidement et facilement déléguer un ensemble de pouvoirs qui représente une tâche d'administration ou un workflow. Pour créer et gérer des rôles, accédez au noeud **Gestion de la délégation > Rôles** au niveau de la console de délégation et de configuration. Sur ce noeud, vous pouvez effectuer les opérations suivantes :

- ♦ Créer des rôles
- ♦ Cloner des rôles existants
- ♦ Modifier les propriétés de rôles
- ♦ Supprimer des rôles
- ♦ Gérer les assignations de rôles
 - ♦ Déléguer une nouvelle assignation
 - ♦ Supprimer une assignation existante
 - ♦ Afficher les propriétés d'un assistant administrateur assigné
 - ♦ Afficher les propriétés d'une instance Active Views assignée
- ♦ Gérer les rôles et les pouvoirs d'un rôle (les rôles peuvent être imbriqués)
- ♦ Générer des rapports sur les changements de rôles

Le workflow général pour exécuter une des actions identifiées dans cette section consiste à sélectionner le noeud **Rôles**, puis à effectuer l'une des opérations suivantes :

- ♦ Utilisez le menu **Tâches** ou le menu contextuel pour ouvrir l'assistant ou la boîte de dialogue applicable pour poursuivre l'action requise.
- ♦ Recherchez l'objet Rôle dans le volet **Lister les éléments qui répondent à mes critères**, puis utilisez le menu **Tâches** ou le menu contextuel pour sélectionner et ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre l'action requise.

Pour exécuter l'une des actions ci-dessus, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle Gérer le modèle de sécurité.

4.4 Pouvoirs

Les pouvoirs sont les composants de base de l'administration basée sur le principe du « privilège minimal ». L'assignation de pouvoirs aux utilisateurs vous aide à implémenter et à gérer votre modèle de sécurité dynamique. Vous effectuez ces procédures au niveau de la console de délégation et de configuration.

4.4.1 Pouvoirs intégrés

Lorsque vous définissez des rôles et effectuez des assignations de délégation, vous disposez de plus de 390 pouvoirs intégrés que vous pouvez utiliser pour gérer les objets et réaliser des tâches administratives courantes. Vous ne pouvez pas supprimer des pouvoirs intégrés, mais vous pouvez les cloner pour créer des pouvoirs personnalisés. Vous trouverez ci-dessous quelques exemples de pouvoirs intégrés :

Créer un groupe et modifier toutes les propriétés

Permet de créer des groupes et de spécifier toutes les propriétés lors de la création d'un groupe.

Supprimer le compte utilisateur

Si la corbeille est activée, permet de déplacer des comptes utilisateur vers la corbeille. Si la corbeille est désactivée, permet de supprimer définitivement des comptes utilisateur.

Modifiez toutes les propriétés de l'ordinateur

Permet de modifier toutes les propriétés des comptes d'ordinateur.

4.4.2 Implémentation de pouvoirs personnalisés

Pour créer un pouvoir personnalisé, vous devez d'abord créer un pouvoir ou cloner un pouvoir existant. Vous pouvez utiliser un pouvoir existant comme modèle pour de nouvelles délégations de pouvoirs. Un pouvoir définit les propriétés d'un objet qu'un assistant administrateur peut afficher, modifier ou créer dans votre domaine ou votre sous-arborescence gérée. Les pouvoirs personnalisés peuvent inclure un accès à de nombreuses propriétés, comme le pouvoir *Afficher toutes les propriétés de l'utilisateur*.

REMARQUE : il n'est pas possible de cloner tous les pouvoirs intégrés.

Vous implémentez des pouvoirs personnalisés à partir du noeud **Gestion de la délégation > Pouvoirs** au niveau de la console de délégation et de configuration. Sur ce noeud, vous pouvez effectuer les opérations suivantes :

- ♦ Afficher toutes les propriétés des pouvoirs
- ♦ Créer des pouvoirs
- ♦ Cloner des pouvoirs existants
- ♦ Modifier des pouvoirs personnalisés
- ♦ Générer des rapports sur les changements de pouvoirs

Pour effectuer l'une de ces actions, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle Gérer le modèle de sécurité.

Avant d'essayer de créer un pouvoir, suivez le processus ci-dessous.

1. Passez en revue les pouvoirs fournis avec DRA.
2. Décidez si vous avez besoin d'un pouvoir personnalisé. Le cas échéant, vous pouvez cloner un pouvoir personnalisé existant.
3. Effectuez les procédures appropriées présentées par un assistant. Par exemple, exécutez l'assistant New Power (Création d'un pouvoir).
4. Affichez votre nouveau pouvoir.
5. Modifiez votre nouveau pouvoir, si nécessaire.

Le workflow général pour exécuter une des actions identifiées dans cette section consiste à sélectionner le noeud **Pouvoirs**, puis à effectuer l'une des opérations suivantes :

- ♦ Utilisez le menu Tâches ou le menu contextuel pour ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre l'action requise.
- ♦ Recherchez l'objet Pouvoir dans le volet **Lister les éléments qui répondent à mes critères**, puis utilisez le menu **Tâches** ou le menu contextuel pour sélectionner et ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre l'action requise.

4.4.3 Extension des pouvoirs

Vous pouvez ajouter des autorisations ou des fonctionnalités à un pouvoir en étendant ce dernier.

Par exemple, pour permettre à un assistant administrateur de créer un compte utilisateur, vous pouvez assigner le pouvoir *Créer un utilisateur et modifier toutes les propriétés* ou le pouvoir *Créer un utilisateur et modifier des propriétés limitées*. Si vous assignez également le pouvoir *Ajouter un utilisateur au groupe*, l'assistant administrateur peut ajouter ce compte utilisateur à un groupe lors de l'utilisation de l'assistant de création d'un utilisateur. Dans ce cas, le pouvoir *Ajouter un utilisateur au groupe* fournit une fonction supplémentaire dans l'assistant. Le pouvoir *Ajouter un utilisateur au groupe* est le **pouvoir d'extension**.

Seuls, les pouvoirs d'extension ne permettent pas d'ajouter des autorisations ou des fonctionnalités. Pour déléguer une tâche qui inclut un pouvoir d'extension, vous devez assigner ce dernier en association avec le pouvoir que vous souhaitez étendre.

REMARQUE

- ♦ Pour pouvoir créer un groupe et l'inclure dans une instance Active Views, vous devez disposer du pouvoir *Ajouter un groupe à une instance Active Views* dans l'instance Active Views spécifiée. Celle-ci doit également inclure l'unité organisationnelle ou le conteneur intégré qui contiendra le nouveau groupe.
- ♦ Pour pouvoir cloner un groupe et l'inclure dans une instance Active Views, vous devez disposer du pouvoir *Ajouter un groupe cloné à une instance Active Views* dans l'instance Active Views spécifiée. Celle-ci doit également inclure le groupe source ainsi que l'unité organisationnelle ou le conteneur intégré qui contiendra le nouveau groupe.

Le tableau suivant répertorie quelques exemples d'actions qui peuvent être configurées lors de la création d'un pouvoir ou de la modification des propriétés d'un pouvoir existant :

Pour déléguer cette tâche	Assignez ce pouvoir...	Et ce pouvoir d'extension
Cloner un groupe et inclure ce nouveau groupe dans une instance Active Views spécifiée	Cloner le groupe et modifier toutes les propriétés	Ajouter le groupe cloné à une instance Active Views
Créer un groupe et inclure ce nouveau groupe dans une instance Active Views spécifiée	Créer un groupe et modifier toutes les propriétés	Ajouter un groupe à une instance Active Views
Créer un contact activé pour la messagerie	Créer un contact et modifier toutes les propriétés Créer un contact et modifier des propriétés limitées	Activer la messagerie pour le nouveau contact
Créer un groupe activé pour la messagerie	Créer un groupe et modifier toutes les propriétés	Activer la messagerie pour le nouveau groupe
Créer un compte utilisateur activé pour la messagerie	Créer un utilisateur et modifier toutes les propriétés Créer un utilisateur et modifier des propriétés limitées	Activer la messagerie pour le nouvel utilisateur

Pour déléguer cette tâche	Assignez ce pouvoir...	Et ce pouvoir d'extension
Créer un compte utilisateur et l'ajouter à des groupes spécifiques	Créer un utilisateur et modifier toutes les propriétés Créer un utilisateur et modifier des propriétés limitées	Ajouter un utilisateur au groupe

4.5 Assignations de délégations

Vous gérez les assignations de délégations à partir du noeud **Gestion de la délégation > Assistant administrateur** au niveau de la console de délégation et de configuration. Ce noeud vous permet d'afficher les pouvoirs et les rôles assignés aux assistants administrateur, ainsi que de gérer les assignations de rôles et d'instances Active Views. Vous pouvez également effectuer les opérations suivantes avec les groupes d'assistants administrateur (AA) :

- ♦ Ajouter des membres de groupe
- ♦ Créer des groupes
- ♦ Cloner des groupes
- ♦ Supprimer des groupes
- ♦ Modifier les propriétés de groupe

Pour afficher et gérer les assignations, et pour apporter des modifications aux groupes AA, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle Gérer le modèle de sécurité.

Le workflow général pour exécuter une des actions identifiées dans cette section consiste à sélectionner le noeud **Assistants administrateur**, puis à effectuer l'une des opérations suivantes :

- ♦ Utilisez le menu **Tâches** ou le menu contextuel pour ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre l'action requise.
- ♦ Recherchez le groupe ou l'assistant administrateur dans le volet **Lister les éléments qui répondent à mes critères**, puis utilisez le menu **Tâches** ou le menu contextuel pour sélectionner et ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre l'action requise.

5 Stratégie et automatisation des processus

Ce chapitre fournit des informations qui vous aident à comprendre le fonctionnement des stratégies dans l'environnement DRA et ce que représentent les options de stratégie. Il explique également comment les déclencheurs et le workflow automatisé permettent d'automatiser les processus lorsque vous travaillez avec des objets dans Active Directory.

5.1 Présentation de la stratégie DRA

DRA vous permet de configurer diverses stratégies qui aident à sécuriser votre entreprise et à éviter l'altération de données. Ces stratégies fonctionnent dans le cadre du modèle de sécurité dynamique, garantissant que l'application des stratégies s'adapte automatiquement à l'évolution de votre entreprise. L'établissement de stratégies, telles que des conventions de dénomination, des limites d'utilisation des disques et la validation de propriétés, vous permet d'appliquer des règles qui aident à maintenir l'intégrité des données de votre entreprise.

DRA vous permet de définir rapidement des règles de stratégie pour les domaines de gestion d'entreprise suivants :

- ♦ Microsoft Exchange
- ♦ Office 365
- ♦ Répertoire privé
- ♦ Génération de mot de passe

DRA fournit également des stratégies intégrées pour les groupes, les comptes utilisateur et les ordinateurs.

Pour gérer ou définir des stratégies, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans les rôles Administrateurs DRA ou Gérer les stratégies et les déclencheurs d'automatisation. Pour vous aider à gérer vos stratégies, DRA fournit le rapport Détails de la stratégie. Ce rapport contient les informations suivantes :

- ♦ Il indique si la stratégie est activée.
- ♦ Il liste les opérations associées.
- ♦ Il répertorie les objets gouvernés par cette stratégie.
- ♦ Il fournit des détails sur l'étendue de la stratégie.

Vous pouvez utiliser ce rapport pour vous assurer que vos stratégies sont définies correctement. Vous pouvez également employer ce rapport pour comparer les propriétés de stratégies, identifier les conflits et améliorer l'application des stratégies au sein de votre entreprise.

5.1.1 Application des stratégies par le serveur d'administration

Vous pouvez associer chaque tâche ou opération d'administration à une ou plusieurs stratégies. Lorsque vous effectuez une opération associée à une stratégie, le serveur d'administration exécute cette dernière et applique les règles spécifiées. Si le serveur détecte une violation de stratégie, il

renvoie un message d'erreur. Si le serveur ne détecte pas de violation de stratégie, il réalise l'opération. Vous pouvez limiter l'étendue d'une stratégie en l'associant à certains groupes d'assistants administrateur ou à des instances Active Views spécifiques.

Si une opération est associée à plusieurs stratégies, le serveur d'administration applique ces dernières selon l'ordre alphabétique. Autrement dit, la stratégie A est appliquée avant la stratégie B, quelles que soient les règles spécifiées.

Pour vous assurer que vos stratégies ne sont pas en conflit les unes avec les autres, utilisez les directives suivantes :

- ♦ Nommez les stratégies de sorte qu'elles s'exécutent dans l'ordre approprié.
- ♦ Vérifiez que chaque stratégie n'interfère pas avec des validations ou des actions effectuées par d'autres stratégies.
- ♦ Testez les stratégies personnalisées dans leur intégralité avant de les implémenter dans votre environnement de production.

À chaque exécution d'une stratégie, le serveur d'administration indique l'état de cette dernière dans le journal d'audit. Ces entrées de journal enregistrent le code de retour, les opérations associées, les objets concernés et si la stratégie personnalisée a réussi.

AVERTISSEMENT : les stratégies sont exécutées à l'aide du compte de service d'administration. Étant donné que le compte de service dispose des autorisations de niveau administrateur, les stratégies disposent d'un accès complet à toutes les données d'entreprise. Par conséquent, les assistants administrateur associés au rôle intégré Gérer les stratégies et les déclencheurs d'automatisation pourraient obtenir davantage de pouvoirs que prévu.

5.1.2 Stratégies intégrées

Des stratégies intégrées sont implémentées lorsque vous installez le serveur d'administration. Lorsque vous utilisez ces stratégies, vous pouvez rencontrer les termes suivants :

Étendue de la stratégie

Définit les objets ou les propriétés auxquels DRA applique la stratégie. Par exemple, certaines stratégies vous permettent de les appliquer à des assistants administrateur spécifiques dans des instances Active Views spécifiques. Certaines stratégies vous permettent de choisir parmi différentes classes d'objets, comme les comptes utilisateur ou les groupes.

Stratégies globales

Appliquent leurs règles à tous les objets de la classe ou du type spécifié dans les domaines gérés. Les stratégies globales ne permettent pas de limiter l'étendue des objets auxquels s'applique la stratégie.

Relation de la stratégie

Définit si la stratégie s'applique avec d'autres ou par elle-même. Pour établir une relation de stratégie, définissez au moins deux règles qui s'appliquent à la même action, puis choisissez le membre d'une option de groupe de stratégies. Si la propriété ou les paramètres de l'opération correspondent à l'une des règles, l'opération réussit.

Présentation des stratégies intégrées

Les stratégies intégrées proposent des règles d'entreprise répondant aux problèmes courants de sécurité et d'intégrité des données. Ces stratégies font partie du modèle de sécurité par défaut, ce qui vous permet d'intégrer des fonctions de sécurité DRA dans votre configuration d'entreprise existante.

DRA permet d'appliquer des stratégies de deux manières. Vous pouvez créer des stratégies personnalisées ou choisir parmi plusieurs stratégies intégrées. Les stratégies intégrées permettent d'appliquer facilement une stratégie, sans devoir développer des scripts personnalisés. Si vous devez implémenter une stratégie personnalisée, vous pouvez adapter une stratégie intégrée existante pour répondre à vos besoins. La plupart des stratégies vous permettent de modifier le texte du message d'erreur, de renommer la stratégie, d'ajouter une description et de spécifier le mode d'application de la stratégie.

Plusieurs stratégies intégrées sont activées lorsque vous installez DRA. Les stratégies suivantes sont implémentées par défaut. Si vous ne souhaitez pas appliquer ces stratégies, vous pouvez les désactiver ou les supprimer.

Nom de la stratégie	Valeur par défaut	Description
\$ComputerNameLengthPolicy	64 15 (versions antérieures à Windows 2000)	Limite le nombre de caractères dans le nom de l'ordinateur ou le nom de l'ordinateur de version antérieure à Windows 2000.
\$GroupNameLengthPolicy	64 20 (versions antérieures à Windows 2000)	Limite le nombre de caractères dans le nom du groupe ou le nom du groupe de version antérieure à Windows 2000.
\$GroupSizePolicy	5000	Limite le nombre de membres dans un groupe.
\$NameUniquenessPolicy	Aucune	Vérifie que les noms CN et ceux antérieurs à Windows 2000 sont uniques dans tous les domaines gérés.
\$SpecialGroupsPolicy	Aucune	Empêche l'escalade non contrôlée de pouvoirs dans l'environnement.
\$UCPowerConflictPolicy	Aucune	Empêche l'escalade de pouvoirs en définissant les pouvoirs Cloner un utilisateur et Créer un utilisateur comme s'excluant mutuellement.
\$UPNUniquenessPolicy	Aucune	Vérifie que les noms UPN sont uniques dans tous les domaines gérés.
\$UserNameLengthPolicy	64 20 (nom de connexion de bas niveau)	Limite le nombre de caractères dans le nom de connexion de l'utilisateur ou le nom de connexion de bas niveau.

Stratégies disponibles

DRA fournit plusieurs stratégies que vous pouvez personnaliser pour votre modèle de sécurité.

REMARQUE : vous pouvez créer une stratégie qui requiert une entrée pour une propriété non disponible actuellement à partir des interfaces utilisateur de DRA. Si une entrée est requise par la stratégie et si l'interface utilisateur ne fournit pas un champ pour spécifier la valeur (par exemple, un service pour le nouveau compte utilisateur), vous ne serez pas en mesure de créer ni de gérer l'objet. Pour éviter ce problème, configurez des stratégies qui exigent uniquement des propriétés accessibles à partir des interfaces utilisateur.

Créer une stratégie personnalisée

Permet de lier un script ou un exécutable à une opération DRA ou Exchange. Les stratégies personnalisées vous permettent de valider toutes les opérations que vous choisissez.

Appliquer une longueur de nom maximale

Permet d'appliquer de manière globale une longueur de nom maximale pour les comptes utilisateur, les groupes, les unités organisationnelles, les contacts ou les ordinateurs.

La stratégie vérifie le conteneur de noms (nom commun ou `cn`) et le nom pour les versions antérieures à Windows 2000 (nom de connexion de l'utilisateur).

Appliquer un nombre maximal de membres de groupe

Permet d'appliquer de manière globale les limites quant au nombre de membres dans un groupe.

Appliquer des noms de compte uniques antérieurs à Windows 2000

Vérifie qu'un nom dans une version antérieure à Windows 2000 est unique sur l'ensemble des domaines gérés. Dans les domaines Microsoft Windows, les noms dans les versions antérieures à Windows 2000 doivent être uniques au sein d'un domaine. Cette stratégie globale applique cette règle sur l'ensemble des domaines gérés.

Appliquer des UPN uniques

Vérifie qu'un nom de principal de type utilisateur (User Principal Name, UPN) est unique sur l'ensemble des domaines gérés. Dans les domaines Microsoft Windows, les UPN doivent être uniques au sein d'un domaine. Cette stratégie applique cette règle sur l'ensemble des domaines gérés. Étant donné qu'il s'agit d'une stratégie globale, DRA fournit le nom de la stratégie, sa description et sa relation.

Limiter les actions sur les membres de groupes spéciaux

Empêche un utilisateur de gérer des membres d'un groupe d'administrateurs, excepté s'il est lui-même membre de ce groupe d'administrateurs. Cette stratégie globale est activée par défaut.

Lorsque vous limitez les actions sur les membres des groupes d'administrateurs, l'assistant Create Policy (Créer une stratégie) ne nécessite pas d'informations supplémentaires. Vous pouvez spécifier un message d'erreur personnalisé. Étant donné qu'il s'agit d'une stratégie globale, DRA fournit le nom de la stratégie, sa description et sa relation.

Empêcher les assistants administrateur de créer et de cloner des utilisateurs dans la même instance Active Views

Empêche l'éventuelle escalade des pouvoirs. Lorsque cette stratégie est activée, vous pouvez créer des comptes utilisateur ou en cloner, mais vous ne pouvez pas disposer des deux pouvoirs. Cette stratégie globale évite qu'un utilisateur puisse à la fois créer et cloner des comptes utilisateur dans la même instance Active Views.

Cette stratégie ne nécessite pas d'informations supplémentaires.

Définir la stratégie de convention de dénomination

Permet d'établir des conventions de dénomination qui s'appliquent à des assistants administrateur, des instances Active Views et des classes d'objets spécifiques, comme des comptes utilisateur ou des groupes.

Vous pouvez également spécifier les noms exacts contrôlés par cette stratégie.

Créer une stratégie pour valider une propriété spécifique

Permet de créer une stratégie pour valider une propriété, une unité organisationnelle ou un objet Compte. Vous pouvez spécifier une valeur par défaut, un masque de format de propriété ainsi que des valeurs et plages valides.

Utilisez cette stratégie pour appliquer l'intégrité des données en validant des champs d'entrée particuliers lorsque vous créez, clonez ou modifiez les propriétés d'objets spécifiques. Cette stratégie offre une flexibilité exceptionnelle et permet de valider des entrées, de spécifier des entrées par défaut et de limiter les choix d'entrée pour différents champs de propriétés. À l'aide de cette stratégie, vous pouvez exiger qu'une entrée correcte soit spécifiée avant que la tâche soit effectuée. De cette façon, vous préservez l'intégrité des données sur l'ensemble de vos domaines gérés.

Supposons, par exemple, que vous avez trois services : Manufacturing, Sales et Administration. Vous pouvez limiter les entrées que DRA acceptera à ces trois valeurs uniquement. Vous pouvez également utiliser cette stratégie pour appliquer les formats de numéro de téléphone appropriés, fournir une plage de données valides ou exiger une entrée pour le champ d'adresse électronique. Pour spécifier plusieurs masques de format pour un numéro de téléphone, comme (123)456 7890 et 456 7890, définissez le masque de format de propriété (###)### ####,### ####.

Créer une stratégie pour appliquer les licences Office 365

Permet de créer une stratégie pour assigner les licences Office 365 en fonction de l'adhésion au groupe Active Directory. Cette stratégie applique également le retrait des licences Office 365 lorsqu'un membre est supprimé du groupe Active Directory concerné.

Si un utilisateur qui n'est pas synchronisé avec le cloud est ajouté au groupe Active Directory, cet utilisateur est synchronisé avant qu'une licence Office 365 lui soit assignée.

Lors de la création de la stratégie, vous pouvez spécifier plusieurs propriétés et paramètres, tels que le nom de la stratégie et le texte du message d'erreur qui apparaît lorsqu'un assistant administrateur tente une action qui viole cette stratégie.

Par défaut, les stratégies que vous créez pour appliquer les licences Office 365 ne sont pas appliquées lorsque des modifications sont apportées en dehors de DRA, excepté si vous activez également la planification de la mise à jour des licences sur la page des propriétés du locataire.

Utilisation des stratégies intégrées

Étant donné que les stratégies intégrées font partie intégrante du modèle de sécurité par défaut, vous pouvez les utiliser pour appliquer votre modèle de sécurité actuel ou les modifier pour mieux répondre à vos besoins. Vous pouvez modifier le nom, les paramètres de règle, l'étendue, la relation et le message d'erreur de plusieurs stratégies intégrées. Vous pouvez activer ou désactiver chaque stratégie intégrée.

Vous pouvez aussi facilement créer des stratégies.

5.1.3 Implémentation d'une stratégie personnalisée

Les stratégies personnalisées permettent de tirer pleinement parti de la puissance et de la flexibilité du modèle de sécurité par défaut. Grâce à l'utilisation de stratégies personnalisées, vous pouvez intégrer DRA aux composants d'entreprise existants, tout en garantissant l'application de vos règles propriétaires. Vous pouvez utiliser la fonction de personnalisation de stratégie pour étendre vos stratégies d'entreprise.

Vous créez et appliquez des stratégies personnalisées en associant un fichier exécutable ou un script avec une opération d'administration. Par exemple, un script de stratégie associé avec l'opération `UserCreate` pourrait vérifier votre base de données des ressources humaines afin de vérifier si l'employé spécifié existe. Si ce dernier existe bien dans la base de données et ne dispose pas d'un compte existant, le script récupère l'ID de l'employé, son prénom et son nom à partir de la base de données. L'opération aboutit et remplit la fenêtre des propriétés du compte utilisateur avec les informations appropriées. En revanche, si l'employé possède déjà un compte, l'opération échoue.

Les scripts représentent une source de flexibilité et de puissance considérable. Pour créer vos propres scripts de stratégie, vous pouvez utiliser le fournisseur ADSI de DRA, un SDK (Software Development Kit) et des applets de commande (cmdlets) PowerShell. Pour plus d'informations sur la création de vos propres scripts de stratégie, reportez-vous à la section Référence (Référence) sur le [site de documentation de DRA](#).

5.1.4 Restriction des groupes de sécurité intégrés natifs

Pour sécuriser davantage votre environnement, DRA permet de limiter les pouvoirs octroyés aux groupes de sécurité intégrés de Microsoft Windows. La possibilité de modifier l'adhésion à un groupe, les propriétés des groupes de sécurité intégrés ou les propriétés des membres de groupes peut avoir des implications importantes en termes de sécurité. Par exemple, si vous pouvez modifier le mot de passe d'un utilisateur dans le groupe Opérateurs de serveur, vous pouvez ensuite vous connecter sous l'identité de cet utilisateur et exercer les pouvoirs délégués à ce groupe de sécurité intégré.

Pour éviter ce problème de sécurité, DRA fournit une stratégie qui vérifie les pouvoirs dont vous disposez pour un groupe de sécurité intégré natif et ses membres. Cette validation vérifie que les actions demandées n'augmentent pas ces pouvoirs. Une fois cette stratégie activée, un assistant administrateur qui est membre d'un groupe de sécurité intégré, tel que le groupe Opérateurs de serveur, ne peut gérer que les autres membres du même groupe.

Groupes de sécurité intégrés natifs pouvant être restreints

Vous pouvez limiter les pouvoirs des groupes de sécurité intégrés de Microsoft Windows suivants à l'aide de stratégies DRA :

- ♦ Opérateurs de compte
- ♦ Administrateurs
- ♦ Opérateurs de sauvegarde
- ♦ Éditeurs de certificats
- ♦ Administrateurs DNS
- ♦ Administrateurs de domaine
- ♦ Administrateurs d'entreprise
- ♦ Propriétaires de créateur de stratégie de groupe
- ♦ Opérateurs d'impression
- ♦ Administrateurs de schéma

REMARQUE : DRA fait référence aux groupes de sécurité intégrés par leur identificateur interne. Par conséquent, il prend en charge ces groupes même s'ils sont renommés. Cette fonction permet à DRA de prendre en charge des groupes de sécurité intégrés portant des noms différents selon les pays. Par exemple, DRA fait référence aux groupes Administrators et *Administrateurs* avec le même identificateur interne.

Restriction des actions sur les groupes de sécurité intégrés natifs

DRA utilise une stratégie pour limiter les pouvoirs que les groupes de sécurité intégrés natifs et leurs membres peuvent exercer. Cette stratégie, nommée `$SpecialGroupsPolicy`, limite les actions qu'un membre d'un groupe de sécurité intégré natif peut effectuer sur d'autres membres ou d'autres groupes de sécurité intégrés natifs. DRA active cette stratégie par défaut. Si vous ne souhaitez pas limiter les actions sur les groupes de sécurité intégrés natifs et leurs membres, vous pouvez désactiver cette stratégie.

Lorsque cette stratégie est activée, DRA utilise les tests de validation suivants pour déterminer si une action est autorisée sur un groupe de sécurité intégré natif ou ses membres :

- ♦ Si vous êtes un administrateur Microsoft Windows, vous pouvez effectuer des actions sur les groupes de sécurité intégrés natifs et leurs membres pour lesquels vous disposez des pouvoirs appropriés.
- ♦ Si vous êtes membre d'un groupe de sécurité intégré, vous pouvez effectuer des actions sur le même groupe de sécurité intégré et ses membres, pour autant que vous possédiez les pouvoirs appropriés.
- ♦ Si vous n'êtes pas membre d'un groupe de sécurité intégré, vous ne pouvez pas modifier un groupe de sécurité intégré ni ses membres.

Par exemple, si vous êtes membre des groupes Opérateurs de serveur et Opérateurs de compte et que vous disposez des pouvoirs appropriés, vous pouvez effectuer des actions sur les membres du groupe Opérateurs de serveur, les membres du groupe Opérateurs de compte ou les membres de ces deux groupes. En revanche, vous ne pouvez pas effectuer des actions sur un compte utilisateur qui est à la fois membre du groupe Opérateurs d'impression et du groupe Opérateurs de compte.

DRA vous empêche d'effectuer les actions suivantes sur les groupes de sécurité intégrés natifs :

- ♦ Clonage d'un groupe
- ♦ Création d'un groupe
- ♦ Suppression d'un groupe
- ♦ Ajout d'un membre à un groupe
- ♦ Suppression d'un membre d'un groupe
- ♦ Déplacement d'un groupe vers une unité organisationnelle
- ♦ Modification des propriétés d'un groupe
- ♦ Copie d'une boîte aux lettres
- ♦ Suppression d'une boîte aux lettres
- ♦ Clonage d'un compte utilisateur
- ♦ Création d'un compte utilisateur
- ♦ Suppression d'un compte utilisateur
- ♦ Déplacement d'un compte utilisateur vers une unité organisationnelle
- ♦ Modification des propriétés d'un compte utilisateur

DRA limite également les actions de sorte que vous ne puissiez pas acquérir des pouvoirs sur un objet. Par exemple, lorsque vous ajoutez un compte utilisateur à un groupe, DRA vérifie que cela ne vous octroie pas des pouvoirs supplémentaires sur le compte utilisateur parce qu'il est membre de ce groupe. Cette validation aide à protéger contre une escalade des pouvoirs.

5.1.5 Gestion des stratégies

Le noeud Gestion des stratégies et de l'automatisation vous permet d'accéder aux stratégies Microsoft Exchange et de répertoire privé, ainsi qu'aux stratégies intégrées et personnalisées. Pour améliorer la sécurité de votre entreprise et l'intégrité de vos données, utilisez les tâches courantes suivantes.

Configurer des stratégies Exchange

Permet de définir des règles de configuration de Microsoft Exchange, de stratégie de boîte aux lettres, de dénomination automatique et de génération de proxy. Ces règles peuvent définir la façon dont les boîtes aux lettres sont gérées lorsqu'un assistant administrateur crée, modifie ou supprime un compte utilisateur.

Configurer des stratégies Office 365

Permet d'appliquer des stratégies concernant les caractères qui ne sont pas valides et le nombre de caractères autorisés pour éviter les échecs de synchronisation des répertoires.

Les règles Office 365 permettent de spécifier la façon dont Exchange Online prend en charge les boîtes aux lettres Office 365 lorsque vous créez ou supprimez des comptes utilisateur.

Configurer des stratégies de répertoire privé

Permet de créer, de renommer ou de supprimer automatiquement des répertoires et partages privés lorsqu'un assistant administrateur crée, renomme ou supprime un compte utilisateur. Les stratégies de répertoire privé permettent également d'activer ou de désactiver la prise en charge de quotas de disques pour les répertoires privés sur des serveurs Microsoft Windows, ainsi que sur des serveurs non-Windows.

Configurer des stratégies de génération de mot de passe

Permet de définir les exigences pour les mots de passe générés par DRA.

Stratégies Microsoft Exchange

Exchange fournit plusieurs stratégies qui vous aident à gérer efficacement les objets Microsoft Exchange. Les stratégies Microsoft Exchange permettent d'automatiser la gestion des boîtes aux lettres, d'appliquer des conventions de dénomination pour les alias et les banques de boîtes aux lettres, et de générer automatiquement des adresses électroniques.

Ces stratégies peuvent vous aider à rationaliser vos workflows et à préserver l'intégrité des données. Par exemple, vous pouvez spécifier la façon dont Exchange gère les boîtes aux lettres lorsque vous créez, modifiez ou supprimez des comptes utilisateur. Pour définir et gérer des stratégies Microsoft Exchange, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation.

Spécification d'une stratégie d'adresse électronique par défaut

Pour spécifier une stratégie d'adresse électronique par défaut, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation, et votre licence doit prendre en charge le produit Exchange.

Pour spécifier une stratégie d'adresse électronique par défaut :

- 1 Accédez à **Gestion des stratégies et de l'automatisation > Configure Exchange Politiques** (Configurer les stratégies Exchange) -> **Proxy Generation** (Génération de proxy).
- 2 Spécifiez le domaine du serveur Microsoft Exchange.
 - 2a Cliquez sur **Parcourir**.
 - 2b Spécifiez des critères de recherche supplémentaires selon vos besoins, puis cliquez sur **Rechercher maintenant**.
 - 2c Sélectionnez le domaine à configurer, puis cliquez sur **OK**.
- 3 Spécifiez les règles de génération de proxy pour le domaine sélectionné.
 - 3a Cliquez sur **Ajouter**.
 - 3b Sélectionnez un type de proxy. Par exemple, cliquez sur **Adresse Internet**.
 - 3c Acceptez la valeur par défaut ou saisissez une nouvelle règle de génération de proxy, puis cliquez sur **OK**.

Pour plus d'informations sur les chaînes de substitution prises en charge pour les règles de génération de proxy, reportez-vous à la section [Stratégie du client de délégation et de configuration](#).
- 4 Cliquez sur **Attributs personnalisés** pour modifier le nom personnalisé des propriétés de boîtes aux lettres personnalisées.
 - 4a Sélectionnez l'attribut, puis cliquez sur le bouton **Modifier**.
 - 4b Dans la fenêtre Attribute Properties (Propriétés de l'attribut), entrez le nom de l'attribut dans le champ **Custom name** (Nom personnalisé), puis cliquez sur **OK**.
- 5 Cliquez sur **OK**.

REMARQUE : les administrateurs des stratégies DRA doivent avoir le pouvoir *Gérer les outils personnalisés* pour pouvoir modifier les attributs personnalisés dans la stratégie Microsoft Exchange.

Règles de boîte aux lettres

Les règles de boîte aux lettres permettent de spécifier la façon dont Exchange gère les boîtes aux lettres lorsque les assistants administrateur créent, clonent, modifient ou suppriment des comptes utilisateur. Les règles de boîte aux lettres gèrent automatiquement les boîtes aux lettres Microsoft Exchange en fonction de la manière dont les assistants administrateur gèrent les comptes utilisateur associés.

REMARQUE : si vous activez l'option **Do not allow Assistant Admins to create a user account without a mailbox** (Ne pas autoriser les assistants administrateur à créer un compte utilisateur sans boîte aux lettres) dans les domaines Microsoft Windows, vérifiez que les assistants administrateur ont le pouvoir de cloner ou de créer un compte utilisateur. L'activation de cette option impose aux assistants administrateur de créer des comptes utilisateur Windows avec une boîte aux lettres.

Pour spécifier des règles de boîte aux lettres Microsoft Exchange, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation, et votre licence doit prendre en charge le produit Exchange.

Pour spécifier des règles de boîte aux lettres Exchange :

- 1 Accédez à **Gestion des stratégies et de l'automatisation > Configure Exchange Policies** (Configurer des stratégies Exchange) > **Mailbox Rules** (Règles de boîte aux lettres).
- 2 Sélectionnez les stratégies de boîte aux lettres qu'Exchange doit appliquer lorsque vous créez ou modifiez des comptes utilisateur.
- 3 Cliquez sur **OK**.

Stratégies Office 365

Pour spécifier des stratégies de boîte aux lettres Office 365, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation. Votre licence doit également prendre en charge le produit Microsoft Exchange.

Pour définir des caractères non valides et des longueurs requises avec des propriétés qui assurent une synchronisation avec Office 365, cliquez sur **Office 365 Rules** (Règles Office 365), puis cochez la case **Enforce online mailbox policies for invalid characters and character lengths** (Appliquer des stratégies de boîte aux lettres en ligne pour les caractères non valides et les longueurs requises).

Autorisation de DRA à gérer vos licences Office 365 (facultatif)

Si vous souhaitez autoriser DRA à gérer vos licences Office 365, vous devez effectuer les opérations suivantes :

- ♦ Créez une stratégie d'application des licences.
- ♦ Activez l'option **License update schedule** (Planification de la mise à jour des licences) sur la page des propriétés du locataire.

Création d'une stratégie pour appliquer les licences Office 365

Pour créer une stratégie afin d'appliquer les licences Office 365, cliquez sur le noeud **Gestion des stratégies et de l'automatisation** au niveau de la console de délégation et de configuration, puis sélectionnez **New Policy > Create New Policy to Enforce Office 365 Licenses** (Nouvelle stratégie > Créer une stratégie pour appliquer les licences Office 365).

Une fois la stratégie appliquée et un utilisateur ajouté à Active Directory, DRA utilise l'adhésion au groupe pour assigner automatiquement la licence Office 365 à l'utilisateur.

Planification de la mise à jour des licences Office 365

Les stratégies que vous créez pour appliquer les licences Office 365 ne sont pas appliquées lorsque des modifications sont apportées en dehors de DRA, excepté si vous activez également l'option **Planification de la mise à jour des licences** (Planification de la mise à jour des licences) sur la page des propriétés du locataire. Le travail de mise à jour des licences garantit que les licences Office 365 assignées à des utilisateurs respectent vos stratégies de licences Office 365.

Le travail de mise à jour des licences et les stratégies de licences Office 365 interagissent de manière à vous assurer que tous les utilisateurs gérés sont assignés uniquement aux licences Office 365 dont ils sont supposés disposer.

REMARQUE

- ♦ DRA ne gère pas les licences Office 365 pour les comptes utilisateur en ligne uniquement. Pour que DRA gère vos utilisateurs avec des licences Office 365, ces derniers doivent être synchronisés avec Active Directory.
 - ♦ Si vous choisissez d'utiliser DRA pour gérer vos licences Office 365, lors de la prochaine exécution du travail de mise à jour des licences, DRA ignorera toutes les modifications manuelles apportées aux licences Office 365 en dehors de DRA.
 - ♦ Si vous activez le travail de mise à jour des licences Office 365 avant de vérifier que vos stratégies de licences Office 365 sont correctement configurées, il se peut que vos licences assignées soient incorrectes une fois le travail de mise à jour des licences exécuté.
-

Création et implémentation de stratégies de répertoire privé

Lorsque vous gérez un grand nombre de comptes utilisateur, la création et la maintenance de ces répertoires et partages privés peuvent nécessiter beaucoup de temps et être sources d'erreurs en termes de sécurité. Des opérations supplémentaires peuvent être nécessaires à chaque fois qu'un utilisateur est créé, renommé ou supprimé. Les stratégies de répertoire privé vous aident à gérer la maintenance des répertoires et partages privés.

DRA vous permet d'automatiser la création et la maintenance des répertoires privés des utilisateurs. Par exemple, vous pouvez facilement configurer DRA afin que le serveur d'administration crée un répertoire privé lorsque vous créez un compte utilisateur. Dans ce cas, si vous spécifiez un chemin de répertoire privé lors de la création du compte utilisateur, le serveur crée automatiquement le répertoire privé à l'emplacement spécifié. Si vous ne spécifiez pas de chemin, le serveur ne crée pas le répertoire privé.

DRA prend en charge les chemins DFS (Distributed File System) lors de la création de répertoires privés des utilisateurs ou lors de la configuration des stratégies de répertoire privé pour les utilisateurs dans des chemins parents autorisés. Vous pouvez créer, renommer et supprimer des répertoires privés sur les partitions ou dans les chemins DFS et de serveurs de fichiers Netapp.

Configuration de stratégies de répertoire privé

Pour configurer des stratégies de quota de disque de partage de volumes, de partages et de répertoires privés, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation. Chaque stratégie gère automatiquement les répertoires, partages et quotas de disques de volume privés en fonction de la manière dont vous gérez les comptes utilisateur associés.

Pour configurer des stratégies de répertoire privé, accédez à **Gestion des stratégies et de l'automatisation > Configure Home Directory Policies** (Configurer des stratégies de répertoire privé) >.

- ♦ Répertoire privé
- ♦ Partage privé
- ♦ Quota de disque de volume privé

Configuration requise pour le serveur d'administration

Pour chaque ordinateur sur lequel vous devez créer un partage privé, le compte de service ou d'accès du serveur d'administration doit être un administrateur sur cet ordinateur ou un membre du groupe Administrateurs du domaine correspondant.

Un partage d'administration, tel que C\$ ou D\$, doit exister pour chaque unité sur laquelle DRA gère et stocke des répertoires privés. DRA utilise les partages d'administration pour effectuer certaines tâches d'automatisation concernant les partages et répertoires privés. Si ces partages n'existent pas, DRA ne peut pas assurer l'automatisation des partages et répertoires privés.

Configuration des chemins de répertoire privé autorisés pour les serveurs de fichiers NetApp

Pour configurer les chemins parents autorisés pour un serveur de fichiers NetApp :

- 1 Accédez à **Gestion des stratégies et de l'automatisation > Configure Home Directory Policies** (Configurer des stratégies de répertoire privé).
- 2 Dans la zone de texte **Allowable parent paths** (Chemins parents autorisés), entrez un des chemins autorisés figurant dans le tableau suivant :

Type de partage	Chemin autorisé
Windows	(\\Nom_fichier\Partage_administration:\chemin_racine_volume\chemin_répertoire)
Non-Windows	(\\non-windows\partage)

- 3 Cliquez sur **Ajouter**.
- 4 Répétez les étapes 1 à 3 pour chaque chemin parent autorisé où vous souhaitez appliquer les stratégies de répertoire privé.

Présentation des stratégies de répertoire privé

Pour garantir la cohérence avec les stratégies de sécurité de Microsoft Windows, DRA crée des restrictions de contrôle d'accès au niveau du répertoire uniquement. En effet, la définition de restrictions de contrôle d'accès à la fois au niveau du nom du partage et de l'objet Répertoire se traduit souvent par un schéma d'accès ambigu pour les administrateurs et les utilisateurs.

Lorsque vous modifiez une restriction de contrôle d'accès pour un partage privé, DRA ne modifie pas la sécurité existante pour ce répertoire. Dans ce cas, vous devez vous assurer que les comptes utilisateur disposent de l'accès approprié à leur propre répertoire privé.

Automatisation et règles des répertoires privés

DRA automatise les tâches de maintenance des répertoires privés en gérant ces derniers lorsque vous modifiez un compte utilisateur. DRA peut effectuer des actions différentes lorsqu'un compte utilisateur est créé, cloné, modifié, renommé ou supprimé.

Pour implémenter efficacement votre stratégie de répertoire privé, tenez compte des directives suivantes :

- ♦ Vérifiez que le chemin spécifié utilise le bon format.
 - ♦ Pour spécifier un chemin pour un répertoire privé unique, utilisez l'un des modèles du tableau suivant :

Type de partage	Modèle de chemin
Windows	<p><code>\\ordinateur\partage\.</code></p> <p>Par exemple, si vous souhaitez que DRA crée automatiquement un répertoire privé dans le dossier Home Share (Partage privé) sur l'ordinateur serveur01, tapez <code>\\serveur01\Home Share\.</code></p>
Non-Windows	<code>\\non-windows\partage</code>

- ◆ Afin d'harmoniser l'administration de répertoire privé dans le répertoire racine du partage privé correspondant, utilisez la syntaxe de la convention universelle de dénomination, telle que `\\nom_serveur\C:\chemin_répertoire_racine`.
- ◆ Pour spécifier un chemin pour des répertoires privés imbriqués, utilisez l'un des modèles du tableau suivant :

Type de partage	Modèle de chemin
Windows	<p><code>\\ordinateur\partage\premier_répertoire\deuxième_répertoire\</code></p> <p>Par exemple, si vous souhaitez que DRA crée automatiquement un répertoire privé dans le répertoire existant JSmith\Home sous le dossier Home Share sur l'ordinateur serveur01, tapez <code>\\server01\Home Share\JSmith\Home</code>.</p>
Non-Windows	<code>\\non-windows\partage\premier_répertoire\deuxième_répertoire\</code>

REMARQUE : DRA prend également en charge les formats suivants :

`\\ordinateur\partage\nom_utilisateur` et `\\ordinateur\partage\%nom_utilisateur%`. Dans chaque cas, DRA crée automatiquement un répertoire privé pour le compte utilisateur associé.

- ◆ Lorsque vous définissez une stratégie ou un déclencheur d'automatisation pour gérer des répertoires privés sur un serveur de fichiers NetApp, vous devez utiliser un format différent pour la spécification du répertoire.
 - ◆ Si vous utilisez des serveurs de fichiers NetApp, indiquez le répertoire parent au format suivant :
`\\serveur_fichiers\partage_administration:\chemin_racine_volume\chemin_répertoire`
 - ◆ La variable `partage_administration` correspond au partage masqué assigné au volume racine sur le serveur de fichiers NetApp, tel que `c$`. Par exemple, si le chemin local du partage sur un serveur de fichiers NetApp, appelé `usfiler`, est `c$\vol\vol0\monrépertoire`, vous pouvez spécifier un chemin racine `\\usfiler\c:\vol\vol0\monrépertoire` pour le serveur de fichiers NetApp.
- ◆ Pour spécifier un chemin DFS lorsque vous créez des répertoires privés d'utilisateurs ou lorsque vous configurez des stratégies de répertoire privé pour des utilisateurs, employez `\\serveur\racine\<lien> format`, où la racine peut être le domaine géré ou un répertoire racine autonome au format suivant :
`\\nom_serveur_fichiers\partage_administration:\chemin_racine_volume\chemin_répertoire`.

- ♦ Créez un répertoire partagé pour stocker le répertoire privé de ce compte utilisateur.
- ♦ Assurez-vous que DRA peut accéder à l'ordinateur ou au partage référencé dans le chemin.

Créer un répertoire privé lors de la création d'un compte utilisateur

Cette règle permet à DRA de créer automatiquement des répertoires privés pour les nouveaux comptes utilisateur. Lorsque DRA crée un répertoire privé, le serveur d'administration utilise le chemin spécifié dans le champ **Répertoire privé** de l'assistant Créer un utilisateur. Vous pouvez modifier ce chemin ultérieurement via l'onglet Profil de la fenêtre Propriétés de l'utilisateur. DRA déplacera alors le répertoire privé vers le nouvel emplacement. Si vous ne spécifiez pas de valeur dans ce champ, DRA ne crée pas de répertoire privé pour ce compte utilisateur.

DRA définit la sécurité du nouveau répertoire en fonction des options **Autorisations de répertoire privé**. Ces options vous permettent de contrôler l'accès général de tous les répertoires privés.

Par exemple, vous pouvez spécifier que les membres du groupe Administrateurs disposent d'un contrôle complet et que les membres du groupe Service d'assistance ont un accès en lecture au partage dans lequel les répertoires privés des utilisateurs sont créés. Ensuite, lorsque DRA crée un répertoire privé d'utilisateur, ce nouveau répertoire privé peut hériter ces droits à partir du répertoire parent. Par conséquent, les membres du groupe Administrateurs ont un contrôle total sur tous les répertoires privés des utilisateurs et les membres du groupe Service d'assistance y ont accès en lecture seule.

Si le répertoire privé spécifié existe déjà, DRA ne le crée pas et ne modifie pas ses autorisations.

Renommer un répertoire privé lorsque le compte utilisateur est renommé

Cette règle permet à DRA d'effectuer automatiquement les actions suivantes :

- ♦ Il crée un répertoire privé lorsque vous spécifiez un nouveau chemin de répertoire privé.
- ♦ Il déplace le contenu du répertoire privé lorsque vous modifiez le chemin de ce dernier.
- ♦ Il renomme un répertoire privé lorsque vous renommez le compte utilisateur.

Lorsque vous renommez un compte utilisateur, DRA renomme le répertoire privé existant sur la base du nouveau nom de compte. Si le répertoire privé existant est en cours d'utilisation, DRA crée un répertoire privé avec le nouveau nom et ne modifie pas le répertoire privé existant.

Vous pouvez renommer le répertoire privé si le nom et l'emplacement du répertoire privé précédent et du nouveau répertoire privé sont identiques. Toutefois, si l'attribution du nouveau nom échoue, DRA crée un répertoire privé, déplace le contenu du répertoire privé précédent vers le nouveau, puis supprime le répertoire privé existant.

Lorsque vous modifiez le chemin du répertoire privé, DRA tente de créer le répertoire privé spécifié et de déplacer le contenu du répertoire privé précédent vers le nouvel emplacement. Vous pouvez également configurer la stratégie de répertoire privé pour créer un répertoire privé sans déplacer le contenu du répertoire privé existant. DRA applique également les listes de contrôle d'accès (ACL) assignées du répertoire précédent au nouveau répertoire. Si le répertoire privé spécifié existe déjà, DRA ne crée pas ce nouveau répertoire et ne modifie pas les autorisations du répertoire existant. Si le répertoire privé précédent n'est pas verrouillé, DRA le supprime.

Lorsque DRA ne parvient pas à renommer le répertoire privé, il tente de créer un répertoire privé avec un nouveau nom et de copier le contenu du répertoire privé précédent vers le nouveau. DRA tente ensuite de supprimer l'ancien répertoire privé. Vous pouvez configurer DRA de sorte

qu'il ne copie pas le contenu de l'ancien répertoire privé vers le nouveau répertoire privé. Cela vous permet d'effectuer ce déplacement manuellement pour éviter des problèmes tels que la copie de fichiers ouverts.

Lors de la suppression de l'ancien répertoire privé, DRA doit disposer d'une autorisation explicite pour supprimer les fichiers et sous-répertoires en lecture seule de ce répertoire. Pour ce faire, vous pouvez fournir à DRA l'autorisation de supprimer explicitement ces fichiers et sous-répertoires de l'ancien répertoire privé.

Autoriser le chemin ou répertoire parent pour un partage privé

DRA permet de spécifier les chemins ou répertoires parents autorisés pour les partages privés sur les serveurs de fichiers. Si vous devez spécifier de nombreux chemins de serveurs de fichiers ou de répertoires, vous pouvez exporter ces chemins dans un fichier CSV pour ensuite les ajouter à DRA à partir de ce fichier à l'aide de la console de DRA. DRA utilise les informations entrées dans le champ **Chemins parents autorisés** (Chemins parents autorisés) afin de vous assurer que :

- ♦ DRA ne supprime pas le répertoire parent sur le serveur de fichiers lorsque des assistants administrateur suppriment un compte utilisateur et son répertoire privé ;
- ♦ DRA déplace le répertoire privé vers un chemin ou un répertoire parent valide sur le serveur de fichiers lorsque vous renommez un compte utilisateur ou que vous modifiez le chemin du répertoire privé d'un compte utilisateur.

Supprimer le répertoire privé lors de la suppression d'un compte utilisateur

Cette règle permet à DRA de supprimer automatiquement un répertoire privé lorsque vous supprimez le compte utilisateur associé. Si vous activez la corbeille, DRA ne supprime le répertoire privé que lorsque vous supprimez le compte utilisateur de la corbeille. Lors de la suppression du répertoire privé, DRA doit disposer d'une autorisation explicite pour supprimer les fichiers et sous-répertoires en lecture seule de ce répertoire. Pour ce faire, vous pouvez fournir à DRA l'autorisation de supprimer explicitement ces fichiers et sous-répertoires.

Automatisation et règles des partages privés

DRA automatise les tâches de maintenance de partages privés en gérant ces derniers lorsque vous modifiez un compte utilisateur ou que vous administrez des répertoires privés. DRA peut effectuer des actions différentes lorsqu'un compte utilisateur est créé, cloné, modifié, renommé ou supprimé.

Pour garantir la cohérence avec les stratégies de sécurité de Microsoft Windows, DRA ne crée pas de restrictions de contrôle d'accès au niveau du nom du partage, mais plutôt au niveau du répertoire uniquement. En effet, la définition de restrictions de contrôle d'accès à la fois au niveau du nom du partage et de l'objet Répertoire se traduit souvent par un schéma d'accès ambigu pour les administrateurs et les utilisateurs.

REMARQUE : l'emplacement spécifié doit comporter un partage privé commun, tel que `HOMEDIRS`, à un niveau au-dessus des répertoires privés.

Par exemple, le chemin suivant est valide : `\\HOUSERV1\HOMEDIRS\%nom_utilisateur%`

En revanche, le chemin suivant n'est pas valide : `\\HOUSERV1\%nom_utilisateur%`

Spécification des noms de partages privés

Lorsque vous définissez les règles d'automatisation relatives aux partages privés, vous pouvez spécifier un préfixe et un suffixe pour chaque partage privé créé automatiquement. En spécifiant un préfixe ou un suffixe, vous pouvez appliquer une convention de dénomination pour les partages privés.

Imaginons, par exemple, que vous activez les règles d'automatisation Créer un répertoire privé et Créer un partage privé. Pour le partage privé, vous spécifiez un caractère de soulignement comme préfixe et un signe dollar comme suffixe. Lorsque vous créez un utilisateur nommé TomS, vous assignez son nouveau répertoire à l'unité U et spécifiez `\\HOUSERV1\HOMEDIRS\%nom_utilisateur%` en tant que chemin du répertoire. Dans cet exemple, DRA crée un partage réseau nommé `_TomS$` qui pointe vers le répertoire `\\HOUSERV1\HOMEDIRS\TomS`.

Création de partages privés pour les nouveaux comptes utilisateur

Lorsque DRA crée un partage privé, le serveur d'administration utilise le chemin spécifié dans le champ **Répertoire privé** de l'assistant Créer un utilisateur. Vous pouvez modifier ce chemin ultérieurement via l'onglet Profil de la fenêtre Propriétés de l'utilisateur.

DRA crée le nom du partage en ajoutant au nom d'utilisateur le préfixe et le suffixe spécifiés, le cas échéant. Si vous utilisez de longs noms de compte utilisateur, il se peut que DRA ne puisse pas ajouter le préfixe et le suffixe spécifiés pour le partage privé. Le préfixe et le suffixe, ainsi que le nombre de connexions autorisées, sont basés sur les options de création de partage privé que vous sélectionnez.

Création de partages privés pour les comptes utilisateur clonés

Si le nom de partage privé généré à partir du nom du compte utilisateur nouvellement créé existe déjà, DRA supprime le partage existant et en crée un nouveau dans le répertoire privé spécifié.

Lors du clonage d'un compte utilisateur, le nom du partage du compte utilisateur existant doit lui-même exister. Lorsque vous clonez un compte utilisateur, DRA clone également les informations du répertoire privé et les personnalise pour le nouvel utilisateur.

Modification des propriétés de partage privé

Lorsque vous modifiez l'emplacement d'un répertoire privé, DRA supprime le partage existant et en crée un dans le nouveau répertoire privé. Si le répertoire privé d'origine est vide, DRA le supprime.

Attribution d'un nouveau nom aux partages privés de comptes utilisateur renommés

Lorsque vous renommez un compte utilisateur, DRA supprime le partage privé existant et en crée un en fonction du nouveau nom du compte. Le nouveau partage pointe vers le répertoire privé existant.

Suppression des partages privés des comptes utilisateur supprimés

Lorsque vous supprimez définitivement un compte utilisateur, DRA supprime le partage privé.

Règles de gestion des quotas de disques de volumes privés

DRA permet de gérer les quotas de disques pour les volumes privés. Vous pouvez mettre en oeuvre cette stratégie dans les domaines natifs pour lesquels le répertoire privé se trouve sur un ordinateur Microsoft Windows. Lorsque vous implémentez cette stratégie, vous devez spécifier un quota de disque d'au moins 25 Mo pour disposer de suffisamment d'espace.

Activation de la génération de mot de passe

Cette fonction permet de spécifier les paramètres de stratégie pour les mots de passe que DRA génère. DRA n'applique pas ces paramètres aux mots de passe créés par les utilisateurs. Lorsque vous configurez les propriétés de la stratégie de mot de passe, la longueur du mot de passe doit être comprise entre 6 et 127 caractères. Toutes les valeurs peuvent être définies sur zéro, à l'exception de la longueur du mot de passe.

Pour configurer des stratégies de génération de mot de passe, accédez à [Gestion des stratégies et de l'automatisation](#) > [Configure Password Generation Policies](#) (Configurer des stratégies de génération de mot de passe), puis cochez la case [Enable Password Policy](#) (Activer une stratégie de mot de passe). Cliquez sur [Password Settings](#) (Paramètres du mot de passe) et configurez les propriétés de la stratégie de mot de passe.

Tâches de stratégie

Pour supprimer, activer ou désactiver des stratégies, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation.

Pour effectuer une de ces actions, accédez à [Gestion des stratégies et de l'automatisation](#) > [Stratégie](#). Dans le volet de droite, cliquez avec le bouton droit sur la stratégie que vous souhaitez supprimer, activer ou désactiver, puis sélectionnez l'action souhaitée.

Implémentation des stratégies intégrées

Pour implémenter des stratégies intégrées, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation. Pour plus d'informations sur les stratégies intégrées, reportez-vous à la section [Présentation des stratégies intégrées](#).

REMARQUE : avant d'associer la stratégie intégrée à un assistant administrateur et à une instance Active Views, vous devez d'abord vérifier que ce dernier est assigné à l'instance en question.

Pour implémenter des stratégies intégrées :

- 1 Accédez à [Gestion des stratégies et de l'automatisation](#) > [Policy](#) (Stratégie).
- 2 Dans le menu Tasks (Tâches), cliquez sur [New Policy](#) (Nouvelle stratégie), puis sélectionnez le type de stratégie intégrée que vous souhaitez créer.
- 3 Dans chaque fenêtre de l'assistant, spécifiez les valeurs appropriées, puis cliquez sur [Next](#) (Suivant). Par exemple, vous pouvez associer cette nouvelle stratégie à une instance Active Views spécifique, ce qui permet à DRA d'appliquer cette stratégie sur les objets inclus dans cette instance.
- 4 Passez en revue le résumé, puis cliquez sur [Finish](#) (Terminer).

Implémentation des stratégies personnalisées

Pour implémenter une stratégie personnalisée, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation.

Pour mettre en oeuvre efficacement une stratégie personnalisée, vous devez écrire un script qui s'exécute lors d'une opération spécifique (tâche d'administration). Dans le script de stratégie personnalisée, vous pouvez définir les messages d'erreur à afficher chaque fois qu'une action viole la stratégie. Vous pouvez également spécifier un message d'erreur par défaut via l'assistant Create Policy (Créer une stratégie).

Pour plus d'informations sur l'écriture de stratégies personnalisées, l'affichage d'une liste des opérations d'administration ou l'utilisation de tableaux d'arguments, reportez-vous au SDK. Pour plus d'informations, reportez-vous à la section [Écriture de scripts et d'exécutables de stratégies personnalisées](#).

REMARQUE

- ♦ Avant d'associer la stratégie personnalisée à un assistant administrateur et à une instance Active Views, vous devez d'abord vérifier que ce dernier est assigné à l'instance en question.
 - ♦ Si le chemin du script ou de l'exécutable de la stratégie personnalisée contient des espaces, indiquez le chemin entre guillemets (").
-

Pour implémenter une stratégie personnalisée :

- 1 Écrivez un script ou un exécutable de stratégie.
- 2 Connectez-vous à un ordinateur client DRA avec un compte auquel est assigné le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation dans le domaine géré.
- 3 Démarrez la console de délégation et de configuration.
- 4 Connectez-vous au serveur d'administration primaire.
- 5 Dans le volet de gauche, développez **Gestion des stratégies et de l'automatisation**.
- 6 Cliquez sur **Policy** (Stratégie).
- 7 Dans le menu Tasks (Tâches), cliquez sur **New Policy > Create a Custom Policy** (Nouvelle stratégie > Créer une stratégie personnalisée).
- 8 Dans chaque fenêtre de l'assistant, spécifiez les valeurs appropriées, puis cliquez sur **Next** (Suivant). Par exemple, vous pouvez associer cette nouvelle stratégie à une instance Active Views spécifique, ce qui permet à DRA d'appliquer cette stratégie sur les objets inclus dans cette instance.
- 9 Passez en revue le résumé, puis cliquez sur **Finish** (Terminer).

Modification des propriétés d'une stratégie

Pour modifier toutes les propriétés d'une stratégie, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation.

Pour modifier les propriétés d'une stratégie :

- 1 Accédez à **Gestion des stratégies et de l'automatisation > Stratégie**.
- 2 Cliquez avec le bouton droit sur la stratégie que vous souhaitez modifier, puis sélectionnez **Propriétés**.
- 3 Modifiez les propriétés et paramètres appropriés pour cette stratégie.

Écriture de scripts et d'exécutables de stratégies personnalisées

Pour plus d'informations sur l'écriture de scripts ou d'exécutables de stratégies personnalisées, consultez le kit de développement logiciel (Software Development Kit, SDK).

Pour accéder au SDK :

- 1 Assurez-vous d'avoir installé le SDK sur votre ordinateur. Le programme d'installation crée un raccourci vers le SDK dans le groupe de programmes Directory and Resource Administrator. Pour plus d'informations, reportez-vous à la liste de contrôle de l'installation de la section [Installation du serveur d'administration DRA](#).
- 2 Cliquez sur le raccourci du SDK dans le groupe de programmes Directory and Resource Administrator.

Pour plus d'informations sur le SDK, reportez-vous au « DRA REST Services Guide » (Guide des services REST de DRA) sur le [site de documentation de DRA](#).

5.1.6 Stratégie du client de délégation et de configuration

La stratégie de dénomination automatique comprend trois configurations de stratégie dans les stratégies Exchange qui sont propres au client de délégation et de configuration, ce qui signifie qu'il s'agit d'une stratégie côté client.

La stratégie de dénomination automatique permet de spécifier des règles de dénomination automatisées pour des propriétés spécifiques d'une boîte aux lettres. Vous pouvez ainsi établir des conventions de dénomination et générer rapidement des valeurs standard pour les propriétés de nom d'affichage, de nom de répertoire et d'alias. Exchange permet de spécifier des chaînes de substitution, telles que %First et %Last, pour plusieurs options de dénomination automatisée.

Lorsque Exchange génère un nom de répertoire ou un alias, il vérifie si la valeur générée est unique. Si la valeur générée n'est pas unique, Exchange ajoute un trait d'union (-) et un nombre à deux chiffres, en commençant par -01, de manière à rendre la valeur unique. Lorsque Exchange génère un nom d'affichage, il ne vérifie pas si la valeur est unique.

Exchange prend en charge les chaînes de substitution suivantes pour les stratégies de dénomination automatique et de génération de proxy :

%First	Indique la valeur de la propriété Prénom du compte utilisateur associé.
%Last	Indique la valeur de la propriété Nom du compte utilisateur associé.
%Initials	Indique la valeur de la propriété Initiales du compte utilisateur associé.
%Alias	Indique la valeur de la propriété de boîte aux lettres Alias.
%DirNam	Indique la valeur de la propriété de boîte aux lettres Nom du répertoire. Lors de la génération des adresses électroniques pour les boîtes aux lettres Microsoft Exchange, Exchange ne prend pas en charge les chaînes de génération de proxy qui spécifient la variable %DirName.
%UserName	Indique la valeur de la propriété Nom d'utilisateur du compte utilisateur associé.

Vous pouvez également spécifier un nombre entre le signe de pourcentage (%) et le nom de la chaîne de substitution pour indiquer le nombre de caractères de cette valeur à inclure. Par exemple, %2First indique les deux premiers caractères de la propriété **Prénom** du compte utilisateur.

Chaque règle de dénomination automatique ou chaque stratégie de génération de proxy peut contenir une ou plusieurs chaînes de substitution. Vous pouvez également spécifier dans chaque règle des caractères comme préfixe ou suffixe d'une chaîne de substitution spécifique, par exemple, un point et un espace (.) après la chaîne de substitution %Initials. Si la propriété de la chaîne de substitution est vide, Exchange n'inclut pas le suffixe de cette propriété.

Imaginez, par exemple, la règle de dénomination automatique suivante pour la propriété **Nom d'affichage** :

```
%First %lInitials. %Last
```

Si la propriété **Prénom** est Susan, la propriété **Initiales** est May et la propriété **Nom** est Smith, Exchange définit la propriété **Nom d'affichage** sur Susan M. Smith.

Si la propriété **Prénom** est Michael, la propriété **Initiales** est vide et la propriété **Nom** est Jones, Exchange définit la propriété **Nom d'affichage** sur Michael Jones.

Spécification d'une stratégie de dénomination automatisée de boîte aux lettres

Pour spécifier des options de dénomination automatisée de boîte aux lettres, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation, et votre licence doit prendre en charge le produit Exchange.

Pour spécifier une stratégie de dénomination automatisée de boîte aux lettres :

- 1 Accédez à **Gestion des stratégies et de l'automatisation > Configure Exchange Politiques** (Configurer des stratégies Exchange) > **Alias naming** (Dénomination d'alias).
- 2 Spécifiez les informations de génération de nom appropriées.
- 3 Sélectionnez l'option **Enforce alias naming rules during mailbox updates** (Appliquer les règles de dénomination d'alias lors des mises à jour de boîte aux lettres).
- 4 Cliquez sur **OK**.

Spécification d'une règle de dénomination de ressource

Pour spécifier des options de dénomination de ressource, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation, et votre licence doit prendre en charge le produit Exchange.

Pour spécifier une stratégie de dénomination de ressource :

- 1 Accédez à **Gestion des stratégies et de l'automatisation > Configure Exchange Politiques** (Configurer des stratégies Exchange > **Resource naming** (Dénomination de ressource).
- 2 Spécifiez les informations de génération de nom de ressource appropriées.
- 3 Sélectionnez l'option **Enforce resource naming rules during mailbox updates** (Appliquer les règles de dénomination de ressource lors des mises à jour de boîte aux lettres).
- 4 Cliquez sur **OK**.

Spécification d'une stratégie de dénomination d'archive

Pour spécifier des options de dénomination d'archive, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation, et votre licence doit prendre en charge le produit Exchange.

Pour spécifier une stratégie de dénomination d'archive :

- 1 Accédez à **Gestion des stratégies et de l'automatisation** > **Configure Exchange Policies** (Configurer des stratégies Exchange) > **Archive naming** (Dénomination d'archive).
- 2 Spécifiez les informations de génération de nom d'archive appropriées pour les comptes utilisateur.
- 3 Sélectionnez l'option **Enforce archive naming rules during mailbox updates** (Appliquer les règles de dénomination d'archive lors des mises à jour de boîte aux lettres).
- 4 Cliquez sur **OK**.

5.2 Automatisation de déclencheurs préalables ou postérieurs à une tâche

Un déclencheur d'automatisation est une règle qui associe un fichier de script ou d'exécutable à une ou plusieurs opérations. Ce fichier de script ou d'exécutable vous permet d'automatiser un workflow existant et d'établir un pont d'informations entre DRA et d'autres espaces de stockage de données. Les déclencheurs d'automatisation permettent d'étendre les fonctionnalités et la sécurité offertes par DRA.

Lorsque vous définissez un déclencheur d'automatisation, vous configurez les paramètres de règle, les opérations à associer au déclencheur, le script ou l'exécutable à exécuter et, le cas échéant, les instances Active Views ou les assistants administrateur qui doivent être associés à ce déclencheur. Ces règles déterminent la manière dont le serveur d'administration applique votre déclencheur.

Vous pouvez également spécifier un script ou un exécutable d'annulation pour votre déclencheur. Un **script d'annulation** vous permet d'annuler vos modifications en cas d'échec de l'opération.

DRA prend en charge les scripts VBScript et PowerShell.

5.2.1 Automatisation des processus par le serveur d'administration

Outre l'administration basée sur des règles Active Views, DRA permet d'automatiser vos workflows existants et d'exécuter automatiquement des tâches associées par le biais de déclencheurs d'automatisation. L'automatisation des workflows existants peut vous aider à rationaliser votre activité tout en fournissant des services plus rapides et de meilleure qualité.

Lorsque le serveur d'administration effectue l'opération associée à votre déclencheur d'automatisation, il exécute également le script ou l'exécutable de ce dernier. S'il s'agit d'un déclencheur préalable à une tâche, le serveur exécute le script ou l'exécutable avant l'opération. S'il s'agit d'un déclencheur postérieur à une tâche, le serveur exécute le script ou l'exécutable après l'opération. Ce processus est désigné sous le terme de transaction. Une **transaction** représente le cycle d'implémentation complet pour chaque tâche ou opération que le serveur d'administration exécute. Une transaction englobe les actions requises pour effectuer une opération ainsi que toutes les actions d'annulation que le serveur d'administration doit effectuer en cas d'échec de l'opération.

À chaque exécution d'un déclencheur d'automatisation, le serveur d'administration indique l'état de ce déclencheur dans le journal d'audit. Ces entrées de journal enregistrent le code de retour, les opérations associées, les objets concernés et si le script du déclencheur a réussi.

AVERTISSEMENT : les déclencheurs d'automatisation sont exécutés à l'aide du compte de service du serveur d'administration. Étant donné que le compte de service dispose des autorisations de niveau administrateur, les stratégies et les déclencheurs d'automatisation disposent d'un accès complet à toutes les données d'entreprise. Pour définir des déclencheurs d'automatisation, vous devez disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation. Ces déclencheurs d'automatisation sont exécutés dans le contexte de sécurité du compte de service. Par conséquent, les assistants administrateur associés au rôle intégré Gérer les stratégies et les déclencheurs d'automatisation pourraient obtenir davantage de pouvoirs que prévu.

5.2.2 Implémentation d'un déclencheur d'automatisation

Pour implémenter des déclencheurs d'automatisation, vous devez d'abord écrire des scripts ou des exécutables de déclencheur et disposer des pouvoirs appropriés, tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation.

Pour mettre en oeuvre efficacement un déclencheur personnalisé, vous devez écrire un script qui s'exécute lors d'une opération spécifique (tâche d'administration). Vous pouvez spécifier si DRA applique le déclencheur avant ou après l'exécution de l'opération. Dans le script du déclencheur, vous pouvez définir les messages d'erreur à afficher chaque fois que le déclencheur échoue. Vous pouvez également spécifier un message d'erreur par défaut via l'assistant Create Automation Trigger (Créer un déclencheur d'automatisation).

Pour plus d'informations sur l'écriture de déclencheurs personnalisés, l'affichage d'une liste des opérations d'administration ou l'utilisation de tableaux d'arguments, reportez-vous au *SDK*.

REMARQUE

- ♦ Avant d'associer le déclencheur d'automatisation personnalisé à un assistant administrateur et à une instance Active Views, vous devez d'abord vérifier que ce dernier est assigné à l'instance en question.
 - ♦ Si le chemin du script ou de l'exécutable du déclencheur d'automatisation personnalisé contient des espaces, indiquez le chemin entre guillemets ("").
-

Pour implémenter un déclencheur d'automatisation :

- 1 Écrivez un script ou un exécutable de déclencheur.
- 2 Connectez-vous à un ordinateur client DRA avec un compte auquel est assigné le rôle intégré **Manage Policies and Automation Triggers** (Gérer les stratégies et les déclencheurs d'automatisation) dans le domaine géré.
- 3 Démarrez la console de délégation et de configuration.
- 4 Connectez-vous à un serveur d'administration primaire.
- 5 Dans le volet de gauche, développez **Gestion des stratégies et de l'automatisation**.
- 6 Cliquez sur **Automation Triggers** (Déclencheurs d'automatisation).
- 7 Dans le menu Tasks (Tâches), cliquez sur **New Trigger** (Nouveau déclencheur).

- 8 Dans chaque fenêtre de l'assistant, spécifiez les valeurs appropriées, puis cliquez sur **Next** (Suivant). Par exemple, vous pouvez associer ce nouveau déclencheur à une instance Active Views spécifique, ce qui permet à DRA d'appliquer ce déclencheur lorsque les assistants administrateur gèrent les objets inclus dans cette instance Active Views.
- 9 Passez en revue le résumé, puis cliquez sur **Finish** (Terminer).

5.3 Workflow automatisé

L'automatisation de workflow permet d'automatiser des processus informatiques en créant des formulaires de workflow personnalisés qui sont exécutés lorsqu'un workflow est effectué ou lorsqu'ils sont déclenchés par un événement de workflow nommé, qui est créé sur le serveur d'automatisation de workflow. Lorsque vous créez un formulaire de workflow, vous définissez les groupes d'administrateurs qui peuvent le consulter. La soumission de formulaire ou l'exécution du processus de workflow dépend des pouvoirs délégués aux groupes inclus lors de la création du formulaire de workflow.

Lorsqu'ils sont créés ou modifiés, les formulaires de workflow sont enregistrés sur le serveur Web. Les assistants administrateur qui se connectent à la console Web de ce serveur ont accès aux formulaires en fonction de la manière dont vous configurez ces derniers. Les formulaires sont généralement accessibles à tous les utilisateurs possédant des informations d'identification pour le serveur Web. Pour limiter l'accès à un formulaire spécifique, vous devez ajouter des groupes d'assistants administrateur (AA), puis masquer le formulaire pour les autres utilisateurs. Pour pouvoir soumettre le formulaire, vous devez disposer de l'un des pouvoirs suivants :

- ♦ Créer un événement de workflow et modifier toutes les propriétés
- ♦ Démarrer le workflow

Lancement d'un formulaire de workflow : les workflows sont créés sur le serveur d'automatisation de workflow, qui doit être intégré à DRA via la console Web. Pour pouvoir enregistrer un nouveau formulaire, l'option **Lancer le workflow spécifique** ou **Déclencher le workflow par événement** doit être configurée dans les propriétés de formulaire. Vous trouverez plus d'informations sur ces options ci-dessous :

- ♦ **Lancer le workflow spécifique** : cette option répertorie tous les workflows disponibles en production sur le serveur de workflow pour DRA. Pour que les workflows apparaissent dans cette liste, ils doivent être créés dans le dossier `DRA_Workflows` sur le serveur d'automatisation de workflow.
- ♦ **Déclencher le workflow par événement** : cette option permet d'exécuter des workflows avec des déclencheurs prédéfinis. Les workflows avec des déclencheurs sont également créés sur le serveur d'automatisation de workflow.

REMARQUE : seuls les formulaires de workflow configurés avec l'option Lancer le workflow spécifique auront un historique d'exécution consultable dans le volet de recherche principal sous **Gestion > Requêtes**.

Vous pouvez modifier un formulaire existant ou en créer un nouveau. Pour créer un formulaire de workflow ou en modifier un existant, accédez à **Personnalisation > Workflow**.

Lorsque vous créez un formulaire, suivez ces étapes de base :

1. Configurez le formulaire pour exécuter un *workflow spécifié* lorsque le formulaire est soumis ou lorsqu'un *événement nommé* prédéfini le déclenche.

2. Choisissez le ou les groupes d'assistants administrateur qui sont inclus dans le processus de workflow et activez l'option **Le formulaire est masqué** sous l'onglet Général pour limiter l'accès au formulaire à ces utilisateurs.
3. Ajoutez au formulaire tous les champs ou pages de propriétés dont vous avez besoin.
4. Le cas échéant, créez des gestionnaires personnalisés pour définir davantage le processus de workflow et la façon dont il s'exécute.

REMARQUE : les options de gestionnaire personnalisé n'apparaissent pour un nouveau formulaire de workflow qu'après son premier enregistrement. Vous pouvez accéder aux gestionnaires personnalisés, les créer et les modifier dans **Propriétés du formulaire**.

Pour plus d'informations sur la personnalisation des formulaires de workflow, reportez-vous à la section [Personnalisation des formulaires de workflow](#).

6 Audit et création de rapports

L'audit des actions des utilisateurs est l'un des aspects les plus importants d'une implémentation saine de la sécurité. Pour vous permettre d'examiner les actions des assistants administrateur (AA) et d'établir des rapports à leur sujet, DRA consigne toutes les opérations des utilisateurs dans l'archive de journal sur l'ordinateur du serveur d'administration. DRA fournit des rapports clairs et complets reprenant les valeurs avant et après les événements audités afin que vous puissiez savoir exactement ce qui a changé.

6.1 Audit des activités

L'audit des activités au niveau des journaux d'événements peut vous aider à isoler, diagnostiquer et résoudre les problèmes dans votre environnement. Cette section fournit des informations pour vous aider à configurer et à comprendre la consignation des événements, ainsi qu'à exploiter les archives de journaux.

6.1.1 Journal natif des événements Windows

Pour vous permettre d'examiner les actions des assistants administrateur et d'établir des rapports à leur sujet, DRA consigne toutes les opérations des utilisateurs dans l'archive de journal sur l'ordinateur du serveur d'administration. Les opérations des utilisateurs incluent toutes les tentatives de modification de définitions, telles que la mise à jour des comptes utilisateur, la suppression de groupes ou la redéfinition des instances Active Views. DRA consigne également des opérations internes spécifiques, telles que l'initialisation du serveur d'administration et des informations serveur associées. En plus de consigner ces événements d'audit, DRA consigne les valeurs avant et après l'événement afin que vous puissiez voir exactement ce qui a changé.

DRA utilise un dossier, `NetIQLogArchiveData`, appelé une **archive de journal**, afin de stocker en toute sécurité les données de journal archivées. DRA archive les journaux au fil du temps, puis supprime les données les plus anciennes afin de libérer de l'espace pour les données plus récentes grâce à un processus dit de nettoyage.

DRA utilise les événements d'audit stockés dans les fichiers d'archivage des journaux pour afficher les rapports de détail des activités, notamment les modifications apportées à un objet au cours d'une période donnée. Vous pouvez également configurer DRA afin d'exporter les informations de ces fichiers d'archivage des journaux vers une base de données SQL Server qui permettra à NetIQ Reporting Center d'afficher les rapports de gestion.

DRA consigne systématiquement les événements d'audit dans l'archive de journal. Vous pouvez aussi activer ou désactiver l'écriture des événements DRA dans les journaux d'événements Windows.

Activation et désactivation de l'audit des journaux d'événements Windows pour DRA

Lorsque vous installez DRA, par défaut, les événements d'audit ne sont pas consignés dans le journal des événements Windows. Vous pouvez activer ce type de consignation en modifiant une clé de registre.

AVERTISSEMENT : soyez prudent lorsque vous modifiez votre registre Windows. Une erreur dans votre registre peut en effet empêcher le bon fonctionnement de votre ordinateur. Si une erreur se produit, vous pouvez restaurer le registre dans l'état qui était le sien lors du dernier démarrage réussi de votre ordinateur. Pour plus d'informations, reportez-vous à l'Aide de l'éditeur de registre Windows.

Pour activer l'audit des événements :

- 1 Cliquez sur **Démarrer > Exécuter**.
- 2 Tapez `regedit` dans le champ **Ouvrir**, puis cliquez sur **OK**.
- 3 Développez la clé de registre suivante : `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
- 4 Cliquez sur **Édition > Nouveau > Valeur DWORD**.
- 5 Entrez `IsNTAuditEnabled` comme nom de clé.
- 6 Cliquez sur **Édition > Modifier**.
- 7 Entrez `1` dans le champ **Données de la valeur**, puis cliquez sur **OK**.
- 8 Fermez l'éditeur du registre.

Pour désactiver l'audit des événements :

- 1 Cliquez sur **Démarrer > Exécuter**.
- 2 Tapez `regedit` dans le champ **Ouvrir**, puis cliquez sur **OK**.
- 3 Développez la clé de registre suivante : `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
- 4 Sélectionnez la clé `IsNTAuditEnabled`.
- 5 Cliquez sur **Édition > Modifier**.
- 6 Entrez `0` dans le champ **Données de la valeur**, puis cliquez sur **OK**.
- 7 Fermez l'éditeur du registre.

Garantie de l'intégrité des audits

Pour garantir que toutes les actions des utilisateurs sont auditées, DRA fournit d'autres méthodes de consignation lorsque le produit ne peut pas vérifier l'activité de consignation. Lorsque vous installez DRA, la clé `AuditFailsFilePath` et son chemin sont ajoutés à votre registre pour assurer les actions suivantes :

- ♦ Si DRA détecte que les événements d'audit ne sont plus consignés dans une archive de journal, il les consigne dans un fichier local sur le serveur d'administration.
- ♦ Si DRA ne peut pas écrire les événements d'audit dans un fichier local, il les consigne dans le journal des événements Windows.
- ♦ Si DRA ne peut pas écrire les événements d'audit dans le journal des événements Windows, il les consigne dans le journal de DRA.
- ♦ Si DRA détecte que les événements d'audit ne sont pas consignés, il bloque les nouvelles opérations des utilisateurs.

Pour activer les opérations d'écriture lorsque l'archive du journal n'est pas disponible, vous devez également définir une valeur de clé de registre pour la clé `AllowOperationsOnAuditFailure`.

AVERTISSEMENT : soyez prudent lorsque vous modifiez votre registre Windows. Une erreur dans votre registre peut en effet empêcher le bon fonctionnement de votre ordinateur. Si une erreur se produit, vous pouvez restaurer le registre dans l'état qui était le sien lors du dernier démarrage réussi de votre ordinateur. Pour plus d'informations, reportez-vous à l'Aide de l'éditeur de registre Windows.

Pour activer les opérations d'écriture :

- 1 Cliquez sur **Démarrer > Exécuter**.
- 2 Tapez `regedit` dans le champ **Ouvrir**, puis cliquez sur **OK**.
- 3 Développez la clé de registre suivante : `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.
- 4 Cliquez sur **Édition > Nouveau > Valeur DWORD**.
- 5 Entrez `AllowOperationsOnAuditFailure` comme nom de clé.
- 6 Cliquez sur **Édition > Modifier**.
- 7 Entrez `736458265` dans le champ **Données de la valeur**.
- 8 Sélectionnez **Décimal** dans le champ **Base**, puis cliquez sur **OK**.
- 9 Fermez l'éditeur du registre.

6.1.2 Présentation des archives de journaux

DRA consigne les données d'activité de l'utilisateur dans les archives de journaux sur le serveur d'administration. DRA crée des partitions d'archivage de journaux quotidiennes pour stocker les données collectées et normalisées chaque jour. DRA utilise la date selon l'heure locale sur le serveur d'administration (`AAAAMMJJ`) comme convention de dénomination pour les partitions d'archivage de journaux quotidiennes.

Si vous avez activé le collecteur de rapports de gestion, DRA exporte les données d'archivage des journaux dans une base de données SQL Server comme source pour les rapports de gestion DRA.

Au départ, DRA conserve par défaut les données de journal dans l'archive de journal indéfiniment. L'archive de journal peut atteindre une taille maximale qui est déterminée au moment de l'installation, en fonction de l'espace disque disponible. Lorsque l'archive de journal dépasse cette taille maximale, plus aucun nouvel événement d'audit n'y est stocké. Vous pouvez définir une limite de temps pour la conservation des données. DRA supprime les données les plus anciennes afin de libérer de l'espace pour les données plus récentes grâce au processus de nettoyage. Assurez-vous que vous disposez d'une stratégie de sauvegarde avant d'activer le nettoyage. Vous pouvez configurer la période de conservation des archives de journaux à l'aide de l'utilitaire de configuration de l'archivage des journaux. Pour plus d'informations, reportez-vous à la section [Modification des paramètres de nettoyage des archives de journaux](#).

Utilisation de l'utilitaire de visionneuse des archives de journaux

L'utilitaire de visionneuse des archives de journaux permet d'afficher les données stockées dans des fichiers d'archivage des journaux. Il est fourni avec le kit NetIQ DRA LARK (Log Archive Resource Kit) que vous pouvez installer avec DRA. Pour plus d'informations, reportez-vous au manuel [NetIQ DRA Log Archive Resource Kit Technical Reference](#) (Référence technique du kit NetIQ DRA LARK).

Sauvegarde des fichiers d'archivage des journaux

Un **fichier d'archivage des journaux** est une collection de blocs d'enregistrement. Étant donné que les fichiers d'archivage des journaux sont des fichiers binaires compressés qui se trouvent en dehors d'une base de données physique, il est inutile d'utiliser Microsoft SQL Server Management Studio pour sauvegarder les archives de journaux. Si vous disposez d'un système de sauvegarde automatique de fichiers, vos fichiers d'archivage des journaux sont sauvegardés automatiquement comme n'importe quel autre fichier.

Tenez compte des meilleures pratiques suivantes lorsque vous planifiez votre stratégie de sauvegarde :

- ♦ Une seule partition est créée chaque jour pour contenir les données d'événement de ce jour-là. Lorsque vous activez le nettoyage, par défaut, le service d'archivage des journaux nettoie les données de ces partitions automatiquement tous les 90 jours. La stratégie de sauvegarde doit tenir compte de la planification du nettoyage pour déterminer la fréquence des sauvegardes. Lorsque les partitions d'archivage de journaux sont effacées, DRA supprime les fichiers binaires. Vous ne pouvez pas récupérer les données nettoyées. Vous devez restaurer les données nettoyées à partir d'une sauvegarde. Pour plus d'informations, reportez-vous à la section [Modification des paramètres de nettoyage des archives de journaux](#).
- ♦ Vous devez sauvegarder les partitions uniquement lorsqu'elles sont fermées. Dans des conditions normales, une partition est fermée dans les 2 heures après minuit le jour suivant.
- ♦ Sauvegardez et restaurez les dossiers de partition et tous leurs sous-dossiers en tant qu'unité. Sauvegardez le fichier `VolumeInfo.xml` dans le cadre de la sauvegarde de la partition.
- ♦ Si vous souhaitez restaurer les partitions d'archivage des journaux pour les rapports, assurez-vous que les archives de journaux sauvegardées soient conservées ou puissent être restaurées dans leur format d'origine.
- ♦ Lorsque vous configurez votre processus de sauvegarde des fichiers d'archivage des journaux, NetIQ vous recommande d'exclure les deux sous-dossiers `index_data` et `CubeExport` situés dans le dossier principal d'archivage des journaux. Ces sous-dossiers contiennent des données temporaires et ne doivent pas être sauvegardés.

Modification des paramètres de nettoyage des archives de journaux

Lorsque vous installez DRA, le nettoyage des archives de journaux est désactivé par défaut. Lorsque vous établissez des procédures régulières de sauvegarde des fichiers d'archivage des journaux, vous devez activer le nettoyage de l'archivage des journaux pour économiser de l'espace disque. Vous modifiez le nombre de jours avant le nettoyage des partitions d'archivage des journaux à l'aide de l'utilitaire de configuration de l'archivage des journaux.

Pour modifier le nombre de jours après lequel les partitions d'archivage des journaux sont nettoyées :

- 1 Connectez-vous au serveur d'administration à l'aide d'un compte qui est membre du groupe Administrateurs locaux.
- 2 Démarrez l'**utilitaire de configuration de l'archivage des journaux (LogArchiveUtility.exe)** à partir du dossier des programmes `NetIQ \DRA\NetIQLogArchive`.
- 3 Cliquez sur **Log Archive Server Settings** (Paramètres du serveur d'archivage des journaux).
- 4 *Si vous souhaitez activer le nettoyage des partitions*, définissez la valeur du champ **Partition Grooming Enabled** (Nettoyage des partitions activé) sur True (Vrai).
- 5 Entrez le nombre de jours pendant lesquels vous souhaitez conserver les partitions d'archivage des journaux avant le nettoyage dans le champ **Number of Days before Grooming** (Nombre de jours avant le nettoyage).

- 6 Cliquez sur **Apply** (Appliquer).
- 7 Cliquez sur **Yes** (Oui).
- 8 Cliquez sur **Close** (Fermer).
- 9 Accédez au dossier <chemin_LogArchiveData>\<nom_partition> et

Si la valeur est

Coché	<p>Cliquez sur Oui dans le message de confirmation pour redémarrer le service d'archivage des journaux de NetIQ Security Manager.</p> <p>REMARQUE : Si vous modifiez un quelconque paramètre de l'archivage des journaux, vous devez redémarrer le service d'archivage des journaux afin que les modifications soient prises en compte.</p>
Non coché	<p>Cliquez sur Non dans le message de confirmation. Reportez-vous à la Pour activer le serveur d'archivage des journaux (Log Archive Server, LAS) de DRA afin qu'il nettoie les données non archivées .</p>

Si l'attribut File is ready for archiving (Le fichier est prêt pour l'archivage) sur les fichiers ou dossiers dans les partitions spécifiées n'est pas coché, vous devez modifier le fichier CONFIG pour activer le nettoyage de l'archivage des journaux. Pour comprendre pourquoi cet attribut peut être ou ne pas être activé, reportez-vous à la section **Additional Information** (Informations supplémentaires) de l'article de la base de connaissances [How do you configure the data retention period for DRA Logarchival Data?](#) (Configuration de la période de conservation des données pour les données d'archivage des journaux de DRA ?).

Pour activer le serveur d'archivage des journaux (Log Archive Server, LAS) de DRA afin qu'il nettoie les données non archivées :

- 1 Connectez-vous localement à chaque console Windows du serveur DRA en tant que membre du groupe Administrateurs locaux.
- 2 Utilisez un éditeur de texte pour ouvrir le fichier C:\ProgramData\NetIQ\Directory resource Administrator\LogArchiveConfiguration.config et repérez la ligne <Property name="GroomUnarchivedData" value="false" />.
- 3 Remplacez "false" par "true" et enregistrez le fichier.
- 4 Redémarrez le service d'archivage des journaux de NetIQ DRA.

REMARQUE : si vous modifiez un quelconque paramètre de l'archivage des journaux, vous devez redémarrer le service d'archivage des journaux afin que les modifications soient prises en compte.

6.2 Création de rapports

Cette section fournit des informations expliquant et permettant d'activer DRA Reporting, la collecte des données de création de rapports, ainsi que la collecte et la création de rapports de l'analyseur ActiveView. Elle indique également comment accéder aux rapports intégrés.

DRA désactive les fonctions et rapports que votre licence ne prend pas en charge. Vous devez également disposer des pouvoirs appropriés afin d'exécuter et d'afficher les rapports. Il se peut donc que vous n'ayez pas accès à certains rapports.

Les rapports de détail des activités sont disponibles dès que vous installez DRA via la console de gestion des comptes et des ressources ainsi que la console de configuration et de délégation afin de fournir les dernières informations sur les modifications apportées à votre réseau.

- ♦ [Section 6.2.1, « Gestion de la collecte des données pour la création de rapports », page 124](#)
- ♦ [Section 6.2.2, « Rapports intégrés », page 125](#)

6.2.1 Gestion de la collecte des données pour la création de rapports

DRA Reporting propose deux méthodes de génération de rapports qui permettent de voir les dernières modifications de votre environnement ainsi que de collecter et de vérifier les définitions de comptes utilisateur, de groupes et de ressources de votre domaine.

Rapports de détail des activités

Accessibles via la console de gestion des comptes et des ressources et la console de délégation et de configuration, ces rapports fournissent des informations de changements en temps réel pour les objets de votre domaine.

Rapports de gestion DRA

Accessibles via NetIQ Reporting Center (centre de création de rapports), ces rapports fournissent des informations relatives aux activités et à la configuration ainsi qu'un résumé des événements survenus dans vos domaines gérés. Certains rapports sont disponibles sous forme de représentations graphiques des données.

Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'un laps de temps spécifié à l'aide des rapports de détail des activités. Vous pouvez également afficher un graphique indiquant le nombre d'événements dans chaque domaine géré pendant une période spécifiée à l'aide de rapports de gestion. La création de rapports vous permet également d'afficher des informations concernant le modèle de sécurité DRA, telles que les définitions de groupe AA et Active Views.

Les rapports de gestion DRA peuvent être installés et configurés en tant que fonction facultative et s'affichent dans NetIQ Reporting Center. Lorsque vous activez et configurez la collecte de données, DRA collecte des informations sur les événements audités et les exporte vers une base de données SQL Server selon la planification que vous définissez. Lorsque vous vous connectez à cette base de données dans NetIQ Reporting Center, vous pouvez accéder à plus de 60 rapports intégrés :

- ♦ Rapports d'activité indiquant qui a fait quoi et quand
- ♦ Rapports de configuration indiquant l'état d'AD ou de DRA à un moment spécifique
- ♦ Rapports de résumé indiquant le volume des activités

Pour plus d'informations sur la configuration de la collecte des données pour les rapports de gestion, reportez-vous à la section [Configuration de la création de rapports](#).

Affichage de l'état des collecteurs

Vous pouvez afficher les détails de chaque collecteur de données sous l'onglet Collectors Status (État des collecteurs).

Pour afficher l'état des collecteurs :

- 1 Développez **Configuration Management**, puis cliquez sur **Update Reporting Service Configuration** (Mettre à jour la configuration du service de création de rapports).
- 2 Sous l'onglet Collectors Status (État des collecteurs), cliquez sur chaque entrée pour afficher des informations supplémentaires concernant la collecte des données, telles que l'heure de la dernière collecte et si celle-ci a réussi.
- 3 Si aucune donnée n'apparaît dans la liste de serveurs, cliquez sur **Rafraîchir**.

Activation de la création de rapports et de la collecte des données

Après avoir installé les composants DRA Reporting, activez et configurez la collecte des données de création de rapports pour accéder aux rapports NetIQ Reporting Center.

Pour activer la création de rapports et la collecte des données :

- 1 Accédez à **Configuration Management > Update Reporting Service Configuration** (Mettre à jour la configuration du service de création de rapports).
- 2 Sous l'onglet SQL Server, sélectionnez **Enable DRA Reporting support** (Activer la prise en charge de DRA Reporting).
- 3 Cliquez sur **Browse** (Parcourir) dans le champ Server Name (Nom du serveur) et sélectionnez l'ordinateur sur lequel SQL Server est installé.
- 4 Sous l'onglet Credentials (Informations d'identification), spécifiez les informations d'identification appropriées à utiliser pour les interactions SQL Server.
- 5 Si le système peut utiliser le même compte pour créer la base de données et initialiser le schéma, cochez la case Use the above credentials for creating a database and initializing the database schema (Utiliser les informations d'identification ci-dessus pour créer une base de données et lancer le schéma de base de données).
- 6 Si vous souhaitez spécifier un autre compte pour la création d'une base de données, sous l'onglet Admin Credentials (Informations d'identification d'administrateur), spécifiez ce compte utilisateur et son mot de passe.
- 7 Cliquez sur **OK**.

Pour plus d'informations sur la configuration des collecteurs spécifiques, reportez-vous à la section [Configuration de la création de rapports](#).

6.2.2 Rapports intégrés

Les rapports intégrés vous permettent de générer des rapports sur les modifications, les listes et les détails des objets. Consultez les rubriques de cette section pour découvrir comment accéder à ces rapports.

Création de rapports sur les modifications des objets

Vous pouvez afficher les informations de modification en temps réel des objets de vos domaines en générant des rapports de détail des activités. Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'une période spécifiée. Vous pouvez également exporter et imprimer les rapports de détail des activités.

Pour générer un rapport sur les modifications des objets :

- 1 Recherchez les objets qui correspondent à vos critères.
- 2 Cliquez avec le bouton droit sur un objet, puis sélectionnez **Création de rapports > Modifications apportées à nom_objet** ou **Reporting > Modifications apportées par nom_objet**.
- 3 Sélectionnez les dates de début et de fin pour spécifier les modifications que vous souhaitez afficher.
- 4 *Si vous souhaitez modifier le nombre de lignes à afficher*, entrez un nombre supérieur à la valeur par défaut qui est de 250.

REMARQUE : le nombre de lignes affichées s'applique à chaque serveur d'administration de votre environnement. Si vous incluez 3 serveurs d'administration dans le rapport et que vous utilisez la valeur par défaut de 250 lignes, le rapport peut afficher jusqu'à 750 lignes.

- 5 *Si vous souhaitez inclure uniquement des serveurs d'administration spécifiques dans le rapport*, sélectionnez l'option **Restrict query to these DRA servers** (Limiter la requête à ces serveurs DRA) et tapez le nom du ou des serveurs que vous souhaitez inclure dans le rapport. Séparez le nom des différents serveurs par une virgule.
- 6 Cliquez sur **OK**.

Création de rapports sur les listes des objets

Vous pouvez exporter ou imprimer les données des listes des objets. Cette fonctionnalité vous permet de créer rapidement et facilement des rapports sur les informations générales relatives à vos objets gérés et de distribuer ces informations.

Lorsque vous exportez une liste d'objets, vous pouvez spécifier l'emplacement du fichier, son nom et son format. DRA prend en charge les formats XML, CSV et HTML, de sorte que vous pouvez exporter ces informations dans des applications de base de données ou publier les résultats sur une page Web.

REMARQUE : vous pouvez également sélectionner plusieurs éléments dans une liste, puis copier ces éléments dans une application de texte, telle que le bloc-notes.

Pour générer un rapport sur les listes des objets :

- 1 Recherchez les objets qui correspondent à vos critères.
- 2 Pour exporter cette liste d'objets, cliquez sur **Export List** (Exporter la liste) dans le menu File (Fichier).
- 3 Pour imprimer cette liste d'objets, cliquez sur **Print List** (Imprimer la liste) dans le menu File (Fichier).
- 4 Spécifiez les informations appropriées pour enregistrer ou imprimer cette liste.

Création de rapports sur les détails des objets

Vous pouvez exporter ou imprimer les données des onglets Détails qui répertorient les attributs des objets tels que les adhésions aux groupes. Cette fonctionnalité vous permet de créer rapidement et facilement des rapports sur les informations nécessaires concernant des objets spécifiques et de les distribuer souvent.

Lorsque vous exportez les informations d'un onglet de détails d'objet, vous pouvez spécifier l'emplacement du fichier, son nom et son format. DRA prend en charge les formats XML, CSV et HTML, de sorte que vous pouvez exporter ces informations dans des applications de base de données ou publier les résultats sur une page Web.

Pour générer un rapport sur les détails d'un objet :

- 1 Recherchez l'objet qui correspond à vos critères.
- 2 Dans le menu View (Afficher), cliquez sur **Details** (Détails).
- 3 Dans le volet Details (Détails), sélectionnez l'onglet approprié.
- 4 Pour exporter ces détails d'objet, cliquez sur **Export Details** (Exporter les détails) dans le menu File (Fichier).
- 5 Pour imprimer ces détails d'objet, cliquez sur **Print Details List** (Imprimer la liste des détails) dans le menu File (Fichier).
- 6 Spécifiez les informations appropriées pour enregistrer ou imprimer cette liste.

7 Fonctions supplémentaires

Les assignations temporaires à des groupes, les groupes dynamiques, l'horodatage des événements et le mot de passe de récupération BitLocker sont des fonctionnalités supplémentaires de DRA que vous pouvez employer dans votre environnement d'entreprise.

7.1 Assignations temporaires à des groupes

DRA permet de créer des assignations temporaires à des groupes qui fournissent aux utilisateurs autorisés un accès temporaire aux ressources. Les assistants administrateur peuvent utiliser des assignations temporaires à des groupes pour assigner des utilisateurs à un groupe cible durant une période spécifique. À la fin de cette période, DRA supprime automatiquement les utilisateurs de ce groupe.

Le rôle Gérer les assignations temporaires à de groupes accorde aux assistants administrateur des pouvoirs pour créer et gérer des assignations temporaires à de groupes.

Pour déléguer la création et la gestion des assignations temporaires à de groupes, utilisez les pouvoirs suivants :

- ♦ Créer des assignations temporaires à des groupes
- ♦ Afficher des assignations temporaires à des groupes
- ♦ Supprimer/modifier des assignations temporaires à des groupes
- ♦ Ajouter un objet à un groupe
- ♦ Supprimer un objet d'un groupe

Le groupe cible et les utilisateurs cibles doivent également être dans la même instance Active Views.

REMARQUE

- ♦ Les assistants administrateur peuvent créer, modifier et supprimer des assignations temporaires à des groupes uniquement sur le serveur d'administration primaire. Ils ne peuvent pas gérer des assignations temporaires à des groupes sur des serveurs d'administration secondaires.
- ♦ DRA réplique les assignations temporaires à des groupes du serveur d'administration primaire vers les serveurs d'administration secondaires lors de la réplication MMS.
- ♦ Vous ne pouvez pas créer une assignation temporaire à un groupe pour un utilisateur qui est déjà membre du groupe cible. Si vous essayez une opération de ce type, DRA affiche un avertissement et ne vous permet pas de créer l'assignation temporaire à un groupe pour l'utilisateur.
- ♦ Si vous créez une assignation temporaire à un groupe pour un utilisateur qui n'est pas membre du groupe cible, DRA supprime l'utilisateur du groupe lorsque l'assignation temporaire à un groupe expire.

Pour plus d'informations sur la création et l'utilisation d'assignations temporaires à des groupes, reportez-vous au *Guide de l'utilisateur*.

7.2 Groupes dynamiques DRA

Un groupe dynamique est un groupe dont l'adhésion change en fonction d'un ensemble défini de critères que vous configurez dans les propriétés du groupe. Vous pouvez rendre n'importe quel groupe dynamique, tout comme vous pouvez supprimer le filtre dynamique de tout groupe pour lequel il a été configuré. Cette fonction permet également d'ajouter des membres de groupe à une liste statique ou à une liste d'exclusion. Les membres de groupe figurant dans ces listes ne sont pas affectés par les critères dynamiques.

Si vous reconvertissez un groupe dynamique en un groupe ordinaire, tous les membres de la liste de membres statiques sont ajoutés comme appartenant au groupe et tous les membres exclus et les filtres dynamiques sont ignorés. Vous pouvez convertir des groupes existants en groupes dynamiques ou créer un groupe dynamique à l'aide de la console Web ou de la console de délégation et de configuration.

Pour rendre un groupe dynamique :

- 1 Recherchez le groupe au niveau de la console applicable.
 - ♦ Console de délégation et de configuration : accédez à **Tous mes objets gérés > Find Now** (Rechercher maintenant).

REMARQUE : pour activer le générateur de requêtes, cliquez sur **Parcourir** et sélectionnez un domaine, un conteneur ou une unité organisationnelle.

- ♦ Console Web : accédez à **Gestion > Rechercher**.
- 2 Ouvrez les propriétés du groupe, puis sélectionnez **Rendre ce groupe dynamique** sous l'onglet Filtre de membres dynamiques.
 - 3 Ajoutez les attributs LDAP et virtuels de votre choix pour filtrer l'adhésion au groupe.
 - 4 Ajoutez les éventuels membres statiques ou exclus souhaités pour ce groupe dynamique et appliquez vos modifications.

Pour créer un groupe dynamique :

- ♦ **Console de délégation et de configuration** : cliquez avec le bouton droit sur le domaine ou le sous-noeud dans Tous mes objets gérés, puis sélectionnez **Nouveau > Groupe dynamique**.
- ♦ **Console Web** : accédez à **Management (Gestion) > Create (Créer) > New Dynamic Group** (Nouveau groupe dynamique).

7.3 Fonctionnement de l'horodatage des événements

Lorsque vous configurez un attribut pour un type d'objet et que DRA effectue l'une des opérations prises en charge, cet attribut est mis à jour (marqué) avec des informations spécifiques à DRA, notamment l'auteur de l'opération. AD génère donc un événement d'audit pour ce changement d'attribut.

Par exemple, supposons que vous avez sélectionné l'attribut `extensionAttribute1` comme attribut utilisateur et que l'audit AD DS est configuré. Chaque fois qu'un assistant administrateur met à jour un utilisateur, DRA actualise l'attribut `extensionAttribute1` avec les données d'horodatage des événements. Cela signifie qu'outre les événements AD DS pour chaque attribut que l'assistant administrateur a mis à jour (par exemple, description, nom, etc.), il y aura un événement AD DS supplémentaire pour l'attribut `extensionAttribute1`.

Chacun de ces événements contient un ID de corrélation qui est identique pour chaque attribut modifié lors de la mise à jour de l'utilisateur. C'est grâce à cela que les applications peuvent associer les données d'horodatage d'événement avec les autres attributs mis à jour.

7.3.1 Événement AD DS

Un événement de ce type apparaît dans le journal des événements de sécurité Windows à chaque fois que DRA exécute une opération prise en charge.

Nom d'affichage LDAP :	<code>extensionAttribute1</code>
Syntaxe (OID) : 2.5.5.12	2.5.5.12
Valeur :	<pre><dra-event user="DRDOM300\drauseradmin" sid="S-1-5-21-53918190-1560392134-2889063332-1914" tid="E0E257E6B4D24744A9B0FE3F86EC7038" SubjectUserSid="S-1-5-21-4224976940-2944197837-1672139851-500" ObjectDN="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/>+a+02ROO+bJbhyPbR4leJpKWCGTp/KXdqI7S3EBhVyniE7iXvxIT6eB6ldcXQ5StkblAHJgKzLN5FCOM5fZcITxyAPLW hbstaA7ZA0VbVC9MGIvIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=</pre>

La valeur d'un événement se compose de deux parties. La première est une chaîne XML qui contient les données d'horodatage des événements. La seconde est une signature des données qui peut être utilisée pour prouver que les données ont effectivement été générées par DRA. Pour valider la signature, une application doit disposer de la clé publique de la signature.

La chaîne XML comprend les informations suivantes :

user	L'assistant administrateur qui a effectué l'opération
sid	Le SID de l'assistant administrateur qui a effectué l'opération
tid	L'ID de la transaction d'audit DRA garantissant l'unicité de chaque événement
SubjectUserSid	Le SID du compte de service ou d'accès DRA qui a effectivement mis à jour AD
ObjectDN	Le nom distinctif de l'objet qui a été modifié

7.3.2 Opérations prises en charge

Utilisateur	<ul style="list-style-type: none"> ◆ Créer ◆ Renommer ◆ Modifier ◆ Cloner
Groupe	<ul style="list-style-type: none"> ◆ Créer ◆ Renommer ◆ Modifier ◆ Cloner

Contact	<ul style="list-style-type: none"> ◆ Créer ◆ Renommer ◆ Modifier ◆ Cloner
Ordinateur	<ul style="list-style-type: none"> ◆ Créer ◆ Activer ◆ Désactiver ◆ Renommer ◆ Modifier
Unité organisationnelle	<ul style="list-style-type: none"> ◆ Créer ◆ Renommer ◆ Cloner

7.4 Mot de passe de récupération BitLocker

Microsoft BitLocker stocke ses mots de passe de récupération dans Active Directory. La fonction de récupération BitLocker de DRA vous permet de déléguer des pouvoirs aux assistants administrateur afin de rechercher et de récupérer les mots de passe BitLocker perdus pour les utilisateurs finaux.

IMPORTANT : avant d'utiliser la fonction de mot de passe de récupération BitLocker, vérifiez que votre ordinateur est assigné à un domaine et que BitLocker est activé.

7.4.1 Affichage et copie d'un mot de passe de récupération BitLocker

En cas de perte d'un mot de passe BitLocker pour un ordinateur, il peut être réinitialisé à l'aide de la clé du mot de passe de récupération à partir des propriétés de l'ordinateur dans Active Directory. Copiez la clé du mot de passe et fournissez-la à l'utilisateur final.

Pour afficher et copier le mot de passe de récupération :

- 1 Lancez la **console de délégation et de configuration** et développez l'arborescence.
- 2 Sur le noeud **Gestion des comptes et des ressources**, accédez à **All My Managed Objects > Domain > Computers** (Tous mes objets gérés > Domaine > Ordinateurs).
- 3 Dans la liste des ordinateurs, cliquez avec le bouton droit sur l'ordinateur requis et sélectionnez **Properties** (Propriétés).
- 4 Cliquez sur l'onglet **Mot de passe de récupération BitLocker** pour afficher la valeur correspondante.
- 5 Cliquez avec le bouton droit sur le mot de passe de récupération BitLocker, cliquez sur **Copier**, puis collez le texte dans la feuille de calcul ou le fichier texte requis.

7.4.2 Recherche d'un mot de passe de récupération

Si le nom d'un ordinateur a été modifié, vous devez rechercher le mot de passe de récupération dans le domaine à l'aide des huit premiers caractères de l'ID de mot de passe.

Pour rechercher un mot de passe de récupération à l'aide d'un ID de mot de passe :

- 1 Lancez la **console de délégation et de configuration** et développez l'arborescence.
- 2 Sur le noeud **Gestion des comptes et des ressources**, accédez à **Tous mes objets gérés**, cliquez avec le bouton droit sur le **domaine géré**, puis cliquez sur **Rechercher un mot de passe de récupération BitLocker**.

Pour connaître les huit premiers caractères du mot de passe de récupération, reportez-vous à la section [Affichage et copie d'un mot de passe de récupération BitLocker](#).

- 3 Sur la page **Rechercher un mot de passe de récupération BitLocker**, collez les caractères copiés dans le champ Rechercher, puis cliquez sur **Rechercher**.

7.5 Analyseur ActiveView

L'analyseur ActiveView vous permet de diagnostiquer les problèmes Active Views. Par exemple, vous pouvez rechercher les anomalies au niveau du traitement Active Views, telles que des temps de traitement prolongés ou un traitement Active Views inutilisé lors de l'exécution d'une opération. L'analyseur ActiveView simplifie également la recherche des instances Active Views en double.

Après avoir exécuté une collecte de données et affiché un rapport, il se peut que vous souhaitiez modifier les règles Active View.

7.5.1 Démarrage d'une collecte de données Active Views

L'analyseur ActiveView vous permet de collecter des données sur les instances Active Views à partir des actions exécutées sur ces dernières par les assistants administrateur (AA). Ces données peuvent ensuite être affichées dans un rapport de l'analyseur. Pour pouvoir collecter les données, vous devez spécifier l'assistant administrateur au sujet duquel vous souhaitez recueillir des données, puis vous devez démarrer une collecte Active View.

REMARQUE : l'assistant administrateur au sujet duquel vous voulez collecter des données doit être connecté au même serveur DRA que celui sur lequel l'analyseur s'exécute.

Pour démarrer une collecte Active View :

- 1 Lancez la console Web et connectez-vous avec des informations d'identification d'administrateur.
- 2 Accédez à **Administrator** (Administrateur) > **ActiveView Analyzer** (Analyseur ActiveView).
- 3 Sur la page Analyseur ActiveView (Analyseur ActiveView), spécifiez les informations suivantes :
 - 3a Assistant administrateur** : utilisez la fonction de recherche pour trouver et ajouter un assistant administrateur (AA) au sujet duquel vous voulez recueillir des données.
 - 3b Afficher les propriétés** : (facultatif) utilisez la fonction Afficher les propriétés pour consulter ou modifier les propriétés de l'assistant administrateur avant de procéder à la collecte.
 - 3c Durée de la collecte** : spécifiez le nombre total d'heures requises pour collecter les données de l'analyseur. Une fois ce délai dépassé, la collecte cesse et un index est créé dans la base de données Mongo.

- 4 Cliquez sur **Démarrer la collecte** pour recueillir les données Active Views.
- 5 (Facultatif) Cliquez sur **Arrêter la collecte** pour cesser l'enregistrement des opérations AA sur les instances Active Views. Un index est créé dans la base de données Mongo.
Vous pouvez arrêter la collecte de données manuellement avant la fin de la durée planifiée et générer malgré tout un rapport.

IMPORTANT : si vous arrêtez la collecte et modifiez l'assistant administrateur, ou si vous redémarrez une collecte de données pour le même assistant administrateur, l'analyseur ActiveView efface les données existantes dans la base de données Mongo. Vous ne pouvez disposer de données de l'analyseur dans la base de données que pour un seul assistant administrateur à la fois.

7.5.2 Génération d'un rapport de l'analyseur

Avant de générer un rapport de l'analyseur, vérifiez que vous avez arrêté la collecte des données et qu'un index est disponible dans la base de données Mongo.

Pour générer un rapport de l'analyseur :

- 1 Accédez à **Administrateur > Analyseur ActiveView**.
- 2 Sur la page Analyseur ActiveView, la liste des opérations effectuées par l'assistant administrateur s'affiche et vous pouvez choisir parmi les options suivantes :
 - ♦ **Afficher les** : sélectionnez le nombre d'opérations les plus longues pour lesquelles vous souhaitez collecter des données de l'analyseur.
 - ♦ **Opération ayant la plus longue durée d'exécution** : sélectionnez l'opération pour laquelle vous souhaitez collecter des données de l'analyseur.
- 3 Cliquez sur **Générer un rapport** pour générer un rapport d'analyse avec les détails des opérations Active Views.

Le rapport vous permet d'analyser les règles qui nécessitent plus de temps pour effectuer des opérations afin que vous puissiez décider si certaines d'entre elles doivent être modifiées, voire supprimées de leur instance Active Views respective.

7.5.3 Purge des données analysées

L'action Purger permet de libérer de l'espace dans la base de données Mongo en supprimant les données en double et inutilisées.

Pour effacer toutes les données Active Views analysées existantes la base de données Mongo, cliquez sur **Purger les données**.

7.6 Corbeille

Vous pouvez activer ou désactiver la corbeille pour chaque domaine Microsoft Windows ou pour les objets au sein de ces domaines, en contrôlant la gestion des comptes dans l'ensemble de votre entreprise. Si vous activez la corbeille, puis supprimez un compte utilisateur, un groupe, un groupe de distribution dynamique, un groupe dynamique, une boîte aux lettres de ressource, un contact ou un compte d'ordinateur, le serveur d'administration désactive le compte sélectionné et le déplace vers le conteneur Corbeille. Une fois que DRA a déplacé le compte dans la corbeille, celui-ci ne s'affiche plus dans l'instance Active Views à laquelle il appartenait. Si vous supprimez un compte utilisateur, un groupe, un contact ou un compte d'ordinateur alors que la corbeille est désactivée, le

serveur d'administration supprime définitivement le compte sélectionné. Vous pouvez désactiver une corbeille qui contient des comptes supprimés précédemment. Cependant, une fois la corbeille désactivée, ces comptes ne sont plus disponibles sur le noeud Corbeille.

7.6.1 Assignation de pouvoirs concernant la corbeille

Pour permettre à un assistant administrateur de supprimer définitivement des comptes du noeud Tous mes objets gérés ainsi que de la corbeille, assignez le pouvoir approprié à partir de la liste suivante :

- ◆ Supprimer définitivement le compte utilisateur
- ◆ Supprimer définitivement le groupe
- ◆ Supprimer définitivement l'ordinateur
- ◆ Supprimer définitivement le contact
- ◆ Supprimer définitivement le groupe de distribution dynamique
- ◆ Supprimer définitivement le groupe dynamique
- ◆ Supprimer définitivement la boîte aux lettres de ressource

Si plusieurs serveurs d'administration gèrent différentes sous-arborescences dans le même domaine Microsoft Windows, vous pouvez utiliser la corbeille pour afficher n'importe quel compte supprimé de ce domaine, quel que soit le serveur d'administration qui gère ce compte.

7.6.2 Utilisation de la corbeille

La corbeille permet de supprimer définitivement des comptes, de restaurer des comptes ou d'afficher les propriétés de comptes supprimés. Vous pouvez également rechercher des comptes spécifiques et savoir depuis combien de jours un compte est dans la corbeille. Un onglet Corbeille est également inclus dans la fenêtre Propriétés pour un domaine sélectionné. Il vous permet de désactiver ou d'activer la corbeille pour l'ensemble du domaine ou pour des objets spécifiques, ainsi que de planifier un nettoyage de la corbeille.

Utilisez les options **Restore All** (Tout restaurer) ou **Empty Recycle Bin** (Vider la corbeille) pour restaurer ou supprimer rapidement et facilement ces comptes.

Lorsque vous restaurez un compte, DRA rétablit ce dernier, y compris toutes les autorisations, les délégations de pouvoirs, les assignations de stratégies, les adhésions aux groupes et les adhésions Active Views. Si vous supprimez définitivement un compte, DRA supprime ce compte de l'annuaire Active Directory.

Pour garantir une suppression sécurisée des comptes, seuls les assistants administrateur ayant les pouvoirs suivants peuvent supprimer définitivement les comptes de la corbeille :

- ◆ Supprimer définitivement le compte utilisateur
- ◆ Supprimer l'utilisateur de la corbeille
- ◆ Supprimer définitivement le compte de groupe
- ◆ Supprimer le groupe de la corbeille
- ◆ Supprimer définitivement le compte d'ordinateur
- ◆ Supprimer l'ordinateur de la corbeille
- ◆ Supprimer définitivement le compte de contact
- ◆ Supprimer le contact de la corbeille
- ◆ Supprimer définitivement le groupe de distribution dynamique

- ♦ Supprimer le groupe de distribution dynamique de la corbeille
- ♦ Supprimer définitivement le groupe dynamique
- ♦ Supprimer le groupe dynamique de la corbeille
- ♦ Supprimer définitivement la boîte aux lettres de ressource
- ♦ Supprimer la boîte aux lettres de ressources de la corbeille
- ♦ Afficher tous les objets Corbeille

Pour restaurer un compte à partir de la corbeille, les assistants administrateur doivent avoir les pouvoirs suivants dans l'unité organisationnelle qui contient le compte :

- ♦ Restaurer l'utilisateur à partir de la corbeille
- ♦ Restaurer le groupe à partir de la corbeille
- ♦ Restaurer le groupe de distribution dynamique à partir de la corbeille
- ♦ Restaurer le groupe dynamique à partir de la corbeille
- ♦ Restaurer la boîte aux lettres de ressources à partir de la corbeille
- ♦ Restaurer l'ordinateur à partir de la corbeille
- ♦ Restaurez le contact à partir de la corbeille
- ♦ Afficher tous les objets Corbeille

REMARQUE

- ♦ Si vous supprimez un compte AA de sorte qu'il se retrouve dans la corbeille, DRA continue d'afficher les assignations de rôles et Active Views pour ce compte. Au lieu d'afficher le nom du compte AA supprimé, DRA indique l'identificateur de sécurité (SID). Vous pouvez supprimer ces assignations avant de supprimer définitivement le compte AA.
 - ♦ DRA supprime le répertoire privé une fois le compte utilisateur supprimé de la corbeille.
 - ♦ Si vous supprimez un utilisateur qui dispose d'une licence Office 365, le compte utilisateur est déplacé dans la corbeille et la licence est supprimée. Si vous restaurez le compte utilisateur ultérieurement, la licence Office 365 sera également restaurée.
-

8 Personnalisation des clients

Vous pouvez personnaliser le client ARM ainsi que le client de délégation et de configuration et la console Web. Pour la personnalisation des clients, il vous faut un accès physique ou distant et des informations d'identification de compte. Pour la console Web, vous avez besoin d'une URL de serveur et d'informations d'identification de compte pour vous connecter à partir d'un navigateur Web.

8.1 Client de délégation et de configuration et client ARM

Cette section fournit des informations qui vous aideront à personnaliser le client de délégation et de configuration ainsi que le client de gestion des comptes et des ressources (Account and Resource Management, ARM). Elle explique notamment comment créer des pages de propriétés personnalisées, comment créer dans DRA des outils personnalisés qui peuvent s'exécuter sur les ordinateurs client et serveur du réseau, et comment personnaliser la configuration de l'interface utilisateur.

8.1.1 Personnalisation de pages de propriétés

Vous pouvez personnaliser et étendre la console de délégation et de configuration ainsi que la console de gestion des comptes et des ressources en implémentant des propriétés personnalisées. Des propriétés personnalisées vous permettent d'ajouter, à des assistants et à des fenêtres de propriétés spécifiques, des propriétés exclusives d'unité organisationnelle (OU) et de compte, telles que des extensions de schéma Active Directory et des attributs virtuels. Ces extensions vous permettent de personnaliser DRA pour répondre à vos besoins spécifiques. L'assistant New Custom Page (Nouvelle page personnalisée) de la console de délégation et de configuration vous permet de créer rapidement et facilement une page personnalisée pour étendre l'interface utilisateur appropriée.

Si vos assistants administrateur ont besoin de pouvoirs particuliers pour gérer en toute sécurité la page personnalisée, vous pouvez également créer et déléguer des pouvoirs personnalisés. Par exemple, vous souhaitez peut-être limiter la gestion des comptes utilisateur aux propriétés figurant sur la page personnalisée uniquement. Pour plus d'informations, reportez-vous à la section [Implémentation de pouvoirs personnalisés](#).

Fonctionnement des pages de propriétés personnalisées

Les extensions d'interface utilisateur sont des pages personnalisées que DRA affiche dans l'assistant et les fenêtres de propriétés appropriés. Vous pouvez configurer des pages personnalisées afin d'exposer des attributs Active Directory, des extensions de schéma et des attributs virtuels au niveau de la console de délégation et de configuration ainsi qu'au niveau de la console de gestion des comptes et des ressources.

Lorsque vous sélectionnez un attribut Active Directory, une extension de schéma ou un attribut virtuel quelconque pris en charge, vous pouvez utiliser les pages personnalisées aux fins suivantes :

- ♦ Limiter les assistants administrateur pour qu'ils gèrent un ensemble de propriétés bien défini et contrôlé. Cet ensemble peut inclure des *propriétés standard* et des extensions de schéma. Les propriétés standard correspondent aux attributs Active Directory exposés par défaut via la console de gestion des comptes et des ressources.

- ♦ Exposer des attributs Active Directory autres que les propriétés standard gérées par DRA.
- ♦ Étendre la console de gestion des comptes et des ressources ainsi que la console de délégation et de configuration pour inclure les propriétés particulières.

Vous pouvez également configurer la manière dont DRA affiche et applique ces propriétés. Par exemple, vous pouvez définir des contrôles d'interface utilisateur avec des valeurs de propriété par défaut.

DRA applique les pages personnalisées à tous les objets gérés applicables dans votre entreprise. Par exemple, si vous créez une page personnalisée pour ajouter des extensions de schéma Active Directory à la fenêtre Group Properties (Propriétés des groupes), DRA applique les propriétés de cette page à chaque groupe géré dans un domaine prenant en charge les extensions de schéma spécifiées. Chaque page personnalisée nécessite un ensemble unique de propriétés. Vous ne pouvez pas ajouter un attribut Active Directory à plusieurs pages personnalisées.

Vous ne pouvez pas désactiver des fenêtres ou des onglets individuels dans l'interface utilisateur existante. Un assistant administrateur peut sélectionner une valeur de propriété à l'aide de l'interface utilisateur par défaut ou d'une page personnalisée. DRA applique à une propriété la valeur sélectionnée en dernier.

DRA fournit un suivi d'audit complet pour les propriétés personnalisées. DRA enregistre les données suivantes dans le journal des événements de l'application :

- ♦ Modifications apportées aux pages personnalisées

IMPORTANT : vous devez configurer manuellement l'audit du journal des applications Windows. Reportez-vous au document « [How do I re-enable DRA to write events to the Application Event log in DRA 8.5 and later?](#) » (Procédure de réactivation de DRA pour l'écriture du journal des événements des applications dans DRA 8.5 et versions ultérieures).

- ♦ Création et suppression de pages personnalisées
- ♦ Extensions de schéma, attributs Active Directory et attributs virtuels exposés inclus dans les pages personnalisées

Vous pouvez également exécuter des rapports d'activité de modification pour surveiller les changements de configuration des propriétés personnalisées.

Implémentez et modifiez les pages personnalisées à partir du serveur d'administration primaire. Lors de la synchronisation, DRA réplique les configurations de pages personnalisées sur le MMS. Pour plus d'informations, reportez-vous à la section [Configuration du MMS](#).

Pages personnalisées prises en charge

Chaque page personnalisée que vous créez permet de sélectionner un ensemble de propriétés Active Directory, d'extensions de schéma ou d'attributs virtuels, et d'exposer ces propriétés sous la forme d'un onglet personnalisé. Vous pouvez créer les types de page personnalisée suivants :

Page d'utilisateur personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ♦ Fenêtre des propriétés des utilisateurs
- ♦ Assistant Créer un utilisateur
- ♦ Assistant Cloner l'utilisateur

Page de groupe personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ◆ Fenêtre des propriétés des groupes
- ◆ Assistant Créer un groupe
- ◆ Assistant Cloner le groupe

Page d'ordinateur personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ◆ Fenêtre des propriétés des ordinateurs
- ◆ Assistant Créer un ordinateur

Page de contact personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ◆ Fenêtre des propriétés des contacts
- ◆ Assistant Créer un contact
- ◆ Assistant Cloner le contact

Page d'unité organisationnelle personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ◆ Fenêtre des propriétés des unités organisationnelles
- ◆ Assistant Créer une unité organisationnelle
- ◆ Assistant Cloner l'unité organisationnelle

Page de boîte aux lettres de ressources personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ◆ Fenêtre des propriétés des boîtes aux lettres de ressource
- ◆ Assistant Créer une boîte aux lettres de ressource
- ◆ Assistant Cloner la boîte aux lettres de ressource

Page de groupe de distribution dynamique personnalisée

Permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- ◆ Fenêtre des propriétés des groupes de distribution dynamique
- ◆ Assistant Créer un groupe de distribution dynamique
- ◆ Assistant Cloner le groupe de distribution dynamique

Contrôles de propriété personnalisée pris en charge

Lorsque vous ajoutez un attribut Active Directory, une extension de schéma ou un attribut virtuel à une page personnalisée, vous configurez également le contrôle d'interface utilisateur avec lequel un assistant administrateur entre la valeur de la propriété. Par exemple, vous pouvez spécifier des valeurs de propriété comme suit :

- ◆ Définir des plages de valeurs spécifiques
- ◆ Définir des valeurs de propriété par défaut
- ◆ Indiquer si une propriété est obligatoire

Vous pouvez également configurer le contrôle d'interface utilisateur pour afficher des instructions ou des informations particulières. Par exemple, si vous définissez une plage spécifique pour un numéro d'identification d'employé, vous pouvez configurer le libellé du contrôle de zone de texte pour qu'il indique **Spécifier le numéro d'identification d'employé (001 à 100)**.

Chaque contrôle d'interface utilisateur prend en charge uniquement un attribut Active Directory, une extension de schéma ou un attribut virtuel. Configurez les contrôles d'interface utilisateur suivants en fonction du type de propriété :

Type d'attribut Active Directory	Contrôles d'interface utilisateur pris en charge
Booléen	Case à cocher
Date	Agenda
Nombre entier	Zone de texte (par défaut) Liste de sélection
Chaîne	Zone de texte (par défaut) Liste de sélection Sélecteur d'objet
Chaîne à valeurs multiples	Liste de sélection

Utilisation des pages personnalisées

Vous pouvez créer des pages personnalisées à partir du noeud Extensions de l'interface utilisateur. Une fois la page créée, vous pouvez ajouter ou supprimer des propriétés d'attribut AD, et désactiver ou supprimer la page. Pour chaque personnalisation à configurer, créez une page personnalisée et assignez le pouvoir ou le rôle approprié à l'assistant administrateur. Tenez compte des meilleures pratiques ci-dessous lorsque vous utilisez les pages personnalisées :

1. Pour vous assurer que DRA reconnaît vos attributs Active Directory, vos attributs d'extension de schéma ou vos attributs virtuels, redémarrez le service d'administration NetIQ sur chaque serveur d'administration.
2. Identifiez le type de page personnalisée que vous souhaitez créer ainsi que les propriétés que les assistants administrateur doivent gérer grâce à cette page personnalisée. Vous pouvez sélectionner n'importe quel attribut Active Directory, y compris les attributs d'extension de schéma, les attributs dans les fenêtres de propriété et les assistants DRA existants ou tout attribut virtuel que vous créez. Chaque page personnalisée nécessite toutefois un ensemble unique de propriétés. Vous ne pouvez pas ajouter un attribut Active Directory à plusieurs pages personnalisées.

Les pages personnalisées ne remplacent pas l'interface utilisateur existante. Pour plus d'informations, reportez-vous aux sections [Fonctionnement des pages de propriétés personnalisées](#) et [Pages personnalisées prises en charge](#).

3. Déterminez comment vous souhaitez que les assistants administrateur spécifient ces propriétés. Par exemple, vous souhaitez peut-être limiter une propriété spécifique à trois valeurs possibles. Vous pouvez définir un contrôle d'interface utilisateur approprié pour chaque propriété. Pour plus d'informations, reportez-vous à la section [Contrôles de propriété personnalisée pris en charge](#).

4. Déterminez si vos assistants administrateur ont besoin d'instructions ou d'informations propriétaires pour gérer correctement ces propriétés. Spécifiez, par exemple, si Active Directory a besoin d'une syntaxe pour la valeur de propriété, telle qu'un nom distinctif (DN) ou un chemin LDAP.
5. Identifiez l'ordre dans lequel ces propriétés doivent s'afficher sur la page personnalisée. Vous pouvez modifier l'ordre d'affichage à tout moment.
6. Déterminez comment DRA doit utiliser cette page personnalisée. Vous pouvez, par exemple, ajouter une page personnalisée utilisateur dans l'assistant New User (Nouvel utilisateur) et dans la fenêtre User Properties (Propriétés de l'utilisateur).
7. Utilisez l'onglet Assignations dans le volet des détails de l'assistant administrateur pour vérifier que vos assistants administrateur disposent des pouvoirs appropriés pour l'ensemble correct d'objets. Si vous avez créé des pouvoirs personnalisés pour cette page personnalisée, déléguez ces pouvoirs aux assistants administrateur appropriés.
8. Déterminez si vos assistants administrateur ont besoin d'un pouvoir personnalisé pour gérer les propriétés sur cette page. Par exemple, si vous ajoutez une page personnalisée dans la fenêtre Propriétés de l'utilisateur, la délégation du pouvoir *Modifier toutes les propriétés de l'utilisateur* risque de conférer un pouvoir trop important à un assistant administrateur. Créez tous les pouvoirs personnalisés nécessaires pour implémenter votre page personnalisée. Pour plus d'informations, reportez-vous à la section [Implémentation de pouvoirs personnalisés](#).
9. À l'aide des réponses apportées aux étapes précédentes, créez les pages personnalisées appropriées.
10. Distribuez les informations sur les pages de propriétés personnalisées mises en oeuvre aux assistants administrateur appropriés, tels que votre service d'assistance.

Pour implémenter la personnalisation de propriétés, vous devez disposer des pouvoirs inclus dans le rôle Administration DRA. Pour plus d'informations sur les pages personnalisées, reportez-vous à la section [Fonctionnement des pages de propriétés personnalisées](#).

Création de pages de propriétés personnalisées

Vous pouvez créer différentes propriétés personnalisées en créant différentes pages personnalisées. Par défaut, les nouvelles pages personnalisées sont activées.

Lorsque vous créez une page personnalisée, vous pouvez la désactiver. Une page personnalisée désactivée n'apparaît pas dans l'interface utilisateur. Si vous créez plusieurs pages personnalisées, vous souhaitez peut-être désactiver les pages jusqu'à ce que vos personnalisations soient testées et finalisées.

REMARQUE : Les comptes d'ordinateur héritent des attributs Active Directory des comptes utilisateur. Si vous étendez votre schéma Active Directory pour y inclure des attributs supplémentaires pour des comptes utilisateur, vous pouvez sélectionner ces attributs lorsque vous créez une page personnalisée pour gérer des comptes d'ordinateur.

Pour créer une page de propriétés personnalisée :

- 1 Accédez au noeud **Configuration Management > Extensions de l'interface utilisateur**.
- 2 Dans le menu Tâche, cliquez sur **Nouveau**, puis sur l'élément de menu approprié pour la page personnalisée que vous souhaitez créer.
- 3 Sous l'onglet Général, entrez le nom de cette page personnalisée, puis cliquez sur **OK**. Si vous souhaitez désactiver cette page, décochez la case **Activé**.

- 4 Pour chaque propriété que vous souhaitez inclure sur cette page personnalisée, procédez comme suit :
 - 4a Sous l'onglet Propriétés, cliquez sur **Ajouter**.
 - 4b Pour sélectionner une propriété, cliquez sur **Parcourir**.
 - 4c Dans le champ **Control label** (Libellé de contrôle), entrez le nom de propriété que DRA doit utiliser comme libellé pour le contrôle de l'interface utilisateur. Assurez-vous que le libellé de contrôle soit convivial et hautement descriptif. Vous pouvez également inclure des instructions, des plages de valeurs valides et des exemples de syntaxe.
 - 4d Sélectionnez le contrôle d'interface utilisateur approprié dans le menu **Control type** (Type de contrôle).
 - 4e Sélectionnez à quel endroit de la console de gestion des ressources et des comptes vous souhaitez que DRA affiche cette page personnalisée.
 - 4f Pour spécifier des attributs supplémentaires, telles que la longueur minimale ou les valeurs par défaut, cliquez sur **Avancé**.
 - 4g Cliquez sur **OK**.
- 5 Pour modifier l'ordre dans lequel DRA affiche ces propriétés sur la page personnalisée, sélectionnez la propriété appropriée, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
- 6 Cliquez sur **OK**.

Modification des propriétés personnalisées

Vous pouvez modifier une page personnalisée en changeant les propriétés personnalisées.

Pour modifier les propriétés personnalisées :

- 1 Accédez au noeud **Configuration Management > Extensions de l'interface utilisateur**.
- 2 Dans le volet liste, sélectionnez la page personnalisée de votre choix.
- 3 Dans le menu Tâches, cliquez sur **Propriétés**.
- 4 Modifiez les propriétés et paramètres appropriés pour cette page personnalisée.
- 5 Cliquez sur **OK**.

Identification des attributs Active Directory gérés à l'aide de pages personnalisées

Vous pouvez identifier rapidement les propriétés Active Directory, les extensions de schéma ou les attributs virtuels qui sont gérés à l'aide d'une page personnalisée spécifique.

Pour identifier les propriétés Active Directory gérées à l'aide de pages personnalisées :

- 1 Accédez au noeud **Configuration Management > Extensions de l'interface utilisateur**.
- 2 Dans le volet liste, sélectionnez la page personnalisée de votre choix.
- 3 Dans le volet détails, cliquez sur l'onglet **Propriétés**. Pour afficher le volet détails, cliquez sur **Détails** dans le menu Afficher.
- 4 Pour vérifier comment DRA affiche et applique une propriété, sélectionnez l'attribut Active Directory, l'extension de schéma ou l'attribut virtuel approprié dans la liste, puis cliquez sur l'icône **Propriétés**.

Activation, désactivation et suppression de pages personnalisées

Lorsque vous activez une page personnalisée, DRA ajoute cette page personnalisée aux fenêtres et assistants associés. Pour spécifier les assistants et fenêtres qui affichent une page personnalisée, modifiez les propriétés de la page personnalisée.

REMARQUE : Pour garantir que chaque page personnalisée propose un ensemble unique de propriétés, DRA n'active pas les pages personnalisées qui contiennent des propriétés proposées sur d'autres pages personnalisées.

Lorsque vous désactivez une page personnalisée, DRA la supprime des assistants et fenêtres associés. DRA ne supprime pas la page personnalisée. Pour garantir qu'une page personnalisée ne s'affiche jamais dans l'interface utilisateur, supprimez-la.

Lorsque vous supprimez une page personnalisée, DRA la supprime des assistants et fenêtres associés. Vous ne pouvez pas restaurer une page personnalisée qui a été supprimée. Pour supprimer temporairement une page personnalisée de l'interface utilisateur, désactivez-la.

Pour activer, désactiver ou supprimer une page personnalisée, accédez au noeud **Configuration Management > Extensions de l'interface utilisateur**, et sélectionnez l'action souhaitée dans le menu Tâches ou le menu contextuel.

Interface de ligne de commande

L'interface de ligne de commande vous permet d'accéder et d'appliquer de puissantes fonctionnalités d'administration à l'aide de commandes ou de fichiers de traitement par lots. Avec l'interface de ligne de commande, vous pouvez émettre une commande pour implémenter des changements sur plusieurs objets.

Par exemple, si vous devez déplacer les répertoires privés de 200 employés vers un nouveau serveur à l'aide de l'interface de ligne de commande, vous pouvez entrer la commande unique suivante pour modifier l'ensemble des 200 comptes utilisateur :

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE  
HOMEDIR:\\HOU2\USERS\@Target()
```

Cette commande indique à DRA de modifier le champ de répertoire privé de chacun des 200 comptes utilisateur dans les groupes HOU_SALES et HOU_MIS, et de le remplacer par \\HOU2\USERS\id_utilisateur. Pour accomplir cette tâche avec les outils d'administration Microsoft Windows natifs, vous devriez effectuer un minimum de 200 opérations distinctes.

REMARQUE : L'outil interface de ligne de commande sera supprimé dans les futures versions, étant donné que des fonctionnalités supplémentaires sont ajoutées à PowerShell.

8.1.2 Outils personnalisés

Les outils personnalisés permettent d'appeler une application pour qu'elle s'exécute sur les ordinateurs client et serveur du réseau en sélectionnant un compte Active Directory géré dans DRA.

DRA prend en charge deux types d'outils personnalisés :

- ♦ Les outils personnalisés qui lancent des utilitaires de bureau courants, tels que Microsoft Office
- ♦ Les outils personnalisés que vous créez et distribuez sur chaque ordinateur client DRA

Vous pouvez créer un outil personnalisé qui lance une analyse antivirus sur tous les ordinateurs où le client DRA est installé. Vous pouvez également créer un outil personnalisé qui lance un outil ou une application externe obligeant DRA à mettre à jour un script régulièrement. Ces mises à jour périodiques peuvent concerner des changements de configuration ou des modifications de la règle d'entreprise. Ensuite, après les mises à jour périodiques, DRA réplique les outils personnalisés du serveur d'administration primaire sur les serveurs d'administration secondaires et les ordinateurs client DRA.

Pour comprendre comment les outils personnalisés sont répliqués dans le MMS, reportez-vous à la section [Réplication des fichiers](#).

Création d'outils personnalisés

Vous pouvez créer des outils personnalisés sur le serveur primaire DRA en association avec un objet Active Directory sélectionné ou tous les objets Active Directory affichés dans l'assistant de création d'outils personnalisés. Ils seront répliqués sur les serveurs secondaires dans le MMS et sur les clients DRA par le biais de la fonctionnalité de réplication de fichiers.

Un nouvel outil personnalisé créera un menu et un sous-menu, au besoin, pour appeler l'opération par rapport aux objets Active Directory associés dans DRA.

Vous pouvez déléguer des pouvoirs aux assistants administrateur pour créer et exécuter des outils personnalisés, ainsi que pour accéder à l'application et l'exécuter.

Lors de la création d'un outil personnalisé, vous devez entrer les paramètres comme suit :

Onglet Général

1. **Nom** : n'importe quel nom client requis pour l'outil.
2. **Menu et sous-menu** : pour créer un élément de menu pour un nouvel outil personnalisé, entrez le titre du menu dans le champ **Menu and Submenu Structure** (Structure des menus et sous-menus). Lorsque vous créez un outil personnalisé et sélectionnez l'objet, DRA affiche l'élément de menu de l'outil personnalisé à l'aide de la structure des menus et sous-menus que vous spécifiez dans le menu Tâches, le menu Raccourci et la barre d'outils DRA.

Exemple de structure de menus et sous-menus : entrez le nom de l'élément de menu, une barre oblique inverse (\), puis le nom de l'élément de sous-menu.

Pour ajouter une touche de raccourci : tapez le caractère esperluette (&) devant le nom de l'élément de menu.

- a. **Exemple** : `SendEmail\ApproveAction --- SendEmail` est le menu et `ApproveAction` est le sous-menu, la touche de raccourci activée étant la première lettre « A » de `ApproveAction`.
3. **Activé(e)** : cochez cette case pour activer l'outil personnalisé.
 4. **Description** : vous pouvez ajouter n'importe quelle description souhaitée.
 5. **Commentaire** : vous pouvez ajouter n'importe quel commentaire requis pour l'outil personnalisé.

Onglet Supported Objects (Objets pris en charge)

Sélectionnez l'objet AD requis auquel l'outil personnalisé créé doit être associé, voire tous les objets AD.

Les options d'outil personnalisé actuellement prises en charge sont les suivantes : Domaine géré, Conteneurs, Utilisateurs, Contacts, Groupes, Ordinateurs, Unité organisationnelle et Published Printers (Imprimantes publiées).

REMARQUE : D'autres objets récents comme Boîte aux lettres de ressources, Groupe dynamique et Exchange Dynamic Group (Groupe dynamique Exchange) ne sont pas pris en charge avec les outils personnalisés.

Onglet Application Settings (Paramètres de l'application)

Location of the application (Emplacement de l'application) : vous devez fournir le chemin d'accès/l'emplacement de l'application, soit en effectuant un copier-coller du chemin exact de l'application, soit en utilisant l'option **Insérer** (Insérer).

Vous pouvez également utiliser les variables DRA, les variables d'environnement et les valeurs de registre pour spécifier l'emplacement de l'application externe dans le champ Emplacement de l'application. Pour utiliser ces variables, cliquez sur **Insérer** et sélectionnez la variable que vous souhaitez utiliser.

Une fois la variable insérée, tapez une barre oblique inverse (\), puis indiquez le reste du chemin de l'application, y compris le nom du fichier exécutable de l'application.

Exemples :

- ♦ *Exemple 1* : pour spécifier l'emplacement d'une application externe que l'outil personnalisé va exécuter, sélectionnez la variable environnementale `{%ProgramFiles%}`, puis spécifiez le reste du chemin de l'application dans le champ Emplacement de l'application :
`{%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe`

REMARQUE : DRA fournit la valeur de registre du répertoire d'installation d'Office à titre d'exemple. Pour spécifier une clé de registre qui contient un chemin en tant que valeur, utilisez la syntaxe suivante : `{HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\Default}`

- ♦ *Exemple 2* : pour spécifier l'emplacement d'un fichier de script personnalisé que l'outil personnalisé va exécuter, sélectionnez la variable DRA `{Chemin_fichiers_répliqués_DRA}`, puis spécifiez le reste du chemin du fichier de script dans le champ Emplacement de l'application : `{Chemin_fichiers_répliqués_DRA}\cscript.vbs ; où {Chemin_fichiers_répliqués_DRA} est le chemin des fichiers répliqués ou {DRAInstallDir}\FileTransfer\Replicate le dossier du serveur d'administration.`

REMARQUE : Avant de créer l'outil personnalisé, téléchargez le fichier de script sur le serveur d'administration primaire à l'aide de la fonction de réplication de fichiers. La fonction de réplication de fichiers télécharge le fichier de script dans le dossier `{DRAInstallDir}\FileTransfer\Replicate` du serveur d'administration primaire.

- ♦ *Exemple 3* : pour spécifier l'emplacement d'un utilitaire DRA que l'outil personnalisé va exécuter, sélectionnez la variable DRA `{Chemin_Application_DRA}`, puis spécifiez le reste du chemin de l'utilitaire dans le champ Emplacement de l'application :
`{Chemin_Application_DRA}\DRADiagnosticUtil.exe ; où {Chemin_Application_DRA} correspond à l'emplacement où DRA est installé.`
- ♦ *Exemple 4* : il suffit d'effectuer un copier-coller de l'emplacement de l'application ainsi que du nom du fichier de l'application avec son extension.

Parameters to pass to the application (Paramètres à transmettre à l'application) : pour définir un paramètre à transmettre à une application externe, effectuez une opération de copier-coller ou entrez un ou plusieurs paramètres dans le champs Paramètres à transmettre à l'application. DRA fournit des paramètres que vous pouvez utiliser dans le champ Paramètres à transmettre à l'application. Pour utiliser ces paramètres, cliquez sur Insérer et sélectionnez le ou les paramètres souhaités. Lorsque

vous spécifiez une propriété d'objet comme paramètre, assurez-vous que l'assistant administrateur possède l'autorisation de lecture requise pour la propriété d'objet, ainsi que le pouvoir *Exécuter les outils personnalisés* pour exécuter l'outil personnalisé.

Exemples :

- ♦ *Exemple 1* : pour transmettre un nom de groupe et un nom de domaine en tant que paramètres à une application externe ou un script, sélectionnez les paramètres Object Property Name (Nom de la propriété d'objet) et Domain Property Name (Nom de la propriété de domaine) et spécifiez les noms des paramètres dans le champ Paramètres à transmettre à l'application :
"`{Object.Name}`" "`{Domain.$McsName}`"
- ♦ *Exemple 2* : pour transmettre le paramètre d'entrée "ipconfig" pour l'application "`C:\Windows\SysWOW64\cmd.exe`", tapez "`{C:\Windows\SysWOW64\cmd.exe}`" "`{ipconfig}`" dans ce champ.

Directory where the application will run (Répertoire dans lequel l'application sera exécutée) : emplacement dans lequel l'application doit s'exécuter sur la machine client ou serveur. Vous devez transmettre le chemin où l'application doit être exécutée. Vous pouvez également utiliser l'option « Insérer » de la même manière que pour transmettre le paramètre pour le champ « Emplacement de l'application ». Les autres paramètres de cet onglet sont suffisamment explicites et ne nécessitent pas d'autres explications.

8.1.3 Personnalisation de l'interface utilisateur

Plusieurs options permettent de personnaliser la configuration de la console de délégation et de configuration. La plupart de ces options permettent de masquer, d'afficher ou de reconfigurer des fonctionnalités dans les différents volets de fonctionnalités de l'application. Vous pouvez également masquer ou afficher la barre d'outils, personnaliser le titre de l'application et aussi ajouter, supprimer ou réorganiser des colonnes. Toutes ces options de personnalisation se situent dans le menu **Afficher**.

Modification du titre de la console

Vous pouvez modifier les informations affichées dans la barre de titre de la console de délégation et de configuration et de la console de gestion des ressources et des comptes. Pour plus de clarté et par facilité, vous pouvez ajouter le nom d'utilisateur avec lequel la console a été lancée et le serveur d'administration auquel la console est connectée. Dans les environnements complexes nécessitant une connexion à plusieurs serveurs d'administration à l'aide de différentes informations d'identification, cette fonctionnalité vous permet de déterminer rapidement quelle console utiliser.

Pour modifier la barre de titre de la console :

- 1 Démarrez la console de délégation et de configuration.
- 2 Cliquez sur **View** (Afficher) > **Options**.
- 3 Sélectionnez l'onglet Window Title (Titre de la fenêtre).
- 4 Spécifiez les options adéquates, puis cliquez sur **OK**. Pour plus d'informations, cliquez sur l'icône ?.

Personnalisation des colonnes de la liste

Vous pouvez sélectionner les propriétés d'objet que DRA affiche dans les colonnes de la liste. Cette fonctionnalité flexible vous permet de personnaliser l'interface utilisateur, notamment les listes de résultats de recherche, afin de mieux répondre aux exigences spécifiques qu'exige l'administration

de votre entreprise. Par exemple, vous pouvez configurer les colonnes pour qu'elles affichent le type de groupe ou le nom de connexion de l'utilisateur, afin de trouver et de trier rapidement et efficacement les données dont vous avez besoin.

Pour personnaliser les colonnes de la liste :

- 1 Sélectionnez le noeud approprié. Par exemple, pour choisir les colonnes qui s'affichent lorsque vous visualisez les résultats d'une recherche sur des objets gérés, sélectionnez **Tous mes objets gérés**.
- 2 Dans le menu View (Afficher), cliquez sur **Choose Columns** (Choisir les colonnes).
- 3 Dans la liste des propriétés disponibles pour ce noeud, sélectionnez les propriétés d'objet que vous souhaitez afficher.
- 4 Pour modifier l'ordre des colonnes, sélectionnez une colonne, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
- 5 Pour spécifier la largeur des colonnes, sélectionnez une colonne, puis entrez le nombre de pixels souhaité dans le champ approprié.
- 6 Cliquez sur **OK**.

8.2 Client Web

Dans le client Web, vous pouvez personnaliser les propriétés d'objet, les formulaires d'automatisation de workflow et l'image de marque de l'interface utilisateur. Si elles sont implémentées correctement, les personnalisations de propriétés et de workflows permettent d'automatiser les tâches des assistants administrateur, dans le cadre de la gestion d'objets et de soumissions de workflow automatisé.

8.2.1 Personnalisation de pages de propriétés

Vous pouvez personnaliser les formulaires de propriété d'objet que vos assistants administrateur utilisent dans leurs rôles de gestion Active Directory par type d'objet. Cela inclut la création et la personnalisation de nouvelles pages d'objet basées sur les types d'objet intégrés à DRA. Vous pouvez également modifier les propriétés des types d'objet intégrés.







Les objets étant clairement définis dans la liste Pages de propriétés de la console Web, vous pouvez facilement identifier les pages d'objet qui sont intégrées, les pages intégrées qui sont personnalisées et les pages qui ne sont pas intégrées et ont été créées par un administrateur.

Personnalisation d'une page de propriétés d'objet

Pour personnaliser les formulaires de propriétés d'objet, vous pouvez ajouter ou supprimer des pages, modifier des pages et des champs existants et créer des questionnaires personnalisés pour les attributs de propriété. Lorsque vous créez des questionnaires personnalisés, ils s'exécutent automatiquement lorsqu'un champ de propriété est modifié ou lorsqu'un administrateur répond à une invite pour exécuter une requête, en fonction de leur configuration.

La liste d'objets dans les pages de propriétés propose deux types d'opération pour chaque type d'objet : Créer un objet et Modifier les propriétés. Ce sont les principales opérations que vos assistants administrateur exécutent dans le client Web. Vos personnalisations permettent aux administrateurs d'être plus efficaces et expérimentés lorsqu'ils gèrent des objets Active Directory dans DRA.

Pour personnaliser une page de propriétés d'objet au niveau de la console Web :

- 1 Connectez-vous à la console Web en tant qu'administrateur DRA.
- 2 Accédez à **Personnalisation > Pages de propriétés**.
- 3 Sélectionnez un objet et un type d'opération (créer ou modifier) dans la liste des pages de propriétés.
- 4 Cliquez sur le bouton **Modifier** .
- 5 Personnalisez le formulaire de propriétés d'objet en effectuant une ou plusieurs des opérations suivantes, puis appliquez vos modifications :
 - ♦ Ajouter une nouvelle page de propriétés : **Ajouter une page**
 - ♦ Sélectionner une page de propriétés et la personnaliser :
 - ♦ Réorganiser les champs de configuration sur la page :  
 - ♦ Modifier les champs ou les sous-champs : 
 - ♦ Ajouter un ou plusieurs champs :  ou **Ajouter un champ**
 - ♦ Supprimer un ou plusieurs champs : 
 - ♦ Créer des gestionnaires personnalisés pour les propriétés à l'aide de scripts, de zones Message ou de requêtes (LDAP, DRA ou REST)
Pour plus d'informations sur l'utilisation des gestionnaires personnalisés, reportez-vous à la section [Ajout de gestionnaires personnalisés](#).

Création d'une page de propriétés d'objet

Pour créer une page de propriétés d'objet :

- 1 Connectez-vous à la console Web en tant qu'administrateur DRA.
- 2 Accédez à **Personnalisation > Pages de propriétés**.
- 3 Sous tâches, cliquez sur **Créer une action**.
- 4 Créez le formulaire initial des propriétés d'objet en définissant son nom, son icône, le type d'objet et la configuration de l'opération.
- 5 Personnalisez le nouveau formulaire en fonction de vos besoins. Reportez-vous à la [Personnalisation d'une page de propriétés d'objet](#).

8.2.2 Personnalisation des formulaires de workflow

Lorsqu'ils sont créés ou modifiés, les formulaires de workflow sont enregistrés sur le serveur Web et accessibles au niveau de la console Web sur la page **Personnalisation > Workflow**. Ces formulaires sont utilisés pour soumettre les workflows automatisés qui sont créés sur le serveur d'automatisation de workflow. Vous pouvez personnaliser les formulaires pour encore améliorer et automatiser leur utilisation par les assistants administrateur afin d'effectuer des tâches de gestion d'objets.

Vous pouvez ajouter et modifier des propriétés de formulaire et des gestionnaires personnalisés. Le comportement de l'interface lors de l'ajout et de la personnalisation de propriétés est identique dans un formulaire d'automatisation de workflow que lors de la personnalisation de propriétés d'objet. Consultez les rubriques ci-dessous pour plus d'informations sur l'ajout et la modification de propriétés, l'ajout de gestionnaires personnalisés et l'automatisation de workflow.

- ♦ [Personnalisation de pages de propriétés](#) (Client Web)

- ♦ [Ajout de gestionnaires personnalisés](#)
- ♦ [Workflow automatisé](#)

Ajout de gestionnaires personnalisés


Les gestionnaires personnalisés sont utilisés dans DRA pour permettre aux attributs de propriété d'interagir entre eux afin d'accomplir une tâche de workflow, ainsi que pour les personnalisations de chargement et de soumission dans un formulaire de workflow, de propriété ou de création.


Les gestionnaires personnalisés de propriété permettent, notamment, d'interroger la valeur d'autres champs, de mettre à jour des valeurs, d'activer/de désactiver l'état en lecture seule d'un champ et d'afficher/de masquer des champs en fonction des variables configurées.

Les gestionnaires de chargement de formulaire permettent aux utilisateurs de personnaliser les formulaires en effectuant généralement une initialisation des contrôles. Les gestionnaires de soumission de formulaire permettent aux utilisateurs d'effectuer une validation et éventuellement d'annuler la soumission en cas d'erreur.


DRA permet également de simplifier la création de gestionnaires personnalisés avec plusieurs macros JavaScript (JS) que vous pouvez sélectionner dans le cadre du processus de création et de validation du gestionnaire personnalisé.

Procédure de base pour créer un gestionnaire personnalisé :

Les étapes ci-dessous commencent à partir d'une page d'un gestionnaire personnalisé présélectionné. Pour y arriver, accédez aux gestionnaires personnalisés des propriétés d'objet via le bouton Modifier  dans un champ de propriété. Pour accéder aux gestionnaires de chargement et de soumission de formulaire, sélectionnez Propriétés du formulaire sur un formulaire de workflow ou sur une page de création d'objet.

- 1 Cliquez sur l'onglet Gestionnaires personnalisés applicable et activez la page .
 - ♦ Gestionnaires personnalisés
 - ♦ Gestionnaires de chargement de formulaire
 - ♦ Gestionnaires de soumission de formulaire
- 2 Sélectionnez un gestionnaire personnalisé dans le menu déroulant, puis choisissez un moment d'exécution. En règle générale, vous utiliserez la deuxième ou troisième option comme moment d'exécution.

REMARQUE : vous n'aurez généralement besoin que d'un seul gestionnaire personnalisé, mais vous pouvez en utiliser plusieurs en configurant des contrôles de flux dans le script pour relier les gestionnaires.

- 3 Vous devrez configurer  chaque gestionnaire personnalisé que vous ajoutez à la page. Les options de configuration varient en fonction du type de gestionnaire, mais l'ensemble des gestionnaires s'exécutent à partir de JavaScript.

Vous pouvez créer vos propres entrées Vanilla JavaScript ou utiliser des macros intégrées.

- ♦ **Gestionnaires de requête LDAP ou REST :**

1. Si vous souhaitez que votre requête repose sur des valeurs statiques, définissez **Informations de connexion** et **Paramètres de requête**.

Pour que votre requête soit dynamique, entrez un texte de marque de réservation dans les champs obligatoires. Cette opération est obligatoire pour permettre l'exécution du script. Le script remplace les valeurs fictives.

REMARQUE : Vous pouvez également configurer des en-têtes et des cookies pour la requête REST.

2. Dans l'action avant la requête, sélectionnez un type de macro : **Global**, **Requête** ou **Champ de formulaire**.
3. Sélectionnez une macro dans la liste déroulante et insérez-la (**</> Insérer la macro**).
4. Insérez d'autres macros selon vos besoins, puis indiquez les valeurs souhaitées pour effectuer le script.

Par exemple, dans l'action avant la requête, nous allons utiliser un script pour vérifier que le nom de groupe entré par un utilisateur n'existait pas encore dans Active Directory au moment de la soumission du formulaire.

Nous devons créer une requête LDAP à l'aide du nom entré par l'utilisateur. Nous utilisons la macro `Field()` pour accéder à la valeur du champ Nom et créer la chaîne de requête que nous définissons ensuite en tant que filtre de requête à l'aide de la macro `Filter()`.

```
Filter() = '(&(objectCategory=group)(objectClass=group)(name=' +  
Field(name) + '))';
```

5. En suivant l'exemple ci-dessus, nous allons vérifier les résultats renvoyés par la requête dans l'action après la requête. Les résultats sont renvoyés sous forme de tableau d'objets correspondant à la requête. Il nous suffit dès lors de vérifier si la longueur du tableau est supérieure à 0.

Lorsqu'un groupe correspondant est trouvé, nous utilisons la macro `Cancel()` pour annuler la soumission du formulaire, en transmettant à la macro un message facultatif à afficher pour l'utilisateur.

```
if (QueryResults().length > 0) { Cancel('Un groupe portant le même nom  
existe déjà, entrez un nom unique.');
```

- ♦ **Script** : insérez un code JavaScript personnalisé ou utilisez les macros pour générer le script.
 - ♦ **Requête DRA** : pour les paramètres de la requête, définissez une charge utile au format JSON. Utilisez ensuite les macros conformément à la description ci-dessus pour les requêtes LDAP et REST.
 - ♦ **Gestionnaires de zones Message** : après avoir défini les propriétés de la zone Message proprement dite, utilisez les macros de la même façon que décrit ci-dessus pour les requêtes LDAP et REST, mais au lieu des actions avant et après la requête, vous composez les scripts de macro des actions avant affichage et après fermeture.
- 4 Cliquez sur **Tester les gestionnaires** pour valider votre script avant l'enregistrement du formulaire.

Cette opération génère un résumé des résultats de test qui vous permet d'afficher les résultats de l'exécution.

REMARQUE : Si le gestionnaire dépend de l'état actuel du formulaire (par exemple, le champ contient une valeur), il ne s'exécute pas correctement, car aucune donnée n'est chargée lors de la modification d'un formulaire. Dans ces cas, le gestionnaire devra être testé en dehors de l'éditeur de formulaires en enregistrant la personnalisation, en accédant au formulaire approprié et en complétant les données requises.

8.2.3 Personnalisation de l'image de marque de l'interface utilisateur

Vous pouvez personnaliser la barre de titre de la console Web DRA avec votre propre titre et votre image de logo. Ils seront placés directement à droite du nom de produit DRA. Dans la mesure où cet emplacement est également utilisé pour la navigation de niveau supérieur, ils sont masqués par les liens de navigation DRA de niveau supérieur après vous être connecté. Toutefois, l'onglet du navigateur continue d'afficher le titre personnalisé.

Pour personnaliser l'image de marque du titre dans DRA :

- 1 Connectez-vous à la console Web en tant qu'administrateur DRA.
- 2 Accédez à **Personnalisation > Image de marque**.
- 3 Si vous ajoutez le logo d'une société, enregistrez l'image du logo dans `components\lib\img` sur le serveur Web.
- 4 Ajoutez les informations requises, le cas échéant, pour les trois champs sur la page de personnalisation de l'image de marque et enregistrez vos modifications.

9 Outils et utilitaires

Les sections suivantes expliquent l'utilitaire de diagnostic, l'utilitaire des objets supprimés, l'utilitaire de contrôle de l'état de santé et l'utilitaire de la corbeille fournis avec DRA.

9.1 Utilitaire de diagnostic

L'utilitaire de diagnostic rassemble les informations reçues de votre serveur d'administration pour diagnostiquer les problèmes liés à DRA. Il permet de générer des fichiers journaux que vous pouvez transmettre au représentant du support technique. L'utilitaire de diagnostic propose une interface d'assistant qui vous aide à définir les niveaux de consignation et à collecter des informations de diagnostic.

L'utilitaire de diagnostic est accessible à partir de n'importe quel ordinateur de serveur d'administration. Toutefois, vous devez exécuter l'utilitaire de diagnostic sur le serveur d'administration sur lequel vous avez rencontré le problème.

Pour accéder à l'utilitaire de diagnostic, connectez-vous à l'ordinateur de serveur d'administration en utilisant le compte administrateur DRA et exécutez `DRADiagnosticUtil.exe` à partir du dossier `Program Files (x86)\NetIQ\DRA`.

Pour plus d'informations sur l'utilisation de cet utilitaire, contactez le [support technique](#).

9.2 Utilitaire des objets supprimés

Cet utilitaire vous permet d'activer la prise en charge du rafraîchissement incrémentiel du cache des comptes pour un domaine spécifique lorsque le compte d'accès au domaine n'est pas un administrateur. Si le compte d'accès au domaine ne possède pas d'autorisations de lecture sur le conteneur Objets supprimés dans le domaine, DRA ne peut pas effectuer de rafraîchissement incrémentiel du cache des comptes.

Cet utilitaire permet d'effectuer les tâches suivantes :

- ♦ Vérifier que le groupe ou le compte utilisateur spécifié dispose d'autorisations de lecture sur le conteneur Objets supprimés dans le domaine spécifié
- ♦ Déléguer ou supprimer les autorisations de lecture pour un groupe ou un compte utilisateur spécifié
- ♦ Déléguer ou supprimer le droit utilisateur Synchroniser les données du service Annuaire pour un compte utilisateur
- ♦ Afficher les paramètres de sécurité pour le conteneur Objets supprimés

Vous pouvez exécuter le fichier de l'utilitaire des objets supprimés (`DraDelObjjsUtil.exe`) à partir du dossier `Program Files (x86)\NetIQ\DRA` sur votre serveur d'administration.

9.2.1 Autorisations requises pour l'utilitaire des objets supprimés

Pour utiliser cet utilitaire, vous devez disposer des autorisations suivantes :

Pour...	Vous avez besoin de l'autorisation suivante...
Vérifier les autorisations de compte	Autorisations de lecture sur le conteneur Objets supprimés
Déléguer des autorisations de lecture sur le conteneur Objets supprimés	Autorisations d'administrateur dans le domaine où se situe le conteneur Objets supprimés
Déléguer le droit utilisateur Synchroniser les données du service Annuaire	Autorisations d'administrateur dans le domaine où se situe le conteneur Objets supprimés
Supprimer les autorisations précédemment déléguées	Autorisations d'administrateur dans le domaine où se situe le conteneur Objets supprimés
Afficher les paramètres de sécurité pour le conteneur Objets supprimés	Autorisations de lecture sur le conteneur Objets supprimés

9.2.2 Syntaxe de l'utilitaire des objets supprimés

```
DRADELOBJSUTIL /DOMAIN:NOM_DOMAINE [/DC:NOM_ORDINATEUR] {/  
DELEGATE:NOM_COMPTE | /VERIFY:NOM_COMPTE | /REMOVE:NOM_COMPTE | /DISPLAY  
[/RIGHT]}
```

9.2.3 Options de l'utilitaire des objets supprimés

Vous pouvez spécifier les options suivantes :

/DOMAIN: <i>domaine</i>	Spécifie le nom DNS ou NETBIOS du domaine où se situe le conteneur Objets supprimés.
/SERVER: <i>nom_ordinateur</i>	Spécifie le nom ou l'adresse IP du contrôleur de domaine pour le domaine spécifié.
/DELEGATE: <i>nom_compte</i>	Délègue des autorisations au groupe ou compte utilisateur spécifié.
/REMOVE: <i>nom_compte</i>	Supprime les autorisations précédemment déléguées au groupe ou compte utilisateur spécifié.
/VERIFY: <i>nom_compte</i>	Vérifie les autorisations du groupe ou compte utilisateur spécifié.
/DISPLAY	Affiche les paramètres de sécurité du conteneur Objets supprimés dans le domaine spécifié.
/RIGHT	Vérifie que le groupe ou compte utilisateur spécifié possède le droit utilisateur Synchroniser les données du service Annuaire. Vous pouvez utiliser cette option pour déléguer ou vérifier ce droit. Le droit utilisateur Synchroniser les données du service Annuaire permet au compte de lire l'ensemble des objets et propriétés dans Active Directory.

REMARQUE

- ♦ Si le nom du groupe ou compte utilisateur que vous souhaitez spécifier contient un espace, entrez le nom du compte entre guillemets. Par exemple, si vous souhaitez spécifier le groupe Houston IT, tapez "Houston IT".
 - ♦ Si vous spécifiez un groupe, utilisez le nom de ce groupe d'une version antérieure à Windows 2000.
-

9.2.4 Exemples pour l'utilitaire des objets supprimés

Voici des exemples de commandes pour des scénarios courants.

Exemple 1

Pour vérifier que le compte utilisateur MYCOMPANY\JSmith possède des autorisations de lecture sur le conteneur Objets supprimés dans le domaine hou.mycompany.com, entrez :

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Exemple 2

Pour déléguer des autorisations de lecture sur le conteneur Objets supprimés dans le domaine MYCOMPANY au groupe MYCOMPANY\DraAdmins, entrez :

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Exemple 3

Pour déléguer des autorisations de lecture sur le conteneur Objets supprimés et le droit utilisateur Synchroniser les données du service Annuaire dans le domaine MYCOMPANY au compte utilisateur MYCOMPANY\JSmith, entrez :

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Exemple 4

Pour afficher les paramètres de sécurité du conteneur Objets supprimés dans le domaine hou.mycompany.com à l'aide du contrôleur de domaine HQDC, entrez :

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Exemple 5

Pour supprimer des autorisations de lecture sur le conteneur Objets supprimés dans le domaine MYCOMPANY à partir du groupe MYCOMPANY\DraAdmins, entrez :

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

9.3 Utilitaire de contrôle de l'état de santé

L'utilitaire de contrôle de l'état de santé DRA est une application autonome livrée avec le kit d'installation de DRA. L'utilitaire de contrôle de l'état de santé est utilisé après l'installation, ainsi qu'avant et après une mise à niveau, afin de vérifier, valider et indiquer l'état des composants et processus pour le serveur DRA, le site Web DRA et les clients DRA. Vous pouvez également l'utiliser pour installer ou mettre à jour une licence produit, pour sauvegarder l'instance AD LDS avant une mise à niveau du produit, pour afficher des descriptions des contrôles, et également pour résoudre des problèmes ou identifier les actions nécessaires pour résoudre des problèmes et ensuite les valider à nouveau.

L'utilitaire de contrôle de l'état de santé est accessible dans le dossier du programme DRA après l'exécution du programme d'installation `NetIQAdminInstallationKit.msi`.

Vous pouvez exécuter l'utilitaire de contrôle de l'état de santé à tout moment en exécutant le fichier `NetIQ.DRA.HealthCheckUI.exe`. Lorsque l'application s'ouvre, vous pouvez choisir d'effectuer une opération spécifique ou d'exécuter des contrôles sur certains composants ou sur l'ensemble des composants. Reportez-vous au tableau ci-dessous pour découvrir des fonctions utiles de l'utilitaire de contrôle de l'état de santé :

Fonction	Actions de l'utilisateur
Sélectionner tout ou désélectionner tout	Utilisez les options du menu Fichier ou de la barre d'outils pour sélectionner ou désélectionner tous les éléments contrôlables, ou cochez certaines cases pour exécuter des contrôles spécifiques.
Exécuter les contrôles sélectionnés	Utilisez cette option du menu Fichier ou de la barre d'outils pour exécuter les contrôles sélectionnés (tous ou certains).
Enregistrer ou écrire les résultats	Utilisez cette option du menu Fichier ou de la barre d'outils pour créer et enregistrer un rapport détaillé sur les contrôles exécutés.
Exécuter ce contrôle	Sélectionnez le titre d'un élément pour afficher une description du contrôle, puis cliquez sur cette icône de la barre d'outils pour exécuter le contrôle. Par exemple, pour exécuter l'une des opérations suivantes : <ul style="list-style-type: none">◆ Installer ou mettre à jour une licence produit (validation de licence)◆ Sauvegarder l'instance AD LDS (sauvegarde de l'instance AD LDS)
Résoudre ce problème	Sélectionnez le titre d'un élément, puis utilisez cette option de la barre d'outils lorsqu'un contrôle a échoué. Si la réexécution du contrôle ne permet pas de corriger le problème, la description doit inclure des informations ou les actions possibles pour résoudre le problème.

9.4 Utilitaire de la corbeille

Cet utilitaire vous permet d'activer la prise en charge de la corbeille lorsque vous gérez une sous-arborescence d'un domaine. Si le compte d'accès au domaine ne possède pas d'autorisations sur le conteneur `NetIQRecycleBin` masqué dans le domaine spécifié, DRA ne peut pas déplacer les comptes supprimés vers la corbeille.

REMARQUE : Après avoir utilisé cet utilitaire pour activer la corbeille, effectuez un rafraîchissement complet du cache des comptes pour garantir que le serveur d'administration applique cette modification.

Cet utilitaire permet d'effectuer les tâches suivantes :

- ♦ Vérifier que le compte spécifié dispose d'autorisations de lecture sur le conteneur NetIQRecycleBin dans le domaine spécifié
- ♦ Déléguer des autorisations de lecture à un compte spécifié
- ♦ Afficher les paramètres de sécurité pour le conteneur NetIQRecycleBin
- ♦ [Section 9.4.1, « Autorisations requises pour l'utilitaire de la corbeille », page 157](#)
- ♦ [Section 9.4.2, « Syntaxe de l'utilitaire de la corbeille », page 157](#)
- ♦ [Section 9.4.3, « Options de l'utilitaire de la corbeille », page 157](#)
- ♦ [Section 9.4.4, « Exemples pour l'utilitaire de la corbeille », page 157](#)

9.4.1 Autorisations requises pour l'utilitaire de la corbeille

Pour utiliser cet utilitaire, vous devez disposer des autorisations suivantes :

Pour...	Vous avez besoin de l'autorisation suivante...
Vérifier les autorisations de compte	Autorisations de lecture sur le conteneur NetIQRecycleBin
Déléguer des autorisations de lecture sur le conteneur NetIQRecycleBin	Autorisations d'administrateur dans le domaine spécifié
Afficher les paramètres de sécurité pour le conteneur NetIQRecycleBin	Autorisations de lecture sur le conteneur NetIQRecycleBin

9.4.2 Syntaxe de l'utilitaire de la corbeille

```
DRARECYCLEBINUTIL /DOMAIN:NOM_DOMAINE [/DC:NOM_ORDINATEUR] {/  
DELEGATE:NOM_COMPTE | /VERIFY:NOM_COMPTE | /DISPLAY}
```

9.4.3 Options de l'utilitaire de la corbeille

Les options suivantes vous permettent de configurer l'utilitaire de la corbeille :

<code>/DOMAIN:<i>domaine</i></code>	Spécifie le nom DNS ou NETBIOS du domaine où se situe la corbeille.
<code>/SERVER:<i>nom_ordinateur</i></code>	Spécifie le nom ou l'adresse IP du contrôleur de domaine pour le domaine spécifié.
<code>/DELEGATE:<i>nom_compte</i></code>	Délègue des autorisations au compte spécifié.
<code>/VERIFY:<i>nom_compte</i></code>	Vérifie les autorisations du compte spécifié.
<code>/DISPLAY</code>	Affiche les paramètres de sécurité du conteneur NetIQRecycleBin dans le domaine spécifié.

9.4.4 Exemples pour l'utilitaire de la corbeille

Voici des exemples de commandes pour des scénarios courants.

Exemple 1

Pour vérifier que le compte utilisateur `MYCOMPANY\JSmith` possède des autorisations de lecture sur le conteneur `NetIQRecycleBin` dans le domaine `hou.mycompany.com`, entrez :

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Exemple 2

Pour déléguer des autorisations de lecture sur le conteneur `NetIQRecycleBin` dans le domaine `MYCOMPANY` au groupe `MYCOMPANY\DraAdmins`, entrez :

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Exemple 3

Pour afficher les paramètres de sécurité du conteneur `NetIQRecycleBin` dans le domaine `hou.mycompany.com` à l'aide du contrôleur de domaine `HQDC`, entrez :

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```