NetIQ Directory and Resource Administrator

Guide de l'administrateur

Juin 2021

Avis juridique

À propos de ce guide

Le *Guide de l'administrateur* fournit des informations conceptuelles sur le produit NetIQ Directory and Resource Administrator (DRA). Cet ouvrage définit la terminologie et divers concepts connexes. Il fournit également des instructions pas à pas pour de nombreuses tâches de configuration et d'exploitation.

Public cible

Ce manuel fournit des renseignements aux personnes responsables de la compréhension des concepts administratifs et de la mise en œuvre d'un modèle d'administration distribué et sécurisé.

Documentation supplémentaire

Ce guide fait partie de la documentation de Directory and Resource Administrator. Pour obtenir la plus récente version de ce guide ainsi que d'autres documents sur DRA, visitez le site web de la documentation de DRA (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Coordonnées

Nous souhaitons recevoir vos commentaires et vos suggestions concernant ce livre et les autres documents inclus dans ce produit. Vous pouvez utiliser le lien **comment on this topic** (Faire un commentaire sur ce sujet) au bas de chaque page de la documentation en ligne, ou envoyer un courriel à Documentation-Feedback@microfocus.com.

Pour les questions spécifiques aux produits, contactez le service clientèle de Micro Focus à partir de l'adresse suivante : https://www.microfocus.com/support-and-services/.

Mise en route

Avant d'installer et de configurer tous les composants de NetIQ Directory and Resource Administrator (DRA), vous devez comprendre les fondements de ce que DRA fera pour votre entreprise et le rôle des composants de DRA dans l'architecture du produit.

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

NetIQ Directory and Resource Administrator est un outil qui offre une administration sécurisée et efficace de l'identité privilégiée de Microsoft Active Directory (AD). DRA effectue une délégation granulaire de « droit d'accès minimal » de sorte que les administrateurs et les utilisateurs ne reçoivent que les autorisations qui leur sont nécessaires pour s'acquitter de leurs responsabilités respectives. DRA assure également le respect des stratégies, fournit des audits et des rapports détaillés sur les activités et simplifie la réalisation de tâches répétitives grâce à l'automatisation des processus informatiques. Chacune de ces fonctionnalités contribue à protéger les environnements AD et Exchange de vos clients contre les risques d'élévation de privilèges, d'erreurs, d'activités malveillantes et de non-conformité réglementaire, tout en réduisant la charge de travail de l'administrateur par l'octroi des capacités de libre-service aux utilisateurs, aux gestionnaires d'entreprise et au personnel du service d'assistance.

DRA étend également les puissantes fonctionnalités de Microsoft Exchange, ce qui permet d'assurer une gestion transparente des objets Exchange. Grâce à 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 fournit les solutions dont vous avez besoin pour contrôler et gérer vos environnements Microsoft Active Directory, Windows, Exchange et Azure Active Directory.

- **Prise en charge d'Azure et d'Active Directory sur site, d'Exchange et de Skype Entreprise :**

  permet la gestion administrative d'Azure et d'Active Directory sur site, du serveur Exchange sur site, de Skype Entreprise sur site, d'Exchange Online et de Skype Entreprises Online.
- **Contrôles granulaires des accès/privilèges d'utilisateur et d'administration :** la technologie brevetée ActiveView ne délègue que les privilèges nécessaires pour s'acquitter de responsabilités précises et éviter l'élévation des privilèges.
- **Console Web personnalisable :** l'approche intuitive permet au personnel non technique d'effectuer facilement et en toute sécurité des tâches administratives grâce à des capacités et à des accès limités (et attribués).
- **Audit approfondi de l'activité et création de rapports :** fournit un enregistrement d'audit complet de toutes les activités effectuées par le produit. Stocke en toute sécurité les données à long terme et démontre aux auditeurs (p. ex. PCI DSS, FISMA, HIPAA et NERC CIP) que des processus sont en place pour contrôler l'accès à AD.
- **Automatisation des processus informatiques :** automatise les flux de travail pour une variété de tâches, comme le provisionnement et le déprovisionnement, les actions des utilisateurs et des boîtes aux lettres, l'application des stratégies et le contrôle des tâches en libre-service; augmente l'efficacité de l'entreprise et réduit les efforts administratifs manuels et répétitifs.
- **Intégrité opérationnelle :** empêche les changements malveillants ou incorrects qui affectent le fonctionnement et la disponibilité des systèmes et des services grâce à un contrôle d'accès granulaire accordé aux administrateurs et à la gestion de l'accès aux systèmes et aux ressources.

- **Application du processus :** garantit l'intégrité des processus clés de gestion du changement qui vous aident à améliorer la productivité, à réduire les erreurs, à gagner du temps et à accroître l'efficacité de l'administration.
- **Intégration avec Change Guardian :** améliore l'audit pour les événements générés dans Active Directory en dehors de DRA et de Workflow Automation.

2 Comprendre les composants de Directory and Resource Administrator

Les composants de DRA que vous utiliserez systématiquement pour gérer les accès privilégiés comprennent les serveurs principaux et secondaires, les consoles d'administrateur, les composants de création de rapports et Workflow Automation Engine pour automatiser les processus de travail.

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

Type d'utilisateur DRA	Interfaces utilisateur	Serveur d'administration
Administrateur DRA (La personne qui gérera la configuration du produit)	Console de délégation et de configuration	Serveur primaire
Administrateur avancé	Configuration du centre de création de rapports de DRA (NRC) PowerShell *(facultatif)* CLI *(facultatif)* Fournisseur DRA ADSI *(facultatif)*	N'importe quel serveur DRA
Administrateur occasionnel du service d'assistance	Console Web	Tout serveur DRA

Serveur d'administration DRA

Le serveur d'administration DRA stocke les données de configuration (environnement, accès délégué et stratégie), exécute les tâches d'automatisation et d'opérateur et audite l'activité du système. Tout en prenant en charge plusieurs clients de niveau console et API, le serveur est conçu pour offrir une haute disponibilité pour la redondance et l'isolation géographique par un modèle d'extension MMS (ensemble multimaître). Dans ce modèle, chaque environnement DRA requiert un serveur d'administration DRA primaire qui se synchronise avec un certain nombre de serveurs d'administration DRA secondaires supplémentaires.

Nous vous recommandons fortement 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 propres au site, telles que les

réinitialisations de mot de passe, vous pouvez spécifier un contrôleur de domaine propre au site pour traiter l'opération. Il est recommandé d'utiliser un serveur d'administration secondaire dédié pour la création de rapports, le traitement par lots et les charges de travail automatisées.

Console de délégation et de configuration

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

- **Gestion de la délégation :** vous permet de spécifier et d'affecter de façon granulaire des ressources et des tâches gérées aux administrateurs assistants.
- **Gestion des stratégies et de l'automatisation :** vous permet de définir et d'appliquer des stratégies pour assurer la conformité aux normes et aux conventions de l'environnement.
- **Gestion de la configuration :** vous permet de mettre à jour les paramètres et les options du système DRA, d'ajouter des personnalisations et de configurer les services gérés (Active Directory, Exchange, Azure Active Directory etc.).
- **Gestion des comptes et des ressources:** permet aux administrateurs assistants de DRA de visualiser et de gérer les objets délégués des domaines et des services connectés à partir de la console de délégation et de configuration.

Console Web

La console Web est une interface utilisateur basée sur le Web qui fournit un accès rapide et facile aux administrateurs assistants pour visualiser et gérer les objets délégués des domaines et services connectés. Les administrateurs peuvent personnaliser l'apparence et l'utilisation de la console Web afin d'inclure une marque d'entreprise et des propriétés de l'objet personnalisées.

Composants de création de rapports

Le module de création de rapports de DRA fournit des modèles intégrés et personnalisables pour la gestion de DRA et des détails sur les domaines et les systèmes gérés par DRA :

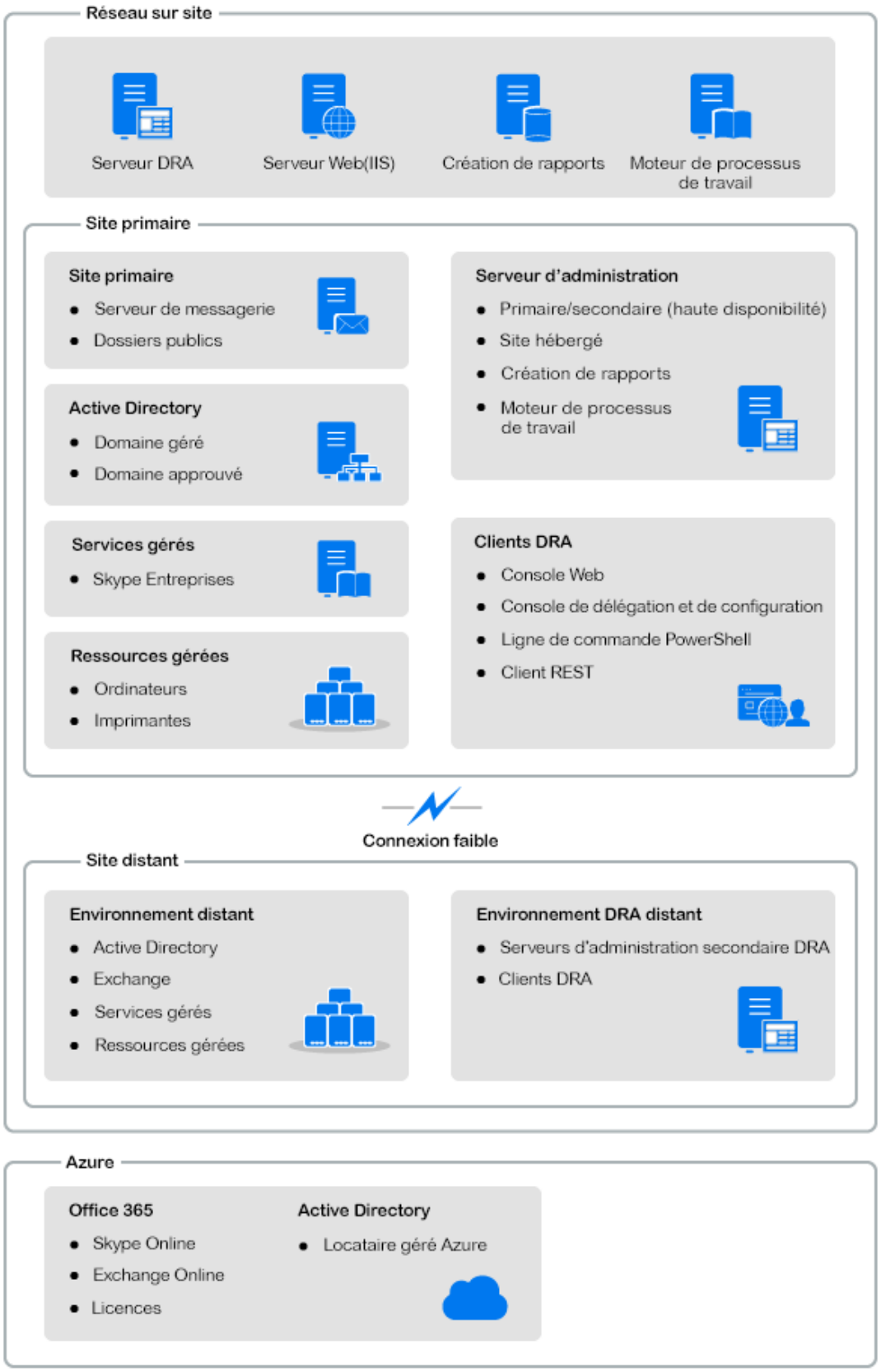
- Rapports de ressources pour les objets Active Directory
- Rapports sur les données d'objets Active Directory
- Rapports de synthèse d'Active Directory
- Rapports de configuration de DRA
- Rapports de configuration d'Exchange
- Rapports d'Office 365 Exchange Online
- Rapports détaillés sur les tendances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

Les rapports de DRA peuvent être planifiés et publiés par l'intermédiaire de SQL Server Reporting Services pour être facilement distribués aux parties prenantes.

Workflow Automation Engine

DRA s'intègre à Workflow Automation Engine afin d'automatiser les tâches de processus de travail au moyen d'une console Web. Grâce à celle-ci, les administrateurs assistants peuvent configurer le serveur de processus de travail et exécuter des formulaires personnalisés d'automatisation des processus de travail, puis visualiser l'état de ces processus de travail. Pour obtenir de plus amples renseignements sur Workflow Automation Engine, consultez le site de la documentation de DRA.

Architecture du produit



II Installation et mise à niveau du produit

Ce chapitre décrit les configurations matérielles, logicielles et de compte nécessaires pour Directory and Resource Administrator. Il vous guide ensuite tout au long du processus d'installation avec une liste de contrôle pour chaque composant de l'installation.

3 Planification de votre 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 pour prendre note des ports et des protocoles requis que vous devrez configurer pour le déploiement.

Recommandations de ressources testées

Cette section fournit des informations de dimensionnement que nous recommandons pour les ressources de base. Vos résultats peuvent varier en fonction du matériel disponible, d'un environnement précis, du type de données traitées et d'autres facteurs. Il est probable qu'il existe des configurations matérielles plus grandes et plus puissantes qui peuvent supporter une charge plus importante. Si vous avez des questions, veuillez consulter NetIQ Consulting Services.

Exécuté dans un environnement d'environ un million d'objets Active Directory :

Composant	UC	Mémoire	Stockage
Serveur d'administration DRA	8 UC/cœur 2,0 GHz	16 Go	120 Go
Console Web DRA	2 UC/cœur 2,0 GHz	8 Go	100 Go
Module de création de rapports de DRA	4 UC/cœur 2,0 GHz	16 Go	100 Go
Serveur de processus de travail DRA	4 UC/cœur 2,0 GHz	16 Go	120 Go

Provisionnement des ressources de l'environnement virtuel

DRA garde de grands segments de mémoire actifs pendant de longues périodes de temps. Lors du provisionnement des ressources pour un environnement virtuel, les recommandations suivantes devraient être prises en compte :

- Effectuer un « provisionnement statique » lors de l'allocation du stockage

- Mettre le paramètre de réservation de la mémoire à Réserver toute la mémoire de l'invité (toutes verrouillées)
- Assurez-vous que le fichier de pagination est suffisamment grand pour couvrir la réallocation potentielle de la mémoire gonflée au niveau de la couche virtuelle.

Ports et protocoles requis

Les ports et protocoles de communication DRA sont fournis dans cette section.

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

Tableaux des composants :

- « Serveurs d'administration DRA » page 24
- « Serveur DRA REST » page 26
- « Console Web (IIS) » page 26
- « Console de délégation et d'administration DRA » page 27
- « Serveur de processus de travail » page 27

Serveurs d'administration DRA

Protocole et port	Direction	Destination	Utilisation
TCP 135	Bidirectionnel	Serveurs d'administration DRA	Mappeur de point d'extrémité, une exigence de base pour la communication DRA; permet aux serveurs d'administration de se localiser dans MMS
TCP 445	Bidirectionnel	Serveurs d'administration DRA	Réplication du modèle de délégation; réplication de fichiers pendant la synchronisation MMS (SMB)
Plage de ports TCP dynamique *	Bidirectionnel	Contrôleurs de domaine Microsoft Active Directory	Par défaut, DRA attribue des ports dynamiquement à partir de la plage de ports TCP comprise entre 1024 et 65535. Vous pouvez toutefois configurer cette plage en utilisant Component Services. Pour plus d'informations, consultez *Utilisation du modèle COM distribué avec des pare-feu*.
TCP 50000 *	Bidirectionnel	Serveurs d'administration DRA	Réplication des attributs et communication entre le serveur DRA et AD LDS. (LDAP)
TCP 50001 *	Bidirectionnel	Serveurs d'administration DRA	Réplication des attributs SSL (AD LDS)

Protocole et port	Direction	Destination	Utilisation
TCP/UDP 389	Sortant	Contrôleurs de domaine Microsoft Active Directory	Gestion d'objets Active Directory (LDAP)
	Sortant	Microsoft Exchange Server	Gestion de la boîte aux lettres (LDAP)
TCP/UDP 53	Sortant	Contrôleurs de domaine Microsoft Active Directory	Résolution de nom
TCP/UDP 88	Sortant	Contrôleurs de domaine Microsoft Active Directory	Permet l'authentification du serveur DRA aux contrôleurs de domaine (Kerberos).
TCP 80 *	Sortant	Microsoft Exchange Server	Nécessaire pour tous les serveurs Exchange sur site à partir de 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 de Change Guardian (HTTPS)
TCP 443, 5986, 5985	Sortant	Microsoft PowerShell	Applets de commande PowerShell natifs (HTTPS) et PowerShell à distance.
TCP 5984	Hôte local	Serveurs d'administration DRA	Accès IIS au service de réplication pour prendre en charge les affectations de groupe temporaires
TCP 8092 * **	Sortant	Serveur de processus de travail	État et déclenchement du processus de travail (HTTPS)
TCP 50101 *	Entrant	Client DRA	Cliquez avec le bouton droit de la souris sur l'historique des modifications dans le rapport d'audit de l'interface utilisateur. Peut être configuré pendant l'installation.
TCP 8989	Hôte local	Service d'archivage des journaux	Communication d'archive de journaux (il n'est pas nécessaire de l'ouvrir au moyen du pare-feu)
TCP 50102	Bidirectionnel	Service de base DRA	Service d'archivage des journaux
TCP 50103	Hôte local	Service de mise en cache DRA	Communication du service de mise en cache sur le serveur DRA (il n'est pas nécessaire de l'ouvrir à travers le pare-feu)
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 unifié

Protocole et port	Direction	Destination	Utilisation
TCP 8898	Bidirectionnel	Serveurs d'administration DRA	Service de réplication de DRA : communication entre les serveurs de DRA pour les affectations de groupe temporaires
TCP 636	Sortant	Contrôleurs de domaine Microsoft Active Directory	Gestion d'objets Active Directory (LDAP SSL).

Serveur DRA REST

Protocole et port	Direction	Destination	Utilisation
TCP 8755 * **	Entrant	Serveur IIS, applets de commande DRA PowerShell	Exécuter les activités de processus de travail basées sur DRA REST (ActivityBroker).
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Autodécouverte à l'aide du Service Connection Point (SCP)
TCP 443	Sortant	Contrôleurs de domaine Microsoft AD	Autodécouverte à l'aide du Service Connection Point (SCP)

Console Web (IIS)

Protocole et port	Direction	Destination	Utilisation
TCP 8755 * **	Sortant	Service DRA REST	Pour la communication entre la console Web de DRA et DRA PowerShell
TCP 443	Entrant	Navigateur client	Ouvrir un site Web DRA
TCP 443 **	Sortant	Serveur d'authentification avancée	Authentification avancée

Console de délégation et d'administration DRA

Protocole et port	Direction	Destination	Utilisation
TCP 135	Sortant	Contrôleurs de domaine Microsoft Active Directory	Autodécouverte à l'aide de SCP
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de processus de travail de l'adaptateur DRA. Par défaut, DCOM attribue des ports dynamiquement à partir de la plage de ports TCP comprise entre 1024 et 65535. Vous pouvez toutefois configurer cette plage en utilisant Component Services. Pour plus d'informations, consultez *Utilisation du modèle COM distribué avec des pare-feu* (DCOM)
TCP 50102	Sortant	Service de base DRA	Génération d'un rapport sur l'historique des modifications

Serveur de processus de travail

Protocole et port	Direction	Destination	Utilisation
TCP 8755	Sortant	Serveurs d'administration DRA	Exécuter les activités de processus de travail basées sur DRA REST (ActivityBroker).
Plage de ports TCP dynamique *	Sortant	Serveurs d'administration DRA	Activités de processus de travail de l'adaptateur DRA. Par défaut, DCOM attribue des ports dynamiquement à partir de la plage de ports TCP comprise entre 1024 et 65535. Vous pouvez toutefois configurer cette plage en utilisant Component Services. Pour de plus amples renseignements, consultez *Utilisation du modèle COM distribué avec des pare-feu* (DCOM)
TCP 1433	Sortant	Microsoft SQL Server	Stockage des données de processus de travail
TCP 8091	Entrant	Console des opérations et console de configuration	Processus de travail BSL API (TCP)
TCP 8092 **	Entrant	Serveurs d'administration DRA	Processus de travail BSL API (HTTP) et (HTTPS)
TCP 2219	Hôte local	Fournisseur d'espace de nommage	Utilisé par le fournisseur d'espace de nommage pour exécuter les adaptateurs.

Protocole et port	Direction	Destination	Utilisation
TCP 9900	Hôte local	Moteur de corrélation	Utilisé par le moteur de corrélation pour communiquer avec Workflow Automation Engine et le fournisseur d'espace de nommage.
TCP 10117	Hôte local	Fournisseur d'espace de nommage pour la gestion des ressources	Utilisé par le fournisseur d'espace de nommage pour la gestion des ressources

Plateformes prises en charge

Pour obtenir les informations les plus récentes sur les plateformes logicielles prises en charge, reportez-vous à la page du produit Directory and Resource Administrator.

Système géré	Produits préalables
Azure Active Directory	Pour activer l'administration d'Azure, vous devez installer les modules PowerShell suivants : ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 ou une version ultérieure ◆ AzureRM.Profile 5.8.2 ou une version ultérieure ◆ Exchange Online PowerShell V2 1.0.1 ou une version ultérieure PowerShell 5.1 ou le module le plus récent est nécessaire pour installer les nouveaux modules Azure PowerShell.
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
Skype Entreprise	◆ Microsoft Skype Entreprise 2015
Historique des modifications	◆ Change Guardian 5.1 ou une version ultérieure
Bases de données	◆ Microsoft SQL Server 2016
Navigateurs Web	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
Automatisation de processus de travail	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019

Configuration requise pour le serveur d'administration et la console Web de DRA

Les composants DRA nécessitent les logiciels et les comptes suivants :

Configuration logicielle requise

Composant	Produits préalables
Cible d'installation **Système d'exploitation**	**Système d'exploitation du serveur d'administration NetIQ :** ◆ Microsoft Windows Server 2012 R2, 2016, 2019 **REMARQUE :** Le serveur doit également faire partie d'un domaine Active Directory pris en charge par Microsoft sur site. **Interfaces DRA :** ◆ Microsoft Windows Server 2012 R2, 2016, 2019
Programme d'installation	◆ Microsoft Net Framework 4.8 et les versions supérieures.

Composant	Produits préalables
Serveur d'administration	**Directory and Resource Administrator:** ◆ Microsoft Net Framework 4.8 et les versions supérieures. ◆ Microsoft Visual C++ 2015 à 2019, Paquets redistribuables (x64 et x86) ◆ Microsoft Message Queuing ◆ Rôles Microsoft Active Directory Lightweight Directory Services ◆ Service de registre distant démarré ◆ Module de réécriture d'URL pour Microsoft Internet Information Services ◆ Routage des demandes d'application pour Microsoft Internet Information Services **REMARQUE :** NetIQ DRA REST Service est installé avec le serveur d'administration. **Microsoft Office 365/Exchange Online Administration :** ◆ Module Active Directory Windows Azure pour Windows PowerShell ◆ Module Windows PowerShell ◆ Module PowerShell Exchange Online V2 ◆ Activez WinRM pour l'authentification de base du côté client pour les tâches d'Exchange Online. Pour obtenir de plus amples renseignements, consultez Plateformes prises en charge.
Interface utilisateur	**Interfaces DRA :** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015 à 2019, Paquets redistribuables (x64 et x86)
Extensions PowerShell	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 ou une version ultérieure
Console Web DRA	**Serveur Web :** ◆ Microsoft .Net Framework 4.x > Services WCF > Activation HTTP ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Module de réécriture d'URL pour Microsoft Internet Information Services ◆ Routage des demandes d'application pour Microsoft Internet Information Services

Domaine du serveur

Composant	Systèmes d'exploitation
Serveur DRA	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

Exigences relatives aux 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 de service DRA	Les autorisations requises pour exécuter le service d'administration NetIQ	◆ Pour autorisations « Utilisateurs du modèle COM distribué »
		◆ Membre du groupe AD LDS Admin
		◆ Groupe d'opérateurs de compte
		◆ Groupes d'archivage de journaux (OnePointOp ConfgAdms et OnePointOp)
		◆ L'une des options de l'onglet Account > **Account options** (Compte > Options de compte) doit être sélectionnée pour l'utilisateur du compte de service DRA si DRA est installé sur un serveur en utilisant la méthodologie STIG :
		  ◆ Chiffrement Kerberos AES 128 bits
		  ◆ Chiffrement Kerberos AES 256 bits
		REMARQUE
		◆ Pour plus d'informations sur la configuration des comptes d'accès aux domaines de droit d'accès minimal, consultez : Comptes d'accès DRA de droit d'accès minimal.
		◆ Pour en savoir plus sur la configuration d'un compte de service géré de groupe pour DRA, reportez-vous à « Configuration des services de DRA pour un compte de service géré de groupe » dans le *Guide de l'administrateur de DRA*.

Compte	Description	Autorisations
Administrateur DRA	compte d'utilisateur ou groupe provisionné dans le rôle DRA Admin intégré.	◆ Groupe de sécurité locale de domaine ou compte d'utilisateur de domaine ◆ Membre du domaine géré ou d'un domaine approuvé ◆ Si vous spécifiez un compte à partir d'un domaine approuvé, vérifiez que l'ordinateur serveur d'administration peut authentifier ce compte.
Comptes d'administrateur assistant DRA	Comptes qui se verront déléguer des pouvoirs par l'intermédiaire de DRA	◆ Ajoutez·tous·les·comptes·d'administrateur·Assistant·DRA·au·groupe·« Utilisateurs du modèle COM distribué » afin qu'ils puissent se connecter au serveur DRA à partir de clients distants. Cela n'est nécessaire que lorsque vous utilisez un client lourd ou la console de délégation et de configuration. **REMARQUE :** DRA peut être configuré pour gérer cela pour vous pendant l'installation.

Comptes d'accès DRA de droit d'accès minimal

Vous trouverez ci-dessous les autorisations et les privilèges nécessaires pour les comptes spécifiés ainsi que les commandes de configuration que vous devez exécuter.

Compte d'accès au domaine : L'utilisation d'ADSI Edit permet d'accorder au compte d'accès au domaine les autorisations Active Directory suivantes au niveau du domaine supérieur pour les types d'objets descendants suivants :

- Contrôle TOTAL sur les objets builtInDomain
- Contrôle TOTAL sur les objets Ordinateurs
- Contrôle TOTAL sur les objets Point de connexion
- Contrôle TOTAL sur les objets Contacts
- Contrôle TOTAL sur les objets Conteneurs
- Contrôle TOTAL sur les objets Groupes
- Contrôle TOTAL sur les objets InetOrgPerson
- Contrôle TOTAL sur les objets MsExchDynamicDistributionList
- Contrôle TOTAL sur les objets MsExchSystemObjectsContainer
- Contrôle TOTAL sur les objets msDS-GroupManagedServiceAccount
- Contrôle TOTAL sur les objets Unités organisationnelles
- Contrôle TOTAL sur les objets Imprimantes

- Contrôle TOTAL sur les objets Dossiers publics
- Contrôle TOTAL sur les objets Dossiers partagés
- Contrôle TOTAL sur les objets Utilisateurs

Accorder au compte d'accès au domaine les autorisations d'Active Directory suivantes au niveau du domaine supérieur pour cet objet et tous les objets descendants :

- Autoriser la création d'objets Ordinateurs
- Autoriser la création d'objets Contacts
- Autoriser la création de Conteneurs
- Autoriser la création d'objets Groupes
- Autoriser la création d'objets MsExchDynamicDistributionList
- Autoriser la création d'objets msDS-GroupManagedServiceAccount
- Autoriser la création d'objets Unités organisationnelles
- Autoriser la création d'objets Dossiers publics
- Autoriser la création d'objets Dossiers partagés
- Autoriser la création d'objets Utilisateurs
- Autoriser la suppression d'objets Ordinateurs
- Autoriser la suppression d'objets Contacts
- Autoriser la suppression de Conteneurs
- Autoriser la suppression d'objets Groupes
- Autoriser la suppression d'objets InetOrgPerson
- Autoriser la suppression d'objets MsExchDynamicDistributionList
- Autoriser la suppression d'objets msDS-GroupManagedServiceAccount
- Autoriser la suppression d'objets Unités organisationnelles
- Autoriser la suppression d'objets Dossiers publics
- Autoriser la suppression d'objets Dossiers partagés
- Autoriser la suppression d'objets Utilisateurs

REMARQUE

- Par défaut, certains objets conteneurs intégrés dans Active Directory n'héritent pas des autorisations du niveau supérieur du domaine. C'est pourquoi il faudra activer l'héritage pour ces objets, ou définir des autorisations explicites.
- Si vous utilisez un compte avec un droit d'accès minimal comme compte d'accès, assurez-vous que le compte se voit attribuer l'autorisation « Reset Password » (Réinitialiser le mot de passe) dans Active Directory pour qu'il soit possible de réinitialiser le mot de passe dans DRA.

Compte d'accès Exchange : Pour gérer les objets Microsoft Exchange sur site, attribuez le rôle de gestion organisationnelle au compte d'accès à Exchange et le compte d'accès à Exchange au groupe des opérateurs de compte.

Compte d'accès Skype : Assurez-vous que ce compte est un utilisateur compatible Skype et qu'il est membre d'au moins l'un des groupes suivants :

- Rôle CSAdministrator
- Les rôles CSUserAdministrator et CSArchiving

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

- Gestion des dossiers publics
- Dossiers publics à extension messagerie

Compte d'accès du locataire Azure : Affectez les autorisations Azure Active Directory suivantes au compte d'accès du locataire Azure :

- Groupes de distribution
- Destinataires du courriel
- Création des destinataires du courriel
- Création du groupe de sécurité et adhésion
- (Facultatif) Administrateur de Skype Entreprise

  Si vous souhaitez gérer Skype Entreprise Online, attribuez les droits d'administrateur de Skype Entreprise au compte d'accès du locataire Azure.
- Administrateur des utilisateurs

Autorisations de compte du service d'administration NetIQ :

- Administrateurs locaux
- Accordez au compte de remplacement avec un droit d'accès minimal une « Autorisation totale » sur les dossiers de partage ou les dossiers DFS où les répertoires privés sont provisionnés.
- **Gestion des ressources :** Pour gérer les ressources publiées dans un domaine Active Directory géré, le compte d'accès au domaine doit obtenir des autorisations d'administration locale sur ces ressources.

Après l'installation de DRA : Vous devez exécuter les commandes suivantes avant de gérer les domaines requis :

- Pour déléguer l'autorisation sur le « conteneur Objets supprimés » à partir du dossier d'installation de DRA (remarque : la commande doit être exécutée par un administrateur de domaine) :

  `DraDelObjsUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<NomCompte>`
- Pour déléguer l'autorisation à « NetIQReceyleBin OU » à partir du dossier d'installation de DRA :

  `DraRecycleBinUtil.exe /domain:<NomDomaineNetBIOS> /delegate:<NomCompte>`

Accès à distance à SAM : Attribuer des contrôleurs de domaine ou des serveurs membres gérés par DRA pour activer les comptes énumérés dans le paramètre GPO ci-dessous, afin qu'ils puissent effectuer des interrogations à distance dans la base de données du gestionnaire de comptes de sécurité (SAM). La configuration doit inclure le compte de service DRA.

Accès au réseau : Restreindre les clients autorisés à passer des appels à distance vers SAM

Pour accéder à ce paramètre, procédez comme suit :

1. Ouvrez la console de gestion des stratégies de groupe sur le contrôleur de domaine.
2. Développez **Domains** > **[domain controller]** > **Group Policy Objects** (Domaines > [contrôleur de domaine] > Objets de stratégie de groupe) dans l'arborescence des nœuds.
3. Cliquez avec le bouton droit de la souris sur **Default Domain Controllers Policy** (Stratégie des contrôleurs de domaine par défaut) et sélectionnez **Edit** (Modifier) pour ouvrir l'éditeur GPO de cette stratégie.
4. Développez **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** (Configuration de l'ordinateur > Stratégies > Paramètres de Windows > Paramètres de sécurité > Stratégies locales) dans l'arborescence de nœuds de l'éditeur GPO.
5. Double-cliquez sur **Network access: Restrict clients allowed to make remote calls to SAM** (Accès au réseau : Restreindre les clients autorisés à effectuer des appels à distance vers SAM) dans le volet des stratégies, et sélectionnez **Define this policy setting** (Définir ce paramètre de stratégie).
6. Cliquez sur **Edit Security** (Modifier la sécurité) et activez **Allow** (Autoriser) pour l'accès à distance. Ajoutez le compte de service DRA s'il n'est pas déjà inclus en tant qu'utilisateur ou partie du groupe des administrateurs.
7. Appliquez les modifications. Cela ajoutera le descripteur de sécurité, `O:BAG:BAD:(A;;RC;;;BA)` aux paramètres de la stratégie.

Pour obtenir de plus amples renseignements, consultez l'article 7023292 de la base de connaissances.

Configuration requise pour la création de rapports

La configuration requise pour le composant de création de rapports de DRA comprend :

Configuration logicielle requise

Composant	Produits préalables
Cible d'installation	**Système d'exploitation** ◆ Microsoft Windows Server 2012 R2, 2016, 2019

Composant	Produits préalables
NetIQ Reporting Center (v3.3)	**Base de données :** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ L'administrateur de domaine qui gère les tâches de l'agent SQL doit disposer d'autorisations de sécurité pour Microsoft SQL Server Integration Services, sinon certains rapports du NRC ne seront pas traités. **Serveur Web :** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Composants Microsoft IIS : ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ Nécessaire pour faire fonctionner le programme d'installation du NRC ◆ Également requis sur le serveur primaire de DRA pour la configuration des services de création de rapports de DRA **REMARQUE :** Lors de l'installation du NetIQ Reporting Center (NRC) sur un ordinateur SQL Server, il peut être nécessaire d'installer .NET Framework 3.5 manuellement avant l'installation du NRC. **Protocole de sécurité des communications :** ◆ SQL Server doit prendre en charge TLS 1.2. Pour plus d'informations, reportez-vous à la rubrique Prise en charge de TLS 1.2 pour Microsoft SQL Server. ◆ Le serveur SQL doit avoir un pilote pris en charge par TLS mis à jour installé sur le serveur DRA. Le pilote suggéré est le dernier Microsoft® SQL Server® 2012 Native Client - QFE. ◆ La même version du protocole TLS doit être prise en charge dans le système d'exploitation du serveur SQL et du serveur d'administration de DRA. Par exemple, seul TLS 1.2 a été activé.
Module de création de rapports de DRA	**Base de données :** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

Exigences relatives aux licences

Votre licence détermine les produits et fonctionnalités que vous pouvez utiliser. DRA requiert une clé de licence installée avec le serveur d'administration.

Après avoir installé le serveur d'administration, vous pouvez utiliser l'utilitaire de contrôle de l'intégrité pour installer la licence que vous avez achetée. Une clé de licence d'essai (TrialLicense.lic) est également incluse dans le paquetage d'installation qui vous permet de gérer un nombre illimité de comptes d’utilisateurs et de boîtes aux lettres pendant 30 jours.

Reportez-vous au contrat de licence d'utilisateur final du produit (CLUF) pour plus de renseignements sur la définition et les restrictions de licence.

4 Installation du produit

Ce chapitre vous guide dans l'installation de Directory and Resource Administrator. Pour de plus amples renseignements sur la planification de votre installation ou de votre mise à niveau, consultez Planification de votre déploiement.

Installer le serveur d'administration DRA

Vous pouvez installer le serveur d'administration DRA en tant que nœud primaire ou secondaire dans votre environnement. Les exigences pour un serveur d'administration primaire et secondaire sont les mêmes; cependant, chaque déploiement DRA doit inclure un serveur d'administration primaire.

Le paquetage du serveur DRA présente les caractéristiques suivantes :

- **Serveur d'administration :** Stocke les données de configuration (environnement, accès délégué et stratégie), exécute les tâches des opérateurs et de l'automatisation, et vérifie l'activité de l'ensemble du système. Il possède les caractéristiques suivantes :
  - **Log Archive Resource Kit :** vous permet de consulter les informations relatives à l'audit.
  - **DRA SDK :** fournit les exemples de scripts ADSI et vous aide à créer vos propres scripts.
  - **Affectations de groupe temporaire:** Fournit les composants permettant d'activer la synchronisation des affectations de groupe temporaires.
- **Interfaces utilisateur :** interface du client Web principalement utilisée par les administrateurs assistants, mais également des options de personnalisation.
  - **Fournisseur ADSI :** vous permet de créer vos propres scripts de stratégie.
  - **Interface de ligne de commande :** vous permet d'effectuer des opérations liées à DRA.
  - **Délégation et configuration :** permet aux administrateurs système d'accéder aux fonctions de configuration et d'administration de DRA. Vous permet également de spécifier et d'affecter de façon granulaire l'accès aux ressources gérées et aux tâches aux administrateurs assistants.
  - **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 :** interface du client Web principalement utilisée par les administrateurs assistants, mais également des options de personnalisation.

Pour obtenir des informations sur l'installation de consoles DRA spécifiques et de clients de ligne de commande sur plusieurs ordinateurs, consultez la rubrique Installer les clients DRA.

Liste de contrôle d'installation interactive :

Étape	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour l'installation avec un compte disposant de droits d'accès d'administration locaux.
Copie et exécution de la trousse d'installation de Admin	Exécutez la trousse d'installation DRA (NetIQAdminInInstallationKit.msi) pour extraire le fichier d'installation de DRA vers le système de fichiers local. **REMARQUE :** La trousse d'installation installera .Net framework sur le serveur cible si nécessaire.
Installation de DRA	Cliquez sur **Install DRA** (Installer DRA), puis sur **Next** (Suivant) pour voir les options d'installation. **REMARQUE :** Pour exécuter l'installation plus tard, accédez à l'emplacement où le fichier d'installation a été extrait (consultez la trousse d'installation) et exécutez `Setup.exe`.
Installation par défaut	Choisissez les composants à installer et acceptez l'emplacement d'installation par défaut `C:\Program Files (x86)\NetIQ\DRA` ou spécifiez un autre emplacement pour l'installation. Options des composants : **Serveur d'administration** ◆ Log Archive Resource Kit (facultatif) ◆ DRA SDK ◆ Affectations de groupe temporaire **Interfaces utilisateur** ◆ Fournisseur ADSI (facultatif) ◆ Interface de ligne de commande (facultatif) ◆ Délégation et configuration ◆ Extensions PowerShell ◆ La console Web
Vérification des produits préalables	La boîte de dialogue **Prerequisites List** (Liste des produits préalables) affichera la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guidera lors de l'installation de tous les produits préalables qui sont nécessaires pour que l'installation réussisse.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final.
Spécification de l'emplacement du journal	Indiquez l'emplacement où DRA stockera tous les fichiers journaux. **REMARQUE :** Les journaux de la console de délégation et de configuration et les journaux d'ADSI sont stockés dans le dossier du profil de l'utilisateur.

Étape	Détails
Sélection du mode de fonctionnement du serveur	Sélectionnez **Primary Administration Server** (Serveur d'administration primaire) pour installer le premier serveur d'administration DRA dans un ensemble multimaître (il n'y aura qu'un seul serveur primaire dans un déploiement) ou **Secondary Administration Server** (Serveur d'administration secondaire) pour joindre un nouveau serveur d'administration DRA à un ensemble multimaître existant. Pour obtenir des informations sur l'ensemble multimaître, consultez la rubrique « Configuration de l'ensemble multimaître » dans le *Guide de l'administrateur de DRA*.
Spécification des comptes d'installation et des informations d'identification	◆ Compte de service DRA ◆ Groupe AD LDS ◆ Administrateur DRA Compte Pour obtenir de plus amples renseignements, consultez :Configuration requise pour le serveur d'administration et la console Web de DRA.
Configuration des autorisations DCOM	Autorisez DRA à configurer l'accès « COM distribué » pour les utilisateurs authentifiés.
Configuration des ports	Pour obtenir de plus amples renseignements sur les ports par défaut, consultez Ports et protocoles requis.
Spécification de l'emplacement de stockage	Spécifiez l'emplacement du fichier local que DRA doit utiliser pour stocker les données d'audit et de mise en cache.
Spécification de l'emplacement de la base de données de réplication de DRA	◆ Spécifiez l'emplacement du fichier pour la base de données de réplication de DRA et le port du service de réplication. ◆ Spécifiez le certificat SSL que vous souhaitez utiliser pour les communications sécurisées avec la base de données via IIS, et indiquez le port de réplication IIS.
Spécification du certificat SSL du service REST	Sélectionnez le certificat SSL que vous utiliserez pour le service REST et spécifiez le port du service REST.
Spécification du certificat SSL de la console Web	Spécifiez le certificat SSL que vous utiliserez pour la liaison HTTPS.
Vérification de la configuration d'installation	Vous pouvez vérifier la configuration sur la page de synthèse de l'installation avant de cliquer sur **Installer** pour procéder à l'installation.
Vérification post-installation	Une fois l'installation terminée, l'outil de contrôle de l'intégrité s'exécute pour vérifier l'installation et mettre à jour la licence du produit. Pour de plus amples renseignements, consultez la section Utilitaire de contrôle de l'intégrité du *Guide de l'administrateur de DRA*.

Installer les clients DRA

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

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 donnés sur plusieurs ordinateurs de votre entreprise, configurez un objet de stratégie de groupe pour installer le paquet .MST correspondant.

1. Démarrez Utilisateurs et ordinateurs Active Directory et créez un objet de stratégie de groupe.
2. Ajoutez le paquet DRAInstaller.msi à cet objet de stratégie de groupe.
3. Assurez-vous que cet objet de stratégie de groupe possède l'une des propriétés suivantes :
   - Chaque compte d'utilisateur du groupe dispose des autorisations d'utilisateur expérimenté pour l'ordinateur approprié.
   - Activez le paramètre de stratégie Toujours installer avec des privilèges élevés.
4. Ajoutez le fichier .mst de l'interface utilisateur à cet objet de stratégie de groupe.
5. Distribuez votre stratégie de groupe.

REMARQUE : Pour obtenir de plus amples renseignements sur la stratégie de groupe, consultez l'aide de Microsoft Windows. Pour tester et déployer facilement et en toute sécurité la stratégie de groupe dans votre entreprise, utilisez *Administrateur de stratégie de groupe*.

Installation de Workflow Automation et configuration des paramètres

Pour gérer les requêtes de Workflow Automation dans DRA, vous devez procéder comme suit :

- Installez et configurez Workflow Automation et DRA Adapter.

  Pour plus d'informations, reportez-vous au *Guide de l'administrateur de Workflow Automation* et au *Guide de référence de Workflow Automation Adapter pour DRA*.
- Configurez l'intégration de Workflow Automation avec DRA.

  Pour en savoir plus, reportez-vous à la rubrique « Configuration du serveur de Workflow Automation » dans le *Guide de l'administrateur de DRA*.
- Déléguez les pouvoirs de Workflow Automation dans DRA.

  Pour en savoir plus, reportez-vous à à la rubrique « Délégation des pouvoirs de configuration du serveur de Workflow Automation » dans le *Guide de l'administrateur de DRA*.

Les documents mentionnés ci-dessus sont disponibles sur le site de la documentation de DRA.

Installez le module de création de rapports de DRA

Le module de création de rapports de DRA nécessite l'installation du fichier DRAReportingSetup.exe à partir de la trousse d'installation NetIQ DRA.

Étapes	Détails
Connexion au serveur cible	Connectez-vous au serveur Microsoft Windows cible pour l'installation avec un compte disposant de droits d'accès d'administration locaux. Assurez-vous que ce compte dispose des privilèges d'administrateur local et de domaine, ainsi que des privilèges d'administrateur système sur le serveur SQL.
Copie et exécution de la trousse d'installation de NetIQ Admin	Copiez la trousse d'installation de DRA NetIQAdminINstallationKit.msi sur le serveur cible et exécutez le programme en double-cliquant sur le fichier ou en l'appelant à partir de la ligne de commande. La trousse d'installation extrait le fichier d'installation de DRA sur le système de fichiers local vers un emplacement personnalisable. De plus, la trousse d'installation installera .Net framework sur le serveur cible si nécessaire pour satisfaire les conditions préalables du programme d'installation du produit DRA.
Exécution de l'installation du module de création de rapports de DRA	Accédez à l'emplacement où le fichier d'installation a été extrait et exécutez DRA`ReportingSetup.exe` pour installer le composant de gestion pour l'intégration du module de création de rapports de DRA.
Vérification et installation des produits préalables	La boîte de dialogue **Produits préalables** affichera la liste des logiciels requis en fonction des composants sélectionnés pour l'installation. Le programme d'installation vous guidera dans l'installation de tous les produits préalables manquants qui sont requis pour que l'installation se termine avec succès. Pour obtenir de plus amples renseignements sur le centre de création de rapport de NetIQ, consultez le *Guide du centre de création de rapports* sur le site de la documentation.
Acceptation du CLUF	Acceptez les termes du contrat de licence d'utilisateur final pour terminer l'installation.

5 Mise à niveau du produit

Ce chapitre fournit un processus qui vous aide à mettre à niveau ou à migrer un environnement distribué en phases contrôlées.

Dans ce chapitre, nous supposons que votre environnement contient plusieurs serveurs d'administration, certains serveurs étant situés sur des sites distants. Cette configuration s'appelle un ensemble multimaître (MMS). Un MMS comprend un serveur d'administration primaire et un ou plusieurs serveurs d'administration secondaires associés. Pour obtenir de plus amples renseignements sur le fonctionnement d'un MMS, consultez la rubrique « Configuration d'un ensemble multimaître » du *Guide de l'administrateur de DRA*.

Planification de la mise à niveau de DRA

Exécutez le `NetIQAdminInstallationKit.msi` pour extraire le fichier d'installation de DRA, puis installez et exécutez l'utilitaire de contrôle de l'intégrité.

Veillez à planifier votre déploiement de DRA avant de commencer le processus de mise à niveau. Lors de la planification de votre déploiement, tenez compte des règles suivantes :

- Testez le processus de mise à niveau dans votre environnement de laboratoire avant de procéder à la mise à niveau vers votre environnement de production. Les tests vous permettent d'identifier et de résoudre tout problème inattendu sans affecter les responsabilités d'administration quotidiennes.
- Examinez Ports et protocoles requis.
- Déterminez combien d'administrateurs assistants dépendent de chaque MMS. Si la majorité de vos administrateurs assistants utilisent des serveurs ou des ensembles de serveurs précis, mettez d'abord à niveau ces serveurs pendant les heures creuses.
- Déterminez quels administrateurs assistants ont besoin de la console de délégation et de configuration. Vous pouvez obtenir ces informations de l'une des façons suivantes :
  - Vérifiez quels sont les administrateurs assistants associés aux groupes d'administrateurs assistants intégrés.
  - Examinez les administrateurs assistants associés aux ActiveViews intégrées.
  - Utilisez Directory and Resource Administrator Reporting pour générer des rapports sur les modèles de sécurité, tels que les rapports sur les détails d'administrateurs assistants ActiveView et les groupes d'administrateurs assistants.

Informez ces administrateurs assistants de vos projets de mise à niveau des interfaces utilisateur.

- Déterminez les administrateurs assistants qui doivent se connecter au serveur d'administration primaire. Ces administrateurs assistants doivent mettre à niveau leurs ordinateurs clients après la mise à niveau du serveur d'administration primaire.

  Informez ces administrateurs assistants de vos projets 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 le processus de mise à niveau. Selon votre environnement, cette décision peut être prise site par site.
- Coordonnez la mise à niveau de vos ordinateurs clients et de vos serveurs d'administration pour garantir des temps d'arrêt minimaux. Sachez que DRA ne prend pas en charge l'exécution simultanée des versions précédentes et actuelle de DRA sur le même serveur d'administration ou ordinateur client.

IMPORTANT

- Si la console de gestion des comptes et des ressources (ARM) est installée sur votre version précédente de DRA, elle sera supprimée lors de la mise à niveau.
- Lorsque vous mettez à niveau le serveur DRA à partir d'une version 9.x de DRA, tous les locataires gérés sont supprimés de DRA. Pour continuer à utiliser ces locataires en utilisant Azure, vous devez les ajouter après la mise à niveau. Pour en savoir plus sur l'ajout de locataires, consultez les rubriques Création d'une application Azure et Ajout d'un locataire Azure dans le *Guide de l'administrateur de DRA*.
- Étant donné qu'Exchange 2010 n'est pas pris en charge dans DRA 10.1, Exchange est désactivé lors de la mise à niveau à partir de DRA 9.x. Pour continuer à effectuer des opérations Exchange après la mise à niveau, désactivez et réactivez l'option **Enable Exchange Policy** (Activer la stratégie Exchange) dans la console de délégation et de configuration. Les deux modifications doivent être « appliquées » pour que la stratégie soit réinitialisée.

  Pour obtenir de plus amples renseignements sur cette configuration de stratégie, consultez la rubrique « Activation de Microsoft Exchange » du *Guide de l'administrateur de DRA*.

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.

Étapes	Détails
Sauvegardez l'instance AD LDS	Ouvrez l'utilitaire de contrôle de l'intégrité et exécutez la vérification **Sauvegarde d'instance AD LDS** pour créer une sauvegarde de votre instance AD LDS actuelle.
Établissez un plan de déploiement	Établissez un plan de déploiement pour la mise à niveau des serveurs d'administration et des interfaces utilisateur (ordinateurs clients d'administrateurs assistants). Pour obtenir de plus amples renseignements, consultez Planification de la mise à niveau de DRA.

Étapes	Détails
Dédiez un serveur secondaire pour exécuter une version précédente de DRA	*Facultatif :* Dédiez un serveur d'administration secondaire pour exécuter une version précédente de DRA lorsque vous mettez à niveau un site.
Apportez les modifications requises 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.
Synchronisez le MMS	Synchronisez les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.
Sauvegardez le registre du serveur primaire	Sauvegardez le registre à partir du serveur d'administration primaire. La sauvegarde de vos paramètres de registre précédents vous permet de récupérer facilement vos paramètres de configuration et de sécurité précédents..
Convertissez les comptes d'utilisateurs gMSA en comptes d'utilisateurs DRA	*Facultatif :* si vous utilisez un compte de service géré de groupe (gMSA) pour le compte de service DRA, remplacez le compte gMSA par un compte d'utilisateur DRA avant la mise à niveau. Après la mise à niveau, vous devrez changer le compte pour revenir à un compte gMSA.

REMARQUE : Si vous devez restaurer la sauvegarde de l'instance AD LDS, procédez comme suit :

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

Rubriques sur les préalables à la mise à niveau :

- « Utilisation d'un serveur d'administration local dédié pour exécuter une version précédente de DRA » page 48
- « Synchronisation de votre ensemble de serveurs DRA des versions précédentes » page 49
- « Sauvegarde du registre du serveur d'administration » page 49

Utilisation d'un serveur d'administration local dédié pour exécuter une version précédente de DRA

L'utilisation d'un ou de plusieurs serveurs d'administration secondaires pour exécuter une version précédente de DRA localement sur un site pendant la mise à niveau peut aider à réduire les temps d'arrêt et les connexions coûteuses aux sites distants. Cette étape est facultative et permet aux administrateurs assistants d'utiliser une version précédente de DRA tout au long du processus de mise à niveau, jusqu'à ce que vous soyez satisfait de votre déploiement.

Considérez cette option si vous avez une ou plusieurs des exigences de mise à niveau suivantes :

- Vous exigez peu ou pas de temps d'arrêt.
- Vous devez prendre en charge un grand nombre d'administrateurs assistants et vous ne pouvez pas mettre à niveau tous les ordinateurs clients immédiatement.
- Vous souhaitez continuer à prendre en charge l'accès à une version précédente de DRA après la mise à niveau du serveur d'administration primaire.
- Votre environnement comprend 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 précédente de DRA. Si vous avez l'intention de mettre à niveau ce serveur, il devrait être le dernier serveur mis à niveau. Sinon, désinstallez complètement DRA de ce serveur lorsque vous terminez 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 des connexions coûteuses à des sites distants, et garantit que vos administrateurs assistants peuvent continuer à utiliser une version précédente de DRA sans interruption. Si votre environnement comprend un MMS qui s'étend sur plusieurs sites, vous devez envisager cette option. Par exemple, si votre MMS se compose d'un serveur d'administration primaire sur votre site de Londres et d'un serveur d'administration secondaire sur votre site de Tokyo, envisagez d'installer un serveur secondaire sur le site de Londres et de l'ajouter au MMS correspondant. Ce serveur supplémentaire permet aux administrateurs assistants du site de Londres d’utiliser une version précédente de DRA jusqu’à la fin de la mise à niveau.

Utilisation d'un serveur secondaire existant

Vous pouvez utiliser un serveur d'administration secondaire existant comme serveur dédié pour une version de DRA précédente. 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 à cette fin. L'utilisation d'un ou de plusieurs serveurs secondaires dédiés pour exécuter une version de DRA précédente permet à vos administrateurs assistants de continuer à utiliser une version de DRA précédente sans interruption jusqu'à la fin de la mise à niveau. Cette option fonctionne mieux dans les environnements plus grands qui utilisent un modèle d'administration centralisé.

Synchronisation de votre ensemble de serveurs DRA des versions précédentes

Avant de sauvegarder le registre des versions précédentes de DRA ou de commencer le processus de mise à niveau, assurez-vous d'avoir synchronisé les ensembles de serveurs afin que chaque serveur d'administration contienne les derniers paramètres de configuration et de sécurité.

REMARQUE : Assurez-vous d'avoir apporté 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. Une fois que vous avez mis à niveau le serveur d'administration primaire, vous ne pouvez plus synchroniser les paramètres de délégation, de configuration ou de stratégie avec les serveurs d'administration exécutant les versions précédentes de DRA.

Pour synchroniser votre ensemble de serveurs existant :

1. Connectez-vous au serveur d'administration primaire en tant qu'administrateur intégré.
2. Ouvrez la console de délégation et de configuration et développez l'option **Configuration Management** (Gestion de la configuration).
3. Cliquez sur **Serveurs d'administration**.
4. Dans le volet droit, sélectionnez le serveur d'administration primaire approprié pour cet ensemble de serveurs.
5. Cliquez sur **Propriétés**.
6. Dans l'onglet Planification de la synchronisation, cliquez sur **Actualiser maintenant**.
7. Vérifiez que la synchronisation est terminée et que tous les serveurs d'administration secondaires sont disponibles.

Sauvegarde du registre du serveur d'administration

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

Toutefois, soyez prudent lorsque vous modifiez votre registre. S'il y a une erreur dans votre registre, le serveur d'administration peut ne pas fonctionner comme prévu. Si une erreur se produit pendant le processus de mise à niveau, vous pouvez utiliser la sauvegarde de vos paramètres de registre pour restaurer ce dernier. Pour obtenir de plus amples renseignements, consultez l'aide de l'*Éditeur de registre*.

IMPORTANT : La version du serveur DRA, le nom du système d'exploitation Windows et la configuration du domaine géré doivent être exactement les mêmes lors de la restauration du registre.

IMPORTANT : Avant de procéder à la mise à niveau, sauvegardez le système d'exploitation Windows de la machine hébergeant 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 de la souris sur le nœud `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint`, puis sélectionnez **Exporter**.
3. Spécifiez le nom et l'emplacement du fichier dans lequel enregistrer la clé de registre, puis cliquez sur **Enregistrer**.

Mise à niveau du serveur d'administration DRA

La liste de contrôle suivante vous guide tout au long du processus de mise à niveau. Utilisez ce processus pour mettre à niveau chaque ensemble de serveurs de votre environnement. Si vous ne l'avez pas encore fait, utilisez l'utilitaire de vérification de l'intégrité pour créer une sauvegarde de votre instance AD LDS actuelle.

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 pour ce MMS.

Vous pouvez répartir le processus de mise à niveau en plusieurs phases, en mettant à niveau un MMS à la fois. Ce processus de mise à niveau vous permet également d'inclure temporairement des serveurs secondaires exécutant une version précédente 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 précédente de DRA et les serveurs exécutant la version actuelle de DRA. Sachez cependant que DRA ne prend pas en charge l'exécution simultanée des versions précédentes et actuelle de DRA sur le même serveur d'administration ou ordinateur client.

IMPORTANT : L'installation de la mise à niveau de DRA apporte les modifications suivantes lorsque vous mettez à niveau le serveur DRA d'une version DRA 9.x vers une version DRA 10.x :

- Déplace les configurations utilisateur du serveur UCH et de Workflow Automation de la console Web vers la console de délégation et de configuration
- Supprime l'ancien composant Web du serveur.
- Supprime tout locataire géré.

  Pour en savoir plus sur l'ajout de locataires, consultez la rubrique « Configuration des locataires Azure » dans le *Guide de l'administrateur de DRA*.
- Si vous avez installé la console de gestion des comptes et des ressources dans une version antérieure, celle-ci est supprimée lorsque vous passez à une version 10.x de DRA.
- Lors d'une mise à niveau de MMS, le serveur primaire est mis à niveau en premier, suivi par les serveurs secondaires. Pour une réplication réussie des affectations de groupe temporaires dans le serveur secondaire, exécutez **Multi-master synchronization schedule** (programme de synchronisation multimaître) manuellement ou attendez son exécution planifiée.

- Étant donné qu'Exchange 2010 n'est pas pris en charge dans DRA 10, Exchange est désactivé lors de la mise à niveau à partir de DRA 9.x. Pour continuer à effectuer des opérations Exchange après la mise à niveau, désactivez et réactivez l'option **Enable Exchange Policy** (Activer la stratégie Exchange) dans la console de délégation et de configuration. Les deux modifications doivent être « appliquées » pour que la stratégie soit réinitialisée.

  Pour obtenir de plus amples renseignements sur cette configuration de stratégie, consultez la rubrique « Activation de Microsoft Exchange » du *Guide de l'administrateur de DRA*.

Étapes	Détails
Exécution de l'utilitaire de contrôle de l'intégrité	Installez l'utilitaire autonome de contrôle de l'intégrité de DRA et exécutez-le à l'aide d'un compte de service. Corrigez les problèmes.
Réalisation d'une mise à niveau d'essai	Effectuez une mise à niveau d'essai dans votre environnement de laboratoire pour identifier les problèmes potentiels et limiter les temps d'arrêt de production.
Définition de l'ordre de 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 obtenir de plus amples renseignements, consultez 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. Pour plus de renseignements, consultez Mise à niveau du serveur d'administration primaire.
Installation du nouveau serveur secondaire	*(Facultatif)* Pour réduire les temps d'arrêt sur les sites distants, installez un serveur d'administration secondaire local exécutant la dernière version de DRA. Pour plus de renseignements, consultez Installation d'un serveur d'administration secondaire local pour la version actuelle de DRA.
Déploiement des interfaces utilisateur	Déployez les interfaces utilisateur vers vos administrateurs assistants. Pour plus de renseignements, consultez Déploiement des interfaces utilisateur DRA
Mise à niveau les serveurs secondaires	Mettez à niveau les serveurs d'administration secondaires dans le MMS. Pour plus de renseignements, consultez Mise à niveau des serveurs d'administration secondaire.
Mise à niveau du module de création de rapports de DRA	Mettez à niveau le module de création de rapports de DRA. Pour plus de renseignements, consultez Mise à niveau du module de création de rapports.
Exécution de l'utilitaire de contrôle de l'intégrité	Exécutez l'utilitaire de contrôle de l'intégrité qui a été installé dans le cadre de la mise à niveau. Corrigez les problèmes.
Ajouter des locataires Azure *(après la mise à niveau)*	(*Facultatif, après la mise à niveau)* Si vous gériez des locataires Azure avant la mise à niveau, alors ils seront supprimés lors de la mise à niveau. Vous devrez ajouter ces locataires à nouveau et exécuter une actualisation complète du cache des comptes à partir de la console de délégation et de configuration. Pour en savoir plus, reportez-vous à la rubrique « Configuration des locataires Azure » dans le *Guide de l'administrateur de DRA*.

Étapes	Détails
Mise à jour de la configuration de la console Web *après la mise à jour)*	*(Conditionnel, après la mise à niveau)* Si vous avez l'une ou l'autre des configurations de la console Web ci-dessous avant la mise à niveau, elles devront être mises à jour une fois l'installation de la mise à niveau terminée : ◆ Connexions au serveur par défaut activées ◆ Fichiers de configuration modifiés Pour obtenir de plus amples renseignements, consultez Mise à jour de la configuration de la console Web - après l'installation.

Rubriques relatives à la mise à niveau du serveur :

- « Mise à niveau du serveur d'administration primaire » page 52
- « Installation d'un serveur d'administration secondaire local pour la version actuelle de DRA » page 52
- « Déploiement des interfaces utilisateur DRA » page 53
- « Mise à niveau des serveurs d'administration secondaire » page 54
- « Mise à jour de la configuration de la console Web - après l'installation » page 54

Mise à niveau du serveur d'administration primaire

Une fois que vous avez terminé avec la préparation de votre MMS, mettez à niveau le serveur d'administration primaire. Ne mettez pas à niveau les interfaces utilisateur sur les ordinateurs clients tant que vous n'avez pas mis à niveau le serveur d'administration primaire. Pour obtenir de plus amples renseignements, consultez Déploiement des interfaces utilisateur DRA.

REMARQUE : Pour obtenir des considérations et des instructions de mise à niveau plus détaillées, consultez les *notes de mise à jour de Directory and Resource Administrator*.

Avant de procéder à la mise à niveau, informez vos administrateurs assistants lorsque vous prévoyez de démarrer ce processus. Si vous avez dédié un serveur d'administration secondaire pour exécuter une version précédente de DRA, identifiez également ce serveur afin que les administrateurs assistants puissent continuer à utiliser la version précédente de DRA lors de la mise à niveau.

REMARQUE : Une fois que vous avez mis à niveau le serveur d'administration primaire, vous ne pouvez plus synchroniser les paramètres de délégation, de configuration ou de stratégie de ce serveur vers les serveurs d'administration secondaires exécutant une version précédente 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 d'arrêt généraux et en permettant un déploiement plus rapide des interfaces

utilisateur. Cette étape est facultative et permet aux administrateurs assistants d'utiliser la version actuelle et une version précédente de DRA tout au long du processus de mise à niveau, jusqu'à ce que vous soyez satisfait de votre déploiement.

Considérez cette option si vous avez une ou plusieurs des exigences de mise à niveau suivantes :

- Vous exigez peu ou pas de temps d'arrêt.
- Vous devez prendre en charge un grand nombre d'administrateurs assistants et vous ne pouvez pas mettre à niveau tous les ordinateurs clients immédiatement.
- Vous souhaitez continuer à prendre en charge l'accès à une version précédente de DRA après la mise à niveau du serveur d'administration primaire.
- Votre environnement comprend 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 Londres 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 administrateurs assistants de chaque site d'utiliser une version précédente de DRA ainsi que la version actuelle de DRA jusqu'à la fin de la mise à niveau. De plus, vos administrateurs assistants ne subissent aucun temps d'arrêt, car vous pouvez immédiatement déployer les interfaces utilisateur actuelles de DRA. Pour obtenir de plus amples renseignements sur la mise à niveau des interfaces utilisateur, consultezDéploiement des interfaces utilisateur DRA.

Déploiement des interfaces utilisateur DRA

En règle générale, vous devez déployer les interfaces utilisateur actuelles de DRA après avoir mis à niveau le serveur d'administration primaire et un serveur d'administration secondaire. Toutefois, pour les administrateurs assistants qui doivent utiliser le serveur d'administration primaire, assurez-vous de mettre à niveau leurs ordinateurs clients en premier en installant la console de délégation et de configuration. Pour obtenir de plus amples renseignements, consultez Planification de la mise à niveau de DRA.

Si vous effectuez souvent un traitement par lots par l'interface CLI, le fournisseur ADSI ou PowerShell, ou si vous générez fréquemment des rapports, envisagez d'installer ces interfaces utilisateur sur un serveur d'administration secondaire dédié afin de maintenir un équilibre de charge approprié dans le MMS.

Vous pouvez laisser vos administrateurs assistants installer les interfaces utilisateur de DRA ou déployer ces interfaces à l'aide d'une stratégie de groupe. Vous pouvez également déployer facilement et rapidement la console Web sur plusieurs administrateurs assistants.

REMARQUE : Vous ne pouvez pas exécuter plusieurs versions de composants DRA côte à côte sur le même serveur DRA. Si vous prévoyez de mettre à niveau progressivement vos ordinateurs clients administrateurs assistants, 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 secondaire

Lors de la mise à niveau de serveurs d'administration secondaires, vous pouvez mettre à niveau chaque serveur en fonction de vos exigences en matière d'administration. Tenez également compte de la manière dont vous envisagez de mettre à niveau et de déployer les interfaces utilisateur DRA. Pour obtenir de plus amples renseignements, consultez Déploiement des interfaces utilisateur DRA.

Par exemple, un schéma de mise à niveau classique peut comprendre les étapes suivantes :

1. Mise à niveau d'un serveur d'administration secondaire.
2. Demandez aux administrateurs assistants qui utilisent ce serveur d'installer les interfaces utilisateur appropriées, telles que la console Web.
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 administrateurs assistants lorsque vous prévoyez de démarrer ce processus. Si vous avez dédié un serveur d'administration secondaire pour exécuter une version précédente de DRA, identifiez également ce serveur afin que les administrateurs assistants puissent continuer à utiliser la version précédente de DRA lors de la mise à niveau. Lorsque vous terminez le processus de mise à niveau pour ce MMS et que tous les ordinateurs clients d'administrateurs assistants exécutent des interfaces utilisateur mises à niveau, déconnectez tous les serveurs ayant des versions précédentes de DRA.

Mise à jour de la configuration de la console Web - après l'installation

Effectuez l'une ou l'autre ou les deux actions suivantes, après l'installation de la mise à niveau, si elles sont applicables à votre environnement DRA :

Connexion par défaut au serveur DRA

Le composant Service REST de DRA est consolidé avec le serveur DRA à partir de DRA 10.1. Si la connexion par défaut au serveur DRA est configurée avant la mise à niveau à partir d'une version DRA 10.0.x ou antérieure, vous devez revoir ces paramètres après la mise à niveau, car il n'existe désormais qu'une seule configuration de connexion, la connexion au serveur DRA. Vous pouvez accéder à cette configuration dans la console Web en cliquant sur **Administration** > **Configuration** > **DRA Server Connection** (Administration > Configuration > Connexion au serveur DRA).

Vous pouvez également mettre à jour ces paramètres après la mise à niveau dans le fichier `web.config` situé à `C:\inetpub\wwwroot\DRAClient\rest` sur le serveur de la console Web de DRA, en procédant comme suit :

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Configuration de la connexion à la console Web

Lors de la mise à niveau à partir de DRA 10.0.x ou de versions antérieures, si le service DRA REST est installé sans le serveur DRA, la désinstallation du service DRA REST est une condition préalable à la mise à niveau. Une copie des fichiers qui ont été modifiés avant la mise à niveau est effectuée sur `C:\ProgramData\NetIQ\DRA\Backup\` sur le serveur. Vous pouvez utiliser ces fichiers comme référence pour mettre à jour ceux qui sont pertinents après la mise à niveau.

Mise à niveau de Workflow Automation

Pour effectuer une mise à niveau sur place dans des environnements 64 bits non regroupés, il suffit d'exécuter le programme d'installation de Workflow Automation sur vos ordinateurs sur lesquels Workflow Automation est déjà installé. Il n'est pas nécessaire d'arrêter les services de Workflow Automation en cours d'exécution.

Tous les adaptateurs de Workflow Automation qui ne sont pas intégrés au programme d'installation de Workflow Automation doivent être désinstallés et réinstallés après la mise à niveau.

Pour des informations plus détaillées sur la mise à niveau de Workflow Automation, consultez la rubrique « Mise à niveau à partir d'une version précédente » dans le *Guide de l'administrateur de Workflow Automation*.

Mise à niveau du module de création de rapports

Avant de mettre à niveau le module de création de rapports de DRA, assurez-vous que votre environnement répond à la configuration minimale requise pour NRC 3.3. Pour obtenir de plus amples renseignements sur les exigences d'installation et les considérations relatives à la mise à niveau, consultez le *Guide de NetIQ Reporting Center Reporting*.

Étapes	Détails
Désactivation de la prise en charge du module de création de rapports de DRA	Pour vous assurer que les collecteurs de rapports ne s'exécutent pas pendant le processus de mise à niveau, désactivez la prise en charge du module de création de rapports de DRA dans la fenêtre 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 le serveur SQL.
Exécution du programme d'installation du module de création de rapports de DRA	Exécutez DRA`ReportingSetup.exe`. à partir de la trousse d'installation et suivez les instructions de l'assistant d'installation.
Activation de la prise en charge du module de création de rapports de DRA	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 devrez redéployer vos rapports. Pour obtenir de plus amples renseignements sur le redéploiement des rapports, consultez le *Guide de Reporting Center* sur le site de la documentation.

III Modèle de délégation

DRA permet aux administrateurs d'implémenter un schéma d'autorisations avec un « droit d'accès minimal » en fournissant un ensemble flexible de paramètres permettant d'octroyer des pouvoirs granulaires à des objets gérés précis dans l'entreprise. Grâce à ces délégations, les administrateurs peuvent s’assurer que les administrateurs assistants reçoivent uniquement les autorisations nécessaires pour s’acquitter de leurs rôles et de leurs responsabilités précises.

6 Comprendre le modèle de délégation dynamique

DRA vous permet de gérer l'accès administratif à votre entreprise dans le contexte d'un modèle de délégation. Le modèle de délégation vous permet de configurer un accès avec un « droit d'accès minimal » pour les administrateurs assistants grâce à un ensemble dynamique de paramètres pouvant s'adapter à l'évolution et au changement de l'entreprise. Le modèle de délégation fournit un contrôle d'accès administratif qui représente plus fidèlement le fonctionnement de votre entreprise en :

- Avec des règles de portée flexibles, les administrateurs peuvent cibler les autorisations sur des objets gérés précis en fonction des besoins de l'entreprise au lieu de la structure de l'entreprise.
- La délégation basée sur les rôles garantit que les autorisations sont accordées de manière cohérente et simplifie le provisionnement.
- L'attribution de privilèges peut être administrée à partir de domaines, de clients hébergés dans le nuage et d'applications gérées à partir d'un emplacement unique.
- Les pouvoirs granulaires vous permettent d'adapter l'accès spécifique accordé aux administrateurs assistants.

Paramètres du modèle de délégation

Les administrateurs utilisent les paramètres suivants pour provisionner l'accès par le modèle de délégation :

- **Délégation :** les administrateurs fournissent un accès aux utilisateurs et aux groupes en affectant un rôle, qui dispose d'autorisations spécifiées dans le contexte d'un ActiveView définissant l'étendue.
- **ActiveView :** un ActiveView représente une étendue précise d'objets gérés définis par une ou plusieurs règles. Les objets gérés identifiés par chaque règle dans ActiveView sont regroupés dans une étendue unifiée.
- **Règle ActiveView:** les règles sont définies par des expressions qui correspondent à un ensemble d'objets gérés en fonction d'un certain nombre de conditions telles que le type d'objet, l'emplacement, le nom, etc.
- **Rôles :** un rôle représente un ensemble précis de pouvoirs (autorisations) nécessaires pour exécuter une fonction d'administration précise. DRA fournit un certain nombre de rôles intégrés pour les fonctions d'entreprise courantes et vous pouvez définir des rôles personnalisés qui répondent le mieux aux besoins de votre organisation.
- **Pouvoirs :** un pouvoir définit une autorisation précise 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 être décomposées en propriétés précises pouvant être modifiées. DRA fournit une liste complète de pouvoirs intégrés pour les objets gérés pris en charge et peut définir des pouvoirs personnalisés pour étendre ce qui peut être provisionné grâce au modèle de délégation.

Traitement des requêtes par DRA

Lorsque le serveur d'administration reçoit une requête pour une action, telle que la modification d'un mot de passe utilisateur, il utilise le processus suivant :

1. Rechercher les ActivevVews qui sont configurés pour gérer l'objet cible de l'opération.
2. Valider les pouvoirs attribués au compte qui demande l'action.
    a. Évaluer toutes les attributions d'ActiveView qui contiennent l'administrateur assistant demandant l'opération.
    b. Une fois cette liste terminée, dressez une liste de toutes les ActiveView qui contiennent à la fois l'objet cible et l'administrateur assistant.
    c. Comparez les pouvoirs à ceux nécessaires pour l'opération requérante.
3. *Si le compte dispose du pouvoir approprié*, le serveur d'administration autorise l'action à effectuer.

    Si le compte ne dispose pas du pouvoir approprié le serveur d'administration renvoie une erreur.
4. Mettre à jour Active Directory.

Exemples de traitement des attributions de délégation par DRA

Les exemples suivants décrivent des scénarios courants rencontrés 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

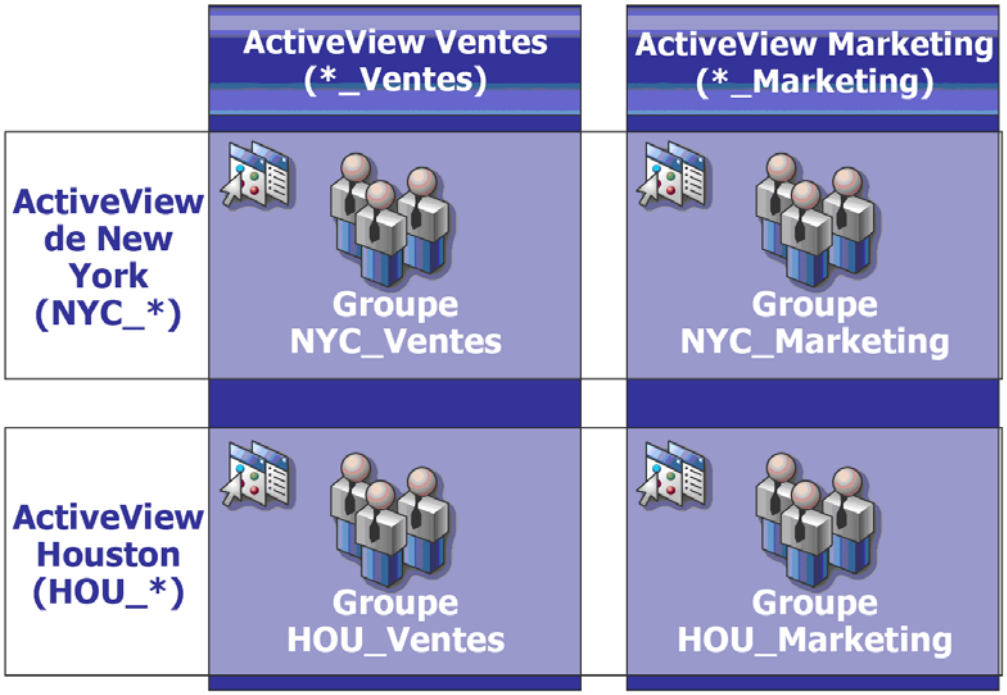
Lorsqu'un administrateur assistant tente de définir un nouveau mot de passe pour le compte d’utilisateur JSmith, le serveur d'administration trouve tous les ActiveViews incluant JSmith. Cette opération recherche tout ActiveView qui spécifie JSmith directement, par une règle générique ou par l'adhésion à un groupe. Si un ActiveView inclut d’autres ActiveView, le serveur d’administration recherche également ces ActiveView supplémentaires. Le serveur d'administration détermine si l'administrateur assistant dispose du pouvoir *Réinitialiser le mot de passe du compte d’utilisateur* dans l'un de ces ActiveViews. Si l'administrateur assistant dispose du pouvoir *Réinitialiser le mot de passe du compte d’utilisateur*, le serveur d'administration réinitialise le mot de passe pour JSmith. S'il ne dispose pas de ce pouvoir, le serveur d'administration n'accède pas à la requête.

Exemple 2 : Superposition d'ActiveView

Un pouvoir définit les propriétés d'un objet qu'un administrateur assistant peut afficher, modifier ou créer dans votre domaine géré ou votre sous-arborescence gérée. Plus d'un ActiveView peut inclure le même objet. Cette configuration s'appelle **Chevauchement d'ActiveView**.

Lorsque des ActiveView se chevauchent, vous pouvez accumuler un ensemble de pouvoirs différents sur les mêmes objets. Par exemple, si un ActiveView vous permet d'ajouter un compte d’utilisateur à un domaine et qu'un autre ActiveView vous permet de supprimer un compte d’utilisateur du même domaine, vous pouvez ajouter ou supprimer des comptes d’utilisateurs dans ce domaine. De cette façon, les pouvoirs que vous avez sur un objet donné sont cumulatifs.

Il est important de comprendre comment des ActiveView peuvent se chevaucher, ce qui vous octroie des pouvoirs accrus sur les objets inclus dans ces ActiveView. Considérons la configuration d'ActiveView illustrée dans la figure suivante.



Les onglets blancs indiquent les ActiveView par emplacement, *New York* et *Houston*. Les onglets noirs indiquent les ActiveView selon leur fonction organisationnelle, *Ventes* et *Marketing*. Les cellules indiquent les groupes inclus dans chaque ActiveView.

Le groupe NYC_Ventes et le groupe HOU_Ventes sont tous deux représentés dans l'ActiveView des Ventes. Si disposez des pouvoirs dans ActiveView des ventes, vous pouvez gérer n'importe quel membre des groupes NYC_Ventes et HOU_Ventes. Si vous disposez également des pouvoirs dans ActiveView de New York, ces pouvoirs supplémentaires s'appliquent au groupe NYC_Marketing. De cette manière, les pouvoirs s'accumulent lorsque les ActiveView se chevauchent.

Le chevauchement d'ActiveView peut fournir un modèle de délégation puissant et flexible. Cependant, cette fonctionnalité peut également avoir des conséquences inattendues. Planifiez soigneusement vos ActiveViews pour vous assurer que chaque administrateur assistant possède uniquement les pouvoirs définis par vous sur chaque compte d'utilisateur, groupe, unité organisationnelle, contact ou ressource.

Groupes dans plusieurs ActiveView

Dans cet exemple, le groupe NYC_Ventes est représenté dans plusieurs ActiveView. Les membres du groupe NYC_Ventes sont représentés dans ActiveView de New York, car le nom du groupe correspond à la règle d'ActiveView NYC_*. Le groupe figure également dans ActiveView des ventes,

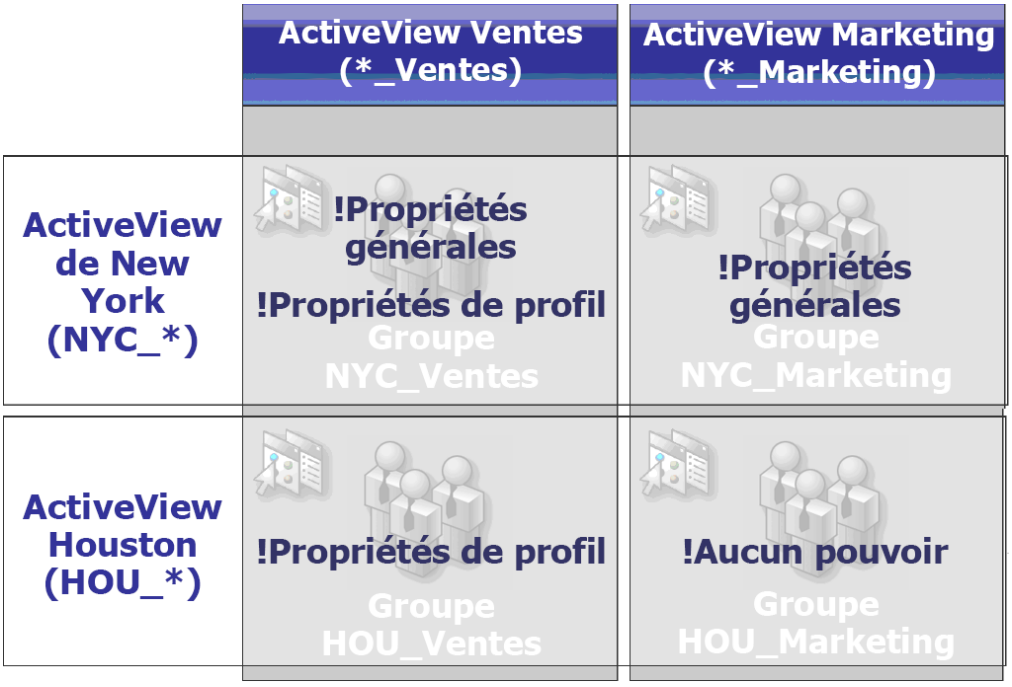
car son nom correspond à la règle d'ActiveView *_Ventes. En incluant le même groupe dans plusieurs ActiveView, vous pouvez permettre à différents administrateurs assistants de gérer les mêmes objets différemment.

Utiliser des pouvoirs dans plusieurs ActiveView

Supposons qu'un administrateur assistant, JSmith, dispose du pouvoir *Modifier les propriétés générales de l'utilisateur* dans ActiveView de New York. Ce premier pouvoir permet à JSmith de modifier toutes les propriétés de l'onglet Général de la fenêtre des propriétés de l'utilisateur. JSmith

dispose du pouvoir *Modifier les propriétés du profil utilisateur* dans ActiveView des ventes. Ce deuxième pouvoir permet à JSmith de modifier toutes les propriétés de l'onglet Profil de la fenêtre des propriétés de l'utilisateur.

La figure suivante indique les pouvoirs de JSmith pour chaque groupe.



JSmith dispose des pouvoirs suivants :

- propriétés de Général dans l'ActiveView de NYC_*
- propriétés de Profil dans l'ActiveView de *_Ventes

La délégation de pouvoir dans ces ActiveView qui se chevauchent permet à JSmith de modifier les propriétés de Général et de Profil du groupe NYC_Ventes. Ainsi, JSmith dispose de tous les pouvoirs accordés dans toutes les ActiveView représentant le groupe NYC_Ventes.

7 ActiveView

ActiveView vous permet d'implémenter un modèle de délégation doté des fonctionnalités suivantes :

- est indépendant de votre structure Active Directory
- vous permet d'attribuer des pouvoirs et de définir des stratégies en corrélation avec vos processus de travail existants
- fournit une automatisation pour vous aider à intégrer et à personnaliser davantage votre entreprise
- réagit dynamiquement aux changements

Un ActiveView représente un ensemble d'objets appartenant à un ou plusieurs domaines gérés. Vous pouvez inclure un objet dans plusieurs ActiveView. Vous pouvez également inclure de nombreux objets provenant de plusieurs domaines ou unités organisationnelles.

ActiveView intégrées

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

DRA offre plusieurs ActiveView intégrées pouvant représenter votre modèle de délégation. Le nœud ActiveView intégrée contient les ActiveView suivants :

Tous les objets

Inclut tous les objets dans tous les domaines gérés. Grâce à cet ActiveView, vous pouvez gérer n'importe quel aspect de votre entreprise. Attribuez cet ActiveView à l'administrateur ou à un administrateur assistant qui a besoin de pouvoirs d'audit dans l'entreprise.

Objets que l'utilisateur actuel gère en tant qu'administrateur Windows

Objets que l'utilisateur actuel gère en tant qu'administrateur Windows. Grâce à cet ActiveView, vous pouvez gérer des comptes d'utilisateurs, des groupes, des contacts, des unités organisationnelles et des ressources. Attribuez cet ActiveView aux administrateurs natifs responsables des objets de compte et de ressource du domaine géré.

Serveurs d'administration et domaines gérés

Comprend les ordinateurs du serveur d'administration et les domaines gérés. Grâce à cet ActiveView, vous pouvez gérer la maintenance quotidienne de vos serveurs d'administration. Attribuez cet ActiveView à des administrateurs assistants dont les tâches consistent notamment à surveiller l'état de la synchronisation ou à rafraîchir le cache.

Stratégies DRA et déclencheurs d'automatisation

Inclut tous les objets de stratégie et les déclencheurs d'automatisation dans tous les domaines gérés. Grâce à cet ActiveView, vous pouvez gérer les propriétés et l'étendue de la stratégie, ainsi que les propriétés du déclencheur d'automatisation. Attribuez cet ActiveView aux administrateurs assistants responsables de la création et de la maintenance des stratégies de votre entreprise.

Objets de sécurité DRA

Inclut tous les objets de sécurité. Grâce à cet ActiveView, vous pouvez gérer des ActiveViews, des groupes d'administrateurs assistants et des rôles. Attribuez cet ActiveView aux administrateurs assistants responsables de la création et de la maintenance de votre modèle de sécurité.

Utilisateurs de SPA de tous les domaines gérés et approuvés

Inclut tous les comptes d'utilisateurs des domaines gérés et approuvés. Grâce à cet ActiveView, vous pouvez gérer les mots de passe utilisateur grâce à Secure Password Administrator (SPA).

Accéder aux ActiveView intégrées

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

Pour accéder aux ActiveView intégrées :

1. Accédez à **Gestion des délégations** > **Gérer les ActiveView**.
2. Assurez-vous que le champ de recherche est vide et cliquez sur **Trouver maintenant** dans le volet**Afficher la liste des éléments qui correspondent à mes critères**.
3. Sélectionnez l'ActiveView approprié.

Utiliser les ActiveView intégrées

Vous ne pouvez pas supprimer, cloner ou modifier des ActiveView intégrées. Cependant, vous pouvez incorporer ces ActiveView dans votre modèle de délégation existant ou utiliser ces ActiveView pour concevoir votre propre modèle.

Vous pouvez utiliser les ActiveView intégrées des manières suivantes :

- Affecter les ActiveViews intégrées aux groupes d'administrateurs assistants appropriés. Cette association permet aux membres du groupe d'administrateurs assistants de gérer l'ensemble des objets correspondant avec les pouvoirs appropriés.
- Utiliser les règles ActiveView intégrées et les associations comme guide pour concevoir et mettre en œuvre le modèle de votre délégation.

Pour obtenir de plus amples renseignements sur la conception d'un modèle de délégation dynamique, consultez Comprendre le modèle de délégation dynamique.

Implémenter un ActiveView personnalisé

Un ActiveView donne accès en temps réel à des objets spécifiques dans un ou plusieurs domaines ou unités organisationnelles. Vous pouvez ajouter ou supprimer des objets d'un ActiveView sans modifier le domaine sous-jacent ou la structure d'unité organisationnelle.

Vous pouvez voir un ActiveView comme un domaine virtuel ou une unité organisationnelle ou encore les résultats d'une instruction select ou de l'affichage d'une base de données relationnelle. Les ActiveView peuvent inclure ou exclure tout ensemble d'objets, contenir d'autres ActiveView et avoir des contenus qui se chevauchent. Les ActiveView peuvent contenir des objets de différents domaines, des arborescences et des forêts. Vous pouvez configurer les ActiveView pour répondre à tout besoin de gestion d'entreprise.

Les ActiveView peuvent inclure les types d'objet suivants :

Comptes :

- utilisateurs
- groupes
- ordinateurs
- contacts
- groupes de distribution dynamiques
- Compte de services gérés de groupe
- imprimantes publiées
- travaux d'impression d'imprimantes publiées
- boîtes aux lettres de ressources
- boîtes aux lettres partagées
- dossiers publics

Objets de répertoire :

- unités organisationnelles
- domaines
- serveurs membres

Objets de délégation :

- activeView
- auto-administration
- subordonné direct
- groupes gérés

Ressources :

- utilisateurs connectés
- périphériques
- journaux d'événements
- fichiers ouverts

- imprimantes
- travaux d'impression
- services
- partages

Objets Azure :

- Utilisateur Azure
- Groupe Azure
- Locataire Azure
- Contact Azure

À mesure que votre entreprise change ou se développe, les ActiveView changent afin d'inclure ou d'exclure les nouveaux objets. Ainsi, vous pouvez utiliser les ActiveView pour réduire la complexité de votre modèle, fournir la sécurité dont vous avez besoin et offrir une flexibilité bien supérieure à celle des autres outils d'organisation d'entreprise.

Règles ActiveView

Un ActiveView peut comprendre des règles qui incluent ou excluent des objets tels que des comptes utilisateurs, 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 dynamiques, des comptes de services gérés de groupe, et des objets Azure tels que des utilisateurs Azure, des utilisateurs invités Azure, des groupes Azure et des contacts Azure. Cette flexibilité rend les ActiveView dynamiques.

Ces correspondances sont appelées **caractères jokers**. Par exemple, vous pouvez définir une règle pour inclure tous les ordinateurs dont le nom correspond à `DOM*`. Cette spécification de caractère joker recherchera tout compte d'ordinateur dont le nom commence par la chaîne de caractères DOM. La correspondance de caractère joker rend l'administration dynamique, car les comptes sont automatiquement inclus lorsqu'ils correspondent à la règle. Ainsi, lorsque vous utilisez des caractères jokers, vous n'avez pas besoin de reconfigurer les ActiveView à mesure que votre organisation change.

Un autre exemple consiste à définir les ActiveViews en fonction de l'adhésion à un groupe. Vous pouvez définir une règle incluant tous les membres des groupes commençant par les lettres NYC. Ensuite, lorsque des membres sont ajoutés à tout groupe correspondant à cette règle, ces membres sont automatiquement inclus dans cet ActiveView. À mesure que votre entreprise change ou se développe, DRA réapplique les règles pour inclure ou exclure les nouveaux objets dans les ActiveView appropriés.

8 Rôles

Cette section comprend une liste avec des descriptions des rôles qui sont intégrés à DRA; elle indique comment utiliser ces rôles et donne de l'information sur la création et la gestion des rôles personnalisés.

Pour obtenir une description des rôles et de leur utilisation en général, consultez Paramètres du modèle de délégation.

Rôles intégrés

Les rôles d'administrateurs assistants intégrés fournissent un accès immédiat à un ensemble de pouvoirs régulièrement utilisés. Vous pouvez étendre votre configuration de sécurité actuelle en utilisant ces rôles par défaut pour déléguer le pouvoir à des comptes d'utilisateurs précis ou à d'autres groupes.

Ces rôles contiennent les pouvoirs nécessaires pour effectuer des tâches d'administration courantes. Par exemple, le rôle d'administration DRA contient tous les pouvoirs nécessaires à la gestion des objets. Toutefois, pour utiliser ces pouvoirs, le rôle doit être associé à un compte d'utilisateur ou à un groupe d'administrateurs assistants et à l'ActiveView géré.

Les rôles intégrés faisant partie du modèle de délégation par défaut, vous pouvez les utiliser pour déléguer rapidement le pouvoir et mettre en œuvre la sécurité. Ces rôles intégrés traitent des tâches courantes que vous pouvez effectuer à l'aide des interfaces utilisateur DRA. Les sections suivantes décrivent chaque rôle intégré et résume les pouvoirs qui leurs sont associés.

Gestion d'Exchange Online

Administration des contacts Azure

Fournit tous les pouvoirs nécessaires pour créer, modifier, supprimer et afficher les propriétés d'un contact Azure. Vous pouvez attribuer ce rôle à tous les administrateurs assistants responsables de la gestion des contacts Azure.

Administration des groupes Azure

Fournit tous les pouvoirs nécessaires pour gérer les groupes Azure et l'adhésion à un groupe Azure.

Administration des utilisateurs Azure

Fournit tous les pouvoirs nécessaires pour créer, modifier, supprimer, activer, désactiver et afficher les propriétés de la gestion de l'utilisateur Azure. Attribuez ce rôle aux administrateurs assistants responsables de la gestion de l'utilisateur Azure.

Administration

Administration des contacts

Fournit tous les pouvoirs nécessaires pour créer un nouveau contact, modifier ses propriétés ou supprimer un contact. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des contacts.

Administration de DRA

Donne tous les pouvoirs à un administrateur assistant. Ce rôle donne à un utilisateur les autorisations nécessaires pour effectuer toutes les tâches d'administration dans DRA. Ce rôle équivaut aux autorisations d'un administrateur. Un administrateur assistant associé au rôle d'administration de DRA peut accéder à tous les nœuds de Directory et Resource Administrator.

Administration des gMSA

Fournit les pouvoirs nécessaires pour créer, modifier, supprimer et afficher les propriétés d'un compte de services gérés de groupe (gMSA). Vous pouvez attribuer ce rôle à tous les administrateurs assistants responsables de la gestion d'un gMSA.

Gérer et exécuter des outils personnalisés

Fournit tous les pouvoirs nécessaires pour créer, gérer et exécuter des outils personnalisés. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des outils personnalisés.

Gérer les exceptions de clonage

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

Gérer les stratégies et les déclencheurs d'automatisation

Fournit tous les pouvoirs nécessaires pour définir les stratégies et les déclencheurs d'automatisation. Attribuez ce rôle aux administrateurs assistants responsables de la mise à jour des stratégies de l'entreprise et de l'automatisation des processus de travail.

Gérer le modèle de sécurité

Fournit tous les pouvoirs nécessaires pour définir les règles d'administration, y compris les ActiveViews, les administrateurs assistants et les rôles. Attribuez ce rôle aux administrateurs assistants responsables de la mise en œuvre et de la maintenance de votre modèle de sécurité.

Gérer les attributs virtuels

Fournit tous les pouvoirs nécessaires pour créer et gérer des attributs virtuels. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des attributs virtuels.

Administration d'unité organisationnelle

Fournit tous les pouvoirs nécessaires pour gérer les unités organisationnelles. Attribuez ce rôle aux administrateurs assistants responsables de la gestion de la structure d'Active Directory.

Administration des dossiers publics

Fournit les pouvoirs de créer, de modifier, de supprimer, d'activer ou de désactiver le courrier et d'afficher les propriétés de vos dossiers publics. Vous pouvez attribuer ce rôle à tous les administrateurs assistants responsables de la gestion des dossiers publics.

Répliquer des fichiers

Fournit tous les pouvoirs nécessaires pour télécharger, supprimer et modifier les informations de fichier. Attribuez ce rôle à des administrateurs assistants responsables de la réplication de fichiers du serveur d'administration primaire vers d'autres serveurs d'administration des ordinateurs client MMS et DRA.

Réinitialiser le mot de passe administrateur local

Fournit tous les pouvoirs nécessaires pour réinitialiser le mot de passe du compte administrateur local et afficher le nom de l'administrateur de l'ordinateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes administrateur.

Auto-administration

Fournit tous les pouvoirs nécessaires pour modifier les propriétés de base, telles que les numéros de téléphone, de votre propre compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants pour leur permettre de gérer leurs renseignements personnels.

Gestion avancée des requêtes

Exécuter des requêtes avancées

Fournit tous les pouvoirs nécessaires pour exécuter des requêtes avancées enregistrées. Attribuez ce rôle aux administrateurs assistants responsables de l'exécution des requêtes avancées.

Gérer les requêtes avancées

Fournit tous les pouvoirs nécessaires pour créer, gérer et exécuter des requêtes avancées. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des requêtes avancées.

Gestion de l'audit

Auditer tous les objets

Fournit tous les pouvoirs nécessaires pour afficher les propriétés des objets, des stratégies et des configurations de votre entreprise. Ce rôle ne permet pas à un administrateurs assistants de modifier des propriétés. Attribuez ce rôle aux administrateurs assistants responsables des activités d'audit dans votre entreprise. Il permet aux administrateurs assistants d'afficher tous les nœuds, à l'exception du nœud Outils personnalisés.

Auditer les certaines propriétés de compte et de ressource

Fournit des pouvoirs pour toutes les propriétés d'objet.

Auditer les ressources

Fournit tous les pouvoirs nécessaires pour afficher les propriétés des ressources gérées. Attribuez ce rôle aux administrateurs assistants responsables de l'audit des objets de ressources.

Auditer les utilisateurs et les groupes

Fournit tous les pouvoirs nécessaires pour afficher les propriétés du compte d'utilisateur et du groupe, mais aucun pouvoir pour modifier ces propriétés. Attribuez ce rôle aux administrateurs assistants responsables de l'audit des propriétés de compte.

Gestion de l'ordinateur

Administration de l'ordinateur

Fournit tous les pouvoirs nécessaires pour modifier les propriétés de l'ordinateur. Ce rôle permet aux administrateurs assistants d'ajouter, de supprimer et d'éteindre des ordinateurs, ainsi que de synchroniser les contrôleurs de domaine. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des ordinateurs dans l'ActiveView.

Créer et supprimer des comptes d'ordinateur

Fournit tous les pouvoirs nécessaires pour créer et supprimer un compte d'ordinateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des ordinateurs.

Gérer les propriétés de l'ordinateur

Fournit tous les pouvoirs nécessaires pour gérer toutes les propriétés d'un compte d'ordinateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des ordinateurs.

Afficher toutes les propriétés de l'ordinateur

Fournit tous les pouvoirs nécessaires pour afficher toutes les propriétés d'un compte d'ordinateur. Attribuez ce rôle aux administrateurs assistants responsables de l'audit des ordinateurs.

Gestion d'Exchange

Cloner un utilisateur avec une boîte aux lettres

Fournit tous les pouvoirs nécessaires pour cloner un compte d'utilisateur existant avec la boîte aux lettres du compte. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d’utilisateurs.

REMARQUE : Pour autoriser l'administrateur assistant à ajouter le nouveau compte d’utilisateur à un groupe lors de la tâche de clonage, attribuez-lui également le rôle Gérer les adhésions aux groupes.

Créer et supprimer une boîte aux lettres de ressources

Fournit tous les pouvoirs nécessaires pour créer et supprimer une boîte aux lettres. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des boîtes aux lettres.

Administration de boîte aux lettres

Fournit tous les pouvoirs nécessaires pour gérer les propriétés de boîte aux lettres Microsoft Exchange. Si vous utilisez Microsoft Exchange, attribuez ce rôle aux administrateurs assistants responsables de la gestion des boîtes aux lettres Microsoft Exchange.

Gérer les droits de la boîte aux lettres Exchange

Fournit tous les pouvoirs nécessaires pour gérer la sécurité et les droits des boîtes aux lettres Microsoft Exchange. Si vous utilisez Microsoft Exchange, attribuez ce rôle aux administrateurs assistants responsables de la gestion des autorisations pour les boîtes aux lettres Microsoft Exchange.

Gérer le courriel du groupe

Fournit tous les pouvoirs nécessaires pour afficher, activer ou désactiver l'adresse électronique d'un groupe. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des groupes ou des adresses de courriel pour les objets de compte.

Gérer les requêtes de déplacement de boîte aux lettres

Fournit tous les pouvoirs nécessaires pour gérer les requêtes de déplacement de boîte aux lettres.

Gérer les propriétés des boîtes aux lettres de ressources

Fournit tous les pouvoirs nécessaires pour gérer toutes les propriétés d'une boîte aux lettres. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des boîtes aux lettres.

Gérer le courriel de l'utilisateur

Fournit tous les pouvoirs nécessaires pour afficher, activer ou désactiver l'adresse de courriel d'un compte d’utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d’utilisateurs ou des adresses de courriel pour les objets de compte.

Réinitialiser les propriétés du code confidentiel de messagerie unifiée

Fournit tous les pouvoirs nécessaires pour réinitialiser les propriétés du code confidentiel de messagerie unifiée pour les comptes d’utilisateurs.

Administration de la boîte aux lettres des ressources

Fournit tous les pouvoirs nécessaires pour gérer les boîtes aux lettres des ressources.

Administration des boîtes aux lettres partagées

Fournit tous les pouvoirs nécessaires pour créer, modifier, supprimer et afficher les propriétés de vos boîtes aux lettres partagées. Attribuez ce rôle à tous les administrateurs assistants responsables de la gestion des boîtes aux lettres partagés.

Afficher toutes les propriétés d'une boîte aux lettres de ressource

Fournit tous les pouvoirs nécessaires pour afficher les propriétés d'une boîte aux lettres de ressource. Attribuez ce rôle aux administrateurs assistants responsables de l'audit des boîtes aux lettres des ressources.

Gestion de groupe

Créer et supprimer des groupes

Fournit tous les pouvoirs nécessaires pour créer et supprimer un groupe. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des groupes.

Administration de groupe dynamique

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

Administration de groupe

Fournit tous les pouvoirs nécessaires pour gérer les groupes et les adhésions aux groupes, ainsi que pour afficher les propriétés utilisateur correspondantes. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des groupes ou des objets de compte et de ressources gérés par le biais de groupes.

Gérer des groupes de distribution dynamiques

Fournit tous les pouvoirs nécessaires pour gérer les groupes de distribution dynamiques Microsoft Exchange.

Gérer la sécurité de l'adhésion à un groupe

Fournit tous les pouvoirs nécessaires pour désigner qui peut afficher et modifier l'adhésion à un groupe Microsoft Windows par Microsoft Outlook.

Gérer les adhésions à un groupe

Fournit tous les pouvoirs nécessaires pour ajouter et supprimer des comptes d’utilisateurs ou des groupes d'un groupe existant et afficher le groupe primaire d'un compte d’utilisateur ou d'un compte d'ordinateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d’utilisateurs ou de groupe.

Gérer les propriétés de groupe

Fournit tous les pouvoirs nécessaires pour gérer toutes les propriétés d'un groupe. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des groupes.

Gérer les affectations de groupe temporaires

Fournit tous les pouvoirs nécessaires pour créer et gérer les affectations de groupe temporaires. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des groupes.

Renommer le groupe et modifier la description

Fournit tous les pouvoirs nécessaires pour modifier le nom et la description d'un groupe. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des groupes.

Afficher toutes les propriétés de groupe

Fournit tous les pouvoirs nécessaires pour afficher toutes les propriétés d'un groupe. Attribuez ce rôle aux administrateurs assistants responsables de l'audit des groupes.

Gestion de la création de rapports

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

Fournit tous les pouvoirs nécessaires pour gérer les collecteurs Active Directory, les collecteurs DRA et les collecteurs de création de rapports de gestion pour la collecte de données. Attribuez ce rôle aux administrateurs assistants responsables 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 nécessaires 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. Attribuez ce rôle aux administrateurs assistants responsables de la gestion de la création des rapports et de la configuration de la base de données.

Gérer la création de rapports d'interface utilisateur

Fournit tous les pouvoirs nécessaires pour générer et exporter des rapports de détail d'activité pour les utilisateurs, les groupes, les contacts, les ordinateurs, les unités d'organisation, les pouvoirs, les rôles, les ActiveView, les conteneurs, les imprimantes publiées et les administrateurs assistants. Attribuez ce rôle aux administrateurs assistants responsables de la génération des rapports.

Gérer la configuration de la base de données

Fournit tous les pouvoirs nécessaires pour gérer la configuration de la base de données pour la création de rapports de gestion. Attribuez ce rôle aux administrateurs assistants responsables de la gestion de la configuration de la base de données de création de rapports.

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 nécessaires pour afficher les collecteurs AD, les collecteurs DRA, les collecteurs de rapports de gestion et les informations de configuration de base de données.

Gestion d'une ressource

Créer et supprimer des ressources

Fournit tous les pouvoirs nécessaires pour créer et supprimer des partages et des comptes d’ordinateur, ainsi que pour effacer les journaux des événements. Attribuez ce rôle aux AA responsables de la gestion des objets ressources et des journaux d'événements.

Gérer les imprimantes et les travaux d'impression

Fournit tous les pouvoirs nécessaires pour gérer les imprimantes, les files d'attente et les travaux d'impression. Pour gérer les travaux d'impression associés à un compte d’utilisateur, le travail d'impression et le compte d’utilisateur doivent être inclus dans le même ActiveView. Attribuez ce rôle aux administrateurs assistants responsables de la maintenance des imprimantes et de la gestion des travaux d'impression.

Gérer les ressources pour les utilisateurs gérés

Fournit tous les pouvoirs nécessaires pour gérer les ressources associées à des comptes d’utilisateurs précis. L'administrateur assistant et les comptes d’utilisateurs doivent être inclus dans le même ActiveView. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des objets de ressources.

Gérer les services

Fournit tous les pouvoirs nécessaires pour gérer les services. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des services.

Gérer les dossiers partagés

Fournit tous les pouvoirs nécessaires pour gérer les dossiers partagés. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des dossiers partagés.

Administration des ressources

Fournit tous les pouvoirs nécessaires pour modifier les propriétés des ressources gérées, y compris les ressources associées à un compte d’utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des objets de ressources.

Démarrer et arrêter des ressources

Fournit tous les pouvoirs nécessaires pour suspendre, démarrer, reprendre ou arrêter un service, démarrer ou arrêter un périphérique ou une imprimante, éteindre un ordinateur ou synchroniser vos contrôleurs de domaine. Fournit également tous les pouvoirs nécessaires pour suspendre, reprendre et démarrer des services, arrêter des périphériques ou des files d'impressions et éteindre des ordinateurs. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des objets de ressources.

Gestion de serveur

Planificateur intégré - Pour usage interne uniquement

Fournit les pouvoirs de planifier le moment de l'actualisation du cache par DRA.

Administrer les serveurs d'applications

Fournit les pouvoirs nécessaires pour configurer, afficher et supprimer les configurations de serveur d'applications.

Configurer les serveurs et les domaines

Fournit tous les pouvoirs nécessaires pour modifier les options du serveur d'administration et les domaines gérés. Fournit également les pouvoirs nécessaires pour configurer et gérer les locataires. Attribuez ce rôle aux administrateurs assistants responsables de la surveillance et de la maintenance des serveurs d'administration et de la gestion des locataires Azure.

Administration du serveur d'historique des modifications unifié

Fournit les pouvoirs nécessaires pour configurer, afficher et supprimer les configurations d'historique des modifications unifié.

Administration du serveur de Workflow Automation

Fournit les pouvoirs nécessaires pour configurer, afficher et supprimer les configurations du serveur de Workflow Automation.

Gestion de compte utilisateur

Créer et supprimer des comptes d’utilisateurs

Fournit tous les pouvoirs nécessaires pour créer et supprimer un compte d’utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d’utilisateurs.

Administration du service d'assistance

Fournit tous les pouvoirs nécessaires pour afficher les propriétés du compte d'utilisateur et pour modifier les mots de passe et les propriétés associées aux mots de passe. Ce rôle permet également aux administrateurs assistants de désactiver, d’activer et de déverrouiller les comptes d’utilisateurs. Attribuez ce rôle aux administrateurs assistants responsables des tâches d'assistance afin de veiller à ce que les utilisateurs aient un accès correct à leurs comptes.

Gérer les propriétés de numérotation de l'utilisateur

Fournit tous les pouvoirs nécessaires pour modifier les propriétés de numérotation des comptes d’utilisateurs. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d’utilisateurs disposant d'un accès distant à l'entreprise.

Gérer le mot de passe utilisateur et déverrouiller le compte

Fournit tous les pouvoirs nécessaires pour réinitialiser le mot de passe, spécifier les paramètres du mot de passe et déverrouiller un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la maintenance de l'accès aux comptes d'utilisateurs.

Gérer les propriétés de l'utilisateur

Fournit tous les pouvoirs nécessaires pour gérer toutes les propriétés d'un compte d'utilisateur, y compris les propriétés de boîte aux lettres Microsoft Exchange. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d'utilisateurs.

Renommer un utilisateur et modifier la description

Fournit tous les pouvoirs nécessaires pour modifier le nom et la description d'un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d'utilisateurs.

Réinitialiser les mots de passe

Fournit tous les pouvoirs nécessaires pour réinitialiser et modifier les mots de passe. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des mots de passe.

Réinitialiser le mot de passe et déverrouiller le compte avec SPA

Fournit tous les pouvoirs nécessaires pour utiliser Secure Password Administrator pour réinitialiser les mots de passe et déverrouiller les comptes d'utilisateurs.

Transformer un utilisateur

Fournit tous les pouvoirs nécessaires pour ajouter ou supprimer un utilisateur à un groupe appartenant à un compte modèle, y compris la possibilité de modifier les propriétés de l'utilisateur tout en le transformant.

Administration des utilisateurs

Fournit tous les pouvoirs nécessaires pour gérer les comptes d'utilisateurs, les boîtes aux lettres Microsoft Exchange associées et les adhésions aux groupes. Attribuez ce rôle aux administrateurs assistants responsables de la gestion des comptes d'utilisateurs.

Afficher toutes les propriétés d'utilisateurs

Fournit tous les pouvoirs nécessaires pour afficher les propriétés d'un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de l'audit des comptes d'utilisateurs.

Administration de WTS

Gérer les propriétés de l'environnement WTS

Fournit tous les pouvoirs nécessaires pour modifier les propriétés de l'environnement WTS d'un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la maintenance de l'environnement WTS ou de la gestion des comptes d'utilisateurs.

Gérer les propriétés du contrôle à distance WTS

Fournit tous les pouvoirs nécessaires pour modifier les propriétés d'accès à distance WTS d'un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la maintenance de l'accès WTS ou de la gestion des comptes d'utilisateurs.

Gérer les propriétés de session WTS

Fournit tous les pouvoirs nécessaires pour modifier les propriétés de session WTS d'un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la maintenance des sessions WTS ou de la gestion des comptes d'utilisateurs.

Gérer les propriétés de terminal WTS

Fournit tous les pouvoirs nécessaires pour modifier les propriétés de terminal WTS d'un compte d'utilisateur. Attribuez ce rôle aux administrateurs assistants responsables de la maintenance des propriétés de terminaux WTS ou de la gestion des comptes d'utilisateurs.

Administration de WTS

Fournit tous les pouvoirs nécessaires pour gérer les propriétés WTS (Windows Terminal Server) des comptes d'utilisateurs dans l'ActiveView. Si vous utilisez WTS, attribuez ce rôle aux administrateurs assistants responsables de la gestion des propriétés WTS des comptes d'utilisateurs.

Accéder 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 des délégations** > **Gérer les rôles**.
2. Assurez-vous que le champ de recherche est vide et cliquez sur **Trouver maintenant** dans le volet**Afficher la liste des éléments qui correspondent à mes critères**.
3. Sélectionnez le rôle approprié.

Utiliser les rôles intégrés

Vous ne pouvez pas supprimer ou modifier les rôles intégrés. Toutefois, vous pouvez incorporer les rôles intégrés dans votre modèle de délégation existant ou utiliser ces rôles pour concevoir et mettre en œuvre votre propre modèle.

Vous pouvez utiliser les rôles intégrés des manières suivantes :

- Associer un rôle intégré à un compte d'utilisateur ou à un groupe d'administrateurs assistants. Cette association fournit à l'utilisateur ou aux membres du groupe d'administrateurs assistants les pouvoirs appropriés pour la tâche.
- Cloner un rôle intégré et utiliser ce clone comme base d'un rôle personnalisé. Vous pouvez ajouter d'autres rôles ou pouvoirs à ce nouveau rôle et supprimer des pouvoirs initialement inclus dans le rôle intégré.

Pour obtenir de plus amples renseignements sur la conception d'un modèle de délégation dynamique, consultez Comprendre le modèle de délégation dynamique.

Créer des rôles personnalisés

Lorsque vous créez un rôle, vous pouvez rapidement et facilement lui déléguer un ensemble de pouvoirs qui représente une tâche administrative ou un processus de travail. Les rôles sont créés et gérés à partir du nœud **Gestion des délégations** > **Rôles** dans la console de délégation et de configuration. Dans ce nœud, vous pouvez effectuer les opérations suivantes :

- créer de nouveaux rôles
- cloner des rôles existants
- modifier les propriétés des rôles
- supprimer des rôles
- gérer les attributions de rôles
  - délégué une nouvelle attribution
  - retirer une attribution existante
  - afficher les propriétés d'un administrateur assistant affecté
  - afficher les propriétés d'un ActiveView affecté
- gérer les rôles et les pouvoirs dans un rôle (les rôles peuvent être imbriqués)
- générer des rapports de changement de rôle

Le processus de travail général permettant d'exécuter l'une des actions identifiées dans cette section consiste à sélectionner le nœud **Rôles** et à effectuer l'une des opérations suivantes :

- Utiliser **Tâches** ou le menu contextuel pour ouvrir l'assistant ou la boîte de dialogue applicable et effectuer l'action nécessaire.
- Trouver l'objet de rôle dans le volet **Afficher la liste des éléments qui correspondent à mes critères** et utilisez le menu **Tâches** ou cliquez à l'aide du bouton droit de la souris pour sélectionner et ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre avec les actions nécessaires.

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.

9 Pouvoirs

Les pouvoirs sont les éléments de base de l’administration des « droits d'accès minimaux ». L'attribution de pouvoirs aux utilisateurs vous aide à mettre en œuvre et à maintenir votre modèle de sécurité dynamique. Vous effectuez ces procédures dans la console de délégation et de configuration.

Pouvoirs intégrés

Il existe plus de 390 pouvoirs intégrés pour la gestion des objets et l'exécution de tâches administratives courantes avec lesquelles vous pouvez travailler lors de la définition de rôles et de l'attribution de délégations. Les pouvoirs intégrés ne peuvent pas être supprimés, 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 du groupe.

Supprimer le compte d’utilisateur

Si la Corbeille est activée, ce pouvoir permet de déplacer les comptes d’utilisateurs vers la Corbeille. Si la Corbeille est désactivée, ce pouvoir permet de supprimer définitivement les comptes d’utilisateurs.

Modifier toutes les propriétés de l'ordinateur

Fournit le pouvoir de modifier toutes les propriétés des comptes d'ordinateur.

Mise en œuvre des pouvoirs personnalisés

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

REMARQUE : Tous les pouvoirs intégrés ne peuvent pas être clonés.

Pour implémenter des pouvoirs personnalisés, utilisez le nœud **Gestion des délégations** > **Pouvoirs** dans la console de délégation et de configuration. Dans ce nœud, vous pouvez effectuer les opérations suivantes :

- afficher toutes les propriétés d'un pouvoir
- créer de nouveaux pouvoirs
- cloner des pouvoirs existants

- modifier des pouvoirs personnalisés
- générer des rapports de changement de pouvoir

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

Suivez le processus ci-dessous avant de tenter de créer un nouveau pouvoir.

1. Passez en revue les pouvoirs fournis avec DRA.
2. Déterminez si vous avez besoin d'un pouvoir personnalisé. Le cas échéant, vous pouvez cloner un pouvoir personnalisé existant.
3. Effectuez les procédures appropriées en suivant un assistant. Par exemple, effectuez toutes les étapes de l'assistant Nouveau pouvoir.
4. Affichez votre nouveau pouvoir.
5. Modifiez votre nouveau pouvoir si nécessaire.

Le processus de travail général permettant d'exécuter l'une des actions identifiées dans cette section consiste à sélectionner le nœud **Pouvoirs** et à effectuer l'une des opérations suivantes :

- Utiliser Tâches ou le menu contextuel pour ouvrir l'assistant ou la boîte de dialogue applicable et effectuer l'action nécessaire.
- Trouver l'objet de pouvoir dans le volet **Afficher la liste des éléments qui correspondent à mes critères** et utilisez le menu **Tâches** ou cliquez à l'aide du bouton droit de la souris pour sélectionner et ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre avec les actions nécessaires.

Étendre des pouvoirs

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

Par exemple, pour autoriser un administrateur assistant à créer un compte d'utilisateur, vous pouvez lui attribuer le pouvoir *Créer un utilisateur et Modifier toutes les propriétés* ou le pouvoir *Créer un utilisateur et Modifier certaines propriétés*. Si vous attribuez également le pouvoir *Ajouter un nouvel utilisateur au groupe*, l'administrateur assistant peut ajouter ce nouveau compte d'utilisateur à un groupe tout en utilisant l'assistant de création d'utilisateur. Dans ce cas, le pouvoir *Ajouter un nouvel utilisateur au groupe* fournit une fonctionnalité d'assistant supplémentaire. Le pouvoir *Ajouter un nouvel utilisateur au groupe* est le **pouvoir d'extension**.

Les pouvoirs d'extension ne peuvent pas ajouter d'autorisations ou de fonctionnalités par eux-mêmes. Pour déléguer correctement une tâche qui inclut un pouvoir d'extension, vous devez attribuer le pouvoir d'extension en même temps que le pouvoir que vous voulez étendre.

REMARQUE

- Pour créer correctement un groupe et l'inclure dans un ActiveView, vous devez disposer du pouvoir *Ajouter un nouveau groupe à l'ActiveView* dans l'ActiveView en question. L'ActiveView spécifié doit également inclure l'unité organisationnelle ou le conteneur intégré qui contiendra le nouveau groupe.
- Pour cloner correctement un groupe et l'inclure dans un ActiveView, vous devez disposer du pouvoir *Ajouter un groupe cloné à l'ActiveView* dans l'ActiveView en question. L'ActiveView en question 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 pouvant être configurées lors de la création d'un nouveau pouvoir ou de la modification des propriétés d'un pouvoir existant :

Pour déléguer cette tâche	**Attribuer ce pouvoir**	**Et ce pouvoir d'extension**
Cloner un groupe et inclure le nouveau groupe dans un ActiveView spécifié	Cloner un groupe et modifier toutes les propriétés	Ajouter un groupe cloné à l'ActiveView
Créer un groupe et inclure le nouveau groupe dans un ActiveView spécifié	Créer un groupe et modifier toutes les propriétés	Ajouter un nouveau groupe à l'ActiveView
Créer un contact à extension messagerie	Créer un contact et modifier toutes les propriétés Créer un contact et modifier seulement quelques propriétés	Activer la messagerie pour le nouveau contact
Créer un groupe à extension messagerie	Créer un groupe et modifier toutes les propriétés	Activer la messagerie pour le nouveau groupe
Créer un compte d'utilisateur à extension messagerie	Créer un utilisateur et modifier toutes les propriétés Créer un utilisateur et modifier seulement quelques propriétés	Activer la messagerie pour le nouvel utilisateur
Créer un compte d'utilisateur et l'ajouter à des groupes précis	Créer un utilisateur et modifier toutes les propriétés Créer un utilisateur et modifier seulement quelques propriétés	Ajouter un nouvel utilisateur au groupe

10 Attribuer une délégation

Vous pouvez gérer les attributions de délégation à partir du nœud **Gestion des délégations** > **Administrateur assistant** de la console de délégation et de configuration. Dans ce nœud, vous pouvez afficher les pouvoirs et les rôles attribués aux administrateurs assistants et gérer les attributions de rôles et d'ActiveView. Vous pouvez également effectuer les opérations suivantes avec les groupes d'administrateurs assistants :

- ajouter des membres de groupe
- créer des groupes
- cloner des groupes
- supprimer des groupes
- modifier les propriétés des groupes

Pour afficher et gérer les attributions et apporter des modifications aux groupes d'administrateurs assistants, vous devez disposer des pouvoirs appropriés tels que ceux inclus dans le rôle Gérer le modèle de sécurité.

Le processus de travail général permettant d'exécuter l'une des actions identifiées dans cette section consiste à sélectionner le nœud **Administrateurs assistants** et à effectuer l'une des opérations suivantes :

- Utiliser Tâches ou le menu contextuel pour ouvrir l'assistant ou la boîte de dialogue applicable et effectuer l'action nécessaire.
- Trouver le groupe ou l'administrateur assistant dans le volet **Afficher la liste des éléments qui correspondent à mes critères** et utilisez le menu **Tâches** ou cliquez à l'aide du bouton droit de la souris pour sélectionner et ouvrir l'assistant ou la boîte de dialogue applicable afin de poursuivre avec les actions nécessaires.

IV Configuration des composants et des processus

Ce chapitre fournit de l'information permettant de configurer DRA pour la première fois, y compris les serveurs et les personnalisations de serveurs, l'administration d'Azure, les consoles et les personnalisations de console, l'administration des dossiers publics et la connexion aux serveurs.

11 Configuration initiale

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

Liste de contrôle de configuration

Utilisez la liste de contrôle suivante pour vous guider dans la configuration de DRA lors de la première utilisation.

Étapes	Détails
Installer une licence DRA	Utilisez l'utilitaire de contrôle de l'intégrité pour appliquer une licence DRA. Pour obtenir de plus amples renseignements sur les licences DRA, consultez Exigences relatives aux licences.
Configurer les serveurs et les fonctionnalités de DRA	Configurez le MMS, les exceptions de clonage, la réplication de fichiers, l'horodatage d'événements, la mise en cache, AD LDS, les groupes dynamiques, la Corbeille, la création de rapports, l'historique des modifications unifié, et le serveur de processus de travail.
Configurer le rapport sur l'historique des modifications (facultatif)	Configurez le rapport sur l'historique des modifications si vous souhaitez effectuer une intégration avec un serveur Change Guardian pour collecter des données sur l'historique des modifications pour les événements utilisateur internes et externes à DRA.
Configurer les services de DRA pour un compte gMSA (facultatif)	Configurez les services de DRA pour un compte de service de gestion de groupe (gMSA) si vous voulez gérer le protocole d'authentification sur plusieurs serveurs par rapport à un seul serveur.
Configurer le client de délégation et de configuration	Configurez la façon dont les éléments sont accessibles et affichés dans le Client de configuration et de délégation.
Configurer le client Web	Configurer la déconnexion automatique, les certificats, les connexions au serveur et les composants d'authentification

Installation ou mise à niveau de licences

DRA requiert 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, utilisez l'utilitaire de contrôle de l'intégrité pour installer la licence que vous avez achetée. Si cela est nécessaire, une clé de licence d'essai (`TrialLicense.lic`) est également incluse dans le paquetage d'installation qui vous permet de gérer un nombre illimité de comptes d'utilisateurs et de boîtes aux lettres pendant 30 jours.

Pour mettre à niveau une licence existante ou d'évaluation, ouvrez la console de délégation et de configuration et accédez à **Configuration Management** > **Update License** (Gestion de la configuration > 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 consulter la licence de votre produit dans la console de délégation et de configuration. Pour afficher la licence de votre produit, accédez au menu **Fichier** > **Propriétés de DRA** > **Licence**.

Configurer les serveurs et les fonctionnalités de DRA

Pour gérer les droits d'accès minimaux pour les tâches Active Directory à l'aide de DRA, de nombreux composants et processus doivent être configurés. Il s'agit notamment des configurations générales et des configurations des composants clients. Cette section fournit de l'information sur les composants et les processus généraux qui doivent être configurés pour DRA.

Configurer l'ensemble multimaître

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 du serveur d'administration est primaire. Lorsque vous ajoutez des serveurs secondaires à votre environnement MMS, gardez à l'esprit qu'un serveur d'administration secondaire ne peut appartenir qu'à un seul ensemble de serveurs.

Pour vous assurer que chaque serveur de l'ensemble gère les mêmes données, synchronisez périodiquement les serveurs secondaires avec le serveur d'administration primaire. Pour réduire la maintenance, utilisez le même compte de service pour tous les serveurs d'administration dans la forêt de domaines.

IMPORTANT

- Lors de l'installation du serveur secondaire, sélectionnez **Serveur d'administration secondaire** dans le programme d'installation.
- La version de DRA du nouveau serveur secondaire doit être identique à celle du serveur DRA primaire pour que toutes les fonctionnalités disponibles sur le serveur primaire soient également disponibles sur le serveur secondaire.

- « Ajouter un serveur d'administration secondaire » page 91
- « Promouvoir un serveur d'administration secondaire » page 92
- « Rétrograder un serveur d'administration primaire » page 93
- « Planifier la synchronisation » page 93

Ajouter un serveur d'administration secondaire

Vous pouvez ajouter un serveur d'administration secondaire à un MMS existant dans le client Délégation et configuration.

REMARQUE : Pour réussir à ajouter un nouveau serveur secondaire, vous devez d'abord installer le produit Directory and Resource Administrator sur l'ordinateur du serveur d'administration. Pour obtenir de plus amples renseignements, consultez Installer le serveur d'administration DRA.

Pour ajouter un serveur d'administration secondaire, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur **Administration Servers** (Serveurs d'administration) dans le nœud de gestion de configuration et sélectionnez **Add Secondary Server** (Ajouter un serveur secondaire).
2. Dans l'assistant Ajouter un serveur secondaire, cliquez sur Next (Suivant).
3. Dans l'onglet Serveur secondaire, indiquez le nom du serveur d'administration secondaire que vous souhaitez ajouter au MMS.

4 Dans l'onglet Access account (Compte d'accès), indiquez un compte de service du serveur d'administration secondaire. DRA utilise ce compte uniquement pour ajouter le serveur d'administration secondaire au MMS.

5 Dans l'onglet Compte d'accès multimaître, spécifiez un compte d'accès à utiliser par le serveur d'administration primaire pour les opérations MMS. Il est recommandé de ne pas utiliser le compte de service du serveur d'administration secondaire comme compte d'accès multimaître. Vous pouvez spécifier n'importe quel compte utilisateur du domaine associé au serveur d'administration secondaire. Le compte d'accès multimaître doit faire partie du groupe Administrateurs locaux sur le serveur secondaire. Si le compte d'accès multimaître ne dispose pas de privilèges suffisants pour effectuer des opérations MMS, le serveur DRA délègue automatiquement les pouvoirs requis au compte d'accès multimaître.

Promouvoir un serveur d'administration secondaire

Vous pouvez promouvoir un serveur d'administration secondaire en serveur d'administration primaire. Lorsque vous effectuez la promotion d'un serveur d'administration secondaire en serveur d'administration primaire, le serveur d'administration primaire existant devient un serveur d'administration secondaire dans le jeu 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 d'effectuer la promotion d'un serveur d'administration secondaire, synchronisez le MMS pour qu'il ait la dernière configuration.

Pour obtenir de plus amples renseignements sur la synchronisation du MMS, consultez Planifier la synchronisation.

REMARQUE : Un serveur primaire nouvellement promu ne peut se connecter qu'aux serveurs secondaires qui étaient disponibles pendant le processus de promotion. Si un serveur secondaire est devenu indisponible pendant le processus de promotion, communiquez avec le service d'assistance technique.

Pour promouvoir un serveur d'administration secondaire :

1 Accédez au nœud **Gestion de la configuration** >**Serveurs d'administration**.

2 Dans le volet de droite, sélectionnez le serveur d'administration secondaire que vous souhaitez promouvoir.

3 Dans le menu Tâches, cliquez sur **Avancé** > **Promouvoir le serveur**.

IMPORTANT : Lorsque le compte de service du serveur secondaire est différent du serveur primaire ou que le serveur secondaire est installé dans un domaine différent de celui du serveur primaire (domaines approuvés/domaines non approuvés), et que vous faites la promotion du serveur secondaire, assurez-vous de déléguer les rôles suivants avant de promouvoir le serveur secondaire : **Vérifier tous les objets**, **Configurer les serveurs et les domaines** et **Générer des rapports d'interface utilisateur**. Ensuite, assurez-vous que les synchronisations des MMS ont réussi.

Rétrograder un serveur d'administration primaire

Vous pouvez rétrograder un serveur d'administration primaire en 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 nœud **Gestion de la configuration** >**Serveurs d'administration**.
2. Dans le volet de droite, sélectionnez le serveur d'administration primaire que vous souhaitez rétrograder.
3. Dans le menu Tâches, cliquez sur **Avancé** > **Rétrograder le serveur**.
4. Spécifiez l'ordinateur que vous souhaitez désigner comme nouveau serveur d'administration primaire, puis cliquez sur **OK**.

Planifier la synchronisation

La synchronisation garantit que tous les serveurs d'administration du MMS utilisent les mêmes données de configuration. Bien qu'il soit possible de synchroniser manuellement les serveurs à tout moment, la planification par défaut prévoit la synchronisation du MMS toutes les 4 heures. Vous modifiez cette planification pour l'adapter aux besoins de votre entreprise.

Pour modifier la planification de 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 a la planification de synchronisation ou aux synchronisations manuelles, accédez à **Gestion de la configuration** > **Serveurs d'administration** et utilisez le menu **Tâches** ou les options du clic droit sur un serveur sélectionné. La planification de synchronisation se trouve dans les propriétés du serveur sélectionné.

Comprendre les options de synchronisation

Il existe essentiellement quatre options différentes pour la synchronisation des serveurs MMS :

- sélectionner le serveur primaire et synchroniser tous les serveurs secondaires « Synchroniser tous les serveurs »
- sélectionner un serveur secondaire et synchroniser uniquement ce serveur
- configurer la planification de synchronisation pour les serveurs principaux et secondaires de manière indépendante
- configurer la planification de synchronisation pour tous les serveurs. Cette option est activée lorsque le paramètre suivant est sélectionné dans la planification de synchronisation du serveur primaire :

  Configurer les serveurs d'administration secondaires lors de l'actualisation du serveur d'administration primaire

  ---

  REMARQUE : Si vous décochez cette option, les fichiers de configuration sont copiés sur les serveurs secondaires de la planification principale, mais ils ne seront pas chargés par la secondaire à ce moment-là; ils seront chargés en fonction de la planification configurée sur le

serveur secondaire. Cela est utile si les serveurs sont dans des fuseaux horaires différents. Par exemple, vous pouvez configurer tous les serveurs pour qu'ils actualisent leur configuration au milieu de la nuit, même si l'heure peut être différente en raison des fuseaux horaires.

Gérer les exceptions de clonage

Les exceptions de clonage vous permettent de définir des propriétés pour les utilisateurs, les groupes, les contacts et les ordinateurs qui ne seront pas copiés lorsque l'un de ces objets est cloné.

Avec les pouvoirs appropriés, vous pouvez gérer les exceptions de clonage. Le rôle Gérer les exceptions de clonage confère le pouvoir d'afficher, de créer et de supprimer des exceptions de clonage.

Pour afficher ou supprimer une exception de clonage existante, ou pour en créer une nouvelle, accédez à **Gestion de configuration**> **Exceptions de clonage** > **Tâches** ou utilisez le menu qui s'affiche avec le clic droit.

Réplication de fichier

Lorsque vous créez des outils personnalisés, vous devrez peut-être installer les fichiers de prise en charge utilisés par ces outils sur l'ordinateur de la console de délégation et de configuration de DRA pour qu'ils puissent fonctionner. Vous pouvez utiliser les fonctionnalités de réplication de fichiers de DRA pour répliquer rapidement et facilement des fichiers de prise en charge d'outils personnalisés du serveur d'administration primaire sur des serveurs d'administration secondaires du MMS, ainsi que sur des ordinateurs clients de DRA. La réplication de fichier peut également être utilisée pour répliquer des scripts de déclencheur de serveurs principaux vers des serveurs secondaires.

Les fonctions Outils personnalisés et Réplication de fichiers sont uniquement disponibles dans la console de délégation et de configuration.

Vous pouvez utiliser simultanément des outils personnalisés et la réplication de fichiers pour vous assurer que les ordinateurs clients de DRA peuvent accéder aux fichiers d'outils personnalisés. DRA réplique les fichiers d'outils personnalisés sur les serveurs d'administration secondaires afin de garantir que les ordinateurs clients de DRA connectés aux serveurs d'administration secondaires puissent accéder aux outils personnalisés.

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

REMARQUE : DRA télécharge les fichiers d'outils personnalisés à l'emplacement suivant sur les ordinateurs clients de DRA :

{DRAInstallDir}\{MMS ID}\Download

MMSID est l'identifiant de l'ensemble multimaître à partir duquel DRA télécharge les fichiers d'outils personnalisés.

- « Télécharger des fichiers d'outils personnalisés pour la réplication » page 95
- « Répliquer plusieurs fichiers entre des serveurs d'administration » page 96
- « Répliquer plusieurs fichiers sur des ordinateurs clients de DRA » page 96

Télécharger des fichiers d'outils personnalisés pour la réplication

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

Le rôle Répliquer les fichiers vous permet de répliquer des fichiers du serveur d'administration primaire vers les serveurs d'administration secondaires du MMS, ainsi que sur les ordinateurs clients de DRA. Le rôle Répliquer les fichiers contient 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 clients de DRA.
- **Définir les informations de fichier :** Ce pouvoir permet à DRA de mettre à jour les informations des fichiers des serveurs d'administration secondaires.
- **Téléverser des fichiers sur le serveur :** Ce pouvoir permet à DRA de télécharger des fichiers de l'ordinateur client DRA vers le serveur d'administration primaire.

REMARQUE : Vous ne pouvez téléverser qu'un seul fichier à la fois pour la réplication à l'aide de l'interface utilisateur de réplication de fichiers dans la console de délégation et de configuration.

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

1. Accédez à **Gestion de la configuration** > **Réplication de fichier**.
2. Dans le menu Tâches, cliquez sur **Téléverser le fichier**.
3. Pour rechercher et sélectionner le fichier à téléverser, cliquez sur **Parcourir**.
4. *Si vous souhaitez télécharger le fichier sélectionné sur tous les ordinateurs clients de DRA*, cochez la case **Télécharger sur tous les ordinateurs clients**.
5. *Si vous souhaitez enregistrer une bibliothèque COM*, cochez la case **Enregistrer la bibliothèque COM**.
6. Cliquez sur **OK**.

REMARQUE

- DRA téléverse le fichier script ou les fichiers de prise en charge qui doivent être répliqués vers d'autres serveurs d'administration secondaires vers le dossier *{DRAInstallDir}*\FileTransfer\Replicate dans le serveur d'administration primaire. Le dossier *{DRAInstallDir}*\FileTransfer\Replicate est également désigné par *{DRA_Replicated_Files_Path}*.

- DRA téléverse le fichier script ou les fichiers de prise en charge qui doivent être répliqués vers les ordinateurs clients de DRA vers le dossier *{DRAInstallDir}*\FileTransfer\Download dans le serveur d'administration primaire.
- Le fichier d'outil personnalisé téléversé sur le serveur d'administration primaire est distribué aux serveurs d'administration secondaires lors de la prochaine synchronisation planifiée ou par synchronisation manuelle.

Répliquer plusieurs fichiers entre des serveurs d'administration

Si vous souhaitez téléverser et répliquer plusieurs fichiers entre le serveur d'administration primaire et les serveurs d'administration secondaires de votre MMS, vous pouvez téléverser manuellement ces fichiers pour la réplication en les copiant dans le répertoire de réplication du serveur d'administration primaire 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 du répertoire de réplication et les répliques entre les serveurs d'administration lors de la prochaine synchronisation planifiée. Après la synchronisation, DRA affiche les fichiers téléversés dans la fenêtre de réplication de fichiers de la console de délégation et de configuration.

REMARQUE : Si vous souhaitez répliquer des fichiers contenant des 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 téléverser chaque fichier et enregistrer la bibliothèque COM.

Répliquer plusieurs fichiers sur des ordinateurs clients de DRA

Si vous souhaitez répliquer plusieurs fichiers entre le serveur d'administration primaire et les ordinateurs clients de DRA, vous pouvez copier les fichiers dans le répertoire de réplication client du serveur d'administration primaire situé à l'emplacement suivant :

{DRAInstallDir}\FileTransfer\Download

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

Le serveur d'administration identifie automatiquement les fichiers du dossier Télécharger et les répliques vers les serveurs d'administration secondaires lors de la prochaine synchronisation planifiée. Après la synchronisation, DRA affiche les fichiers téléversés dans la fenêtre de réplication de fichiers de la console de délégation et de configuration. DRA télécharge les fichiers répliqués sur les ordinateurs clients de DRA la première fois que les ordinateurs clients de DRA se connectent aux serveurs d'administration après la réplication.

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

Synchronisation Azure

La synchronisation Azure vous permet d'appliquer les stratégies sur les caractères non valides et sur le nombre de caractères afin d'empêcher les échecs de synchronisation de répertoire. Lorsque cette option est sélectionnée, les propriétés synchronisées avec Azure Active Directory limitent les caractères non valides et imposent des limites de longueur de caractères.

Pour activer la synchronisation Azure :

1. Dans le volet de gauche, cliquez sur **Gestion de la configuration**.
2. Sous Tâches courantes dans le volet de droite, cliquez sur **Mettre à jour les options du serveur d'administration**.
3. Sélectionnez **Enforce online mailbox policies for invalid characters and character length** (Appliquer les stratégies de boîte aux lettres en ligne pour les caractères non valides et la longueur des caractères) sur l'onglet Synchronisation Azure.

Activer plusieurs gestionnaires pour les groupes

Lorsque vous activez la prise en charge de plusieurs gestionnaires pour gérer un groupe, l'un des deux attributs par défaut est utilisé pour stocker les gestionnaires du groupe. L'attribut lors de l'exécution de Microsoft Exchange est `msExchCoManagedByLink`. L'attribut par défaut lorsque vous n'exécutez pas Microsoft Exchange est `nonSecurityMember`. Cette dernière option peut être modifiée. Toutefois, nous vous recommandons de contacter le service d'assistance technique pour déterminer un attribut approprié si vous devez modifier ce paramètre.

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

1. Dans le volet de gauche, cliquez sur **Gestion de la configuration**.
2. Sous Tâches courantes dans le volet de droite, cliquez sur **Mettre à jour les options du serveur d'administration**.
3. Dans l'onglet Activer la prise en charge de plusieurs gestionnaires de groupe, cochez la case **Activer la prise en charge de plusieurs gestionnaires du groupe**.

Communications chiffrées

Cette fonction vous permet d'activer ou de désactiver l'utilisation les communications chiffrées entre le client de délégation et de configuration et le serveur d'administration. Par défaut, DRA chiffre les mots de passe des comptes. Cette fonctionnalité ne chiffre pas les communications du client Web ou de PowerShell, qui sont gérées séparément par des certificats de serveur.

L'utilisation de communications chiffrées peut avoir un impact sur les performances. Les communications chiffrées sont désactivées par défaut. Si vous activez cette option, les données sont chiffrées pendant les communications entre les interfaces utilisateur et le serveur d'administration. DRA utilise le chiffrement standard Microsoft pour l'appel de procédure distante (RPC).

Pour activer les communications chiffrées, accédez à **Gestion de la configuration** > **Mettre à jour les options du serveur d'administration**. Sur l'onglet **Général**, cochez la case **Communications chiffrées**.

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

Définir les attributs virtuels

À l'aide des attributs virtuels, vous pouvez créer de nouvelles propriétés et associer ces propriétés aux utilisateurs, aux groupes, aux groupes de distribution dynamique, aux contacts, aux ordinateurs et aux unités organisationnelles. Les attributs virtuels vous permettent de créer de nouvelles propriétés sans obliger à étendre le schéma Active Directory.

À l'aide des attributs virtuels, vous pouvez ajouter de nouvelles propriétés aux objets dans Active Directory. Vous pouvez uniquement créer, activer, désactiver, associer et dissocier des attributs virtuels sur le serveur d'administration primaire. DRA stocke les attributs virtuels que vous créez dans AD LDS. DRA réplique les attributs virtuels du serveur d'administration primaire sur des serveurs d'administration secondaires au cours du processus de synchronisation MMS.

Avec les pouvoirs appropriés, vous pouvez gérer les attributs virtuels. Le rôle Gérer les attributs virtuels confère le pouvoir de créer, d'activer, d'associer, de dissocier, de désactiver et d'afficher des attributs virtuels.

- « Créer des attributs virtuels » page 98
- « Associer des attributs virtuels à des objets » page 98
- « Dissocier des attributs virtuels » page 99
- « Désactiver des attributs virtuels » page 99

Créer des attributs virtuels

Vous devez disposer du pouvoir *Créer des attributs virtuels* pour créer des attributs virtuels et du pouvoir *Afficher les attributs virtuels* pour afficher des attributs virtuels.

Pour créer un attribut virtuel, accédez au nœud **Gestion de la configuration** > **Attributs virtuels** > **Attributs gérés**, puis cliquez sur **Nouvel attribut virtuel** dans le menu Tâches.

Associer des attributs virtuels à des objets

Vous ne pouvez associer que les attributs virtuels activés aux objets Active Directory. Une fois que vous avez associé un attribut virtuel à un objet, celui-ci est disponible dans les propriétés de l'objet.

Pour exposer des attributs virtuels à l'aide des interfaces utilisateur DRA, vous devez créer une page de propriétés personnalisée.

Pour associer un attribut virtuel à un objet, accédez au nœud **Gestion de la configuration** > **Attributs virtuels**> **Attributs gérés**, cliquez avec le bouton droit sur l'attribut virtuel à utiliser et sélectionnez **Associer**> (type d'objet).

REMARQUE

- Vous pouvez uniquement associer des attributs virtuels à des utilisateurs, à des groupes, à des groupes de distribution dynamiques, à des ordinateurs, à des contacts et à des unités organisationnelles.
- Lorsque vous associez un attribut virtuel à un objet, DRA crée automatiquement deux pouvoirs personnalisés par défaut. Les administrateurs assistants ont besoin de ces pouvoirs personnalisés pour gérer l'attribut virtuel.

Dissocier des attributs virtuels

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

Pour dissocier un attribut virtuel d'un objet Active Directory, accédez au nœud **Gestion de la configuration** > **Attributs virtuels** > **Classes gérées**> (type d'objet). Cliquez avec le bouton droit de la souris sur l'attribut virtuel, puis sélectionnez **Dissocier**.

Désactiver des attributs virtuels

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

Pour désactiver un attribut virtuel, accédez à **Gestion de la configuration** > **Attributs gérés**. Cliquez avec le bouton droit de la souris sur l'attribut souhaité dans le volet de liste et sélectionnez **Désactiver**.

Configurer la mise en cache

Le serveur d'administration crée et gère un **cache des comptes** contenant des parties d'Active Directory pour les domaines gérés. DRA utilise le cache des comptes pour améliorer les performances lors de la gestion des comptes d'utilisateurs, des groupes, des contacts et des comptes d'ordinateurs.

Pour planifier une actualisation du cache ou afficher son état, vous devez disposer des pouvoirs appropriés tels que ceux inclus dans le rôle intégré Configurer les serveurs et les domaines.

REMARQUE : Pour effectuer des actualisations incrémentielles du cache des comptes dans les domaines contenant des sous-arborescences gérées, assurez-vous que le compte de service dispose d'un accès en lecture au conteneur Objets supprimés ainsi qu'à tous les objets du domaine de la sous-arborescence. Vous pouvez utiliser l'utilitaire Objets supprimés pour vérifier et déléguer les autorisations appropriées.

- « Actualisations complètes et incrémentielles » page 100
- « Fréquence planifiée par défaut » page 101

Actualisations complètes et incrémentielles

Une actualisation incrémentielle du cache des comptes ne met à jour que les données qui ont changé depuis la dernière actualisation. L'actualisation incrémentielle offre un moyen simplifié de suivre l'évolution de votre Active Directory. Utilisez l’actualisation incrémentielle pour mettre rapidement à jour le cache des comptes tout en ayant le moins d’impacts sur votre 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. Assurez-vous donc que le même compte d'utilisateur est limité à cinq shells pour les serveurs secondaires DRA.

Une actualisation incrémentielle met à jour les données suivantes :

- les nouveaux objets et ceux qui ont été clonés
- les objets supprimés et ceux qui ont été déplacés
- les adhésions à un groupe
- toutes les propriétés de l'objet mises en cache pour les objets modifiés

Une actualisation complète du cache des comptes reconstruit le cache des comptes de DRA pour le domaine spécifié.

REMARQUE : Le domaine n'est pas disponible pour les utilisateurs DRA pendant une actualisation complète du cache des comptes.

Effectuer une actualisation complète du cache des comptes

Pour effectuer une actualisation du 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 immédiatement une actualisation complète du cache des comptes :

1. Accédez à **Gestion de la configuration** > **Domaines gérés**.
2. Cliquez avec le bouton droit de la souris sur le domaine souhaité, puis sélectionnez **Propriétés**.
3. Cliquez sur **Actualiser maintenant**dans l'onglet **Actualisation complète**.

Fréquence planifiée par défaut

La fréquence d'actualisation du cache des comptes dépend de la fréquence à laquelle votre entreprise change. Utilisez l'actualisation incrémentielle pour mettre à jour le cache des comptes fréquemment, en vous assurant que DRA dispose des informations les plus récentes sur Active Directory.

Par défaut, le serveur d'administration effectue une actualisation incrémentielle du cache des comptes aux fréquences suivantes :

Type de domaine	Fréquence d'actualisation planifiée par défaut
Domaines gérés	Toutes les 5 minutes
Domaines approuvés	Toutes les heures
Locataire Azure	Toutes les 15 minutes

Vous ne pouvez pas planifier d'actualisation complète du cache des comptes. Cependant, DRA exécute une actualisation complète du cache des comptes automatique dans les cas suivants :

- 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 ensemble de modifications provisoires DRA.

Effectuer une actualisation complète du cache des comptes peut nécessiter plusieurs minutes.

Considérations

Vous devez régulièrement actualiser le cache des comptes pour vous assurer que DRA dispose des informations les plus récentes. Avant d'effectuer ou de planifier l'actualisation du cache des comptes, prenez en compte les considérations suivantes :

- Pour effectuer une actualisation incrémentielle du cache des comptes, le compte de service du serveur d'administration ou le compte d'accès doit avoir l'autorisation d'accéder aux objets supprimés dans l'Active Directory du domaine géré ou approuvé.
- Lorsque DRA actualise le cache des comptes, le serveur d'administration n'inclut pas les groupes de sécurité locaux de domaine provenant des domaines approuvés. Étant donné que le cache ne contient pas ces groupes, DRA ne vous permet pas d'ajouter un groupe de sécurité local de domaine provenant du domaine approuvé à un groupe local sur le serveur membre géré.
- Si vous omettez un domaine approuvé lors de l'actualisation du cache des comptes, le serveur d'administration omet également ce domaine de l'actualisation de la configuration du domaine.
- Si vous incluez un domaine approuvé précédemment omis dans l'actualisation du cache des comptes, effectuez une actualisation complète du cache des comptes pour le domaine géré. Cela garantit que le cache des comptes sur le serveur d'administration du domaine géré reflète correctement les données d'adhésion à un groupe dans vos domaines gérés et approuvés.
- Si vous mettez la valeur de l'intervalle d'actualisation incrémentielle du cache des comptes à **Jamais**, le serveur d'administration effectue uniquement l'actualisation du cache des comptes. Une actualisation complète du cache des comptes peut prendre un certain temps, pendant lequel vous ne pouvez pas gérer les objets de ce domaine.

- DRA ne peut pas déterminer automatiquement le moment où les modifications sont apportées par d'autres outils tels que Microsoft Directory Services. Les opérations effectuées en dehors de DRA peuvent affecter la précision des informations mises en cache. Par exemple, si vous utilisez un autre outil pour ajouter une boîte aux lettres à un compte d'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'actualisation complète du cache des comptes supprime les dernières statistiques de connexion conservées dans le cache. Le serveur d'administration collecte ensuite les dernières informations de connexion de tous les contrôleurs de domaine.

Activer la collection d'imprimantes d'Active Directory

La collection d'imprimantes d'AD est désactivée par défaut. Pour l'activer, accédez à **Gestion de la configuration** > **Mettre à jour les options du serveur d'administration**. Sur l'onglet **Général**, cochez la case Collecter les imprimantes.

AD LDS

Vous pouvez configurer l'actualisation du nettoyage d'AD LDS pour qu'elle s'exécute selon une planification pour des domaines précis. Le paramètre par défaut est ne « Jamais » actualiser. Vous pouvez également afficher l'état du nettoyage et des informations précises relatives à la configuration d'AD LDS (ADAM).

Pour configurer la planification ou afficher l'état du nettoyage d'AD LDS, cliquez à l'aide du bouton droit de la souris sur le domaine souhaité dans le nœud **Gestion des comptes et des ressources** > **Tous mes objets gérés**, puis sélectionnez **Propriétés** > **Planification d'actualisation du nettoyage Adlds**ou **État de nettoyage Adlds**, respectivement.

Pour afficher les informations de configuration d'AD LDS (ADAM), accédez à **Gestion de la configuration** > **Options du serveur de mise à jour**> **Configuration d'ADAM**.

Groupe dynamique

Un groupe dynamique est un groupe dont l'adhésion change en fonction d'un ensemble de critères que vous configurez dans les propriétés du groupe. Dans les propriétés du domaine, vous pouvez configurer l'actualisation du groupe dynamique pour qu'elle s'exécute selon une planification pour des domaines précis. Le paramètre par défaut est ne « Jamais » actualiser. Vous pouvez également afficher l'état de l'actualisation.

Pour configurer la planification ou afficher l'état d'actualisation du groupe dynamique, cliquez à l'aide du bouton droit de la souris sur le domaine souhaité dans le nœud **Gestion des comptes et des ressources** > **Tous mes objets gérés**, puis sélectionnez **Propriétés** > **Actualisation du groupe dynamique** ou **État du groupe dynamique**, respectivement.

Pour obtenir de plus amples renseignements sur les groupes dynamiques, consultez la section Groupes dynamiques DRA.

Configurer la Corbeille

Vous pouvez activer ou désactiver la Corbeille pour chaque domaine ou objet Microsoft Windows de chaque domaine et configurer quand et comment vous souhaitez que le nettoyage de la Corbeille ait lieu.

Pour obtenir de plus amples renseignements sur l'utilisation de la Corbeille, consultez la section Corbeille.

Activer la Corbeille

Vous pouvez activer la Corbeille pour des domaines Microsoft Windows précis et des objets de ces domaines. Par défaut, DRA active la Corbeille pour chaque domaine qu'il gère et pour tous les objets du domaine. Vous devez être membre du groupe Administrateurs DRA ou Administrateurs assistants de Configuration DRA pour activer la Corbeille.

Si votre environnement inclut la configuration suivante, utilisez l'utilitaire de la Corbeille pour activer cette fonctionnalité :

- DRA gère une sous-arborescence de ce domaine.
- Le service du serveur d'administration ou le compte d'accès n'a pas l'autorisation nécessaire pour créer le conteneur de la Corbeille, pour déplacer les comptes vers ce conteneur et pour modifier les comptes dans ce conteneur.

Vous pouvez également utiliser l'utilitaire de la Corbeille pour vérifier le service du serveur d'administration ou accéder aux autorisations du compte sur le conteneur de la Corbeille.

Pour activer la Corbeille, cliquez à l'aide du bouton droit de la souris sur le domaine souhaité dans le nœud **Corbeille**, puis sélectionnez **Activer la Corbeille**.

Désactiver la Corbeille

Vous pouvez désactiver la Corbeille pour des domaines Microsoft Windows précis et des objets de ces domaines. Si une Corbeille désactivée contient des comptes, vous ne pouvez pas afficher, supprimer définitivement ou restaurer ces comptes.

Vous devez être membre des groupes Administrateurs DRA ou Administrateurs assistants de Configuration DRA pour désactiver la Corbeille.

Pour désactiver la Corbeille, cliquez à l'aide du bouton droit de la souris sur le domaine souhaité dans le nœud **Corbeille**, puis sélectionnez **Désactiver la Corbeille**.

Configurer des objets de la Corbeille et le nettoyage

Le réglage par défaut pour le nettoyage de la Corbeille est quotidien. Vous pouvez modifier cette configuration pour nettoyer la Corbeille du domaine tous les x jours. Au cours du nettoyage planifié, la Corbeille supprime les objets plus anciens que le nombre de jours que vous avez défini pour

chaque type d'objet. Le réglage par défaut pour chaque type permet de supprimer les objets âgés de plus d'un jour. Vous pouvez personnaliser le comportement du nettoyage de la Corbeille en désactivant, en réactivant et en définissant l'âge des objets à supprimer pour chaque type d'objet.

Pour configurer le nettoyage de la Corbeille, sélectionnez le domaine souhaité dans la console de délégation et de configuration et accédez à l'onglet **Tâches** > **Propriétés** > **Corbeille**.

Configurer la création des rapports

Les sections suivantes fournissent de l'information conceptuelle sur les rapports de gestion DRA et les collecteurs de rapports que vous pouvez activer. Pour accéder à l'assistant dans lequel vous pouvez configurer les collecteurs, allez dans **Gestion de la configuration** > **Mettre à jour la configuration du service de création des rapports**.

Configurer le collecteur d'Active Directory

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

Vous pouvez configurer le collecteur d'Active Directory pour spécifier les attributs à collecter et à stocker dans la base de données de rapports. Vous pouvez également configurer le serveur d'administration DRA sur lequel le collecteur s'exécutera.

Configurer DRA Collector

DRA Collector collecte des informations sur votre configuration DRA et les stocke dans la base de données de rapports utilisée pour générer des rapports dans la console de création de rapports.

Pour activer DRA Collector, vous devez spécifier le serveur d'administration DRA sur lequel le collecteur s'exécutera. Il est recommandé de planifier l'exécution de DRA Collector après le bon fonctionnement du collecteur Active Directory et pendant les périodes où le serveur est le moins chargé ou en dehors des heures normales de travail.

Configurer le collecteur du locataire Azure

Le collecteur du locataire Azure collecte des informations sur les utilisateurs et les groupes Azure qui sont synchronisés avec le locataire Azure Active Directory et stocke ces informations dans la base de données de rapports, qui est utilisée pour générer des rapports dans la console de création de rapports.

Pour activer le collecteur du locataire Azure, vous devez spécifier le serveur d'administration DRA sur lequel le collecteur s'exécutera.

REMARQUE : Le locataire Azure ne peut exécuter une collecte réussie qu'une fois que le collecteur Active Directory de son domaine correspondant a exécuté une collecte réussie.

Configurer le collecteur de rapports de gestion

Le collecteur de rapports de gestion collecte les informations d'audit DRA et les stocke dans la base de données de rapports utilisée pour générer des rapports dans la console de création de rapports. Lorsque vous activez le collecteur, vous pouvez configurer la fréquence de mise à jour des données dans la base de données pour les requêtes exécutées dans l'outil DRA Reporting.

Cette configuration nécessite que le compte du Service DRA ait l'autorisation **sysadmin** dans SQL Server sur le serveur de création de rapports. Les options configurables sont définies ci-dessous :

- **Intervalle de données d'exportation d'audit :**il s'agit de l'intervalle de temps pendant lequel les données d'audit du journal de suivi DRA (LAS) sont exportées vers la base de données « SMCubeDepot » dans SQL Server.
- **Intervalle de synthèse des rapports de gestion :** il s'agit de l'intervalle de temps pendant lequel les données d'audit de la base de données SMCubeDepot sont pompées dans la base de données de DRA Reporting, où elles peuvent être interrogées par l'outil DRA Reporting.

Rassembler les statistiques de dernière connexion

Vous pouvez configurer DRA pour collecter les statistiques de dernière connexion de tous les contrôleurs de domaine du 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 fonctionnalité de collecte des statistiques de dernière connexion est désactivée. Si vous souhaitez collecter les données statistiques de dernière connexion, vous devez activer cette fonctionnalité. Une fois que vous avez activé la collecte de statistiques de dernière connexion, vous pouvez afficher les statistiques de dernière connexion d'un utilisateur particulier ou afficher l'état de la collecte de statistiques de dernière connexion.

Pour rassembler les statistiques de la dernière connexion :

1. Accédez à **Gestion de la configuration** > **Domaines gérés**.
2. Cliquez avec le bouton droit de la souris sur le domaine souhaité, puis sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Planification de la dernière connexion** pour configurer la collecte des statistiques de dernière connexion.

Délégation des pouvoirs de configuration du serveur de Workflow Automation

Pour gérer le processus de travail, attribuez le rôle d'administrateur du serveur de Workflow Automation ou les pouvoirs applicables ci-dessous aux administrateurs assistants :

- Créer un événement de processus de travail et modifier toutes les propriétés
- Supprimer la configuration du serveur de Workflow Automation
- Définir les informations de configuration du serveur de Workflow Automation
- Démarrer un processus de travail
- Afficher toutes les propriétés des événements de processus de travail

- Afficher toutes les propriétés de processus de travail
- Afficher les informations de configuration du serveur de Workflow Automation

Pour déléguer les pouvoirs de configuration du serveur de Workflow Automation :

1. Cliquez sur **Powers** (Pouvoir) dans le nœud Gestion des délégations, puis utilisez la fonctionnalité de recherche d'objets pour rechercher et sélectionner les pouvoirs de processus de travail souhaités.
2. Cliquez avec le bouton droit de la souris sur l'un des pouvoirs de processus de travail sélectionnés et cliquez sur **Delegate Roles and Powers** (Déléguer des rôles et des pouvoirs).
3. Recherchez l'utilisateur, le groupe ou le groupe d'administrateurs assistants à qui vous souhaitez déléguer des pouvoirs.
4. Utilisez le **Object Selector** (Sélecteur d'objets) pour trouver et ajouter les objets souhaités, puis cliquez sur **Roles and Powers** (Rôles et pouvoirs) dans le **Wizard** (Assistant).
5. Cliquez sur **ActiveViews** et utilisez le **Object Selector** (Sélecteur d'objets) pour rechercher et ajouter les ActiveViews souhaités.
6. Cliquez sur **Next** (Suivant), puis sur **Finish** (Terminer) pour terminer le processus de délégation.

Configuration du serveur de Workflow Automation

Pour utiliser Workflow Automation dans DRA, vous devez installer Workflow Automation Engine sur un serveur Windows, puis configurer le serveur Workflow Automation à l'aide de la console de délégation et de configuration.

Pour configurer le serveur de Workflow Automation :

1. Connectez-vous à la console de délégation et de configuration.

   Pour en savoir davantage sur les pouvoirs de Workflow Automation, reportez-vous à la rubrique Délégation des pouvoirs de configuration du serveur de Workflow Automation.
2. Développez **Configuration Management** > **Integration Servers** (Gestion de la configuration > Serveurs d'intégration.
3. Cliquez à l'aide du bouton droit de la souris sur **Workflow Automation**, puis sélectionnez **New Workflow Automation Server** (Nouveau serveur de Workflow Automation).
4. Dans l'assistant **Add Workflow Automation Server** (Ajouter le serveur de Workflow Automation), indiquez les détails tels que le nom du serveur, le port, le protocole et le compte d'accès.
5. Testez la connexion au serveur et cliquez sur **Finish** (Terminer) pour enregistrer la configuration.

Pour en savoir plus sur l'installation de Workflow Automation Engine, consultez le *Guide de l'administrateur de Workflow Automation* sur le site de la documentation de DRA.

Délégation des pouvoirs de recherche LDAP

DRA vous permet de rechercher des objets LDAP dans des domaines Active Directory locaux tels que des utilisateurs, des contacts, des ordinateurs, des groupes et des unités d'organisation à partir du serveur LDAP. Le serveur DRA gère toujours l'opération; c'est lui le contrôleur de domaine sur lequel la recherche est exécutée. Utilisez les filtres de recherche pour des recherches plus efficaces. Vous pouvez également enregistrer la requête de recherche pour une utilisation ultérieure et la partager avec le public ou l'utiliser pour votre propre compte en la marquant comme privée. Vous pouvez

modifier les requêtes enregistrées. Le rôle Requêtes avancées LDAP accorde aux administrateurs assistants le pouvoir de créer et de gérer des requêtes de recherche LDAP. Utilisez les pouvoirs suivants pour déléguer la création et la gestion des requêtes de recherche LDAP :

- Créer une requête avancée privée
- Créer une requête avancée publique
- Supprimer une requête avancée publique
- Exécuter une requête avancée
- Exécuter une requête avancée enregistée
- Modifier une requête publique
- Afficher une requête avancée

Pour déléguer des pouvoirs de requête LDAP :

1. Cliquez sur **Powers** (Pouvoir) dans le nœud Gestion des délégations, puis utilisez la fonctionnalité de recherche d'objets pour rechercher et sélectionner les pouvoirs de requête LDAP avancés souhaités.
2. Cliquez à l'aide du bouton droit de la souris sur l'un des pouvoirs de requête LDAP sélectionnés et cliquez sur **Delegate Roles and Powers** (Déléguer des rôles et des pouvoirs).
3. Recherchez l'utilisateur, le groupe ou le groupe d'administrateurs assistants à qui vous souhaitez déléguer des pouvoirs.
4. Utilisez le **Object Selector** (Sélecteur d'objets) pour trouver et ajouter les objets souhaités, puis cliquez sur **Roles and Powers** (Rôles et pouvoirs) dans le **Wizard** (Assistant).
5. Cliquez sur **ActiveViews** et utilisez le **Object Selector** (Sélecteur d'objets) pour rechercher et ajouter les ActiveViews souhaités.
6. Cliquez sur **Next** (Suivant), puis sur **Finish** (Terminer) pour terminer le processus de délégation.

Pour accéder à la fonction de recherche dans la console Web, accédez à **Management > LDAP Search** (Gestion > Recherche LDAP).

Configuration de la création de rapports sur l'historique des modifications

DRA permet de déléguer les modifications gérées dans une organisation d'entreprise et Change Guardian (CG) permet de surveiller les modifications gérées et non gérées survenant dans Active Directory. L'intégration de DRA et de CG offre les avantages suivants :

- Possibilité de voir l'administrateur assistant délégué par DRA qui a apporté une modification à Active Directory dans les événements CG pour les modifications apportées par DRA.
- Possibilité de voir l'historique des modifications récentes d'un objet dans DRA, qu'il s'agisse de modifications effectuées par DRA ou de modifications capturées par CG et provenant de l'extérieur de DRA.
- Les modifications apportées par DRA sont désignées comme des modifications « gérées » dans CG.

Pour configurer la création de rapports d'historique des modifications de DRA, procédez comme suit :

1. Installez l'agent Windows pour Change Guardian.
2. Ajoutez une clé de licence Active Directory.
3. Configurez Active Directory.
4. Créez et attribuez une stratégie Active Directory.
5. Gérez les domaines Active Directory.
6. Activez le marquage d'événement.
7. Configurez l'historique des modifications unifié.

Une fois que vous avez effectué les étapes ci-dessus pour installer Change Guardian et configurer l'intégration de DRA et de CG, les utilisateurs peuvent générer et visualiser les rapports UCH dans la console Web.

Pour en savoir plus, consultez la rubrique « Génération de rapports sur l'historique des modifications » du *Guide d'utilisation de Directory and Resource Administrator*.

Installer l'agent Windows pour Change Guardian

Avant de commencer l'intégration de DRA et de CG, installez l'agent Windows de Change Guardian. Pour en savoir plus, consultez le *Guide d'installation et d'administration de Change Guardian*.

Ajouter une clé de licence Active Directory

Vous devez ajouter des licences à la fois pour le serveur Change Guardian et pour les applications ou modules que vous prévoyez de surveiller..

Ajout d'une clé de licence pour le serveur

Vous pouvez utiliser la console d'administration ou la ligne de commande pour ajouter la clé de licence du serveur Change Guardian..

Si vous utilisez la clé de licence d'évaluation, vous devez ajouter la clé de licence d'entreprise avant l'expiration de la clé d'évaluation pour éviter une interruption des fonctionnalités de Change Guardian. Pour plus d'informations sur l'achat d'une licence, consultez le site Web du produit Change Guardian.

Ajout à partir de la console d'administration

Pour ajouter une clé de licence, procédez comme suit :

1 Dans la console web, cliquez sur **ADMINISTRATION**.

2 Cliquez sur **Aide > À propos de > Licences > Ajouter une licence**.

3 Spécifiez la clé de licence et enregistrez.

REMARQUE : Après l'expiration d'une licence, la console Web de Change Guardian apparaît vide.

Ajout à partir de la ligne de commande

Pour ajouter une clé de licence à l'aide de la ligne de commande, procédez comme suit :

1. Connectez-vous au serveur Change Guardian en tant que `root` (racine).
2. Allez dans le répertoire `/opt/novell/sentinel/bin`.
3. Changez pour l'utilisateur novell suivant :

   ```
   su novell
   ```
4. Exécutez le script `softwarekey.sh` :

   ```
   ./softwarekey.sh
   ```
5. Saisissez 1 pour insérer la clé de licence.
6. Spécifiez la clé de licence, puis appuyez sur Entrée

Ajout d'une licence pour les applications

Module Manager vous fournit des informations sur les applications sous licence et vous permet d'importer des licences d'application dans Policy Editor.

Lorsque vous installez Change Guardian, toutes les applications disponibles sont installées automatiquement sur Policy Editor. Cependant, vous devez ajouter une nouvelle application à Policy Editor. Pour permettre à Change Guardian de commencer la surveillance, importez la clé de licence de chaque application.

Pour ajouter une nouvelle application à Module Manager :

1. Dans **Module Manager**, cliquez sur **Install > From Local Directory** (Installer à partir du répertoire local).

Pour importer une licence :

1. Connectez-vous à Policy Editor, cliquez sur **Change Guardian**.
2. Sélectionnez **Module Manager**.
3. Cliquez sur **Import License Key** (Importer la clé de licence).
4. Sélectionnez la clé de licence pour l'application requise.

Configurer Active Directory

Pour configurer Active Directory pour l'historique des modifications, consultez les sections suivantes :

Configuration du journal des événements de sécurité

Configurez le journal des événements de sécurité pour que les événements Active Directory restent dans le journal des événements jusqu'à ce que Change Guardian les traite.

Pour configurer le journal des événements de sécurité procédez comme suit :

1. Connectez-vous en tant qu'administrateur à un ordinateur du domaine que vous voulez configurer.

2 Pour ouvrir la console de gestion des politiques de groupe, entrez ce qui suit à l'invite de commande : `gpmc.msc`

3 Ouvrez **Forest > Domains** > ***domainName***> **Domain Controllers** (Forêt > Domaines > nom de domaine > Contrôleurs de domaine).

4 Cliquez à l'aide du bouton droit sur **Default Domain Controllers Policy** (Stratégie des contrôleurs de domaine par défaut), puis cliquez sur **Edit** (Éditer).

REMARQUE : La modification de la stratégie par défaut des contrôleurs de domaine est importante car une GPO liée à l'unité organisationnelle (OU) du contrôleur de domaine (DC) avec un ordre de liaison supérieur peut remplacer cette configuration lorsque vous redémarrez l'ordinateur ou exécutez `gpUpdate` à nouveau. Si les normes de votre entreprise ne vous permettent pas de modifier la stratégie par défaut des contrôleurs de domaine, créez un GPO pour vos paramètres Change Guardian, ajoutez ces paramètres au GPO et définissez-le pour qu'il ait l'ordre de lien le plus élevé dans l'unité organisationnelle Domain Controllers (Contrôleurs de domaines).

---

5 Développez **Computer Configuration > Policies > Windows Settings > Security Settings** (Configuration de l'ordinateur > Politiques > Paramètres de Windows > Paramètres de sécurité).

6 Sélectionnez **Event Log** (Journaux des événements) et définissez les paramètres ci-dessous comme suit :

- **Taille maximale du journal de sécurité** à 10240 Ko (10 Mo) ou plus
- **Méthode de rétention du journal de sécurité** à **Supprimer les événements si nécessaire** (Supprimer les événements si nécessaire)

7 Pour mettre à jour les paramètres de stratégie, exécutez la commande `gpUpdate` à l'invite de commande.

Pour vérifier que la configuration est réussie :

1 Ouvrez une invite de commande en tant qu'administrateur sur l'ordinateur.

2 Lancez la visionneuse d'événements : `eventvwr`

3 Sous Journaux Windows, cliquez à l'aide du bouton droit de la souris sur **Sécurité**, puis sélectionnez **Propriétés**.

4 Assurez-vous que les paramètres indiquent que la taille maximale du journal est de 10240 Ko (10 Mo) ou plus et que l'option « Supprimer les événements si nécessaire » est sélectionnée..

Configuration de l'audit d'AD

Configurez l'audit d'AD pour activer la journalisation des événements AD dans le journal des événements de sécurité.

Configurer le GPO de la stratégie des contrôleurs de domaine par défaut avec un accès au service Audit Directory pour surveiller les événements de réussite et d'échec.

Pour configurer l'audit d'AD :

1 Connectez-vous en tant qu'administrateur à un ordinateur du domaine que vous voulez configurer.

2 Pour ouvrir la console de gestion des stratégies de groupe, exécutez `gpmc.msc` à l'invite de commande.

3 Développez **Forêt > Domaines** > ***nomdedomaine***> **Contrôleurs de domaine**.

4 Cliquez à l'aide du bouton droit sur **Stratégie des contrôleurs de domaine par défaut**, puis cliquez sur **Éditer**.

REMARQUE : La modification de la stratégie par défaut des contrôleurs de domaine est importante car une GPO liée à l'unité organisationnelle (OU) du contrôleur de domaine (DC) avec un ordre de liaison supérieur peut remplacer cette configuration lorsque vous redémarrez l'ordinateur ou exécutez `gpUpdate` à nouveau. Si les normes de votre entreprise ne vous permettent pas de modifier la stratégie par défaut des contrôleurs de domaine, créez un GPO pour vos paramètres Change Guardian, ajoutez ces paramètres au GPO et définissez-le pour qu'il ait l'ordre de lien le plus élevé dans l'unité organisationnelle Contrôleurs de domaines.

---

5 Développez **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies** (Configuration de l'ordinateur > Stratégies > Paramètres de Windows > Paramètres de sécurité > Configuration avancée de la stratégie d'audit > Stratégies d'audit).

5a Pour configurer AD et la stratégie de groupe, sous **Gestion des comptes**, et **Changement de stratégie**, sélectionnez les éléments suivants pour chaque sous-catégorie : **Configure the following audit events** (Configurer les événements d'audit suivants), **Succès**, et **Échec**.

5b Pour configurer uniquement AD, sous **DS Access** (Accès DS), sélectionnez les éléments suivants pour chaque sous-catégorie : **Configurer les événements d'audit suivants**, **Succès**, et **Échec**.

6 Cliquez sur **Configuration de l'ordinateur > Stratégies > Paramètres de Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité**, et activez **Audit : forcer les paramètres de sous-catégorie de la stratégie d'audit... à remplacer les paramètres de catégorie de la stratégie d'audit**.

7 Accédez à **Configuration de l'ordinateur > Stratégies > Paramètres de Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit**.

8 Sous **Audit account management**, **Audit directory service access**, and **Audit policy change** (Auditer la gestion des comptes, Auditer l'accès au service d'annuaire et Auditer les modifications de stratégie), sélectionnez les éléments suivants pour chaque sous-catégorie dans Propriétés : **Define these policy settings** (Définir ces paramètres de stratégie), **Success** (Succès), et **Failure** (Échec).

9 Pour mettre à jour les paramètres de stratégie, exécutez la commande `gpUpdate` à l'invite de commande.

Pour en savoir plus, consultez la rubrique *Surveillance d'Active Directory à la recherche de signes de compromission* sur le site de la documentation Microsoft.

Configuration de l'audit des utilisateurs et des groupes

Configurez l'audit des utilisateurs et des groupes pour auditer les activités suivantes :

- Activités de connexion et de déconnexion des utilisateurs locaux et des utilisateurs Active Directory
- Paramètres locaux d'utilisateur
- Paramètres locaux du groupe

Pour configurer l'audit des utilisateurs et des groupes procédez comme suit :

1. Connectez-vous en tant qu'administrateur à un ordinateur du domaine que vous voulez configurer.
2. Ouvrez la console de gestion Microsoft, sélectionnez **Fichier > Ajouter/Supprimer un Snap-in**.
3. Sélectionnez **Group Policy Management Editor** (Éditeur de gestion de stratégie de groupe) et cliquez sur **Ajouter**.
4. Dans la fenêtre Select Group Policy Object (Sélectionner un objet de stratégie de groupe), cliquez sur **Browse** (Parcourrir).
5. Sélectionnez **Contrôleurs de domaine.*FQDN***, où *FQDN* est le nom de domaine entièrement qualifié de l'ordinateur du contrôleur de domaine.
6. Sélectionnez **Stratégie des contrôleurs de domaine par défaut**.
7. Dans la console de gestion Microsoft, développez **Stratégie des contrôleurs de domaine par défaut *FQDN* > Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit**.
8. Sous **Auditer les événements de connexion du compte** et **Auditer les événements de connexion**, sélectionnez **Définir ces paramètres de stratégie**, **Succès** et **Échec**.
9. Dans la console de gestion Microsoft, développez **Stratégie des contrôleurs de domaine par défaut *FQDN* > Configuration des ordinateurs > Stratégies > Paramètres Windows > Paramètres de sécurité > Configuration avancée de la stratégie d'audit > Stratégies d'audit > Connexion/Déconnexion**.
10. Sous **Audit Logon** (Auditer la connexion), sélectionnez **Auditer la connexion**, **Succès** et **Échec**.
11. Sous **Audit Logoff** (Auditer la déconnexion), sélectionnez **Auditer la déconnexion**, **Succès** et **Échec**.
12. Pour mettre à jour les paramètres de stratégie, exécutez la commande `gpupdate /force` à l'invite de commande..

Configuration des listes de contrôle d'accès de sécurité

Pour surveiller toutes les modifications des objets actuels et futurs dans Active Directory, configurez le nœud de domaine.

Pour configurer les listes de contrôle d'accès à la sécurité (SACL) procédez comme suit :

1. Connectez-vous en tant qu'administrateur à un ordinateur du domaine que vous voulez configurer.
2. Pour ouvrir l'outil de configuration ADSI Edit, exécutez `adsiedit.msc` à l'invite de commande.
3. Cliquez avec le bouton droit de la souris sur **ADSI Edit**, et sélectionnez **Connecter à**.
4. Dans la fenêtre Paramètres de connexion, spécifiez les éléments suivants :
   - **Nom** comme `Default naming context` (Contexte d'attribution de nom par défaut).
   - **Chemin** vers le domaine à configurer.
   - Si vous effectuez cette étape pour la première fois, sélectionnez **Contexte d'attribution de nom par défaut**.
   - Si vous le faites pour la deuxième fois, sélectionnez **Schéma**.
   - Si vous le faites pour la troisième fois, sélectionnez **Configuration**.

REMARQUE : Vous devez exécuter trois fois les Etapes 4 à Étape 11, afin de configurer les points de connexion pour **le contexte d'attribution de nom par défaut**, **le schéma**, et **la configuration**.

5 Dans **Connection Point** (Point de connexion), définissez **Select a well known Naming Context** (Sélectionner un contexte d'attribution de nom bien connu) sur **Contexte d'attribution de nom par défaut**.

6 Dans la fenêtre ADSI Edit, développez **Contexte d'attribution de nom par défaut**.

7 Cliquez à l'aide du bouton droit de la souris sur le nœud situé sous le point de connexion (commence par DC= ou CN=), puis cliquez sur **Propriétés**.

8 Dans l'onglet **Sécurité**, cliquez sur **Avancé > Audit > Ajouter**.

9 Dans **Appliquer à** ou **Appliquer sur**, sélectionnez **This object and all descendant objects** (Cet objet et tous les objets descendants).

10 Configurez l'audit pour surveiller chaque utilisateur :

10a Cliquez sur **Select a principal** (Sélectionner un principal), et tapez `everyone` (tout le monde) dans **Enter the object name to select** (Entrer le nom de l'objet à sélectionner).

10b Indiquqez les options suivantes :

- Pour **Type**, sélectionnez **Tout**
- Pour **Permissions**, sélectionnez :
  - **Écriture de toutes les propriétés**
  - **Supprimer**
  - **Modifier les autorisations**
  - **Modifier le propriétaire**
  - **Créer tous les objets enfant**

    Les autres nœuds liés aux objets enfants sont sélectionnés automatiquement.
  - **Supprimer tous les objets enfants**

    Les autres nœuds liés aux objets enfants sont sélectionnés automatiquement.

11 Désélectionnez l'option **Apply these auditing entries to objects and/or containers within this container only** (Appliquer ces entrées d'audit aux objets et/ou conteneurs de ce conteneur uniquement).

12 Répétez lesétapes 4 à Étape 11 deux fois de plus.

Créez et attribuez une stratégie Active Directory

Vous pouvez créer une nouvelle stratégie sans paramètres préconfigurés.

Pour créer une stratégie :

1 Dans l'éditeur de stratégie, sélectionnez l'une des applications, par exemple Active Directory.

2 Développez la liste des stratégies et sélectionnez le type de stratégie que vous souhaitez créer. Par exemple, sélectionnez **Stratégies Active Directory > Objet AD**.

3 Sur l'écran Stratégie de configuration, apportez les modifications appropriées.

4 (Conditionnel) Si vous voulez activer la stratégie immédiatement, sélectionnez **Enable this policy revision now** (Activer cette révision de stratégie maintenant)..

Pour affecter une stratégie ou un ensemble de stratégies à une ressource :

1. Cliquez sur **Change Guardian > Policy Assignment** (Attribution de stratégie).
2. Sélectionnez un poste ou un groupe de postes, puis cliquez sur **Attribuer les stratégies**.
3. Sélectionnez un ensemble de stratégies ou une stratégie, puis cliquez sur **Appliquer**.

REMARQUE : Vous ne pouvez pas attribuer de stratégies à l'aide de **groupes de ressources** pour les types de ressources suivants : Azure AD, AWS for IAM, Dell EMC, Microsoft Exchange, Microsoft Office 365 et NetApp..

Gérez les domaines Active Directory.

Pour configurer un domaine dans DRA comme un domaine géré, reportez-vous à la rubrique Gérer des domaines Active Directory.

Activer l'horodatage d'événements dans le DRA

Lorsque l'audit des services de domaine AD est activé, les événements DRA sont consignés comme ayant été générés par le compte de service DRA ou le compte d'accès au domaine, si un tel compte a été configuré. L'horodatage des événements va encore plus loin dans cette fonctionnalité en générant un événement AD DS supplémentaire identifiant l'administrateur assistant qui a 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 afficher les modifications apportées par les administrateurs assistants dans les rapports sur les événements de Change Guardian.

- Pour configurer l'audit d'AD DS, reportez-vous à la documentation de Microsoft *Guide pas à pas de l'audit d'AD DS*.
- Pour configurer l'intégration de Change Guardian, consultez la rubrique Configurer les serveurs d'historique des modifications unifié.
- Pour activer l'horodatage des événements, ouvrez la console de délégation et de configuration en tant qu'administrateur DRA, puis procédez comme suit :
  1. Accédez à **Gestion de la configuration**>**Update Administration Server Options** (Mettre à jour les options du serveur d'administration) > **Event Stamping** (Horodatage des événements).
  2. Sélectionnez un type d'objet et cliquez sur **Mettre à jour**.
  3. Sélectionnez un attribut à utiliser pour l'horodatage des événements pour 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 exige également que les attributs existent dans le schéma AD pour chacun de vos domaines gérés. Vous devez en être conscient si vous ajoutez des domaines gérés après avoir configuré l'horodatage des événements. Si vous devez ajouter un domaine géré qui ne contient pas d'attribut sélectionné, les opérations de ce domaine ne seront pas auditées avec les données d'horodatage des événements.

     DRA modifiera ces attributs afin que vous puissiez sélectionner les attributs qui ne sont pas utilisés par DRA ou par toute autre application dans votre environnement.

Pour obtenir de plus amples renseignements sur l'horodatage des événements, consultez Fonctionnement de l'horodatage des événements.

Configurer l'historique des modifications unifié

La fonction d'historique des modifications unifié (UCH) vous permet de générer des rapports pour les modifications apportées en dehors de DRA.

Délégation des pouvoirs de configuration du serveur d'historique des modifications unifiées

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

- supprimer la configuration du serveur d'historique des modifications unifié
- définir l'information de configuration de l'historique des modifications unifié
- afficher l'information de configuration de l'historique des modifications unifié

Pour déléguer les pouvoirs du serveur d'historique des modifications unifiées :

1. Cliquez sur **Powers** (Pouvoir) dans le nœud Gestion des délégations, puis utilisez la fonctionnalité de recherche d'objets pour rechercher et sélectionner les pouvoirs UCH souhaités.
2. Cliquez avec le bouton droit de la souris sur l'un des pouvoirs d'UCH sélectionnés et cliquez sur **Delegate Roles and Powers** (Déléguer des rôles et des pouvoirs).
3. Recherchez l'utilisateur, le groupe ou le groupe d'administrateurs assistants à qui vous souhaitez déléguer des pouvoirs.
4. Utilisez le **Object Selector** (Sélecteur d'objets) pour trouver et ajouter les objets souhaités, puis cliquez sur **Roles and Powers** (Rôles et pouvoirs) dans le **Wizard** (Assistant).
5. Cliquez sur **ActiveViews** et utilisez le **Object Selector** (Sélecteur d'objets) pour rechercher et ajouter les ActiveViews souhaités.
6. Cliquez sur **Next** (Suivant), puis sur **Finish** (Terminer) pour terminer le processus de délégation.

Configurer les serveurs d'historique des modifications unifié

Pour configurer les serveurs de l'historique des modifications unifiées :

1. Connectez-vous à la console de délégation et de configuration.
2. Développez **Configuration Management** > **Integration Servers** (Gestion de la configuration > Serveurs d'intégration.
3. Cliquez à l'aide du bouton droit de la souris sur **Unified Change History** (Historique des modifications unifiées) et sélectionnez **New Unified Change History Server** (Nouvel historique des modifications unifiées).
4. Spécifiez le nom du serveur UCH ou l'adresse IP, le numéro de port, le type de serveur et les détails du compte d'accès dans la configuration de l'historique des modifications unifié.

5 Testez la connexion au serveur et cliquez sur **Finish** (Terminer) pour enregistrer la configuration.

6 Ajoutez des serveurs supplémentaires si nécessaire.

Accès aux rapports sur l'historique des modifications unifié

Pour générer et visualiser les rapports d'historique des modifications unifié sur les objets Active Directory via Change Guardian, consultez la rubrique « Génération de rapports d'historique des modifications » du *Guide de l'utilisateur de Directory and Resource Administrator*.

Configurer des services DRA pour un compte de service géré de groupe

Si nécessaire, vous pouvez utiliser un compte de service géré de groupe (gMSA) pour les services DRA. Pour obtenir de plus amples renseignements sur l'utilisation d'un gMSA, consultez la référence Microsoft *Présentation des comptes de services gérés de groupe*. Cette section explique comment configurer DRA pour un compte de service de gestion de groupe après avoir préalablement ajouté le compte à Active Directory.

IMPORTANT : N'utilisez pas le gMSA comme un compte de service lors de l'installation de DRA.

Pour configurer le serveur d'administration primaire de DRA pour un gMSA :

1 Ajoutez le gMSA en tant que membre des groupes suivants :
   - Groupe d'administrateurs locaux sur le serveur de DRA
   - Groupe AD LDS dans le domaine géré par DRA

2 Remplacez le compte de connexion dans les propriétés du service pour chacun des services ci-dessous par gMSA :
   - Service d'administration NetIQ
   - Service d'audit NetIQ DRA
   - Service de cache de BD NetIQ DRA

     Service de cache NetIQ DRA
   - Service de base NetIQ DRA
   - Archivage des journaux NetIQ DRA
   - Service de réplication NetIQ DRA
   - Service Rest NetIQ DRA
   - Service Skype NetIQ DRA

3 Redémarrez tous les services.

Pour configurer le serveur d'administration secondaire de DRA pour un gMSA :

1 Installez le serveur secondaire.

2 Sur le serveur primaire, attribuez le rôle **Configure Servers and Domains** (Configurer les serveurs et les domaines) à l'ActiveView **Administration Servers and Managed Domains** (Serveurs d'administration et domaines gérés) pour le compte de service du serveur secondaire.

3. Sur le serveur primaire, ajoutez un nouveau serveur secondaire et spécifiez le compte de service du serveur secondaire.
4. Ajoutez le gMSA au groupe d'administrateurs local sur le serveur d'administration secondaire de DRA.
5. Sur le serveur secondaire, remplacez le compte d'ouverture de session de tous les services DRA par gMSA, puis redémarrez les services DRA.

Configurer le client de délégation et de configuration

Le client de délégation et de configuration fournit un accès aux tâches de configuration et de délégation, ce qui permet de répondre aux besoins de l'entreprise en matière de gestion, de l'administration distribuée à l'application des stratégies. La console de délégation et de configuration vous permet de configurer le modèle de sécurité et les configurations de serveur nécessaires pour gérer efficacement votre entreprise.

Pour configurer le client de délégation et de configuration :

1. Lancez le client de délégation et de configuration, puis accédez à **Gestion de la configuration** > **Options de mise à jour du serveur d'administration**.
2. Cliquez sur l'onglet **Options du client** et définissez vos paramètres préférés à partir des options de configuration affichées :
   - Autoriser les utilisateurs à effectuer une recherche par ActiveView
   - Masquer les objets source seulement des listes de console
   - Afficher les objets Active Directory avancés
   - Afficher la commande de sécurité
   - Afficher les ressources et les boîtes aux lettres partagées lors de la recherche d'utilisateurs
   - Suffixe UPN d'utilisateur par défaut vers le domaine actuel
   - Nombre maximal d'éléments pouvant être édités à la fois (sélection multiple)
   - Options de recherche
   - Option de retour chariot
   - Unités des limites de capacité de stockage de la boîte aux lettres Exchange

Configurer le client Web

Vous pouvez configurer l'authentification de la console Web afin d'utiliser des cartes à puce ou l'authentification multifacteur. Vous pouvez également personnaliser la marque avec votre propre logo et le titre de l'application.

- « Démarrer la console Web » page 118
- « Déconnexion automatique » page 118
- « Connexion au serveur DRA » page 118
- « Authentification » page 119

Démarrer la console Web

Vous pouvez démarrer la console Web à partir de n'importe quel ordinateur, appareil iOS ou appareil Android exécutant un navigateur Web. Pour démarrer la console Web, spécifiez l'URL correspondante dans le champ d'adresse de votre 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 les plus récentes sur le compte et sur Microsoft Exchange dans la Console Web, configurez votre navigateur Web pour qu'il vérifie les versions les plus récentes des pages mises en cache à chaque visite.

Déconnexion automatique

Vous pouvez définir un incrément de temps pour que la console Web se déconnecte automatiquement après un temps d'inactivité. Vous pouvez également la configurer pour qu'elle ne se déconnecte jamais automatiquement.

Pour configurer la déconnexion automatique dans la console Web, accédez à **Administration** > **Configuration** >**Se déconnecter automatiquement**.

Connexion au serveur DRA

Vous pouvez utiliser l'une des quatre options suivantes pour vous connecter à la console Web. Le comportement de chaque option, lors de la connexion, est décrit dans le tableau suivant :

Écran d'ouverture de session - Options	Descriptions des options de connexion
Utiliser Découverte automatique	Trouve automatiquement un serveur DRA; aucune option de configuration n'est disponible
Connecter au serveur DRA par défaut	Les détails du serveur et du port préconfigurés sont utilisés. **REMARQUE :** Cette option s'affiche uniquement lorsque vous avez configuré le serveur DRA par défaut dans la console Web. De même, si vous spécifiez que le client doit toujours se connecter au serveur DRA par défaut, vous ne pouvez voir que l'option **Connecter au serveur DRA par défaut** sur l'écran de connexion.
Établir une connexion avec un serveur DRA précis	L'utilisateur configure le serveur et le port
Établir une connexion avec un serveur DRA qui gère un domaine précis	L'utilisateur fournit un domaine géré et choisit une option de connexion : ◆ Utiliser Découverte automatique (dans le domaine fourni) ◆ Serveur primaire pour ce domaine ◆ Rechercher un serveur DRA (dans le domaine fourni)

Pour configurer la connexion au serveur DRA dans la console Web, accédez à **Administration** > **Configuration** >**Connexion au serveur DRA**.

Authentification

Cette section contient de l'information sur la configuration de l'authentification par carte à puce, de l'authentification Windows et de l'authentification multifacteur à l'aide de l'intégration de l'authentification avancée.

Authentification par carte à puce

Pour configurer la console Web afin qu'elle accepte un utilisateur en fonction des informations d'identification de client de sa carte à puce, vous devez configurer les services Internet (IIS) et le fichier de configuration des services REST.

IMPORTANT : Assurez-vous que les certificats de la carte à puce sont également installés dans le magasin de certificats racines du serveur Web, car IIS doit pouvoir rechercher des certificats correspondant à ceux de la carte.

---

1. Installez les composants d'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, puis cliquez sur **Ajouter des services de rôle**.
   - **1d** Accédez au nœud Services de rôle de sécurité et sélectionnez **Authentification Windows** et **Authentification de mappage de certificat client**.
2. Activer l'authentification sur le serveur Web.
   - **2a** Démarrez **Gestionnaire IIS**.
   - **2b** Sélectionnez votre serveur Web.
   - **2c** Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.
   - **2d** Activez « Authentification par 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 « Authentification Windows » et désactiver « 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**, puis **Exiger** sous Certificats clients.

     SUGGESTION : Si cette option est disponible, sélectionnez **Exiger SSL 128 bits**.

     ---

5 Configurez l'application Web des services REST.

5a Sélectionnez votre application Web des services REST.

5b Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.

5c Activez « Authentification Windows » et désactiver « Authentification anonyme ».

6 Activez les certificats SSL et client sur l'application Web des services REST.

6a Recherchez l'icône **Services SSL** sous la section IIS et double-cliquez dessus.

6b Sélectionnez **Exiger SSL**, puis **Exiger** sous Certificats clients.

SUGGESTION : Si cette option est disponible, sélectionnez **Exiger SSL 128 bits**.

---

7 Configurez le fichier de service Web WCF.

7a Sélectionnez votre application Web des services REST et passez en affichage du contenu.

7b Localisez le fichier `.svc` et cliquez dessus avec le bouton droit de la souris.

7c Sélectionnez **Basculer vers l'affichage des fonctionnalités**.

7d Recherchez l'icône **Authentification** sous la section IIS et double-cliquez dessus.

7e Activez « Authentification anonyme » et désactivez toutes les autres méthodes d'authentification.

8 Éditez 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 Supprimez les commentaires des lignes indiquées ci-dessous :

- 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>
```

- Sous la ligne `<serviceDebug includeExceptionDetailInFaults="false"/ >` :

```
<serviceAuthorization impersonateCallerForAllOperations="true" /
> <serviceCredentials> <clientCertificate> <authentication
mapClientCertificateToWindowsAccount="true" /> </
clientCertificate> </serviceCredentials>
```

- 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 les services Internet (IIS) et le fichier de configuration des services REST.

1. Ouvrez le gestionnaire IIS.
2. Dans le volet Connexions, recherchez l'application Web Services REST et sélectionnez-la.
3. Dans le volet de droite, accédez à la section IIS et double-cliquez sur **Authentification**.
4. Activez **Authentification Windows** et désactivez toutes les autres méthodes d'authentification.
5. Une fois que vous avez activé l'authentification Windows, l'option **Providers** (Providers) est ajoutée au menu contextuel et au panneau Actions sur le côté droit de la fenêtre du gestionnaire. Ouvrez la boîte de dialogue Fournisseurs et déplacez **NTLM** en haut de la liste.
6. Utilisez un éditeur de texte pour ouvrir le fichier `C:\inetpub\wwwroot\DRAClient\rest\web.config` et localisez la ligne `<authentication mode="None" />`.
7. Remplacez « `Aucun` » par « `Windows` » et enregistrez le fichier.
8. Redémarrez le serveur IIS.

Authentification multifacteur avec Advanced Authentication

AAF (Advanced Authentication Framework) est notre logiciel de premier plan qui vous permet d'aller au-delà de l'utilisation d'un simple nom d'utilisateur et d'un mot de passe et qui vous offre un moyen plus sécurisé de protéger vos informations sensibles grâce à l'authentification multifacteur.

Advanced Authentication prend en charge les protocoles de communication suivants pour la sécurité :

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

L'authentification multifacteur est une méthode de contrôle d'accès d'ordinateur qui utilise plusieurs méthodes d'authentification à partir de catégories distinctes d'informations d'identification afin de vérifier l'identité d'un utilisateur.

Il existe trois types de catégories d'authentification, ou facteurs :

- *La connaissance*. Cette catégorie exige que vous connaissiez un élément d'information précis, comme un mot de passe ou un code d'activation.
- *La possession*. Cette catégorie exige que vous disposiez d'un dispositif d'authentification tel qu'une carte à puce ou un téléphone intelligent.
- *Le corps*. Cette catégorie exige que vous utilisiez une partie de votre anatomie, par exemple votre empreinte digitale, comme méthode de vérification.

Chaque facteur d'authentification contient au moins une méthode d'authentification. Une méthode d'authentification est une technique particulière que vous pouvez utiliser pour établir l'identité d'un utilisateur, par exemple en utilisant une empreinte digitale ou en demandant un mot de passe.

Vous pouvez considérer un processus d'authentification fort s'il utilise plus d'un type de méthode d'authentification, par exemple s'il requiert un mot de passe et une empreinte digitale.

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

- mot de passe LDAP
- Remote Authentication Dial-In User Service (RADIUS) (service d'authentification distante des utilisateurs d'accès à distance)
- téléphone intelligent

SUGGESTION : La méthode du téléphone intelligent exige que l'utilisateur télécharge une application iOS ou Android. Pour obtenir de plus amples renseignements, consultez le *Guide de l'utilisateur de l'authentification avancée - Applications pour téléphones intelligents*, disponibles sur le site Web de la documentation de NetIQ.

Utilisez l'information fournie dans les sections suivantes pour configurer la console Web afin qu'elle utilise une authentification à plusieurs facteurs.

IMPORTANT : Certaines des étapes décrites dans les sections suivantes ont lieu dans la console Web, mais la majorité du processus de configuration de l'authentification multifacteur nécessite l'accès à AAF. Ces procédures supposent que vous avez déjà installé AAF et que vous avez accès à la documentation d'aide d'AAF.

Ajouter des référentiels à Advanced Authentication Framework

La première étape de la configuration de la console Web en vue de l'utilisation de l'authentification multifacteur est d'ajouter tous les domaines Active Directory contenant les administrateurs DRA et les administrateurs assistants gérés par DRA à AAF. Ces domaines s'appellent des référentiels et contiennent les attributs d'identité des utilisateurs et des groupes que vous souhaitez 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 et cliquez sur **Référentiels**.
3. Cliquez sur **Ajouter**.
4. Remplissez le formulaire.

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

   SUGGESTION : Saisissez 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 référentiels AD gérés par DRA.
9. Pour chaque référentiel répertorié dans la page Référentiels, cliquez sur **Synchroniser maintenant** pour le synchroniser avec le serveur AAF.

Créer des chaînes d'authentification

Une chaîne d'authentification contient au moins une méthode d'authentification. Les méthodes de la chaîne sont invoquées dans l'ordre dans lequel elles ont été ajoutées à la chaîne. Pour qu'un utilisateur soit authentifié, il doit valider toutes les méthodes de la chaîne. Par exemple, vous pouvez créer une chaîne contenant la méthode Mot de passe LDAP et la méthode SMS. Lorsqu'un utilisateur essaie de s'authentifier à l'aide de cette chaîne, il doit d'abord s'authentifier à l'aide de son mot de passe LDAP, après quoi un message texte sera envoyé à son téléphone portable avec un mot de passe à usage unique. Après avoir saisi le mot de passe, toutes les méthodes de la chaîne seront validées et l'authentification réussira. Une chaîne d'authentification peut être attribuée à un utilisateur ou à un groupe précis.

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 et cliquez sur **Chaînes**. Le panneau de droite affiche une liste des chaînes actuellement disponibles.
3. Cliquez sur **Ajouter**.
4. Remplissez le formulaire. Tous les champs sont obligatoires.

   IMPORTANT : Ajoutez les méthodes dans l'ordre dans lequel elles doivent être appelées. Si vous voulez que l'utilisateur entre d'abord 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 terminal** est sur DÉSACTIVÉ.
5. Le paramètre **Est activé** est mis à ACTIVÉ.
6. Saisissez les noms des rôles ou des groupes à soumettre à la demande d'authentification dans le champ **Rôles et groupes**.

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

   Tout utilisateur ou groupe sélectionné sera ajouté sous le champ **Rôles et groupes**.
7. Cliquez sur **Enregistrer**.

Créer des événements d'authentification

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

Un nœud d'extrémité est un périphérique réel, tel qu'un ordinateur ou un téléphone intelligent, qui exécute le logiciel qui déclenche l'événement d'authentification. DRA enregistre le point d'extrémité auprès d'AAF après la création de l'événement.

Vous pouvez utiliser la liste blanche des points d'extrémité pour restreindre l'accès à un événement à des points d'extrémité précis, ou vous pouvez autoriser tous les points 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 et cliquez sur **Événements**. Le panneau de droite affiche une liste d'événements actuellement disponibles.
3. Cliquez sur **Ajouter**.
4. Remplissez le formulaire. Tous les champs sont obligatoires.

   IMPORTANT : Assurez-vous que le paramètre **Est activé** est mis à ACTIVÉ.

5. Si vous souhaitez limiter l'accès à des points d'extrémité précis, accédez à la section Liste blanche des points d'extrémité et déplacez les points d'extrémité ciblés de la liste *Disponibles* vers la liste *Utilisés*.

   SUGGESTION : S'il n'y a pas de points d'extrémité dans la liste *Utilisés*, l'événement sera disponible pour tous les points d'extrémité.

Activer la console Web

Après avoir configuré les chaînes et les événements, vous pouvez vous connecter à la console Web en tant qu'administrateur et activer Advanced Authentication.

Une fois l'authentification activée, chaque utilisateur devra s'authentifier en utilisant AAF, pour pouvoir accéder à la console Web.

IMPORTANT : Avant d'activer la console Web, vous devez déjà être inscrit aux méthodes d'authentification que celle-ci utilisera pour authentifier les utilisateurs. Consultez le *Guide de l'utilisateur d'Advanced Authentication Framework* pour savoir comment s'inscrire à des méthodes d'authentification.

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

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

Étapes finales

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

12 Connecter des systèmes gérés

Cette section fournit de l'information sur la connexion et la configuration de systèmes gérés relatifs aux domaines et aux composants Microsoft Exchange, notamment les dossiers publics, Exchange, Office 365 et Skype Entreprise Online.

Gérer des domaines Active Directory

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

REMARQUE : Une fois l'ajout des domaines gérés terminé, assurez-vous que les planifications d'actualisation du cache des comptes pour ces domaines sont correctes.

Ajouter des domaines et des ordinateurs gérés

Pour ajouter un domaine ou un ordinateur géré :

1 Accédez à **Configuration Management** >**New Managed Domain** (Gestion de la configuration > Nouveau domaine géré).

2 Spécifiez le composant que vous ajoutez en sélectionnant le bouton radio applicable et en fournissant le nom de domaine ou d'ordinateur :

- **Manage a domain** (Gérer un domaine)
  - Si vous souhaitez gérer la sous-arborescence d'un domaine, consultez la rubrique Ajouter une sous-arborescence gérée.
  - Si vous ajoutez un nouveau domaine avec LDAP sécurisé activé sur vos contrôleurs de domaine et que vous souhaitez que DRA utilise SSL pour communiquer avec vos contrôleurs de domaine, sélectionnez **This domain is configured for LDAP over SSL** (Ce domaine est configuré pour LDAP sur SSL). Pour obtenir de plus amples renseignements, consultez Configurer DRA pour l'exécution de Secure Active Directory.
- **Manage a computer** (Gérer un ordinateur)

Cliquez sur **Next** (Suivant) après avoir terminé la configuration.

3 Dans l'onglet **Domain access** (Accès au domaine), spécifiez les informations d'identification du compte que vous souhaitez que DRA utilise pour accéder à ce domaine ou à cet ordinateur. Par défaut, DRA utilise le compte de service du serveur d'administration.

4 Examinez le résumé, puis cliquez sur **Terminer**.

5 Pour commencer à gérer les objets de ce domaine ou de cet ordinateur, actualisez la configuration du domaine.

Spécifier les comptes d'accès de domaine

Pour chaque domaine ou sous-arborescence gérée, vous pouvez spécifier un compte à utiliser à la place du compte de service du serveur d'administration pour accéder à ce domaine. Ce compte de remplacement est appelé 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.

Pour spécifier un compte d'accès pour un serveur membre, vous devez avoir l'autorisation de gérer le domaine dans lequel le membre de domaine se trouve. Vous ne pouvez gérer les membres du domaine que s'ils se trouvent dans un domaine géré auquel vous pouvez accéder par le serveur d'administration.

Pour spécifier un compte d'accès :

1 Accédez au nœud **Gestion de la configuration** > **Domaines gérés**.

2 Cliquez avec le bouton droit de la souris sur le domaine ou la sous-arborescence pour lequel vous souhaitez spécifier un compte d'accès, puis cliquez sur **Propriétés**.

3 Dans l'onglet Compte d'accès au domaine, cliquez sur **Utilisez le compte suivant pour accéder à ce domaine**.

4 Spécifiez et confirmez les informations d'identification pour ce compte, puis cliquez sur **OK**.

Pour obtenir de plus amples renseignements sur la configuration de ce compte disposant des droits d'accès minimaux, consultez Comptes d'accès DRA de droit d'accès minimal.

Spécifier les comptes d'accès Exchange

Pour chaque domaine dans DRA, vous pouvez gérer des objets Exchange à l'aide du compte d'accès au 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. Assurez-vous donc que le même compte d'utilisateur est limité à cinq shells pour les serveurs secondaires DRA.

Pour spécifier un compte d'accès Exchange :

1. Accédez au nœud **Gestion de la configuration** > **Domaines gérés**.
2. Cliquez avec le bouton droit de la souris sur le domaine ou la sous-arborescence pour lequel vous souhaitez spécifier un compte d'accès, puis cliquez sur **Propriétés**.
3. Dans l'onglet Compte d'accès au domaine Exchange, cliquez sur **Utilisez le compte suivant pour accéder à tous les serveurs Exchange**.
4. Spécifiez et confirmez les informations d'identification pour ce compte, puis cliquez sur **OK**.

Pour obtenir de plus amples renseignements sur la configuration de ce compte disposant des droits d'accès minimaux, consultez Comptes d'accès DRA de droit d'accès minimal.

Ajouter une sous-arborescence gérée

Vous pouvez ajouter des sous-arborescences gérées et manquantes à partir de domaines Microsoft Windows précis après avoir installé le 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 obtenir de plus amples renseignements sur les versions prises en charge de Microsoft Windows, consultez Configuration requise pour le serveur d'administration et la console Web de 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 étendu.

Par exemple, vous pouvez spécifier la sous-arborescence Houston dans le domaine SOUTHWEST, permettant à DRA de gérer de manière sécurisée 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 avoir besoin d'autorisations administratives pour l'ensemble du domaine.

REMARQUE

- Pour vous assurer que le compte spécifié dispose des autorisations nécessaires pour gérer cette sous-arborescence et effectuer des actualisations incrémentielles du cache des comptes, utilisez l'utilitaire Objets supprimés pour vérifier et déléguer les autorisations appropriées.
- Une fois l'ajout des sous-arborescences gérées terminé, assurez-vous que les planifications d'actualisation du cache des comptes pour les domaines correspondants sont correctes.

Pour ajouter une sous-arborescence gérée :

1. Accédez à **Gestion de la configuration** > **Nouveau domaine géré**.
2. Dans l'onglet Domaine ou serveur, cliquez sur **Gérer un domaine**, puis spécifiez le domaine de la sous-arborescence que vous souhaitez gérer.
3. Spécifiez le domaine de la sous-arborescence que vous souhaitez gérer.
4. Sélectionnez **Gérer une sous-arborescence de ce domaine**, puis cliquez sur **Suivant**.
5. Dans l'onglet Sous-arborescences, cliquez sur **Ajouter** pour spécifier la sous-arborescence que vous souhaitez gérer. Vous pouvez spécifier plusieurs sous-arborescences.
6. Dans l'onglet Compte d'accès, spécifiez les informations d'identification du compte que vous souhaitez que DRA utilise pour accéder à cette sous-arborescence. Par défaut, DRA utilise le compte de service du serveur d'administration.
7. Examinez le résumé, puis cliquez sur **Terminer**.
8. Pour commencer à gérer les objets de cette sous-arborescence, actualisez la configuration du domaine.

Ajouter un domaine approuvé

Les domaines approuvés permettent l'authentification des utilisateurs sur les systèmes gérés dans votre environnement géré. Une fois que vous avez ajouté un domaine approuvé, vous pouvez spécifier des comptes d’accès au domaine et Exchange, planifier l’actualisation du cache et entreprendre d’autres actions dans les propriétés du domaine, comme dans un domaine géré.

Pour ajouter un domaine approuvé :

1. Dans le nœud **Gestion de la configuration** > **Domaines gérés**, sélectionnez le domaine géré auquel est associé un domaine approuvé.
2. Cliquez sur **Domaines approuvés** dans le volet Détails. Le volet Détails doit être activé dans le menu Affichage.
3. Cliquez avec le bouton droit de la souris sur le domaine approuvé, puis sélectionnez **Propriétés**.
4. Décochez **Ignorez ce domaine approuvé** et appliquez vos modifications.

REMARQUE : L'ajout d'un domaine approuvé déclenchera une actualisation complète du cache des comptes, mais vous en serez averti par une invite de confirmation lorsque vous cliquez sur **Appliquer**.

Configurer DRA pour l'exécution de Secure Active Directory

Secure Active Directory est défini par un environnement DRA qui est configuré pour fonctionner en utilisant le protocole LDAPS (LDAP sur SSL) pour chiffrer les communications entre DRA et Active Directory afin de fournir un environnement plus sûr.

Lors de la mise à niveau vers une version 10.x de DRA à partir d'une version 9.x, LDAPS doit être activé après la mise à niveau pour utiliser Secure Active Directory. La fonction de découverte automatique pour la détection et la connexion aux serveurs DRA et REST doit également être configurée pour cette fonction.

Activer le protocole LDAP sur SSL (LDAPS)

Si vous passez d'une version 9.x à la version 10.x de DRA, suivez les étapes ci-dessous. Si vous configurez DRA pour une nouvelle installation, consultez la rubrique Ajouter des domaines et des ordinateurs gérés.

1. Accédez à **Configuration Management** > **Managed Domains** (Gestion de la configuration > Domaines gérés) dans la console de délégation et de configuration de DRA.
2. Cliquez à l'aide du bouton droit de la souris sur le domaine et ouvrez Propriétés.
3. Activez **This domain is configured for LDAP over SSL** (Ce domaine est configuré pour LDAP sur SSL) dans l'onglet Général, et cliquez sur **OK**.
4. Redémarrez le service d'administration de NetIQ.

REMARQUE : Si vous configurez également la découverte automatique pour utiliser Secure Active Directory, vous pouvez attendre pour redémarrer les services après avoir terminé cette configuration. Pour obtenir de plus amples renseignements, consultez Configurer la découverte automatique pour LDAPS.

Configurer la découverte automatique pour LDAPS

La découverte automatique est le mécanisme utilisé par le client pour se connecter automatiquement à l'environnement DRA disponible.

Pour configurer DRA pour un environnement exécutant Secure Active Directory, configurez la clé de registre `ClientSSLAllDomains` :

1. Lancez l'utilitaire Éditeur du registre.
2. Cliquez à l'aide du bouton droit de la souris sur le nœud `HKEY_LOCAL_MACHINE SOFTWARE\Wow6432Node\Mission Critical Software\RestExtentions`.
3. Sélectionnez **New** > **DWORD (32-bit) Value** (Nouveau > Valeur DWORD (32 bits)).
4. Nommez la nouvelle clé `ClientSSLAllDomains`.
5. Donnez à la clé de registre la valeur 1.
6. Après avoir ajouté la clé de registre `ClientSSLAllDomains`, redémarrez les services suivants :
   - Service de publication sur le World Wide Web
   - Service Rest NetIQ DRA

Connecter des dossiers publics

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

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

- Pour obtenir de plus amples renseignements sur l'activation de Microsoft Exchange, consultez Activer Microsoft Exchange.
- Pour obtenir de plus amples renseignements sur les autorisations de compte, consultez Comptes d'accès DRA de droit d'accès minimal.

Pour configurer la prise en charge des dossiers publics Exchange :

1. Cliquez avec le bouton droit sur **Forêts de dossiers publics gérés** dans le nœud Configuration et gestion, puis cliquez sur **Nouvelle forêt de dossiers publics**.
2. Cliquez sur **Domaine de la forêt**, indiquez la forêt Active Directory où se trouvent les objets de dossiers publics, puis cliquez sur **Suivant**.
3. Dans **Domain access** (Accès au domaine), spécifiez le compte d'accès.

   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) sera disponible.

   ---
4. Dans **Exchange access** (Accès Exchange), indiquez le compte que vous souhaitez que DRA utilise pour un accès sécurisé aux serveurs Exchange.

   IMPORTANT : Si vous utilisez le serveur secondaire, l'option **Utiliser le compte d'accès Exchange du serveur d'administration primaire** sera disponible.

   ---
5. Dans **Serveur Exchange**, sélectionnez le serveur Exchange que vous souhaitez que DRA utilise pour gérer les dossiers publics.
6. Dans **Résumé**, vérifiez les détails du compte et ceux du serveur Exchange, puis cliquez sur **Terminer** pour terminer le processus.

   Le serveur DRA exécute l'actualisation complète du cache des comptes sur le dossier public. La nouvelle forêt de dossiers publics apparaîtra dans la console à la fin de l'actualisation du cache, ce qui peut prendre quelques minutes.

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

- « Afficher et modifier les propriétés d'un domaine de dossier public » page 133
- « Délégation des pouvoirs de dossiers publics » page 133

Afficher et modifier les propriétés d'un domaine de dossier public

Pour afficher ou modifier les propriétés du domaine de dossiers publics :

1. Cliquez sur **Forêts de dossiers publics gérés** dans le nœud de gestion de la configuration pour afficher les dossiers publics.
2. Cliquez avec le bouton droit de la souris sur le compte de dossier public à afficher, puis sélectionnez **Propriétés**.
3. Dans les propriétés de **Forêt de dossiers publics**, vous pouvez effectuer les opérations suivantes :
   - **Général :** affichez les détails du compte de dossier public et mettez à jour le champ **Exchange Server** utilisé par le serveur DRA pour effectuer une activité Exchange sur le serveur de dossiers publics.
   - **Statistiques :** affichez le nombre de dossiers publics et le nombre de dossiers publics à extension messagerie.
   - **État incrémentiel :** affichez ou mettez à jour l'état du cache des comptes incrémentiels.
   - **Planification incrémentielle :** affichez la planification d'actualisation incrémentielle du cache et replanifiez une actualisation du cache.
   - **État complet :** affichez l'état de l'actualisation complète du cache du compte.
   - **Actualisation complète :** effectuez immédiatement une actualisation complète du cache des comptes.

     NetIQ vous recommande d’effectuer une **actualisation complète** uniquement si les données du cache de dossiers publics sont corrompues.
   - **Accès au domaine :** affichez les détails du compte de service DRA ou remplacez les comptes d'accès.
   - **Accès Exchange :** affichez ou mettez à jour l'accès sécurisé aux serveurs Exchange.

Délégation des pouvoirs de dossiers publics

Utilisez les ActiveViews pour définir les pouvoirs et gérer la délégation de dossiers publics. Vous pouvez spécifier des règles pour ajouter des objets gérés, choisir des domaines et attribuer des pouvoirs, puis déléguer ces pouvoirs de dossiers publics à des administrateurs assistants.

Pour créer une ActiveView et déléguer des pouvoirs de dossier public :

1. Dans le nœud **Gestion des délégations**, cliquez sur **ActiveView**.
2. Cliquez sur **Suivant** dans l'assistant **Créer une ActiveView** , sélectionnez la règle requise dans la liste déroulante **Ajouter** et choisissez Dossiers publics comme type d'objet. Par exemple, pour créer une règle de correspondance d'objet : sélectionnez **Objets correspondant à une règle**, puis choisissez **Dossiers publics** comme type d'objet.
3. Spécifiez la règle d'ActiveView que vous souhaitez ajouter au dossier public, puis cliquez sur **Next** (Suivant).
4. Spécifiez le nom de l'ActiveView, puis cliquez sur **Finish** (Terminer).
5. Cliquez avec le bouton droit de la souris sur **ActiveViews** et accédez à **Delegate Administration** > **Assistant Admins**, puis spécifiez le type d'administrateur dans la liste déroulante **Add** de **Wizard** (Assistant).

6. Recherchez l'utilisateur, le groupe ou le groupe d'administrateurs assistants à qui vous souhaitez déléguer des pouvoirs.
7. Utilisez le **Object Selector** (Sélecteur d'objets) pour trouver et ajouter les objets souhaités, puis cliquez sur **Roles and Powers** (Rôles et pouvoirs) dans le **Wizard** (Assistant).
8. Sélectionnez **Rôles** dans la liste déroulante **Ajouter**, puis recherchez et ajoutez le rôle Administration des dossiers publics.
9. Sélectionnez Pouvoirs dans la liste déroulante **Ajouter**, puis recherchez et ajoutez tout pouvoir supplémentaire que vous souhaitez attribuer à vos administrateurs assistants ne faisant pas partie du rôle Administration des dossiers publics.
10. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer le processus de délégation.

Une fois la délégation des pouvoirs sur les dossiers publics terminée, les utilisateurs autorisés pourront effectuer des opérations de création, de lecture, de mise à jour et de suppression sur les propriétés des dossiers publics dans des domaines configurés à l'aide de la console Web.

Activer Microsoft Exchange

L'activation de Microsoft Exchange vous permet d'exploiter les fonctionnalités d'Exchange et d'Exchange Online, notamment les stratégies Microsoft Exchange, la boîte aux lettres intégrée et la gestion des objets à extension messagerie. Vous pouvez activer ou désactiver la prise en charge de Microsoft Exchange sur chaque serveur d'administration pour Microsoft Exchange Server 2013 et les versions ultérieures.

Pour activer Exchange, vous devez disposer des privilèges requis, 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 de plus amples renseignements sur les exigences de Microsoft Exchange, consultez la rubrique Plateformes prises en charge.

Pour permettre la prise en charge de Microsoft Exchange et d'Exchange Online :

1. Accédez à **Policy and Automation Management** > **Configure Exchange Policies** (Gestion des stratégies et de l'automatisation > Configurer les stratégies Exchange) dans la console de délégation et de configuration.
2. Sélectionnez **Enable Exchange Policy** (Activer la stratégie Exchange) et cliquez sur **Apply** (Appliquer).

Configurer les locataires Azure

Avec un compte Azure actif et un ou plusieurs locataires Azure, vous pouvez configurer DRA pour qu'il fonctionne avec Azure Active Directory afin de gérer les objets des utilisateurs et des groupes. Ces objets comprennent les utilisateurs et les groupes créés dans Azure et les utilisateurs et les groupes synchronisés avec le locataire Azure à partir des domaines gérés par DRA.

Les modules Azure PowerShell, Azure Active Directory et Azure Resource Manager Profile sont nécessaires pour gérer les tâches Azure. Vous avez également besoin d'un compte dans Azure Active Directory. Pour de plus amples renseignements sur les autorisations du compte d'accès du locataire Azure, consultez la rubrique Comptes d'accès DRA de droit d'accès minimal.

IMPORTANT : Les opérations sur les objets Azure telles que la création, la modification, la suppression, la désactivation et l'activation ne sont pas prises en charge dans la console de délégation et de configuration.

Délégation des rôles et des pouvoirs

Vous pouvez utiliser l'administrateur DRA ou un administrateur assistant avec le rôle délégué « Configurer les serveurs et les domaines » pour gérer les locataires Azure; les rôles intégrés Azure sont requis pour gérer les objets Azure.

Rôles intégrés Azure

Pour déléguer des objets Azure, attribuez les rôles Azure suivants :

- **Administration des groupes Azure :** Fournit tous les pouvoirs nécessaires pour gérer les groupes Azure et l'adhésion à un groupe Azure.
- **Administration des utilisateurs Azure :** Fournit tous les pouvoirs nécessaires pour gérer les utilisateurs Azure.
- **Administration des contacts Azure :** Fournit tous les pouvoirs nécessaires pour gérer les contacts Azure.

Pouvoirs Azure

Utilisez les pouvoirs suivants pour déléguer la création et la gestion des utilisateurs, des contacts et des groupes Azure.

Pouvoirs du compte d'utilisateur Azure :

- Créer un utilisateur Azure et modifier toutes ses propriétés
- Supprimer définitivement un compte d'utilisateur Azure
- Gérer la connexion des utilisateurs Azure
- Gérer la connexion pour les utilisateurs Azure synchronisés avec le locataire Azure
- Modifier toutes les propriétés des utilisateurs Azure
- Réinitialiser un mot de passe de compte d'utilisateur Azure
- Afficher toutes les propriétés des utilisateurs Azure

Pouvoirs de groupe Azure :

- Ajouter un objet au groupe Azure
- Créer un groupe Azure et modifier toutes ses propriétés
- Supprimer le compte du groupe Azure
- Modifier toutes les propriétés du groupe Azure

- Retirer un objet du groupe Azure
- Afficher toutes les propriétés du groupe Azure

Pouvoirs des contacts d'Azure :

- Créer un contact Azure et modifier toutes ses propriétés
- Supprimer le compte du contact Azure
- Modifier toutes les propriétés du contact Azure
- Afficher toutes les propriétés du contact Azure

Pour gérer les propriétés de niveau granulaire pour les utilisateurs, les contacts ou les groupes Azure, vous pouvez créer des pouvoirs personnalisés en sélectionnant les attributs d'objet spécifiés.

Objets Azure pris en charge

Les types de groupes Azure suivants sont pris en charge :

- Liste de distribution
- Sécurité à extension messagerie
- Office 365
- Sécurité

REMARQUE : Les utilisateurs invités créés dans Azure ne sont pas pris en charge.

Création d'une application Azure et ajout d'un locataire Azure

Pour gérer un nouveau locataire Azure, ajoutez le nouveau locataire en remplissant une application Azure dans la console de délégation et de configuration. DRA prend en charge la création de l'application Azure à la fois en ligne et hors ligne et nécessite une application Azure avec les autorisations suivantes pour gérer les objets dans le locataire :

- Lire et écrire le profil complet de tous les utilisateurs
- Lire et écrire tous les groupes
- Lire les données du répertoire

Ces autorisations seront accordées automatiquement à l'application Azure, tant en ligne que hors ligne.

Pour créer une application Azure en ligne et pour ajouter un locataire :

1. Accédez à **Configuration Management** > **Azure Tenants** (Gestion de la configuration > Locataires Azure) dans la console de délégation et de configuration.
2. Cliquez à l'aide du bouton droit de la souris sur **Azure Tenants** (Locataires Azure) et sélectionnez New Azure Tenant (Nouveau locataire Azure).
3. (Facultatif) Indiquez l'attribut d'ancrage source utilisé pour faire correspondre vos objets Active Directory à Azure pendant la synchronisation.
4. Indiquez le compte utilisé pour accéder au locataire Azure, puis validez les informations d'identification.

Pour de plus amples renseignements sur les autorisations du compte d'accès du locataire Azure, consultez la rubrique Comptes d'accès DRA de droit d'accès minimal.

5 Sélectionnez l'option **Allow DRA to create the Azure application** (Autoriser DRA à créer l'application Azure).

6 Fournissez les informations d'identification pour un compte d'utilisateur avec le rôle d'administrateur d'entreprise Azure AD, puis validez ces informations d'identification.

7 Cliquez sur **Finish** (Terminer).

L'ajout du locataire Azure peut prendre plusieurs minutes. Une fois que le locataire est ajouté avec succès, DRA effectue une actualisation complète du cache des comptes pour le locataire et ce dernier est affiché dans le volet d'affichage Locataires Azure.

REMARQUE : Une fois l'actualisation terminée, si vous souhaitez vérifier l'état des comptes de tous les locataires Azure gérés, installez le module PowerShell `msonline`, puis exécutez la vérification **Tenant Accounts Overview** (Aperçu des comptes locataires) dans l'utilitaire de contrôle de l'intégrité. Pour installer le module, exécutez la commande `install-module msonline` dans PowerShell.

Pour créer une application Azure hors ligne pour DRA et ajouter un locataire :

1 Accédez à **Configuration Management** > **Azure Tenants** (Gestion de la configuration > Locataires Azure) dans la console de délégation et de configuration.

2 Cliquez à l'aide du bouton droit de la souris sur **Azure Tenants** (Locataires Azure) et sélectionnez **New Azure Tenant** (Nouveau locataire Azure).

3 (Facultatif) Indiquez l'attribut d'ancrage source utilisé pour faire correspondre vos objets Active Directory à Azure pendant la synchronisation.

4 Indiquez le compte utilisé pour accéder au locataire Azure, puis validez les informations d'identification.

5 Sélectionnez l'option **Create the Azure application offline** (Créer l'application Azure hors ligne).

6 Lancez une session PowerShell dans le serveur d'administration DRA et accédez à `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`

7 Executez `. .\NewDraAzureApplication.ps1` pour charger PowerShell.

8 Exécutez le cmdlet `New-DRAAzureApplication` pour demander les paramètres.

9 Précisez les paramètres suivants pour `New-DraAzureApplication` :

- `<nom>` - Nom de l'application de l'assistant de locataire.

IMPORTANT : Micro Focus vous recommande d'utiliser le nom spécifié dans la console DRA.

- (Facultatif) `<environnement>` - Indiquez AzureCloud, AzureChinaCloud, AzureGermanyCloud ou AzureUSGovernment, en fonction du locataire que vous utilisez.

10 Dans la boîte de dialogue Informations d'identification, spécifiez les informations d'identification de l'administrateur de l'entreprise.

L'ID et le mot de passe de l'application Azure sont alors générés.

11 Copiez l'ID et le mot de passe de l'application dans la console DRA (Assistant locataire **DRA Azure Application Credentials** - Informations d'identification de l'application Azure DRA), puis validez les informations d'identification.

12 Cliquez sur **Finish** (Terminer).

L'ajout du locataire Azure peut prendre plusieurs minutes. Une fois que le locataire est ajouté avec succès, DRA effectue une actualisation complète du cache des comptes pour le locataire et ce dernier est affiché dans le volet d'affichage Locataires Azure.

REMARQUE : Une fois l'actualisation terminée, si vous souhaitez vérifier l'état des comptes de tous les locataires Azure gérés, installez le module PowerShell `msonline`, puis exécutez la vérification **Tenant Accounts Overview** (Aperçu des comptes locataires) dans l'utilitaire de contrôle de l'intégrité. Pour installer le module, exécutez la commande `install-module msonline` dans PowerShell.

Réinitialisation du mot de passe d'une application Azure

Suivez les étapes ci-dessous si vous devez réinitialiser un mot de passe Azure, que ce soit en ligne ou hors ligne, selon le cas écheant.

Pour réinitialiser un mot de passe d'application Azure pour DRA à l'aide des informations d'identification Azure :

1 Accédez à **Configuration Management** > **Azure Tenants** (Gestion de la configuration > Locataires Azure) dans la console de délégation et de configuration.

2 Cliquez à l'aide du bouton droit de la souris sur le locataire Azure géré et sélectionnez **Properties** (Propriétés).

3 Cliquez sur **Azure Application** (Application Azure) dans la page Propriétés.

4 Choisissez l'option **Allow DRA to reset the password using your Azure Credentials** (Autoriser DRA à réinitialiser le mot de passe en utilisant vos informations d'identification Azure), puis spécifiez les informations d'identification Azure.

5 Appliquez les modifications.

Pour réinitialiser le mot de passe d'une application Azure pour DRA hors ligne :

1 Lancez une session PowerShell dans le serveur d'administration DRA et accédez à `C:\Program Files (x86)\NetIQ\DRA\SupportingFiles`

2 Executez `. .\ResetDraAzureApplicationPassword.ps1` pour charger PowerShell.

3 Exécutez le `. .\ResetDraAzureApplicationPassword` cmdlet pour demander les paramètres.

4 Précisez les paramètres suivants pour `Reset-DRAAzureApplicationPassword` :

- <nom> - Nom de l'application de l'assistant de locataire.

  IMPORTANT : Micro Focus vous recommande d'utiliser le nom spécifié dans la console DRA.

- (Facultatif) <environnement> - Indiquez AzureCloud, AzureChinaCloud, AzureGermanyCloud ou AzureUSGovernment, en fonction du locataire que vous utilisez.

5 Dans la boîte de dialogue Informations d'identification, spécifiez les informations d'identification de l'administrateur de l'entreprise.

L'ID et le mot de passe de l'application Azure sont alors générés.

6 Copiez l'ID et le mot de passe de l'application dans la console DRA (Assistant locataire **DRA Azure Application Credentials** - Informations d'identification de l'application Azure DRA), puis validez les informations d'identification.

7 Ouvrez la console de délégation et de configuration et accédez à **Configuration Management** > **Azure Tenants** (Gestion de la configuration > Locataires Azure).

8 Cliquez à l'aide du bouton droit de la souris sur un locataire Azure et allez à **Properties** > **Azure Application** (Propriétés > Application Azure).

9 Choisissez l'option **Reset the password offline** (Réinitialiser le mot de passe hors ligne) à l'aide de l'option de script fournie, puis collez le mot de passe de l'application Azure généré à partir du script.

10 Appliquez les modifications.

Gestion des mots de passe pour les comptes d'accès

Vous pouvez réinitialiser les mots de passe des comptes d'accès qui sont utilisés pour gérer un domaine, un serveur secondaire, Exchange ou un locataire Azure à partir de DRA. Si le mot de passe de l'un de ces comptes d'accès arrive à expiration ou si vous l'oubliez, vous pouvez réinitialiser le mot de passe du compte d'accès en procédant comme suit :

- Réinitialisez le mot de passe manuellement dans la console de délégation et de configuration.
- Planifiez une tâche pour surveiller l'expiration du mot de passe des comptes d'accès et réinitialiser le mot de passe des comptes d'accès qui doivent expirer.

Vous pouvez réinitialiser le mot de passe des comptes d'accès à partir du serveur primaire et du serveur secondaire. Si le même compte d'accès est utilisé à plusieurs instances dans le même domaine, par exemple, pour gérer une boîte aux lettres Exchange ou un serveur secondaire, le serveur DRA met automatiquement à jour le mot de passe pour toutes les instances d'utilisation du compte d'accès, éliminant ainsi la nécessité de mettre à jour manuellement le mot de passe pour chaque instance. Si le serveur d'administration secondaire utilise le compte d'accès au domaine du serveur d'administration primaire, le serveur DRA rafraîchit automatiquement le mot de passe du compte d'accès dans le serveur d'administration secondaire.

- « Réinitialiser le mot de passe manuellement » page 139
- « Planifier une tâche pour réinitialiser le mot de passe » page 140

Réinitialiser le mot de passe manuellement

Utilisez la console de délégation et de configuration pour réinitialiser manuellement le mot de passe d'un compte d'accès.

Pour réinitialiser manuellement le mot de passe d'un compte d'accès :

1 Dans la console de délégation et de configuration, cliquez sur **Gestion de la configuration**.

2 Sélectionnez un domaine géré ou un locataire Azure et affichez les propriétés.

3 Dans la page des propriétés, spécifiez les informations suivantes :

- Pour mettre à jour le mot de passe d'un compte d'accès au domaine, dans l'onglet Domain access (Accès au domaine), indiquez un nouveau mot de passe pour le compte d'accès au domaine. Sélectionnez **Update password in Active Directory** (Mettre à jour le mot de passe dans Active Directory).
- Pour mettre à jour le mot de passe d'un compte Exchange, dans l'onglet Exchange access (Accès à Exchange), indiquez un nouveau mot de passe pour le compte d'accès à Exchange. Sélectionnez **Mettre à jour le mot de passe dans Active Directory**.
- Pour mettre à jour le mot de passe d'un compte au locataire Azure, dans l'onglet Tenant access (Accès au locataire), indiquez un nouveau mot de passe pour le compte d'accès au locataire. Sélectionnez **Update Azure tenant access account password** (Mettre à jour le mot de passe du compte d'accès du locataire Azure).
- Pour mettre à jour le mot de passe d'un compte d'accès à un serveur d'administration secondaire, sélectionnez **Gestion de la configuration** > **Serveurs d'administration** dans le serveur d'administration primaire. Sélectionnez le serveur d'administration secondaire pour lequel vous souhaitez mettre à jour le mot de passe, cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**. Dans l'onglet Compte d'accès, indiquez un nouveau mot de passe pour le compte d'accès. Sélectionnez **Mettre à jour le mot de passe dans Active Directory**.

REMARQUE

- Assurez-vous que le compte d'accès du serveur d'administration secondaire n'est pas le compte de service du serveur d'administration secondaire. Le compte d'accès doit faire partie du groupe Administrateurs locaux sur le serveur d'administration secondaire.
- Si vous utilisez un compte avec un droit d'accès minimal comme compte d'accès, assurez-vous que le compte se voit attribuer l'autorisation « Reset Password » (Réinitialiser le mot de passe) dans Active Directory pour qu'il soit possible de réinitialiser le mot de passe dans DRA.

Planifier une tâche pour réinitialiser le mot de passe

Vous pouvez planifier l'exécution de la tâche de réinitialisation du mot de passe à un intervalle prédéfini afin de réinitialiser les mots de passe arrivant à expiration pour vos comptes d'accès. La tâche réinitialisera tous les mots de passe des comptes d'accès qui doivent expirer avant la prochaine exécution de la tâche. Un nouveau mot de passe sera automatiquement généré conformément à la stratégie en matière de mots de passe.

Cette tâche est désactivée par défaut. Vous pouvez planifier la tâche une fois par semaine ou à un intervalle spécifique, selon vos besoins. Dans un environnement MMS, si vous configurez la tâche sur le serveur primaire, assurez-vous que la tâche est configurée sur tous les serveurs du MMS.

Pour configurer la tâche :

1 Sur le serveur sur lequel vous souhaitez planifier la tâche, accédez à l'entrée de registre `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\UpdateAccessAccPWD.Freq`.

2 Cliquez avec le bouton droit de la souris et sélectionnez **Modifier**.

3 Dans le champ **Value data** (Données de valeur), spécifiez la fréquence à laquelle vous souhaitez que la tâche soit exécutée.

- Pour planifier une tâche hebdomadaire, spécifiez la fréquence au format `Semaine <Jour de la semaine> <Heure au format 24 heures>`. Par exemple, pour planifier l'exécution de la tâche tous les samedis à 18h00, entrez :

  `Weekly 06 18:00` (Hebdomadaire 06 18:00)

  Où 6 indique le jour de la semaine et `18:00` indique l'heure au format 24 heures.

- Pour planifier l'exécution de la tâche à un intervalle spécifique, spécifiez la fréquence au format `Intervalle <Heure au format 24 heures>`. Par exemple, pour planifier l'exécution de la tâche toutes les 8 heures, entrez :

  `Interval 08:00` (Intervalle 08:00)

Il est recommandé de planifier l'exécution de la tâche pendant les fins de semaine.

REMARQUE : La tâche de réinitialisation du mot de passe ne prend pas en charge la fréquence quotidienne. Si vous configurez une fréquence quotidienne, le serveur DRA réinitialise automatiquement le calendrier à `Weekly 06 00:00` lorsque vous redémarrez NetIQ Administration Service.

---

4 Cliquez sur **OK**.

5 Redémarrez le **service d'administration de NetIQ** pour que les changements prennent effet.

REMARQUE : Pour chaque locataire Azure configuré, la tâche crée la clé de registre suivante pour la stratégie de mot de passe par défaut avec une validité de 90 jours : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\<tenantName>.ValidityPeriod`. La date d'expiration du mot de passe pour le compte d'accès du locataire est calculée en fonction de la période de validité du locataire. Lorsque le mot de passe arrive à expiration, la tâche réinitialise le mot de passe du compte d'accès au locataire.

Activer l'authentification de remplacement LDAP

Vous pouvez configurer une authentification de remplacement LDAP pour les modifications du gestionnaire personnalisé LDAP dans la console Web. Lorsque cette fonction est activée, vous pouvez définir le type d'authentification pour les gestionnaires de requêtes LDAP personnalisés afin d'exiger le compte de remplacement LDAP pour l'authentification de la connexion.

Pour activer cette fonction :

1 Naviguez jusqu'à **Gestion de la configuration**. > **Mettre à jour les options du serveur d'administration** dans la console de délégation et de configuration.

2 Sélectionnez l'onglet **LDAP Override Account** (Compte de remplacement LDAP) dans la fenêtre Administration Server Options (Options du serveur d'administration).

3 Fournissez le nom de compte, le domaine et le mot de passe et appliquez les modifications.

Par exemple : `nom@domaine` ou `domaine\nom`

Pour en savoir plus sur l'utilisation de cette fonctionnalité dans les personnalisations de la console Web, reportez-vous à la rubrique Étapes de base pour créer un gestionnaire personnalisé.

V Automatisation des stratégies et des processus

Ce chapitre fournit de l'information qui vous aidera à comprendre le fonctionnement des stratégies dans l'environnement DRA et les options de stratégie. Il explique également comment les déclencheurs et le processus de travail automatisé sont utilisés pour automatiser les processus lors de l'utilisation d'objets dans Active Directory.

13 Comprendre la stratégie de DRA

DRA vous permet de configurer diverses stratégies qui vous aident à sécuriser votre entreprise et à empêcher la corruption des données. Ces stratégies fonctionnent dans le contexte du modèle de sécurité dynamique, garantissant que l'application de la stratégie s'adapte automatiquement à l'évolution de votre entreprise. L'établissement de stratégies, telles que les conventions de nommage, les limites d'utilisation du disque et la validation des propriétés, vous permet d'appliquer des règles qui aident à préserver l'intégrité de vos données d'entreprise.

Dans DRA, vous pouvez définir rapidement des règles de stratégie pour les aspects de gestion d'entreprise suivants :

- Microsoft Exchange
- Office 365 Licence
- Répertoire privé
- génération de mot de passe

DRA fournit également des stratégies intégrées pour les groupes, les comptes d’utilisateurs 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 Gestion des stratégies et des déclencheurs d'automatisation. Pour vous aider à gérer vos stratégies, DRA fournit le rapport Détails de la stratégie. Ce rapport fournit les informations suivantes :

- indique si la stratégie est activée
- répertorie les opérations associées
- répertorie les objets régis par cette stratégie
- fournit les détails de l'étendue de la stratégie

Vous pouvez utiliser ce rapport pour vous assurer que vos stratégies sont définies correctement. Vous pouvez également utiliser ce rapport pour comparer les propriétés de stratégie, résoudre les conflits et mieux appliquer les stratégies dans votre entreprise.

Application de la stratégie 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 l'exécute 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 termine l'opération. Vous pouvez limiter l'étendue d'une stratégie en l'associant à des groupes d'ActiveView ou d'administrateurs assistants particuliers.

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

Pour vous assurer que vos stratégies n'entrent pas en conflit, suivez les directives suivantes :

- nommez les stratégies afin qu'elles s'exécutent dans le bon ordre
- vérifiez que chaque stratégie n'interfère pas avec les validations ou les actions effectuées par d'autres stratégies
- testez minutieusement les stratégies personnalisées avant de les mettre en œuvre dans votre environnement de production

Le serveur d'administration entre le statut de la stratégie dans le journal d'audit à chaque exécution d'une stratégie. Ces entrées de journal enregistrent le code de retour, les opérations associées, les objets sur lesquels il y a eu une action 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 d'autorisations d'administrateur, les stratégies ont un accès complet à toutes les données d'entreprise. Ainsi, les administrateurs assistants associés au rôle intégré Gérer les stratégies et les déclencheurs d'automatisation peuvent obtenir plus de pouvoir que prévu.

Stratégies intégrées

Les stratégies intégrées sont mises en œuvre lorsque vous installez le serveur d'administration. Lorsque vous travaillez avec ces stratégies, vous pouvez rencontrer les termes suivants :

Étendue de la stratégie

Elle définit les objets ou les propriétés auxquels DRA applique la stratégie. Par exemple, certaines stratégies vous permettent d'appliquer une stratégie à des administrateurs assistants précis dans les ActiveViews. Certaines stratégies vous permettent de choisir parmi différentes classes d'objets, telles que des comptes d'utilisateurs ou des groupes.

Stratégies globales

Permet d'appliquer les règles de stratégie à tous les objets de la classe ou du type spécifié dans les domaines gérés. Avec les stratégies globales, vous ne pouvez pas limiter l'étendue des objets auxquels la stratégie s'applique.

Relation de stratégie

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

Rubriques liées aux stratégies intégrées :

- « Comprendre les stratégies intégrées » page 147
- « Stratégies disponibles » page 148
- « Utiliser des stratégies intégrées » page 150

Comprendre les stratégies intégrées

Les stratégies intégrées fournissent des règles d'entreprise pour résoudre les problèmes courants de sécurité et d'intégrité des données. Ces stratégies font partie du modèle de sécurité par défaut, vous permettant d'intégrer les fonctionnalités de sécurité DRA dans votre configuration d'entreprise existante.

DRA fournit deux moyens d'appliquer les stratégies. Vous pouvez créer des stratégies personnalisées ou choisir parmi plusieurs stratégies intégrées. Les stratégies intégrées facilitent l'application des stratégies sans qu'il soit nécessaire de développer des scripts personnalisés. Si vous devez implémenter une stratégie personnalisée, vous pouvez adapter une stratégie intégrée existante 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.

Un certain nombre de 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 (antérieur à Windows 2000)	Limite le nombre de caractères du nom de l'ordinateur ou le nom de l'ordinateur antérieur à Windows 2000
$GroupNameLengthPolicy	64 20 (antérieur à Windows 2000)	Limite le nombre de caractères du nom du groupe ou le nom du groupe antérieur à Windows 2000
$GroupSizePolicy	5000	Limite le nombre de membres dans un groupe
$NameUniquenessPolicy	Aucun	Garantit que les noms antérieurs à Windows 2000 et les noms CN sont uniques dans tous les domaines gérés
$SpecialGroupsPolicy	Aucun	Empêche une escalade incontrôlée des pouvoirs dans l'environnement.
$UCPowerConflictPolicy	Aucun	Empêche l'escalade des pouvoirs en rendant les commandes User Clone (Cloner un utilisateur) et User Create (Créer un utilisateur) exclusifs
$UPNUniquenessPolicy	Aucun	Veille à ce que les noms UPN soient uniques dans tous les domaines gérés
$UserNameLengthPolicy	64 20 (nom de connexion de niveau inférieur)	Limite le nombre de caractères du nom de connexion de l'utilisateur ou du nom de connexion de niveau inférieur

Stratégies disponibles

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

REMARQUE : Vous pouvez créer une stratégie nécessitant une entrée pour une propriété qui n'est actuellement pas disponible à partir des interfaces utilisateur DRA. Si la stratégie exige une entrée et que l'interface utilisateur ne fournit pas de champ pour entrer la valeur en question, par exemple un service pour un nouveau compte d'utilisateur, vous ne pourrez pas créer ou gérer l'objet. Pour éviter ce problème, configurez des stratégies qui nécessitent uniquement les propriétés accessibles à partir des interfaces utilisateur.

Créer une stratégie personnalisée

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

Appliquer une longueur de nom maximale

Cette option vous permet d'appliquer globalement la longueur maximale du nom pour les comptes d'utilisateurs, les groupes, les unités organisationnelles, les contacts ou les ordinateurs.

La stratégie vérifie le conteneur de noms (nom commun ou cn) et le nom antérieur à Windows 2000 (nom de connexion de l'utilisateur).

Appliquer le nombre maximum de membres du groupe

Cette option vous permet d'appliquer globalement des limites au nombre de membres d'un groupe.

Appliquer les noms de compte uniques antérieurs à Windows 2000

Cette option permet de vérifier qu'un nom antérieur à Windows 2000 est unique pour tous les domaines gérés. Dans les domaines Microsoft Windows, les noms antérieurs à Windows 2000 doivent être uniques dans un domaine. Cette stratégie globale applique cette règle à tous les domaines gérés.

Appliquer des noms d'utilisateur principaux (UPN) uniques

Cette option permet de vérifier qu'un nom d'utilisateur principal est unique pour tous les domaines gérés. Dans les domaines Microsoft Windows, les noms d'utilisateur principaux doivent être uniques dans un domaine. Cette stratégie applique cette règle à tous les domaines gérés. Comme il s'agit d'une stratégie globale, DRA fournit le nom, la description et la relation de la stratégie.

Limiter les actions aux membres de groupes spéciaux

Cette option vous empêche de gérer les membres d'un groupe d'administrateurs, sauf si vous êtes membre de ce groupe d'administrateurs. Cette stratégie globale est activée par défaut.

Lorsque vous limitez les actions aux membres des groupes d'administrateurs, l'assistant de création de stratégie ne nécessite aucune information supplémentaire. Vous pouvez spécifier un message d'erreur personnalisé. Comme il s'agit d'une stratégie globale, DRA fournit le nom, la description et la relation de la stratégie.

Empêcher les administrateurs assistants de créer et de cloner des utilisateurs dans le même AV

Cette option empêche une éventuelle escalade des pouvoirs. Lorsque cette stratégie est activée, vous pouvez créer des comptes d'utilisateurs ou cloner des comptes d'utilisateur, mais vous ne pouvez pas disposer des deux pouvoirs. Cette stratégie globale garantit que vous ne pouvez pas créer et cloner des comptes d'utilisateurs dans le même ActiveView.

Cette stratégie ne nécessite pas d'informations supplémentaires.

Définir une stratégie de convention de nommage

Cette option vous permet d'établir des conventions de nommage qui s'appliquent à des administrateurs assistants, à des ActiveViews et à des classes d'objets précis tels qu'un compte d'utilisateur ou des groupes.

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

Créer une stratégie pour valider une propriété précise

Cette option vous permet de créer une stratégie pour valider toute propriété d'une unité organisationnelle ou d'un objet de compte. Vous pouvez spécifier une valeur par défaut, un masque de format de propriété, ainsi que des valeurs et des plages valides.

Utilisez cette stratégie pour appliquer l'intégrité des données en validant des champs de saisie particuliers lorsque vous créez, clonez ou modifiez les propriétés d'objets précis. Cette stratégie offre une flexibilité et un pouvoir considérables pour valider les entrées, fournir des entrées par défaut et limiter les choix d'entrée pour divers champs de propriété. En utilisant cette stratégie, vous pouvez exiger qu'une entrée soit correcte pour qu'une tâche se termine, préservant ainsi l'intégrité des données dans vos domaines gérés.

Par exemple, supposons que vous ayez trois services : Fabrication, Ventes et Administration. Vous pouvez limiter les entrées acceptées par DRA 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 des masques de formats multiples pour un numéro de téléphone tels que `(123)456 7890` ou `456 7890`, définissez le masque de format de propriété ainsi `(###)### ####,### ####`.

Créer une stratégie pour appliquer les licences Office 365

Vous permet de créer une stratégie pour attribuer des licences Office 365 en fonction de l'adhésion à un groupe Active Directory. Cette stratégie applique également la suppression des licences Office 365 lorsqu'un membre est supprimé du groupe Active Directory correspondant.

Si un utilisateur non synchronisé dans le nuage est ajouté au groupe Active Directory, il sera synchronisé avant l'attribution d'une licence Office 365 à l'utilisateur.

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

Le paramètre **Ensure only licenses assigned by DRA policies are enabled on accounts. All other licenses will be removed.** (Vérifier que seules les licences attribuées par les stratégies DRA sont activées sur les comptes. Toutes les autres licences seront supprimées.) est inclus dans la page

Propriétés du locataire, qui est configurable par locataire. Ce paramètre est utilisé pour les stratégies de licence de DRA Office 365 afin de configurer la manière dont les attributions de licence seront appliquées :

Lorsque ce paramètre est activé, l'application de la licence DRA garantit que seules les licences attribuées à l'aide des stratégies DRA sont provisionnées aux comptes (les licences attribuées en dehors de DRA seront supprimées des comptes affectés à la stratégie de licence). Lorsque ce paramètre est désactivé (par défaut), l'application des licences DRA garantit uniquement que les licences spécifiques que vous avez incluses dans vos stratégies Office 365 sont provisionnées sur les comptes (lorsqu'un compte n'est pas affecté à une stratégie de licence, seules les licences attribuées par cette stratégie sont déprovisionnées).

Utiliser des stratégies intégrées

Les stratégies intégrées faisant partie 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 de stratégie et le message d'erreur de plusieurs stratégies intégrées. Vous pouvez activer ou désactiver chaque stratégie intégrée.

Vous pouvez également créer facilement de nouvelles stratégies.

Implémenter une stratégie personnalisée

Les stratégies personnalisées vous permettent d'exploiter pleinement la puissance et la flexibilité du modèle de sécurité par défaut. En utilisant des stratégies personnalisées, vous pouvez intégrer DRA aux composants d'entreprise existants tout en veillant à l'application de vos règles propriétaires. Vous pouvez utiliser la fonctionnalité de stratégie personnalisée pour étendre les stratégies de votre entreprise.

Vous créez et appliquez des stratégies personnalisées en associant un exécutable ou un script à une opération d'administration. Par exemple, un script de stratégie associé à l'opération `UserCreate` (Créer un utilisateur) pourrait vérifier votre base de données de ressources humaines pour voir si l'employé spécifié existe. Si l'employé existe dans la base de données des ressources humaines et ne possède pas de compte existant, le script extrait l'ID, le prénom et le nom de l'employé de la base de données. L'opération se termine correctement et remplit la fenêtre de propriétés du compte d’utilisateur avec les renseignements appropriés. Cependant, si l'employé a déjà un compte, l'opération échoue.

Les scripts vous donnent une flexibilité et une puissance énorme. Pour créer vos propres scripts de stratégie, vous pouvez utiliser les fournisseurs ADSI (fournisseur ADSI), les kits de développement logiciel (SDK) et les applets de commande PowerShell de Directory and Resource Administrator. Pour obtenir de plus amples renseignements sur la création de vos propres scripts de stratégie, consultez la section Référence du site Documentation de DRA.

Restreindre les groupes de sécurité intégrés natifs

Pour fournir un environnement plus sécurisé, DRA vous permet de limiter les pouvoirs accordés aux groupes de sécurité intégrés à Microsoft Windows. La possibilité de modifier l'adhésion à un groupe, les propriétés de groupe de sécurité intégrées ou les propriétés des membres du groupe peut avoir

des conséquences importantes pour la sécurité. Par exemple, si vous pouvez modifier le mot de passe d'un utilisateur du groupe Opérateurs de serveur, vous pouvez vous connecter en tant qu'utilisateur et exercer les pouvoirs délégués à ce groupe de sécurité intégré.

DRA empêche ce problème de sécurité en fournissant une stratégie qui vérifie vos pouvoirs pour un groupe de sécurité natif intégré et ses membres. Cette validation garantit que les actions demandées n'escaladent pas ces pouvoirs. Une fois que vous avez activé cette stratégie, un administrateur assistant 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 que vous pouvez limiter

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

- opérateurs de compte
- administrateurs
- opérateurs de sauvegarde
- diffuseur de certifications
- administrateurs DNS
- administrateurs de domaine
- administrateurs d'entreprise
- propriétaires créateurs de la stratégie de groupe
- opérateurs d'impression
- administrateurs de schéma

REMARQUE : DRA fait référence aux groupes de sécurité intégrés par leurs identificateurs internes. Par conséquent, DRA prend en charge ces groupes même si ceux-ci sont renommés. Cette fonctionnalité garantit que DRA prend en charge les groupes de sécurité intégrés portant différents noms dans différents pays. Par exemple, DRA fait référence au groupe Administrateurs et au groupe *Administratoren* ayant le même identificateur interne.

Restreindre les actions sur les groupes de sécurité intégrés natifs

DRA utilise une stratégie pour limiter le pouvoir des groupes de sécurité intégrés natifs et de leurs membres. Cette stratégie, appelée `$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 aux groupes de sécurité intégrés natifs et à 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, à condition de disposer des 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 des deux groupes. Toutefois, vous ne pouvez pas effectuer d'actions sur un compte d'utilisateur 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 :

- cloner un groupe
- créer un groupe
- supprimer un groupe
- ajouter un membre à un groupe
- supprimer un membre d'un groupe
- déplacer un groupe vers une unité organisationnelle
- modifer les propriétés d'un groupe
- copier une boîte aux lettres
- Supprimer une boîte aux lettres
- cloner un compte d’utilisateur
- créer un compte d’utilisateur
- supprimer un compte d’utilisateur
- déplacer un compte d’utilisateur vers une unité organisationnelle
- modifier les propriétés d'un compte d’utilisateur

DRA limite également les actions afin de garantir que vous n'obtenez pas de pouvoirs sur un objet. Par exemple, lorsque vous ajoutez un compte d’utilisateur à un groupe, DRA vérifie que vous n'obtenez pas de pouvoirs supplémentaires sur le compte d’utilisateur parce qu'il est membre de ce groupe. Cette validation est une protection contre une escalade de pouvoir.

Gérer les stratégies

Grâce au nœud Gestion des stratégies et de l'automatisation, vous pouvez accéder aux stratégies de Microsoft Exchange et des répertoires privés, ainsi qu'aux stratégies intégrées et personnalisées. Utilisez les tâches courantes suivantes pour améliorer la sécurité de votre entreprise et l'intégrité des données.

Configurer les stratégies Exchange

Cette tâche vous permet de définir la configuration Microsoft Exchange, la stratégie de boîte aux lettres, le nommage automatique et les règles de génération de mandataire. Ces règles peuvent définir le mode de gestion des boîtes aux lettres lorsqu'un administrateur assistant crée, modifie ou supprime un compte d’utilisateur.

Configurer les stratégies de répertoire privé

Cette tâche vous permet de créer, de renommer ou de supprimer automatiquement des répertoires privés et des partages privés lorsqu'un administrateur assistant crée, renomme ou supprime un compte d'utilisateur. La stratégie de répertoire privé vous permet également d'activer ou de désactiver la prise en charge des quotas de disque pour les répertoires privés sur les serveurs Microsoft Windows ainsi que sur les serveurs autres que Windows.

Configurer les stratégies de génération de mot de passe

Cette tâche vous permet de définir les exigences pour les mots de passe générés par DRA.

Pour de plus amples renseignements sur la gestion des stratégies dans DRA, reportez-vous aux sections suivantes :

- « Stratégie Microsoft Exchange » page 153
- « Stratégie de licence Office 365 » page 155
- « Créer et mettre en œuvre une stratégie de répertoire privé » page 156
- « Activer la génération de mots de passe » page 162
- « Tâches de stratégie » page 162

Stratégie Microsoft Exchange

Exchange offre plusieurs stratégies pour vous aider à gérer plus efficacement les objets Microsoft Exchange. La stratégie Microsoft Exchange vous permet d'automatiser la gestion des boîtes aux lettres, d'appliquer les conventions d'affectation des noms pour les alias et les banques de boîtes aux lettres ainsi que de générer automatiquement des adresses de courriel.

Ces stratégies peuvent vous aider à rationaliser vos processus de travail et à maintenir l'intégrité des données. Par exemple, vous pouvez spécifier comment Exchange gère les boîtes aux lettres lorsque vous créez, modifiez ou supprimez des comptes d'utilisateurs. Pour définir et gérer les 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.

Spécifier une stratégie d'adresse de courriel par défaut

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 spécifier une stratégie d'adresse de courriel par défaut :

1. Accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies Exchange** > **Génération de mandataire**.
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 mandataire pour le domaine sélectionné.

   3a Cliquez sur **Ajouter**.

   3b Sélectionnez un type de mandataire. Par exemple, cliquez sur **Adresse Internet**.

   3c Acceptez la valeur par défaut ou tapez une nouvelle règle de génération de mandataire, puis cliquez sur **OK**.

   Pour obtenir de plus amples renseignements sur les chaînes de substitution prises en charge pour les règles de génération de mandataires, consultez Stratégie client de délégation et de configuration.

4 Cliquez sur **Attributs personnalisés** pour modifier le nom personnalisé des propriétés de la boîte aux lettres personnalisée.

   4a Sélectionnez l'attribut et cliquez sur le bouton **Éditer**.

   4b Dans la fenêtre Propriétés de l'attribut, entrez le nom de l'attribut dans le champ **Nom personnalisé**, puis cliquez sur **OK**.

5 Cliquez sur **OK**.

REMARQUE : Les administrateurs de stratégie DRA devraient avoir le pouvoir *Gérer les outils personnalisés* pour modifier les attributs personnalisés dans la stratégie Microsoft Exchange.

Rêgles de boîte aux lettres

Les règles de boîte aux lettres vous permettent de spécifier comment Exchange gère les boîtes aux lettres lorsque les administrateurs assistants créent, clonent, modifient ou suppriment des comptes d'utilisateurs. Les règles de boîte aux lettres gèrent automatiquement les boîtes aux lettres Microsoft Exchange en fonction de la manière dont l'administrateur assistant gère les comptes d'utilisateurs associés.

REMARQUE : Lorsque vous activez l'option **Do not allow Assistant Admins to create a user account without a mailbox** (Ne pas autoriser les administrateurs assistants à créer un compte d'utilisateur sans boîte aux lettres) dans les domaines Microsoft Windows, assurez-vous que l'administrateur assistant a le pouvoir de cloner ou de créer un compte d'utilisateur. Lorsque cette option est activée, les administrateurs assistants doivent créer des comptes d'utilisateurs Windows avec une boîte aux lettres.

Pour spécifier les 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 les règles de boîte aux lettres Exchange :

1 Accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies Exchange** > **Règles de boîte aux lettres**.

2 Sélectionnez les stratégies de boîte aux lettres qu'Exchange doit appliquer lors de la création ou de la modification de comptes d'utilisateurs.

3 Cliquez sur **OK**.

Stratégie de licence Office 365

Pour spécifier les stratégies de licences 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.

Autoriser DRA à gérer vos licences Office 365 (facultatif)

Si vous souhaitez autoriser DRA à gérer vos licences Office 365, vous devez procéder comme suit :

- Créez une stratégie d'application de licence.
- Activez la **Planification de mise à jour de licence** sur la page de propriétés du locataire.

Créer une stratégie d'application de licences Office 365

Pour créer une stratégie d'application de licences Office 365, cliquez sur le nœud **Policy and Automation Management** (Gestion des stratégies et de l'automatisation) de la console de délégation et de configuration, puis sélectionnez **New Policy** >**Create New Policy to Enforce Office 365 Licenses** (Nouvelle stratégie > Créer une nouvelle stratégie pour appliquer des licences Office 365).

Lorsque la stratégie est appliquée et qu'un utilisateur est ajouté à Active Directory, DRA utilise l'adhésion à un groupe pour attribuer automatiquement la licence Office 365 à l'utilisateur.

Planification de 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, à moins que vous n'activiez également la **Planification de mise à jour de licence** sur la page de propriétés du locataire. La tâche de mise à jour des licences garantit que les licences Office 365 attribuées aux utilisateurs correspondent à vos stratégies de licence Office 365.

La tâche de mise à jour des licences et les stratégies de licence Office 365 fonctionnent ensemble pour garantir que tous vos utilisateurs gérés se voient attribuer uniquement les licences Office 365 qu'ils sont censés posséder.

REMARQUE

- DRA ne gère pas les licences Office 365 pour les comptes d'utilisateurs en ligne uniquement. Pour que DRA puisse gérer vos utilisateurs avec des licences Office 365, ces utilisateurs doivent être synchronisés avec Active Directory.
- Si vous choisissez d'utiliser DRA pour gérer vos licences Office 365, DRA annulera toute modification manuelle des licences Office 365 effectuée en dehors de DRA lors de la prochaine exécution de la tâche de mise à jour des licences.
- Si vous activez la tâche de mise à jour des licences Office 365 avant de vous assurer que vos stratégies de licence Office 365 sont correctement configurées, les licences attribuées peuvent être incorrectes après l'exécution de la tâche de mise à jour des licences.

Créer et mettre en œuvre une stratégie de répertoire privé

Lorsque vous gérez un grand nombre de comptes d'utilisateurs, la création et la maintenance des répertoires et des partages privés peuvent prendre beaucoup de temps et constituer une source d'erreur de sécurité. Un travail de maintenance supplémentaire peut être nécessaire chaque fois qu'un utilisateur est créé, renommé ou supprimé. Les stratégies de répertoire privé vous aident à gérer la maintenance des répertoires et des partages privés.

DRA vous permet d'automatiser la création et la maintenance des répertoires privés des utilisateurs. Par exemple, vous pouvez facilement configurer DRA pour que le serveur d'administration crée un répertoire privé lorsque vous créez un compte d'utilisateur. Dans ce cas, si vous spécifiez un chemin de répertoire privé lors de la création du compte d'utilisateur, le serveur crée automatiquement le répertoire privé selon le chemin 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 utilisateurs ou de la configuration de stratégies de répertoires privés pour les utilisateurs dans des chemins parents autorisés. Vous pouvez créer, renommer et supprimer des répertoires privés sur Netapp Filers et sur des chemins ou des partitions DFS.

Configurer les stratégies de répertoire privé

Pour configurer les stratégies de répertoire privé, de partage privé et de quota de disque de volume privé, 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 privés, les partages privés et les quotas de disques de volume privés en fonction de la gestion des comptes d'utilisateurs associés.

Pour configurer les stratégies de répertoire privé, accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies de répertoire privé** >

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

Configuration requise du serveur d'administration

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

Un partage administratif, tel que C$ou D$, doit exister pour chaque lecteur sur lequel DRA gère et stocke les répertoires privés. DRA utilise les partages administratifs pour effectuer certaines tâches d'automatisation du répertoire privé et du partage privé. Si ces partages n'existent pas, DRA ne peut pas automatiser le répertoire privé et le partage privé.

Configurer les chemins d'accès autorisés du répertoire privé pour NetApp Filer

Pour configurer les chemins d'accès parents autorisés pour NetApp Filer :

1. Accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies de répertoire privé**.
2. Dans la zone de texte **Chemins parents autorisés**, entrez l'un des chemins autorisés du tableau suivant :

Type de partage	Chemin autorisé
Windows	(*NomFichier**PartageAdmin:**CheminRacineVolume*h*CheminRépertoire*)
Non-Windows	(*non-windows**partage*)

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

Comprendre la stratégie de répertoire privé

Pour être cohérent avec les stratégies de sécurité Microsoft Windows appropriées, DRA crée uniquement des restrictions de contrôle d'accès au niveau du répertoire. Placer des restrictions de contrôle d'accès à la fois au niveau du nom de partage et au niveau du fichier ou de l'objet répertoire entraîne souvent un schéma d'accès confus 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 d’utilisateurs disposent d'un accès approprié à leurs propres répertoires privés.

Automatisation de répertoire privé et règles

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

Pour réussir la mise en œuvre de votre stratégie de répertoire privé, suivez les directives ci-dessous :

- Assurez-vous que le chemin spécifié utilise le bon format.
  - Pour spécifier un chemin d'accès pour un seul répertoire privé, utilisez l'un des modèles du tableau suivant :

Type de partage	Modèle de chemin
Windows	*ordinateur**partage*\. Par exemple, si vous souhaitez que DRA crée automatiquement un répertoire privé dans le dossier Home Share sur l'ordinateur server01, tapez \\server01\Home Share\
Non-Windows	*non-windows**partage*

- Pour standardiser l'administration du répertoire privé sur le répertoire racine du partage privé correspondant, utilisez la syntaxe de convention de nommage comme suit : *nom du serveur**C:**chemin du répertoire racine*.
- Pour spécifier un chemin d'accès pour des répertoires privés imbriqués, utilisez l'un des modèles du tableau suivant :

Type de partage	Modèle de chemin
Windows	*ordinateur**partage**premier répertoire**deuxième répertoire*\ Par exemple, si vous voulez que DRA crée automatiquement un répertoire privé dans le répertoire JSmith\Home directory sous le dossier Home Share de l'ordinateur server01, tapez\\server01\Home Share\JSmith\Home.
Non-Windows	*non-windows**partage**premier répertoire**deuxième répertoire*\

REMARQUE : DRA prend également en charge les formats suivants : *computer**share**username*et *computer**share**%username%*. Dans chaque cas, DRA crée automatiquement un répertoire privé pour le compte d'utilisateur associé.

- Lorsque vous définissez un déclencheur de stratégie ou d'automatisation pour gérer les répertoires privés sur NetApp Filer, vous devez utiliser un format différent pour la spécification de répertoire.
  - Si vous utilisez des NetApp Filer, spécifiez le répertoire parent au format suivant : *FilerName**adminshare:**volumerootpat*h*directorypath*
  - La variable adminshare est le partage masqué mappé sur le volume racine du NetApp filer tel que *c$*. Par exemple, si le chemin d'accès local du partage sur un NetApp filer, appelé usfiler, est c$\vol\vol0\mydirectory, vous pouvez spécifier un chemin racine \\usfiler\c:\vol\vol0\mydirectory pour le NetApp filer.
- Pour spécifier un chemin DFS lors de la création de répertoires privés d'utilisateurs ou de la configuration de stratégies de répertoires privés pour les utilisateurs, utilisez *server**root**<link>* format, où root peut être le domaine géré ou un répertoire racine autonome au format suivant : *FilerName**adminshare:**volumerootpath**directorypath* .

- Créez un répertoire partagé pour stocker le répertoire privé de ce compte d'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 du compte d'utilisateur

Cette règle permet à DRA de créer automatiquement des répertoires privés pour les nouveaux comptes d'utilisateurs. Lorsque DRA crée un répertoire privé, le serveur d'administration utilise le chemin spécifié dans les champs **Répertoire privé** de l'assistant de création d'utilisateur. Vous pouvez modifier ce chemin ultérieurement en utilisant l'onglet Profil de la fenêtre des propriétés de l'utilisateur et DRA déplacera le répertoire privé vers le nouvel emplacement. Si vous ne spécifiez pas de valeurs pour ces champs, DRA ne crée pas de répertoire privé pour ce compte d'utilisateur.

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

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

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

Renommer un répertoire privé lors de la création du compte d'utilisateur

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

- créer un répertoire privé lorsque vous spécifiez un nouveau chemin de répertoire privé
- déplacer le contenu du répertoire privé lorsque vous modifiez le chemin du répertoire privé
- renommer un répertoire privé lorsque vous renommez le compte d'utilisateur

Lorsque vous renommez un compte d'utilisateur, DRA renomme le répertoire privé existant en fonction du nouveau nom du compte. Si le répertoire privé existant est en cours d'utilisation, DRA crée un nouveau répertoire privé avec le nouveau nom et ne modifie pas 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 Répertoire privé pour créer un répertoire privé sans déplacer le contenu du répertoire privé existant. DRA applique également les listes de contrôle d'accès affectées du répertoire précédent au nouveau répertoire. Si le répertoire privé spécifié existe déjà, DRA ne crée pas le nouveau et ne modifie pas les autorisations de répertoire existantes. 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 nouveau répertoire privé avec un nouveau nom et de copier le contenu du répertoire privé précédent dans le nouveau. DRA tente ensuite de supprimer le répertoire privé précédent. Vous pouvez

configurer DRA pour ne pas copier le contenu du répertoire privé précédent dans le nouveau et déplacer manuellement le contenu du répertoire privé précédent vers le nouveau pour éviter des problèmes tels que la copie de fichiers ouverts.

Lors de la suppression du répertoire privé précédent, DRA a besoin d'une autorisation explicite pour supprimer les fichiers et les sous-répertoires en lecture seule du répertoire privé précédent. Vous pouvez donner à DRA l'autorisation de supprimer explicitement les fichiers et les sous-répertoires en lecture seule du répertoire privé précédent.

Autoriser le répertoire parent ou le chemin d'accès pour un partage privé

DRA vous permet de spécifier les répertoires ou chemins parents autorisés pour les partages privés sur les serveurs de fichiers. Si vous avez plusieurs chemins de répertoire ou de serveur de fichiers à spécifier, vous pouvez exporter ces chemins vers un fichier CSV et ajouter les chemins de fichier CSV à DRA à l'aide de la console DRA. DRA utilise les renseignements saisis dans le champ **Chemins parents autorisés** pour veiller à ce que :

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

Supprimer un répertoire privé lorsqu'un compte d'utilisateur est supprimé

Cette règle permet à DRA de supprimer automatiquement un répertoire privé lorsque vous supprimez le compte d'utilisateur associé. Si vous activez la Corbeille, DRA ne supprime pas le répertoire privé tant que vous n'avez pas supprimé le compte d'utilisateur de la Corbeille. Lors de la suppression du répertoire privé, DRA a besoin d'une autorisation explicite pour supprimer les fichiers et les sous-répertoires en lecture seule du répertoire privé précédent. Vous pouvez donner à DRA l'autorisation de supprimer explicitement les fichiers et les sous-répertoires en lecture seule du répertoire privé précédent.

Automatisation de partage privé et règles

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

Pour être cohérent avec les stratégies de sécurité Microsoft Windows appropriées, DRA ne crée pas de restrictions de contrôle d'accès au niveau du nom de partage. À la place, DRA crée des restrictions de contrôle d'accès uniquement au niveau du répertoire. Placer des restrictions de contrôle d'accès à la fois au niveau du nom de partage et au niveau du fichier ou de l'objet répertoire entraîne souvent un schéma d'accès confus pour les administrateurs et les utilisateurs.

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

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

Le chemin suivant n'est pas valide : `\\`*`HOUSERV1`*`\%username%`

Spécifier des noms de partage privé

Lors de la définition des règles d'automatisation du partage privé, 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 nommage pour les partages privés.

Par exemple, vous activez les règles d'automatisation Créer un répertoire privé et Créer un partage privé. Pour le partage privé, vous spécifiez un préfixe qui est le caractère soulignement et un suffixe qui est le signe dollar. Lorsque vous créez un utilisateur nommé TomS, vous mappez son nouveau répertoire sur le lecteur U et spécifiez `\\HOUSERV1\HOMEDIRS\%username%` comme chemin de répertoire. Dans cet exemple, DRA crée un partage réseau nommé `_TomS$` qui pointe vers le répertoire `\\HOUSERV1\HOMEDIRS\TomS directory`.

Créer des partages privés pour les nouveaux comptes d'utilisateurs

Lorsque DRA crée un partage privé, le serveur d'administration utilise le chemin spécifié dans les champs **Répertoire privé** de l'assistant de création d'utilisateur. Vous pouvez modifier ce chemin ultérieurement sur l'onglet Profil de la fenêtre des propriétés de l'utilisateur.

DRA crée le nom de partage en ajoutant les préfixes et les suffixes spécifiés, le cas échéant, au nom d'utilisateur. Si vous utilisez des noms de compte d'utilisateur longs, DRA risque de ne pas pouvoir ajouter le préfixe et le suffixe de partage privé spécifié. Le préfixe et le suffixe, ainsi que le nombre de connexions autorisées, sont basés sur les options de création de partage privé que vous avez sélectionnées.

Créer des partages privés pour les comptes d'utilisateurs clonés

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

Lors du clonage d'un compte d'utilisateur, le nom de partage du compte d'utilisateur existant doit exister à ce moment-là. Lorsque vous clonez un compte d'utilisateur, DRA clone également les renseignements du répertoire privé et les personnalise pour le nouvel utilisateur.

Modifier les propriétés d'un partage privé

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

Renommer les partages privés pour les comptes d'utilisateurs renommés

Lorsque vous renommez un compte d'utilisateur, DRA supprime le partage privé existant et crée un nouveau partage basé sur le nouveau nom du compte. Le nouveau partage pointe vers le répertoire privé existant.

Supprimer des partages privés pour les comptes d'utilisateurs supprimés

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

Règles de gestion de quota de disque de volume privé

DRA vous permet de gérer les quotas de disque des volumes privés. Vous pouvez implémenter cette stratégie dans des domaines natifs où le répertoire privé réside sur un ordinateur Microsoft Windows. Lorsque vous implémentez cette stratégie, vous devez spécifier un quota de disque d'au moins 25 Mo pour laisser suffisamment d'espace.

Activer la génération de mots de passe

Cette fonctionnalité vous permet de spécifier les paramètres de stratégie pour les mots de passe générés par DRA. DRA n'applique pas ces paramètres sur les mots de passe créés par les utilisateurs. Lors de la configuration des propriétés de la stratégie des mots de passe, la longueur du mot de passe ne doit pas être inférieure à 6 caractères ni supérieure à 127 caractères, toutes les valeurs peuvent être mises à zéro, à l'exception de la longueur du mot de passe et de la limite maximale.

Pour configurer la stratégie de génération de mot de passe, accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies de génération de mot de passe**, puis cochez la case **Activer la stratégie de mot de passe**. Cliquez sur **Paramètres de mot de passe** et configurez les propriétés de la stratégie de mot de passe.

Tâches de stratégie

Pour supprimer, activer ou désactiver les 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 l'une de ces actions, accédez à **Gestion des stratégies et de l'automatisation** > **Stratégies**. Cliquez avec le bouton droit de la souris sur la stratégie que vous souhaitez supprimer, activer ou désactiver dans le volet de droite, puis sélectionnez l'action souhaitée.

Mettre en œuvre des stratégies intégrées

Pour mettre en œuvre 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 obtenir de plus amples renseignements sur les stratégies intégrées, consultez Comprendre les stratégies intégrées.

REMARQUE : Avant d'associer la stratégie intégrée à un administrateur assistant et à un ActiveView, vérifiez d'abord que l'administrateur assistant est affecté à cet ActiveView.

Pour mettre en œuvre des stratégies intégrées :

1. Accédez à **Gestion des stratégies et de l'automatisation** > **Stratégies**.
2. Dans le menu Tâches, cliquez sur **Nouvelle stratégie**, puis sélectionnez le type de stratégie intégrée à créer.
3. Dans chaque fenêtre de l'assistant, spécifiez les valeurs appropriées, puis cliquez sur **Suivant**. Par exemple, vous pouvez associer cette nouvelle stratégie à un ActiveView précis, ce qui permet à DRA d'appliquer cette stratégie aux objets inclus par cet ActiveView.
4. Examinez le résumé, puis cliquez sur **Terminer**.

Mettre en œuvre des stratégies personnalisées

Pour mettre en œuvre 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 implémenter correctement une stratégie personnalisée, vous devez écrire un script qui s'exécute au cours d'une opération précise (tâche administrative). Vous pouvez associer un exécutable ou un script à l'opération. DRA prend en charge le script PowerShell 32 bits et le script

PowerShell 64 bits. Dans le script de stratégie personnalisée, vous pouvez définir des messages d'erreur à afficher chaque fois qu'une action enfreint la stratégie. Vous pouvez également spécifier un message d'erreur par défaut à l'aide de l'assistant de création de stratégie.

Pour obtenir de plus amples renseignements sur l'écriture de stratégies personnalisées, l'affichage d'une liste d'opérations d'administration ou l'utilisation de tableaux d'arguments, consultez le SDK. Pour obtenir de plus amples renseignements, consultez Écrire des scripts de stratégie ou des exécutables personnalisés.

REMARQUE

- Avant d'associer la stratégie personnalisée à un administrateur assistant et à un ActiveView, vérifiez d'abord que l'administrateur assistant est affecté à cet ActiveView.
- Si le chemin du script de la stratégie personnalisée ou de l'exécutable contient des espaces, insérez des guillemets anglais (") autour du chemin.

Pour implémenter une stratégie personnalisée :

1. Écrivez un script de stratégie ou un exécutable.
2. Connectez-vous à un ordinateur client DRA avec un compte auquel le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation est attribué 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 **Stratégie**.
7. Dans le menu Tâches, cliquez sur **Nouvelle stratégie > Créer une stratégie personnalisée**.
8. Dans chaque fenêtre de l'assistant, spécifiez les valeurs appropriées, puis cliquez sur **Suivant**. Par exemple, vous pouvez associer cette nouvelle stratégie à un ActiveView précis, ce qui permet à DRA d'appliquer cette stratégie aux objets inclus par cet ActiveView.
9. Examinez le résumé, puis cliquez sur **Terminer**.

Modifier des propriétés de 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** > **Stratégies**.
2. Cliquez avec le bouton droit de la souris sur la stratégie à modifier, puis sélectionnez **Propriétés**.
3. Modifiez les propriétés et les paramètres appropriés pour cette stratégie.

Écrire des scripts de stratégie ou des exécutables personnalisés

Pour obtenir de plus amples renseignements sur la création de scripts ou d'exécutables de stratégies personnalisés, consultez le 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 obtenir de plus amples renseignements, consultez la liste de vérification de l'installation dans Installer le serveur d'administration DRA.
2. Cliquez sur le raccourci SDK dans le groupe de programmes Directory and Resource Administrator.

Stratégie client de délégation et de configuration

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

La stratégie de nommage automatique vous permet de spécifier des règles de nommage automatisées pour des propriétés précises d'une boîte aux lettres. Ces options vous permettent d'établir des conventions de nommage et de générer rapidement des valeurs standard pour le nom complet, le nom de répertoire et les propriétés d'alias. Exchange vous permet de spécifier des chaînes de substitution, telles que `%Premier` et `%Dernier`, pour plusieurs options de nommage automatique.

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, commençant par `-01`, pour 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 mandataire :

`%First`	**Indique la valeur de la propriété Prénom pour le compte d'utilisateur associé.**
`%Last`	Indique la valeur de la propriété Nom pour le compte d'utilisateur associé.
`%Initials`	Indique la valeur de la propriété Initiales pour le compte d'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 de répertoire. Lors de la génération d'adresses de courriel pour les boîtes aux lettres Microsoft Exchange, Exchange ne prend pas en charge les chaînes de génération de mandataires spécifiant la variable `%DirName`.
`%UserName`	Indique la valeur de la propriété Nom d'utilisateur pour le compte d'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 à inclure à partir de cette valeur. Par exemple, `%2First` indique les deux premiers caractères de la propriété **First name** (Prénom) du compte d'utilisateur.

Chaque règle de nommage automatique ou de stratégie de génération de mandataire peut contenir une ou plusieurs chaînes de substitution. Vous pouvez également spécifier des caractères dans chaque règle sous forme de préfixe ou de suffixe pour une chaîne de substitution précise, telle qu'un point et une 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.

Par exemple, considérons la règle de nommage automatique suivante pour la propriété de nom **Afficher** :

```
%First %1Initials. %Last
```

Si la propriété **Prénom** est `Susan`, la propriété **Initiales** est `May` et la propriété **Nom** est `Smith`, Exchange donne à la propriété **Nom d'affichage** la valeur `Susan M. Smith`.

Si la propriété **Prénom** est `Michael`, la propriété **Initiales** est vide et la propriété **Nom** est `Jones`, Exchange donne à la propriété **Nom d'affichage** la valeur `Michael Jones`.

Spécifier une stratégie de nommage automatique de boîte aux lettres

Pour spécifier des options de nommage automatique 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 nommage automatique de boîte aux lettres :

1. Accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies Exchange** > **Nommage d'alias**.
2. Spécifiez les renseignements de génération de nom appropriés.
3. Sélectionnez **Appliquer les règles de nommage d'alias lors des mises à jour des boîtes aux lettres**.
4. Cliquez sur **OK**.

Spécifier une stratégie de nommage de ressources

Pour spécifier des options de nommage de ressources, 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 nommage de ressources :

1. Accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies Exchange** > **Nommage de ressources**.
2. Spécifiez les renseignements de génération de nom de ressources appropriés.
3. Sélectionnez **Appliquer les règles de nommage de ressources lors des mises à jour des boîtes aux lettres**.
4. Cliquez sur **OK**.

Spécifier une politique de nommage d'archives

Pour spécifier des options de nommage d'archives, 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 politique de nommage d'archives :

1. Accédez à **Gestion des stratégies et de l'automatisation** > **Configurer les stratégies Exchange** > **Nommage d'archives**.
2. Spécifiez les renseignements de génération de nom d'archives appropriés pour les comptes d’utilisateurs.
3. Sélectionnez **Appliquer les règles de nommage d'archives lors des mises à jour des boîtes aux lettres**.
4. Cliquez sur **OK**.

14 Automatisation du déclenchement avant et après la tâche

Un déclencheur d'automatisation est une règle associant un script ou un fichier exécutable à une ou plusieurs opérations. Grâce au script ou au fichier exécutable, vous pouvez automatiser un processus de travail existant et établir un pont d'information entre DRA et d'autres référentiels de données. Les déclencheurs d'automatisation vous permettent d'étendre les fonctionnalités et la sécurité offertes par DRA.

Lorsque vous définissez un déclencheur d'automatisation, vous définissez les paramètres de règle, les opérations à associer au déclencheur, le script ou le fichier exécutable à exécuter et, le cas échéant, les ActiveViews ou les administrateurs assistants à associer à ce déclencheur. Ces règles déterminent la façon dont le serveur d'administration applique votre déclencheur.

Vous pouvez également spécifier un script d'annulation ou un exécutable pour votre déclencheur. Un **script d'annulation** vous permet d'annuler vos modifications si l'opération échoue.

DRA prend en charge les scripts VBScript et PowerShell.

Automatisation des processus par le serveur d'administration

Outre l'administration basée sur les règles ActiveView, DRA vous permet d'automatiser vos processus de travail existants et d'exécuter automatiquement les tâches connexes en utilisant des déclencheurs d'automatisation. L'automatisation des processus de travail existants peut vous aider à rationaliser votre entreprise tout en fournissant des services meilleurs et plus rapides.

Lorsque le serveur d'administration exécute l'opération associée à votre déclencheur d'automatisation, il exécute également le script ou l'exécutable du déclencheur. Si votre déclencheur est un déclencheur qui s'exécute avant la tâche, le serveur exécute le script ou l'exécutable avant d'exécuter l'opération. Si votre déclencheur est un déclencheur qui s'exécute après la tâche, le serveur exécute le script ou l'exécutable après avoir exécuté l'opération. Ce processus s'appelle une transaction. Une **transaction** représente le cycle d'implémentation complet pour chaque tâche ou opération effectuée par le serveur d'administration. Une transaction comprend les actions requises pour terminer une opération, ainsi que les actions d'annulation que le serveur d'administration doit effectuer en cas d'échec de l'opération.

Le serveur d'administration entre le statut du déclencheur dans le journal d'audit à chaque exécution d'un déclencheur d'automatisation. Ces entrées de journal enregistrent le code de retour, les opérations associées, les objets sur lesquels il y a eu une action et si le script du déclencheur personnalisé 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 d'autorisations d'administrateur, les stratégies et les déclencheurs d'automatisation ont 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 s'exécutent dans le contexte de sécurité du compte de service. Ainsi, les administrateurs assistants associés au rôle intégré Gérer les stratégies et les déclencheurs d'automatisation peuvent obtenir plus de pouvoir que prévu.

Implémenter un déclencheur d'automatisation

Pour implémenter des déclencheurs d'automatisation, vous devez d'abord écrire des scripts de déclencheur ou des exécutables et disposer des pouvoirs appropriés tels que ceux inclus dans le rôle intégré Gérer les stratégies et les déclencheurs d'automatisation.

Pour implémenter correctement un déclencheur personnalisé, vous devez écrire un script qui s'exécute au cours d'une opération précise (tâche administrative). Vous pouvez associer un exécutable ou un script à l'opération. DRA prend en charge le script PowerShell 32 bits et le script PowerShell 64 bits. Vous pouvez spécifier si DRA applique le déclencheur avant (avant la tâche) ou après (après la tâche) l'exécution d'une opération. Dans le script de déclencheur, vous pouvez définir des messages d'erreur à afficher chaque fois que le déclencheur échoue. Vous pouvez également spécifier un message d'erreur par défaut à l'aide de l'assistant de création de déclencheurs d'automatisation.

Pour obtenir de plus amples renseignements sur l'écriture de déclencheurs personnalisés, l'affichage d'une liste d'opérations d'administration ou l'utilisation de tableaux d'arguments, consultez le *SDK*.

REMARQUE

- Avant d'associer le déclencheur d'automatisation personnalisé à un administrateur assistant et à un ActiveView, vérifiez d'abord que l'administrateur assistant est affecté à cet ActiveView.
- Si le chemin du script du déclencheur personnalisé ou de l'exécutable contient des espaces, insérez des guillemets anglais (") autour du chemin.
- Actuellement, si l'opération **UserSetInfo** est utilisée pour un déclencheur d'automatisation de script et qu'un attribut utilisateur est modifié (exécution du déclencheur), l'attribut modifié n'est pas répercuté dans l'entreprise tant qu'une opération **FindNow** n'a pas été exécutée sur l'objet utilisateur.

Pour implémenter un déclencheur d'automatisation :

1. Écrivez un script de déclencheur ou un fichier exécutable.
2. Connectez-vous à un ordinateur client DRA avec un compte auquel le rôle intégré **Gérer les stratégies et les déclencheurs d'automatisation** est attribué dans le domaine géré.
3. Démarrez la console de délégation et de configuration.
4. Connectez-vous au serveur d'administration primaire.
5. Utilisez Réplication de fichier pour télécharger le fichier de déclenchement sur les serveurs primaire et secondaire de DRA.

   Le chemin du dossier doit déjà exister sur tous les serveurs DRA dans le domaine géré. Ce chemin, y compris le fichier, sera utilisé dans le **Do file path** (chemin du fichier Do) de l'assistant de déclenchement d'automatisation.
6. Dans le volet de gauche, développez **Gestion des stratégies et de l'automatisation**.

7 Cliquez sur **Déclencheur d'automatisation**.

8 Dans le menu Tâches, cliquez sur **Nouveau déclencheur**.

9 Dans chaque fenêtre de l'assistant, spécifiez les valeurs appropriées, puis cliquez sur **Suivant**. Par exemple, vous pouvez associer ce nouveau déclencheur à un ActiveView précis, ce qui permet à DRA d'appliquer ce déclencheur lorsque les administrateurs assistants gèrent les objets regroupé par l'ActiveView.

10 Examinez le résumé, puis cliquez sur **Finish** (Terminer).

IMPORTANT : Si vous avez plus d'un ActiveView configuré pour un déclencheur en ajoutant une virgule entre les ActiveViews, ces ActiveViews seront séparés en deux dans le déclencheur lors de la mise à niveau vers une nouvelle version de DRA et le déclencheur ne s'exécutera pas. Pour que l'opération puisse s'exécuter après la mise à niveau, le déclencheur devra être reconfiguré ou un nouveau déclencheur devra être créé.

---

15 Processus de travail automatisé

Grâce à Workflow Automation, vous pouvez automatiser les processus informatiques en créant des formulaires de processus de travail personnalisés qui s'exécutent en même temps que les processus de travail ou lorsqu'ils sont déclenchés par un événement de processus de travail nommé créé sur le serveur de Workflow Automation. Lorsque vous créez un formulaire de processus de travail, vous définissez les groupes d'administrateurs pouvant afficher le formulaire. La soumission d'un formulaire ou l'exécution du processus de travail dépend des pouvoirs délégués au groupe ou aux groupes inclus lors de la création du formulaire de processus de travail.

Les formulaires de processus de travail sont enregistrés sur le serveur Web lorsqu'ils sont créés ou modifiés. Les administrateurs assistants qui se connectent à la console Web pour ce serveur auront accès aux formulaires en fonction de leur configuration. Les formulaires sont généralement disponibles pour tous les utilisateurs disposant des informations d'identification du serveur Web. Vous limitez l'accès à un formulaire précis en ajoutant des groupes d'administrateurs adjoints, puis en masquant le formulaire aux autres utilisateurs. Pour pouvoir soumettre le formulaire, il faut disposer de l'un des pouvoirs suivants :

- Créer un événement de processus de travail et modifier toutes les propriétés
- Démarrer un processus de travail

Lancer un formulaire de processus de travail : Les processus de travail sont créés dans le serveur de Workflow Automation, qui doit être intégré à DRA à l'aide de la console de délégation et de configuration. Pour enregistrer un nouveau formulaire, l'option **Lancer un processus de travail précis**ou **Déclencher un processus de travail à l'aide d'un événement** doit être configuré dans les propriétés du formulaire. De plus amples renseignements sur ces options sont fournis ci-dessous :

- **Lancer un processus de travail précis :** Cette option répertorie tous les processus de travail disponibles qui sont en production dans le serveur de processus de travail pour DRA. Les processus de travail à remplir dans cette liste doivent être créés dans le dossier `DRA_Workflows` du serveur de Workflow Automation.
- **Déclencher le processus de travail par un événement :** Cette option permet d'exécuter des processus de travail à l'aide de déclencheurs prédéfinis. Les processus de travail avec déclencheurs sont également créés dans le serveur de Workflow Automation.

REMARQUE : Seuls les requêtes de processus de travail configurés avec Lancer un processus de travail précis auront un historique d'exécution qui peut être interrogé dans le volet de recherche principal sous **Tasks** > **Requests** (Tâches > Requêtes).

Vous pouvez modifier une requête existante ou en créer une autre. Pour modifier une requête existante, naviguez vers **Tâches** > **Requêtes**.

Pour créer une requête de processus de travail, accédez à **Administration** > **Personnalisation** > **Requêtes**.

Pour créer une requête, suivez ces étapes de base :

1. Configurez la requête pour exécuter un *processus de travail spécifié* lors de la soumission du formulaire ou configurez la requête pour qu'elle s'exécute lorsqu'elle est déclenchée par un événement *nommé prédéfini*.
2. Choisissez le ou les groupes d'administrateurs assistants inclus dans le processus de travail et activez l'option **Form is hidden** (Le formulaire est masqué) dans l'onglet **General** (Général) pour limiter l'accès aux formulaires à ces utilisateurs.
3. Ajoutez les champs de propriété requis ou des pages de propriété supplémentaires au formulaire.
4. Le cas échéant, créez des gestionnaires personnalisés pour définir plus précisément le processus de travail et son exécution.

   REMARQUE : Les options de gestionnaire personnalisé ne s'affichent pas pour une nouvelle requête de processus de travail tant que la requête n'est pas initialement enregistrée. Pour accéder, créer et modifier des gestionnaires personnalisés, utilisez **Form Properties** (Propriétés du formulaire).

   ---

5. Désactivez l'option **Form is hidden** (Le formulaire est masqué) pour permettre aux utilisateurs d'afficher les formulaires.

Pour des informations sur la configuration du serveur Workflow Automation, consultez la rubrique Configuration du serveur de Workflow Automation et pour la personnalisation des requêtes de processus de travail, consultez la rubrique Personnalisation des formulaires de requête.

VI Auditer et créer des rapports

L’audit des actions des utilisateurs est l’un des aspects les plus importants d’une bonne mise en œuvre de la sécurité. Afin de permettre la vérification et la création de rapport sur les actions de l'administrateur assistant, DRA enregistre toutes les opérations de l'utilisateur dans l'archive des journaux sur l'ordinateur du serveur d'administration. DRA fournit des rapports clairs et complets qui incluent les valeurs d'avant et d'après les événements audités afin que vous puissiez voir exactement ce qui a changé.

16 Activité d'audit

L'audit des activités dans les journaux des événements peut vous aider à isoler, diagnostiquer et résoudre les problèmes de votre environnement. Cette section fournit de l'information pour vous aider à activer et à comprendre la journalisation des événements et à utiliser les archives de journaux.

Journal des événements Windows natif

Afin de permettre la vérification et la création de rapport sur les actions de l'administrateur assistant, DRA enregistre toutes les opérations de l'utilisateur dans l'archive des journaux sur l'ordinateur du serveur d'administration. Les opérations utilisateur incluent toutes les tentatives de modification de définitions telles que la mise à jour de comptes d'utilisateurs, la suppression de groupes ou la redéfinition d'ActiveViews. DRA enregistre également des opérations internes précises telles que l'initialisation du serveur d'administration et les informations relatives au serveur. En plus de la journalisation de ces événements d'audit, DRA enregistre les valeurs avant et après de l'événement, afin que vous puissiez voir exactement ce qui a changé.

DRA utilise un dossier, **NetIQLogArchiveData**, appelé **archive de journal** pour stocker en toute sécurité les données archivées. DRA archive les journaux au fil du temps et supprime ensuite les données plus anciennes pour faire de la place aux données plus récentes par un processus appelé nettoyage.

DRA utilise les événements d'audit stockés dans les fichiers d'archive de journal pour afficher les rapports d'activité détaillés tels que les modifications apportées à un objet au cours d'une période spécifiée. Vous pouvez également configurer DRA pour exporter les informations de ces fichiers d'archivage de journaux vers une base de données SQL Server utilisée par NetIQ Reporting Center pour afficher les rapports de gestion.

DRA consigne toujours des événements d'audit dans l'archive de journal. Vous pouvez également activer ou désactiver la consignation d'événements par DRA dans les journaux d'événements Windows.

Activer et désactiver l'audit du journal des événements Windows pour DRA

Lorsque vous installez DRA, les événements d'audit ne sont pas enregistrés dans le journal des événements Windows par défaut. Vous pouvez activer ce type de journalisation en modifiant une clé de registre.

AVERTISSEMENT : Soyez prudent lorsque vous modifiez votre registre Windows. S'il y a une erreur dans votre registre, votre ordinateur peut devenir non fonctionnel. Si une erreur se produit, vous pouvez restaurer le registre à son état lors du dernier démarrage de votre ordinateur. Pour obtenir de plus amples renseignements, consultez l'aide de l'éditeur de registre Windows.

Pour activer l'audit d'événements :

1. Cliquez sur **Démarrer > Exécuter**.
2. Tapez `regedit` dans le champ **Ouvrir** et cliquez sur **OK**.
3. Développez la clé de registre suivante : `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
4. Cliquez sur **Éditer > Nouveau > Valeur DWORD**.
5. Tapez `IsNTAuditEnabled` comme nom de la clé.
6. Cliquez sur **Éditer > Modifier**.
7. Tapez `1` dans le champ **Données de valeur** et cliquez sur **OK**.
8. Fermez l'éditeur de registre.

Pour désactiver l'audit d'événements :

1. Cliquez sur **Démarrer > Exécuter**.
2. Tapez `regedit` dans le champ **Ouvrir** et 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 **Éditer > Modifier**.
6. Tapez `0` dans le champ **Données de valeur** et cliquez sur **OK**.
7. Fermez l'éditeur de registre.

Assurer l'intégrité des audits

Pour s'assurer que toutes les actions des utilisateurs sont auditées, DRA fournit d'autres méthodes de journalisation lorsque le produit ne peut pas vérifier l'activité de journalisation. Lorsque vous installez DRA, la clé AuditFailsFilePath et son chemin sont ajoutés à votre registre pour garantir les actions suivantes :

- Si DRA détecte que les événements d'audit ne sont plus consignés dans une archive de journal, il enregistre les événements d'audit dans un fichier local sur le serveur d'administration.
- Si DRA ne peut pas consigner les événements d'audit dans un fichier local, il les enregistre dans le journal des événements Windows.
- Si DRA ne peut pas consigner les événements d'audit dans le journal des événements Windows, le produit les consigne dans le journal DRA.
- Si DRA détecte que les événements d'audit ne sont pas consignés, il bloque les opérations ultérieures de l'utilisateur.

Pour activer les opérations d'écriture lorsque l'archive de 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. S'il y a une erreur dans votre registre, votre ordinateur peut devenir non fonctionnel. Si une erreur se produit, vous pouvez restaurer le registre à son état lors du dernier démarrage de votre ordinateur. Pour obtenir de plus amples renseignements, consultez 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** et cliquez sur **OK**.
3. Développez la clé de registre suivante : `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.
4. Cliquez sur **Éditer > Nouveau > Valeur DWORD**.
5. Tapez `AllowOperationsOnAuditFailure` comme nom de la clé.
6. Cliquez sur **Éditer > Modifier**.
7. Tapez 736458265 dans le champ **Données de valeur**.
8. Sélectionnez **Décimal** dans le champ **Base**, puis cliquez sur **OK**.
9. Fermez l'éditeur de registre.

Comprendre les archives de journaux

DRA enregistre les données d'activité de l'utilisateur dans des archives de journaux sur le serveur d'administration. DRA crée chaque jour des partitions d'archives de journaux pour stocker les données collectées et normalisées ce jour-là. DRA utilise la date à l'heure locale sur le serveur d'administration (*AAAMMJJ*) comme convention de nommage pour les partitions quotidiennes d'archives de journaux.

Si vous avez activé le collecteur de rapports de gestion, DRA exporte les données d'archives de journaux vers une base de données SQL Server en tant que source des rapports de gestion DRA.

Initialement, DRA conserve indéfiniment les données de journal dans l'archive de journal par défaut. La taille des archives de journaux peut atteindre une valeur maximale déterminée au moment de l'installation en fonction de l'espace disponible sur le disque dur. Lorsqu'une archive de journal dépasse cette taille maximale, aucun nouvel événement d'audit n'est stocké. Vous pouvez définir une limite de temps de conservation des données. DRA supprime les données les plus anciennes pour laisser de la place aux données les plus récentes grâce à un processus appelé nettoyage. Assurez-vous d'avoir une stratégie de sauvegarde en place avant d'activer le nettoyage. Vous pouvez configurer la période de conservation des archives de journaux à l'aide de l'utilitaire Log Archive Configuration (Configuration d'archives de journaux). Pour obtenir de plus amples renseignements, consultez Modifier les paramètres de nettoyage des archives de journaux.

Utiliser l'utilitaire Log Archive Viewer (Visualisateur d'archives de journaux)

Vous utilisez l'utilitaire Log Archive Viewer pour afficher les données stockées dans les fichiers d'archives de journaux. NetIQ DRA Log Archive Resource Kit (LARK), que vous pouvez choisir d'installer avec DRA, fournit l'utilitaire Log Archive Viewer. Pour obtenir de plus amples renseignements, consultez le *Guide technique de NetIQ DRA Log Archive Resource Kit*.

Sauvegarde des fichiers d'archives de journaux

Un **fichier d'archives de journaux** est une collection de blocs d'enregistrement. Les fichiers d'archives de journaux étant des fichiers binaires compressés situés en dehors d'une base de données physique, vous n'avez pas besoin d'utiliser Microsoft SQL Server Management Studio pour sauvegarder les archives de journaux. Si vous disposez d'un système de sauvegarde de fichiers automatisé, vos fichiers d'archives de journaux sont sauvegardés automatiquement, comme tout autre fichier.

N'oubliez pas les meilleures pratiques suivantes lors de la planification de votre stratégie de sauvegarde :

- Une seule partition est créée chaque jour et contient les données d'événement pour ce jour. Lorsque vous activez le nettoyage, le service d'archivage des journaux nettoie automatiquement les données de ces partitions tous les 90 jours par défaut. La stratégie de sauvegarde doit prendre en compte le calendrier de nettoyage pour déterminer la fréquence des sauvegardes. Lorsque les partitions d'archives du journal sont nettoyées, 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 obtenir de plus amples renseignements, consultez Modifier les paramètres de nettoyage des archives de journaux.
- Vous ne devez sauvegarder les partitions qu'après leur fermeture. Dans des conditions normales, une partition est fermée dans les 2 heures après minuit le lendemain.
- 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 des partitions d'archives de journaux pour les rapports, assurez-vous que les archives de journaux sauvegardées sont conservées ou peuvent être restaurées dans leur format d'origine.
- Lors de la configuration de votre processus de sauvegarde des fichiers d'archives de journaux, NetIQ vous recommande d'exclure les sous-dossiers `index_data` et `CubeExport` situés dans le dossier d'archivage de journaux principal. Ces sous-dossiers contiennent des données temporaires et ne doivent pas être sauvegardés.

Modifier les 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 de sauvegarde régulières pour vos fichiers d'archives de journaux, vous devez activer le nettoyage d'archives de journaux pour économiser de l'espace sur le disque. Vous pouvez modifier le nombre de jours qui doit s'écouler avant le nettoyage des partitions d'archives de journaux à l'aide de l'utilitaire Log Archive Configuration.

Pour changer le nombre de jours qui doit s'écouler avant que les partitions d'archives de journaux ne soient nettoyées :

1. Connectez-vous au serveur d'administration à l'aide d'un compte membre du groupe Administrateurs locaux.
2. Démarrez **Log Archive Configuration** (Configuration des archives de journaux) dans le groupe de programmes d'administration de NetIQ.
3. Cliquez sur **Paramètres du serveur d'archives de journaux**.

4 *Si vous souhaitez activer le nettoyage des partitions,* définissez la valeur du champ **Nettoyage des partitions activé** sur Vrai.

5 Entrez le nombre de jours pendant lesquels vous souhaitez conserver les partitions d'archives de journaux avant le nettoyage dans le champ **Nombre de jours avant le nettoyage**.

6 Cliquez sur **Appliquer**.

7 Cliquez sur **Oui**.

8 Cliquez sur **Fermer**.

9 Recherchez le chemin d'accès au dossier *NetIQLogArchiveData*\<*Nom de la partition*>, généralement : `C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData`

Si l'attribut « Le fichier est prêt pour l'archivage » des fichiers ou des dossiers des partitions spécifiées n'est pas coché (dans les propriétés de fichier ou de dossier), vous devez éditer le fichier CONFIG pour permettre le nettoyage des archives de journaux. Pour comprendre pourquoi cet attribut peut ou non être vérifié, reportez-vous à la section **Informations complémentaires** de l'article de la base de connaissance *Comment configurer la période de conservation des données d'archives des journaux DRA*.

Si la valeur est	
Vérifié	Cliquez sur **Oui** dans le message de confirmation pour redémarrer le service d'archives des journaux de NetIQ Security Manager. **REMARQUE :** Si vous modifiez un paramètre d'archives de journaux, vous devez redémarrer le service d'archives de journaux pour que la modification soit prise en compte.
Non vérifié	Cliquez sur **Non** dans le message de confirmation. Veuillez consulter la rubrique Pour permettre au serveur d'archives de journaux DRA de nettoyer des données non archivées :.

Pour permettre au serveur d'archives de journaux DRA de nettoyer des 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`, puis localisez la ligne `<Property name="GroomUnarchivedData" value="false" />`.

3 Remplacez « `false` » par « `true` » et enregistrez le fichier.

4 Redémarrez le service d'archives de journaux NetIQ DRA.

REMARQUE : Si vous modifiez un paramètre d'archives de journaux, vous devez redémarrer le service d'archives de journaux pour que la modification soit prise en compte.

17 Création de rapports

Cette section fournit des informations permettant de comprendre et d'activer les rapports DRA, la collecte de données de rapports, la collecte et la création de rapports ActiveView Analyzer et d'accéder aux rapports intégrés.

DRA désactive les fonctions et les rapports que votre licence ne prend pas en charge. Vous devez également disposer des pouvoirs appropriés pour exécuter et afficher les rapports. Par conséquent, vous pouvez ne pas avoir accès à certains rapports.

Les rapports détaillés d'activité sont disponibles dans la console de délégation et de configuration dès que vous installez DRA afin de fournir les derniers détails sur les changements apportés à votre réseau.

- « Gérer la collecte de données pour la création de rapports » page 181
- « Rapports intégrés » page 183

Gérer la collecte de données pour la création de rapports

DRA Reporting utilise deux méthodes de création de rapports vous permettant de visualiser les dernières modifications apportées à votre environnement ainsi que de collecter et d'examiner les définitions de compte d'utilisateur, de groupe et de ressource de votre domaine.

Rapports détaillés d'activité

Accessibles à l'aide de la console de délégation et de configuration, ces rapports fournissent des informations en temps réel sur les changements des objets dans votre domaine.

Rapports de gestion de DRA

Accessibles à l'aide de NetIQ Reporting Center (Reporting Center), ces rapports fournissent des informations sur l'activité, la configuration et la synthèse 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'une période donnée à l'aide des rapports détaillés d'activité. Vous pouvez également afficher un graphique indiquant le nombre d'événements dans chaque domaine géré au cours d'une période précise à l'aide des rapports de gestion. La création de rapports vous permet également d'afficher des détails sur le modèle de sécurité de DRA tels que les définitions de groupes ActiveView et Administrateurs assistants.

Les rapports de gestion de DRA peuvent être installés et configurés en tant que fonctionnalité facultative et sont affichés dans 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 une planification que vous définissez. Lorsque vous vous connectez à cette base de données dans Reporting Center, vous avez accès à plus de 60 rapports intégrés :

- Rapports d'activité indiquant l'auteur et le moment de chaque événement

- Rapports de configuration indiquant l'état d'AD ou de DRA à un moment donné
- Rapports de synthèse indiquant le volume d'activité

Pour obtenir de plus amples renseignements sur la configuration de la collecte de données pour les rapports de gestion, consultez le Configurer la création des rapports.

Afficher l'état des collecteurs

Vous pouvez afficher les détails de chaque collecteur de données dans l'onglet État des collecteurs.

Pour afficher l'état des collecteurs :

1. Développez **Gestion de la configuration**, puis cliquez sur **Mettre à jour la configuration du service de création des rapports**.
2. Dans l'onglet État des collecteurs, cliquez sur chaque entrée pour afficher des informations supplémentaires sur la collecte de données telles que la date et l'information sur la réussite ou non de la dernière collecte de données.
3. Si aucune donnée n'apparaît dans la liste Serveur, cliquez sur **Rafraîchir**.

Activer la création de rapports et la collecte de données

Après avoir installé les composants de DRA Reporting, activez et configurez la collecte de données de rapport pour accéder aux rapports de Reporting Center.

Pour activer la création des rapports et la collecte des données :

1. Accédez à **Gestion de la configuration** > **Mettre à jour la configuration du service de création des rapports**.
2. Sur l'onglet SQL Server, sélectionnez **Activer la prise en charge de DRA Reporting**.
3. Cliquez sur **Parcourir** dans le champ Nom du serveur et sélectionnez l'ordinateur sur lequel SQL Server est installé.
4. Sous l'onglet Informations d'identification, spécifiez les informations d'identification appropriées à utiliser pour les interactions avec SQL Server.
5. S'il s'agit du même compte que celui qui peut être utilisé pour créer la base de données et initialiser le schéma, cochez la case Utiliser les informations d'identification ci-dessus pour créer une base de données et initialiser le schéma de base de données.
6. Si vous souhaitez spécifier un autre compte pour la création d'une base de données, dans l'onglet Informations d'identification de l'administrateur, spécifiez ce compte d’utilisateur et son mot de passe.
7. Cliquez sur **OK**.

Pour obtenir de plus amples renseignements sur la configuration de collecteurs précis, consultez Configurer la création des rapports.

Rapports intégrés

Les rapports intégrés vous permettent de générer des rapports sur les modifications, les listes et les détails sur les objets. Ces rapports ne font pas partie des services de création de rapports de DRA et aucune configuration n'est requise pour activer les rapports d'historique des modifications intégrés. Référez-vous aux rubriques de cette section pour savoir comment accéder à ces rapports.

REMARQUE : Les rapports sur l'historique des modifications peuvent également être consultés pour des événements extérieurs à DRA lorsque DRA est intégré à Change Guardian. Pour de plus amples renseignements sur ces types de rapports et la configuration d'un serveur Change Guardian, consultez la rubrique « Configurer l'historique des modifications unifié » page 115.

Créer des rapports sur les modifications d'objet

Vous pouvez afficher les informations de modification en temps réel des objets de vos domaines en générant des rapports d'activité détaillés. Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'une période donnée. Vous pouvez également exporter et imprimer des rapports d'activité détaillés.

Pour créer un rapport sur les modifications d'objet :

1. Trouvez les objets qui correspondent à vos critères.
2. Cliquez avec le bouton droit de la souris sur un objet, puis sélectionnez **Création de rapports > Modifications apportées à NomObjet** ou **Création de rapports > Modifications apportées par NomObjet**.
3. Sélectionnez les dates de début et de fin pour spécifier les modifications à afficher.
4. *Si vous souhaitez modifier le nombre de lignes à afficher*, entrez un nombre supérieur à la valeur par défaut 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 utilisez la valeur par défaut de 250 lignes à afficher, vous pouvez afficher jusqu'à 750 lignes dans le rapport.

   ---

5. *Si vous voulez inclure uniquement des serveurs d'administration précis dans le rapport*, sélectionnez **Restreindre la requête à ces serveurs DRA** et saisissez le ou les noms de serveur que vous voulez inclure dans le rapport. Séparez plusieurs noms de serveur par des virgules.
6. Cliquez sur **OK**.

Créer des rapports sur les listes d'objets

Vous pouvez exporter ou imprimer des données à partir de listes d'objets. Grâce à cette fonctionnalité, vous pouvez rapidement et facilement créer des rapports et distribuer des informations générales sur vos objets gérés.

Lorsque vous exportez une liste d'objets, vous pouvez spécifier l'emplacement, le nom et le format du fichier. DRA prend en charge les formats HTML, CSV et XML, ce qui vous permet d'exporter ces informations vers des applications de base de données ou de publier des résultats de liste sur une page Web.

REMARQUE : Vous pouvez également sélectionner plusieurs éléments dans une liste, puis les copier dans une application de texte telle que Bloc-notes.

Pour créer un rapport sur les listes d'objets :

1. Trouvez les objets qui correspondent à vos critères.
2. Pour exporter cette liste d'objets, cliquez sur **Exporter la liste** dans le menu Fichier.
3. Pour imprimer cette liste d'objets, cliquez sur **Imprimer la liste** dans le menu Fichier.
4. Spécifiez les informations appropriées pour enregistrer ou imprimer cette liste.

Créer des rapports sur les détails d'objets

Vous pouvez exporter ou imprimer des données à partir d'onglets de détails répertoriant les attributs d'objet, tels que les adhésions à un groupe. Grâce à cette fonctionnalité, vous pouvez rapidement et facilement créer des rapports et distribuer les informations fréquemment demandées sur des objets précis.

Lorsque vous exportez un onglet de détails d'objets, vous pouvez spécifier l'emplacement, le nom et le format du fichier. DRA prend en charge les formats HTML, CSV et XML, ce qui vous permet d'exporter ces informations vers des applications de base de données ou de publier des résultats de liste sur une page Web.

Pour créer un rapport sur les détails d'objets :

1. Trouvez l'objet qui correspond à vos critères.
2. Dans le menu Afficher, cliquez sur **Détails**.
3. Dans le volet Détails, sélectionnez l'onglet approprié.
4. Pour exporter ces détails d'objets, cliquez sur **Exporter la liste des détails** dans le menu Fichier.
5. Pour imprimer ces détails d'objets, cliquez sur **Imprimer la liste des détails** dans le menu Fichier.
6. Spécifiez les informations appropriées pour enregistrer ou imprimer cette liste.

VII Fonctionnalités supplémentaires

Les affectations de groupe temporaires, les groupes dynamiques, l'horodatage des événements et le mot de passe de récupération BitLocker sont des fonctionnalités supplémentaires de DRA que vous pouvez utiliser dans votre environnement d'entreprise.

18 Affectations de groupe temporaires

DRA vous permet de créer des affectations de groupe temporaires offrant aux utilisateurs autorisés un accès temporaire aux ressources. Les administrateurs assistants peuvent utiliser des affectations de groupe temporaires pour affecter des utilisateurs à un groupe cible pour une période donnée. À la fin de la période, DRA supprime automatiquement les utilisateurs du groupe.

Le rôle Gérer les affectations de groupe temporaires confère aux administrateurs assistants le pouvoir de créer et de gérer des affectations de groupe temporaires.

Les administrateurs assistants ne peuvent consulter que les affectations de groupe temporaires pour lesquels l'administrateur assistant a le pouvoir d'ajouter ou de retirer des membres.

Utilisez les pouvoirs suivants pour déléguer la création et la gestion des affectations de groupe temporaires :

- Créer des affectations de groupe temporaires
- Supprimer des affectations de groupe temporaires
- Modifier des affectations de groupe temporaires
- Rétablir l'état d'affectation de groupe temporaire
- Afficher des affectations de groupe temporaires
- Ajouter un objet au groupe
- Retirer un objet du groupe

Le groupe cible et les utilisateurs doivent appartenir au même ActiveView.

REMARQUE

- Vous ne pouvez pas créer d'affectation de groupe temporaire pour un utilisateur qui est déjà membre du groupe cible. Si vous essayez de créer une affectation de groupe temporaire pour un utilisateur qui est déjà membre du groupe cible, DRA affiche un message d'avertissement et ne vous y autorise pas.
- Si vous créez une affectation de groupe temporaire pour un utilisateur qui n'est pas membre du groupe cible, DRA supprime l'utilisateur du groupe à l'expiration de l'affectation de groupe temporaire.

Exemple :

Robert, le responsable des ressources humaines, informe Jean, un administrateur du service d'assistance, que l'entreprise a engagé un employé temporaire nommé Jean pour une période déterminée afin de mener à bien un projet. Jean fait ce qui suit :

- Il crée une affectation de groupe temporaire (AGT)
- Il ajoute un groupe de RH pour les employés temporaires à l'AGT

- Il ajoute Joseph comme membre du groupe des employés temporaires
- Il fixe la durée de l'AGT à un mois (du 07/03/2019 au 08/02/2019)

Résultat attendu :

Par défaut, à l'expiration de l'AGT, l'adhésion de Joseph sera retirée du groupe des ressources humaines. Cette AGT restera disponible pendant sept jours, à moins que Jean n'ait choisi l'option **Keep this temporary group assignment for future use** (Conserver cette affectation de groupe temporaire pour une utilisation future).

Pour en savoir plus sur la création et l'utilisation des affectations de groupe temporaires, consultez le *Guide de l'utilisateurde DRA*.

19 Groupes dynamiques DRA

Un groupe dynamique est un groupe dont l'adhésion change en fonction d'un ensemble de critères que vous configurez dans les propriétés du groupe. Vous pouvez rendre n'importe quel groupe dynamique ou supprimer le filtre dynamique de tout groupe pour lequel il est configuré. Cette fonctionnalité permet également d'ajouter des membres du groupe à une liste statique ou à une liste d'exclusion. Les membres des groupes figurant sur ces listes ne seront pas touchés par les critères dynamiques.

Si un groupe dynamique redevient un groupe normal, tous les éléments de la liste des membres statiques seront ajoutés aux membres du groupe et les membres exclus ainsi que les filtres dynamiques seront ignorés. Vous pouvez transformer des groupes existants en groupes dynamiques ou créer un nouveau groupe dynamique dans la console de délégation et de configuration et dans la console Web.

Pour rendre un groupe dynamique :

1. Localisez le groupe dans la console applicable.
   - Pour la console de délégation et de configuration : accédez à **Tous mes objets gérés** > **Trouver maintenant**.

     REMARQUE : Pour activer le Générateur de requêtes, cliquez sur **Parcourir** et sélectionnez un domaine, un conteneur ou une unité organisationnelle.
   - Pour la console Web : accédez à **Gestion** > **Rechercher**.
2. Ouvrez les propriétés du groupe, puis sélectionnez **Rendre le groupe dynamique** dans l'onglet Filtre des membres dynamiques.
3. Ajoutez les attributs virtuels et LDAP souhaités pour filtrer l'adhésion à un groupe.
4. Ajoutez les membres statiques ou exclus souhaités au groupe dynamique et appliquez vos modifications.

Pour créer un nouveau groupe dynamique :

- **Console de délégation et de configuration :**cliquez avec le bouton droit de la souris sur le domaine ou le sous-nœud dans Tous mes objets gérés, puis sélectionnez **Nouveau** > **Groupe dynamique**.
- **Console Web :** accédez à **Gestion** > **Créer** > **Nouveau groupe dynamique**.

20 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) à l'aide d'informations spécifiques de DRA, y compris l'identité de la personne qui a effectué l'opération. Cela force AD à générer un événement d'audit pour ce changement d'attribut.

Par exemple, supposons que vous ayez sélectionné l'attribut `extensionAttribute1` en tant qu'attribut d'utilisateur et que l'audit AD DS soit configuré. Chaque fois qu'un administrateur assistant met à jour un utilisateur, DRA met à jour l'attribut `extensionAttribute1` avec les données d'horodatage des événements. Cela signifie que, parallèlement aux événements AD DS pour chaque attribut mis à jour par l'administrateur assistant (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 identique pour chaque attribut modifié lors de la mise à jour de l'utilisateur. C'est ainsi que les applications peuvent associer les données d'horodatage des événements aux autres attributs mis à jour.

Pour connaître les étapes permettant d'activer l'horodatage d'événements, reportez-vous à la rubrique Activer l'horodatage d'événements dans le DRA.

Pour un exemple d'événement AD DS et de types d'opération pris en charge, consultez les rubriques ci-dessous :

- « L'événement AD DS » page 191
- « Opérations prises en charge » page 192

L'événement AD DS

Vous verrez un événement comme celui-ci dans le journal des événements de sécurité Windows chaque fois que DRA exécute une opération prise en charge.

Nom LDAP affiché :	**`extensionAttribute1`**
Syntaxe (OID) : 2.5.5.12	2.5.5.12
Valeur :	<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/ KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLWhbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=

La valeur de l'événement se compose de deux parties. La première est une chaîne XML contenant les données d'horodatage des événements. La deuxième est une signature des données pouvant être utilisée pour vérifier que les données ont été générées par DRA. Pour valider la signature, une application doit avoir la clé publique pour la signature.

La chaîne XML comprend les informations suivantes :

Utilisateur	L'administrateur assistant qui a effectué l'opération
Sid	Le SID de l'administrateur assistant qui a effectué l'opération
Tid	L'ID de transaction d'audit DRA pour garantir que chaque événement est unique
SubjectUserSid	Le SID du compte de service DRA ou du compte d'accès qui a réellement mis à jour AD
ObjectDN	Le nom distinctif de l'objet qui a été modifié

Opérations prises en charge

Utilisateur	◆ Créer ◆ Renommer ◆ Modifier ◆ Cloner
Groupe	◆ Créer ◆ Renommer ◆ Modifier ◆ Cloner
Contact	◆ Créer ◆ Renommer ◆ Modifier ◆ Cloner
Ordinateur	◆ Créer ◆ Activer ◆ Désactiver ◆ Renommer ◆ Modifier
Unité organisationnelle	◆ Créer ◆ Renommer ◆ Cloner

21 Mot de passe de récupération BitLocker

Microsoft BitLocker stocke ses mots de passe de récupération dans Active Directory. À l'aide de la fonctionnalité de récupération DRA BitLocker, vous pouvez déléguer des pouvoirs aux administrateurs assistants pour rechercher et récupérer les mots de passe BitLocker perdus pour les utilisateurs finaux.

IMPORTANT : Avant d'utiliser la fonction Mot de passe de récupération BitLocker, assurez-vous que votre ordinateur est affecté à un domaine et que BitLocker est activé.

Afficher et copier un mot de passe de récupération BitLocker

Si le mot de passe BitLocker d'un ordinateur est perdu, il peut être réinitialisé en utilisant la clé de récupération du mot de passe depuis les 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 la structure de l'arborescence.
2. Dans le nœud **Account and Resource Management**, accédez à **All My Managed Objects** > **Domain** > **Computers** (Account and Resource Management, accédez à Tous mes objets gérés > Domaine > Ordinateurs).
3. Dans la liste des ordinateurs, cliquez avec le bouton droit de la souris sur l'ordinateur approprié, puis sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Mot de passe de récupération BitLocker** pour afficher le mot de passe de récupération BitLocker.
5. Cliquez avec le bouton droit de la souris sur le mot de passe de récupération BitLocker, puis cliquez sur **Copier**; collez le texte dans un fichier texte ou une feuille de calcul.

Trouver un mot de passe de récupération

Si le nom d'un ordinateur a été modifié, le mot de passe de récupération doit être recherché dans le domaine en utilisant les huit premiers caractères de l'ID de mot de passe.

Pour trouver un mot de passe de récupération en utilisant un ID de mot de passe :

1. Lancez la **console de délégation et de configuration** et développez la structure de l'arborescence.
2. Dans le nœud **Account and Resource Management**, accédez à **Tous mes objets gérés**, cliquez avec le bouton droit de la souris sur **Domaine géré**, puis cliquez sur **Trouver le mot de passe de récupération BitLocker**.

Pour trouver les huit premiers caractères du mot de passe de récupération, consultez la rubrique Afficher et copier un mot de passe de récupération BitLocker.

3 Dans la page **Trouver le mot de passe de récupération BitLocker**, collez les caractères copiés dans le champ de recherche, puis cliquez sur **Rechercher**.

22 Corbeille

Vous pouvez activer ou désactiver la Corbeille pour chaque domaine Microsoft Windows ou pour les objets au sein de ces domaines, ce qui permet de contrôler la gestion des comptes au sein de votre entreprise. Si vous activez la Corbeille, puis supprimez un compte d'utilisateur, un groupe, un groupe de distribution dynamique, un groupe dynamique, une boîte aux lettres de ressources, 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 vers la Corbeille, le compte ne s'affiche pas dans les ActiveView auxquelles il appartenait. Si vous supprimez un compte d'utilisateur, un groupe, un contact ou un compte d'ordinateur lorsque la Corbeille est désactivée, le serveur d'administration supprime définitivement le compte sélectionné. Vous pouvez désactiver une Corbeille contenant des comptes précédemment supprimés. Cependant, une fois la Corbeille désactivée, ces comptes ne sont plus disponibles dans le nœud Corbeille.

Affecter des pouvoirs de Corbeille

Pour permettre à un administrateur assistant de supprimer définitivement des comptes du nœud Tous mes objets gérés ainsi que de la Corbeille, attribuez le pouvoir correspondant dans la liste suivante :

- Supprimer définitivement un compte d'utilisateur
- Supprimer définitivement un groupe
- Supprimer définitivement un ordinateur
- Supprimer définitivement un contact
- Supprimer définitivement un groupe de distribution dynamique
- Supprimer définitivement un groupe dynamique
- Supprimer définitivement une boîte aux lettres de ressources

Si plusieurs serveurs d'administration gèrent différentes sous-arborescences dans le même domaine Microsoft Windows, vous pouvez utiliser la Corbeille pour afficher tout compte supprimé de ce domaine, quel que soit le serveur d'administration qui gère ce compte.

Utiliser la Corbeille

Utilisez la Corbeille pour supprimer définitivement des comptes, restaurer des comptes ou afficher les propriétés des comptes supprimés. Vous pouvez également rechercher des comptes précis et surveiller le nombre de jours pendant lesquels un compte supprimé rester dans la Corbeille. Un onglet Corbeille est également inclus dans la fenêtre Propriétés d'un domaine sélectionné. Dans cet onglet, vous pouvez désactiver ou activer la Corbeille pour l'ensemble du domaine ou pour des objets précis; vous pouvez également planifier un nettoyage de la Corbeille.

Utilisez les options **Restaurer tout** ou **Vider la Corbeille** pour restaurer ou supprimer rapidement et facilement ces comptes.

Lorsque vous restaurez un compte, DRA le rétablit, y compris toutes les autorisations, les délégations de pouvoir, les attributions de stratégies, les adhésions aux groupes et les adhésions aux ActiveView. Si vous supprimez définitivement un compte, DRA supprime ce compte d'Active Directory.

Pour garantir une suppression sécurisée des comptes, seuls les administrateurs assistants disposant des pouvoirs suivants peuvent supprimer définitivement les comptes de la Corbeille :

- Supprimer définitivement un compte d'utilisateur
- Supprimer l'utilisateur de la Corbeille
- Supprimer définitivement un compte de groupe
- Supprimer le groupe de la Corbeille
- Supprimer définitivement un compte d'ordinateur
- Supprimer l'ordinateur de la Corbeille
- Supprimer définitivement un compte de contact
- Supprimer le contact de la Corbeille
- Supprimer définitivement un groupe de distribution dynamique
- Supprimer un groupe de distribution dynamique de la Corbeille
- Supprimer définitivement un groupe dynamique
- Supprimer un groupe dynamique de la Corbeille
- Supprimer définitivement une boîte aux lettres de ressources
- Supprimer une boîte aux lettres de ressources de la Corbeille
- Afficher tous les objets de la Corbeille

Pour restaurer un compte à partir de la Corbeille, les administrateurs assistants doivent disposer des pouvoirs suivants dans l'unité organisationnelle contenant le compte :

- Restaurer un utilisateur de la Corbeille
- Restaurer un groupe de la Corbeille
- Restaurer un groupe de distribution dynamique de la Corbeille
- Restaurer un groupe dynamique de la Corbeille
- Restaurer une boîte aux lettres de ressources de la Corbeille
- Restaurer un ordinateur de la Corbeille
- Restaurer un contact de la Corbeille
- Afficher tous les objets de la Corbeille

REMARQUE

- Si vous supprimez un compte d'administrateur assistant et le placez dans la Corbeille, DRA continue d'afficher les attributions ActiveView et de rôle pour ce compte. Au lieu d'afficher le nom du compte d'administrateur assistant supprimé, DRA affiche l'identificateur de sécurité (SID). Vous pouvez supprimer ces attributions avant de supprimer définitivement le compte d'administrateur assistant.

- DRA supprime le répertoire privé après avoir supprimé le compte d’utilisateur de la Corbeille.
- Si vous supprimez un utilisateur disposant d'une licence Office 365, le compte d'utilisateur est placé dans la Corbeille et la licence est supprimée. Si vous restaurez ultérieurement le compte d’utilisateur, la licence Office 365 sera également restaurée.

VIII Personnalisation du client

Vous pouvez personnaliser le client de délégation et de configuration et la console Web. Le client de délégation et de configuration requiert un accès physique ou à distance et des identifiants de compte. La console Web quant à elle nécessite l'URL du serveur et les informations d'identification du compte pour se connecter à partir d'un navigateur Web.

23 Client de délégation et de configuration

Cette section contient de l'information qui vous aidera à personnaliser le client de délégation et de configuration. Grâce à cette section, vous pourrez notamment créer des pages de propriétés personnalisées, créer des outils personnalisés dans DRA pouvant être exécutés sur les ordinateurs clients et les serveurs du réseau. Vous pourrez également personnaliser la configuration de l'interface utilisateur.

Personnaliser les pages des propriétés

Vous pouvez personnaliser et étendre la console de délégation et de configuration en implémentant des propriétés personnalisées. Les propriétés personnalisées vous permettent d'ajouter des comptes propriétaires et des propriétés d'unités organisationnelles, telles que des extensions de schéma et des attributs virtuels Active Directory, à des assistants et à des fenêtres de propriétés en particulier. Ces extensions vous permettent de personnaliser DRA pour répondre à vos besoins particuliers. À l'aide de l'assistant Nouvelle page personnalisée de la console de délégation et de configuration, vous pouvez créer rapidement et facilement une page personnalisée pour étendre l'interface utilisateur appropriée.

Si vos administrateurs assistants ont besoin de pouvoirs uniques pour gérer la page personnalisée en toute sécurité, vous pouvez également créer et déléguer des pouvoirs personnalisés. Par exemple, vous pouvez décider de limiter la gestion des comptes d'utilisateurs aux propriétés de la page personnalisée uniquement. Pour obtenir de plus amples renseignements, consultez Mise en œuvre des 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 pour exposer les attributs, les extensions de schéma et les attributs virtuels Active Directory dans la console de délégation et de configuration.

Lorsque vous sélectionnez un attribut, une extension de schéma ou un attribut virtuel Active Directory pris en charge, vous pouvez utiliser des pages personnalisées comme indiqué ci-après :

- Limiter la gestion des administrateurs assistants à un ensemble bien défini et contrôlé de propriétés. Cet ensemble de propriétés peut inclure des *propriétés standard* et des extensions de schéma. Les propriétés standard sont des attributs Active Directory exposés par défaut par la console Accounts and Resource Management.
- Exposer les attributs Active Directory autres que les propriétés standard gérées par DRA.
- Étendre la console de délégation et de configuration pour y inclure des propriétés propriétaires.

Vous pouvez également configurer la façon 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 des pages personnalisées à tous les objets gérés applicables de votre entreprise. Par exemple, si vous créez une page personnalisée pour ajouter des extensions de schéma Active Directory à la fenêtre Propriétés du groupe, 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 plus d'une page personnalisée.

Vous ne pouvez pas désactiver des fenêtres ou des onglets individuels dans l'interface utilisateur existante. Un administrateur assistant peut sélectionner une valeur de propriété à l'aide de l'interface utilisateur par défaut ou d'une page personnalisée. DRA applique la dernière valeur sélectionnée pour une propriété.

DRA fournit un suivi d'audit complet pour les propriétés personnalisées. DRA enregistre les données suivantes dans le journal des événements de l'application :

- modification des pages personnalisées

  IMPORTANT : Vous devez configurer manuellement l'audit du journal des applications Windows. Pour en savoir plus, consultez Activer et désactiver l'audit du journal des événements Windows pour DRA.

- création et suppression de pages personnalisées
- extension de schéma exposée, attributs Active Directory et attributs virtuels inclus sur des pages personnalisées

Vous pouvez également exécuter des rapports d'activité de modification pour surveiller les modifications de configuration des propriétés personnalisées.

Implémentez et modifiez des pages personnalisées à partir du serveur d'administration primaire. Au cours de la synchronisation, DRA réplique les configurations de page personnalisées sur l'ensemble multimaître. Pour obtenir de plus amples renseignements, consultez Configurer l'ensemble multimaître.

Pages personnalisées prises en charge

Chaque page personnalisée que vous créez vous 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 pages personnalisées suivants :

Page utilisateur personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés de l'utilisateur
- assistant de création d'utilisateur
- assistant de clonage d'utilisateur

Page de groupe personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés du groupe
- assistant de création de groupe
- assistant de clonage de groupe

Page d'ordinateur personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés de l'ordinateur
- assistant de création d'ordinateur

Page de contact personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés du contact
- assistant de création de contact
- assistant de clonage de contact

Page d'unité organisationnelle personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés d'unité organisationnelle
- assistant de création d'unité organisationnelle
- assistant de clonage d'unité organisationnelle

Page de boîte aux lettres de ressources personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés de la boîte aux lettres de ressources
- assistant de création de boîte aux lettres de ressources
- assistant de clonage de boîte aux lettres de ressources

Page de groupe de distribution dynamique personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés du groupe de distribution dynamique

- assistant de création de groupe de distribution dynamique
- assistant de clonage de groupe de distribution dynamique

Page de boîte aux lettres partagée personnalisée

Vous permet d'afficher des onglets personnalisés dans les fenêtres suivantes :

- fenêtre Propriétés de la boîte aux lettres partagée
- assistant de création de boîte aux lettres partagée
- assistant de création de boîte aux lettres clonée

Contrôles de propriétés personnalisées 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 administrateur assistant entre la valeur de la propriété. Par exemple, vous pouvez spécifier les valeurs de propriété de différentes façons :

- définir des plages de valeurs précises
- définir les valeurs de propriété par défaut
- indiquer si une propriété est requise

Vous pouvez également configurer le contrôle de l'interface utilisateur pour afficher des informations ou des instructions propriétaires. Par exemple, si vous définissez une plage précise pour un numéro d'identification d'employé, vous pouvez configurer l'étiquette de contrôle de la zone de texte pour afficher **Spécifier le numéro d'identification d'employé (001 à 100)**.

Chaque contrôle d'interface utilisateur prend en charge un seul attribut, une extension de schéma ou un attribut virtuel Active Directory. 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	Contrôle de l'agenda
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

Utiliser des pages personnalisées

Vous pouvez créer des pages personnalisées à partir du nœud Extensions de l'interface utilisateur. Une fois qu'une page est créée, vous pouvez ajouter ou supprimer des propriétés d'attribut AD et désactiver ou supprimer la page. Pour chaque personnalisation que vous souhaitez configurer, créez

une page personnalisée et attribuez le pouvoir ou le rôle approprié à l'administrateur assistant. Tenez compte des meilleures pratiques ci-dessous lorsque vous commencez à utiliser des 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 NetIQ Administration Service sur chaque serveur d'administration.
2. Identifiez le type de page personnalisée que vous souhaitez créer et les propriétés que vous souhaitez que les administrateurs assistants gèrent avec cette page personnalisée. Vous pouvez sélectionner n'importe quel attribut Active Directory, y compris les attributs d'extension de schéma et les attributs des assistants DRA existants ainsi que des fenêtres de propriété ou tout autre attribut virtuel que vous créez. Cependant, chaque page personnalisée nécessite un ensemble unique de propriétés. Vous ne pouvez pas ajouter un attribut Active Directory à plus d'une page personnalisée.

   Les pages personnalisées ne remplacent pas l'interface utilisateur existante. Pour obtenir de plus amples renseignements, consultez Fonctionnement des pages de propriétés personnalisées et Pages personnalisées prises en charge.
3. Déterminez comment vous voulez que les administrateurs assistants spécifient ces propriétés. Par exemple, vous pouvez vouloir limiter une propriété spécifiée à trois valeurs possibles. Vous pouvez définir un contrôle d'interface utilisateur approprié pour chaque propriété. Pour obtenir de plus amples renseignements, consultez Contrôles de propriétés personnalisées pris en charge.
4. Déterminez si vos administrateurs assistants ont besoin d'informations ou d'instructions propriétaires pour gérer correctement ces propriétés. Par exemple, déterminez si Active Directory requiert une syntaxe pour la valeur de la 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. Par exemple, vous pouvez ajouter une page personnalisée utilisateur à l'assistant de création d'utilisateur et à la fenêtre Propriétés de l'utilisateur.
7. Utilisez l'onglet Assignations du volet d'informations de l'administrateur assistant pour vérifier que vos administrateurs assistants ont les pouvoirs appropriés pour le bon ensemble d'objets. Si vous avez créé des pouvoirs personnalisés pour cette page personnalisée, déléguez ces pouvoirs aux administrateurs assistants appropriés.
8. Déterminez si vos administrateurs assistants ont besoin d'un pouvoir personnalisé pour gérer les propriétés de cette page. Par exemple, si vous ajoutez une page personnalisée à la fenêtre Propriétés de l'utilisateur, la délégation du pouvoir *Modifier toutes les propriétés de l'utilisateur* peut donner trop de pouvoir à un administrateur assistant. Créez tous les pouvoirs personnalisés nécessaires pour implémenter votre page personnalisée. Pour obtenir de plus amples renseignements, consultez Mise en œuvre des pouvoirs personnalisés.
9. En utilisant vos réponses aux étapes ci-dessus, créez les pages personnalisées appropriées.
10. Distribuez des informations sur les pages de propriétés personnalisées que vous avez implémentées aux administrateurs assistants appropriés tels que ceux du service d'assistance à la clientèle.

Pour implémenter la personnalisation des propriétés, vous devez disposer des pouvoirs inclus dans le rôle Administration DRA. Pour obtenir de plus amples renseignements sur les pages personnalisées, consultez la rubrique Fonctionnement des pages de propriétés personnalisées.

Créer des 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. La désactivation d'une page personnalisée la masque de l'interface utilisateur. Si vous créez plusieurs pages personnalisées, vous pouvez désactiver les pages jusqu'à ce que vos personnalisations soient testées et terminées.

REMARQUE : Les comptes d'ordinateur héritent des attributs Active Directory des comptes d'utilisateurs. Si vous étendez votre schéma Active Directory pour inclure des attributs supplémentaires pour les comptes d'utilisateurs, vous pouvez sélectionner ces attributs lorsque vous créez une page personnalisée pour gérer les comptes d'ordinateur.

Pour créer une page de propriétés personnalisée :

1. Accédez au nœud **Gestion de la configuration** > **Extensions de l'interface utilisateur**.
2. Dans le menu Tâche, cliquez sur **Nouveau**, puis cliquez sur l'élément de menu approprié pour la page personnalisée à créer.
3. Dans l'onglet Général, tapez 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** Sur l'onglet Propriétés, cliquez sur **Ajouter**.
   - **4b** Pour sélectionner une propriété, cliquez sur **Parcourir**.
   - **4c** Dans le champ **Etiquette de contrôle**, tapez le nom de propriété que DRA doit utiliser comme étiquette pour le contrôle de l'interface utilisateur. Assurez-vous que l'étiquette de contrôle est conviviale et très descriptive. 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 **Type de contrôle**.
   - **4e** Sélectionnez l'emplacement où vous souhaitez que DRA affiche cette page personnalisée dans la console de délégation et de configuration.
   - **4f** Pour spécifier des attributs supplémentaires, tels 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**.

Modifier des propriétés personnalisées

Vous pouvez modifier une page personnalisée en modifiant les propriétés personnalisées.

Pour modifier des propriétés personnalisées :

1. Accédez au nœud **Gestion de la configuration** > **Extensions de l'interface utilisateur**.
2. Dans le volet liste, sélectionnez la page personnalisée souhaitée.
3. Sur le menu Tâches, cliquez sur **Propriétés**.
4. Modifiez les propriétés et les paramètres appropriés pour cette page personnalisée.
5. Cliquez sur **OK**.

Identifier les attributs Active Directory gérés avec des pages personnalisées

Vous pouvez rapidement identifier les propriétés Active Directory, les extensions de schéma ou les attributs virtuels qui sont gérés en utilisant une page personnalisée particulière.

Pour identifier les propriétés d'Active Directory gérées à l'aide de pages personnalisées :

1. Accédez au nœud **Gestion de la configuration** > **Extensions de l'interface utilisateur**.
2. Dans le volet liste, sélectionnez la page personnalisée souhaitée.
3. Dans le volet Détails, cliquez sur l'onglet **Propriétés**. Pour afficher le volet de 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**.

Activer, désactiver et supprimer des pages personnalisées

Lorsque vous activez une page personnalisée, DRA ajoute cette page personnalisée aux assistants et aux fenêtres associés. Pour spécifier les assistants et les fenêtres affichant une page personnalisée, modifiez les propriétés de la page personnalisée.

REMARQUE : Pour s'assurer que chaque page personnalisée expose un ensemble unique de propriétés, DRA n'active pas les pages personnalisées contenant des propriétés exposées sur d'autres pages personnalisées.

Lorsque vous désactivez une page personnalisée, DRA supprime cette page personnalisée dans les assistants et les fenêtres associés. DRA ne supprime pas la page personnalisée. Pour vous assurer qu'une page personnalisée ne s'affiche jamais dans l'interface utilisateur, supprimez la page personnalisée.

Lorsque vous supprimez une page personnalisée, DRA supprime cette page personnalisée dans les assistants et les fenêtres associés. Vous ne pouvez pas restaurer une page personnalisée supprimée. Pour supprimer temporairement une page personnalisée de l'interface utilisateur, désactivez-la.

Pour activer, désactiver ou supprimer une page personnalisée, accédez au nœud **Gestion de la configuration** > **Extensions d'interface utilisateur** et sélectionnez l'action souhaitée dans le menu Tâches ou cliquez dessus avec le bouton droit de la souris.

Interface de ligne de commande

L'interface de ligne de commande vous permet d'accéder aux puissantes fonctionnalités du produit d'administration et de les appliquer à l'aide de commandes ou de fichiers de traitement par lots. Avec l'interface de ligne de commande, vous pouvez émettre une seule commande pour implémenter les modifications sur plusieurs objets.

Par exemple, si vous devez déplacer les répertoires privés de 200 employés sur un nouveau serveur, à l'aide de l'interface de ligne de commande, vous pouvez entrer la commande unique suivante pour modifier les 200 comptes d'utilisateurs :

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE
HOMEDIR:\\HOU2\USERS\@Target()
```

Cette commande demande à DRA de modifier le champ du répertoire privé de chacun des 200 comptes d'utilisateurs de `HOU_SALES` et les groupes `HOU_MIS` en `\\HOU2\USERS\`*user_id*. Pour accomplir cette tâche avec les outils d'administration Microsoft Windows natifs, vous devez effectuer au moins 200 actions distinctes.

REMARQUE : L'outil Interface de ligne de commande sera obsolète dans les versions futures à mesure que d'autres fonctionnalités seront ajoutées à PowerShell.

Outils personnalisés

Les outils personnalisés peuvent être utilisés pour appeler n'importe quelle application à exécuter sur les ordinateurs client et les serveurs du réseau en sélectionnant tout 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 à partir de tous les ordinateurs sur lesquels le client DRA est installé. Vous pouvez également créer un outil personnalisé qui lance une application externe ou un outil nécessitant que DRA mette à jour un script périodiquement. Ces mises à jour périodiques peuvent être des modifications de la configuration ou des modifications de la règle de gestion. Par la suite, après les mises à jour périodiques, DRA réplique les outils personnalisés du serveur d'administration primaire vers les serveurs d'administration secondaires et les ordinateurs clients DRA.

Pour comprendre comment les outils personnalisés sont répliqués dans les ensembles multimaîtres du serveur, reportez-vous à Réplication de fichier.

Créer des outils personnalisés

Vous pouvez créer des outils personnalisés dans le serveur DRA primaire en les associant à un objet Active Directory sélectionné ou à tous les objets Active Directory affichés dans cet assistant de création d'outils personnalisés. La même action sera répliquée sur les serveurs secondaires du MMS et sur les clients DRA grâce à la réplication de fichiers.

Un nouvel outil personnalisé créera un menu et un sous-menu, si nécessaire, pour appeler l'opération sur le ou les objets Active Directory associés dans DRA.

Vous pouvez déléguer des pouvoirs à des administrateurs assistants pour créer et exécuter des outils personnalisés, ainsi que pour accéder à l'application et l'exécuter.

Lorsque vous créez un outil personnalisé, vous devez saisir ses paramètres, comme suit :

Onglet Général

1. **Nom :** n'importe quel nom de 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 **Structure de menu et de sous-menu**. Lorsque vous créez un outil personnalisé et sélectionnez l'objet, DRA affiche l'élément de menu d'outil personnalisé à l'aide de la structure de menu et de sous-menu que vous spécifiez dans le menu Tâches, le menu Raccourci et la barre d'outils DRA.

   *Exemple de structure de menu et de sous-menu :*entrez le nom de l'élément de menu, une barre oblique inverse (\), puis le nom de l'élément de sous-menu.

   Pour utiliser la touche de raccourci : entrez le caractère esperluette (&) avant le nom de l'élément de menu.

   a. Exemple : `SendEmail\ApproveAction` ---- `SendEmail`est le menu et `ApproveAction` est le sous-menu, la première lettre « A » dans `ApproveAction` étant la touche de raccourci activée.
3. **Activé :** Cochez cette case pour activer l'outil personnalisé.
4. **Description :** vous pouvez ajouter toutes les valeurs de description requises.
5. **Commentaire :** vous pouvez ajouter les commentaires requis à l'outil personnalisé.

Onglet Objets pris en charge

Sélectionnez l'objet AD requis ou tous les objets AD auxquels l'outil personnalisé créé doit être associé.

Les options d'outil personnalisé actuellement prises en charge incluent : les domaines gérés, les conteneurs, les utilisateurs, les contacts, les groupes, les ordinateurs, les unités organisationnelles et les imprimantes publiées.

REMARQUE : D'autres objets récemment introduits, tels que la boîte aux lettres de ressources, le groupe dynamique et le groupe dynamique Exchange, ne sont pas pris en charge avec les outils personnalisés.

Onglet Paramètres d'application

Emplacement de l'application : vous devez indiquer le chemin d'accès à l'application ou l'emplacement d'installation en copiant et en collant le chemin d'accès exact de l'application; vous pouvez également utiliser l'option **Insérer**.

Ce même chemin doit déjà exister sur tous les serveurs DRA dans le MMS. Si nécessaire, vous pouvez utiliser Réplication de fichier pour téléverser et répliquer un fichier vers un chemin utilisable sur les serveurs MMS avant de créer un nouvel outil personnalisé.

Vous pouvez également utiliser des variables DRA, des variables d'environnement et des 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**, puis sélectionnez la variable que vous souhaitez utiliser.

Après avoir inséré la variable, tapez une barre oblique inverse (\), puis spécifiez le reste du chemin d'accès à 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 exécutera, sélectionnez la variable d'environnement `{%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 sous forme d'échantillon. Pour spécifier une clé de registre contenant un chemin d'accès 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 exécutera, sélectionnez la variable DRA `{DRA_Replicated_Files_Path}`, puis spécifiez le reste du chemin du fichier de script dans le champ Emplacement de l'application : `{DRA_Replicated_Files_Path}\cscript.vbs ;` dans cet exemple, `{DRA_Replicated_Files_Path}` est le chemin du fichier répliqué et `{DRAInstallDir}\FileTransfer\Replicate` est le dossier dans le 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 fonctionnalité de réplication de fichier. La fonction de réplication de fichiers charge le fichier 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 exécutera, sélectionnez la variable DRA `{DRA_Application_Path}`puis spécifiez le reste du chemin de l'utilitaire dans le champ Emplacement de l'application : `{DRA_Application_Path}\DRADiagnosticUtil.exe`; dans cet exemple, `{DRA_Application_Path}` est l'emplacement où DRA est installé.
- *Exemple 4 :*Il vous suffit de copier-coller l'emplacement de l'application avec le nom du fichier d'application avec l'extension.

Paramètres à transmettre à l'application : pour définir un paramètre à transmettre à une application externe, copiez-collez ou tapez un ou plusieurs paramètres dans le champ 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 à utiliser. Lorsque vous fournissez une propriété de l'objet en tant que paramètre, assurez-vous que l'administrateur assistant dispose de l'autorisation de lecture requise sur la propriété de l'objet, ainsi que du pouvoir *Exécuter les outils personnalisés* pour exécuter l'outil personnalisé.

Exemples :

- *Exemple 1 :* Pour transmettre le nom de groupe et le nom de domaine en tant que paramètres à une application ou à un script externe, sélectionnez les paramètres Nom de propriété de l'objet et Nom de propriété de domaine et spécifiez les noms de paramètre dans le champ Paramètres à transmettre à l'application : « `{Object.Name}` » « `{Domain.$McsName}` »
- *Exemple 2 :* Pour passer le paramètre d'entrée « ipconfig » de l'application « C:\Windows\SysWOW64\cmd.exe », entrez simplement « `{C:\Windows\SysWOW64\cmd.exe}` » « `{ipconfig}` »dans ce champ.

Répertoire dans lequel l'application sera exécutée : il s'agit de l'emplacement où l'application doit être exécutée sur le poste client ou le serveur. Vous devez transmettre le chemin où l'application doit être exécutée. Vous pouvez également utiliser l'option « Insérer » de la même manière, le paramètre pour le champ « Emplacement de l'application » est transmis. Les autres paramètres de cet onglet servent implicitement à expliquer son utilisation.

Personnaliser l'interface utilisateur

Il existe plusieurs options pour 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 ajouter, supprimer ou réorganiser des colonnes. Toutes ces options de personnalisation se trouvent dans le menu **Afficher**.

Modifier le titre de la console

Vous pouvez modifier les informations affichées dans la barre de titre de la console de délégation et de configuration. Pour plus de commodité et de clarté, vous pouvez ajouter le nom d'utilisateur avec lequel la console a été lancée et le serveur d'administration auquel la console est connectée. Pour des environnements complexes dans lesquels vous devez vous connecter à plusieurs serveurs d'administration à l'aide de différentes informations d'identification, cette fonctionnalité vous permet de déterminer rapidement la console à utiliser.

Pour modifier la barre de titre de la console :

1. Démarrez la console de délégation et de configuration.
2. Cliquez sur **Afficher** > **Options**.
3. Sélectionnez l'onglet Titre de la fenêtre.
4. Spécifiez les options appropriées, puis cliquez sur **OK**. Pour obtenir de plus amples renseignements, cliquez sur l'icône **?**.

Personnaliser les colonnes de la liste

Vous pouvez sélectionner les propriétés de l'objet que DRA affiche dans les colonnes de liste. Cette fonctionnalité flexible vous permet de personnaliser des éléments de l'interface utilisateur comme les listes de résultats de recherche, afin de mieux répondre aux exigences propres à l'administration de votre entreprise. Par exemple, vous pouvez définir des colonnes pour afficher le nom de connexion de l'utilisateur ou le type de groupe, vous permettant ainsi de rechercher et de trier rapidement et efficacement les données dont vous avez besoin.

Pour personnaliser les colonnes de la liste :

1. Sélectionnez le nœud approprié. Par exemple, pour choisir les colonnes qui s'affichent lors de l'affichage des résultats de recherche sur les objets gérés, sélectionnez **Tous mes objets gérés**.
2. Dans le menu Affichage, cliquez sur **Choisir les colonnes**.
3. Dans la liste des propriétés disponibles pour ce nœud, sélectionnez les propriétés de l'objet que vous voulez 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 de colonne, sélectionnez une colonne, puis tapez le nombre approprié de pixels dans le champ prévu à cet effet.
6. Cliquez sur **OK**.

24 Client Web

Dans le client Web, vous pouvez personnaliser les propriétés des objets, les formulaires de Workflow Automation et la marque qui s'affiche sur l'interface utilisateur. Lorsqu'elles sont correctement implémentées, les personnalisations de propriété et de processus de travail permettent d'automatiser les tâches de l'administrateur assistant lors de la gestion des objets et des soumissions automatisées de processus de travail.

Personnaliser les pages des propriétés

Vous pouvez personnaliser les formulaires des propriétés de l'objet que vos administrateurs assistants utiliseront dans leurs rôles de gestion Active Directory par type d'objet. Cela comprend la création et la personnalisation de nouvelles pages d'objet basées sur les types d'objets qui sont intégrés dans DRA. Vous pouvez également modifier les propriétés des types d'objets intégrés.

Les propriétés de l'objet sont clairement définies dans la liste accessible sur Customization > Property Pages (Personnalisation > Pages des propriétés) de la console Web afin que vous puissiez facilement reconnaitre les pages d'objet qui sont intégrées, les pages intégrées qui sont personnalisées et les pages non intégrées qui ont été créées par un administrateur.

Personnalisation d'une page des propriétés de l'objet

Vous pouvez personnaliser les formulaires des propriétés de l'objet en ajoutant ou en supprimant des pages, en modifiant des pages et des champs existants et en créant des gestionnaires personnalisés pour les attributs de propriété. Les gestionnaires personnalisés d'un champ sont exécutés chaque fois que la valeur de ce champ est modifiée. Il est possible de faire une planification de sorte que l'administrateur puisse spécifier si les gestionnaires doivent être exécutés immédiatement (à chaque pression sur une touche), lorsque le champ perd son focus, ou après un délai déterminé.

La liste d'objets dans les pages des propriétés fournit les types d'opération pour chaque type d'objet, Créer un objet et Éditer les propriétés. Ce sont les principales opérations que vos administrateurs assistants effectuent dans la console Web. Pour effectuer ces opérations, ils doivent accéder à **Management** > **Search** or **Advanced Search** (Gestion > Recherche ou Recherche avancée). Ils peuvent y créer des objets à partir du menu déroulant Créer ou modifier les objets existants sélectionnés dans le tableau des résultats de la recherche grâce à l'icône Propriétés.

Pour personnaliser une page de propriété de l'objet dans la console Web procédez comme suit :

1. Connectez-vous à la console Web en tant qu'administrateur DRA.
2. Accédez à **Administration** > **Customization** > **Property Pages** (Administration > Personnalisation > Pages des propriétés).
3. Sélectionnez un objet et un type d'opération (Créer un objet ou Éditer un objet) dans la liste Pages des propriétés.
4. Cliquez sur l'icône **Properties** (Propriétés) .

5 Personnalisez le formulaire de propriété de l'objet en effectuant une ou plusieurs des opérations suivantes, puis appliquez vos modifications :

- Ajouter une nouvelle page de propriétés : **+ Add Page** (+ Ajouter une page)
- Réorganiser et supprimer les pages de propriété
- Sélectionner une page de propriétés et personnaliser la page :
  - Réorganiser les champs de configuration sur la page : ↑ ↓
  - Éditer des champs ou des sous-champs : 
  - Ajouter un ou plusieurs champs : + ou **Insert a new Field** (Insérer un nouveau champ)
  - Supprimer un ou plusieurs champs : 
- Créer des gestionnaires personnalisés pour les propriétés à l'aide de scripts, de boîtes de message ou de requêtes (LDAP, DRA ou REST)

  Pour obtenir de plus amples renseignements sur l'utilisation des gestionnaires personnalisés, consultez la rubrique Ajouter des gestionnaires personnalisés.

Définir des filtres personnalisés

Vous pouvez utiliser des filtres pour personnaliser les informations qui sont affichées pour chaque type d'objet en ajoutant le champ **Managed Object Browser** (Navigateur d'objets gérés) à une page de propriété. Lorsque vous configurez les paramètres des champs, vous pouvez ajouter des filtres dans les paramètres par le biais de l'onglet Managed Object Browser Options (Options du navigateur d'objets gérés).. En définissant des filtres personnalisés, vous pouvez restreindre les informations qui sont affichées dans les navigateurs d'objets pour les administrateurs assistants. Les administrateurs assistants ne peuvent afficher que les objets qui répondent aux conditions de filtrage que vous avez définies.

Pour définir un filtre, dans l'onglet Options du navigateur d'objets gérés, cochez la case **Specify Object Filters** (Spécifier les filtres d'objets). Pour chaque condition de filtrage, indiquez le type d'objet, l'attribut à filtrer, la condition de filtrage et la valeur de l'attribut qui sera utilisée pour filtrer les informations. Lorsque vous créez plusieurs filtres pour le même type d'objet, ils sont combinés avec l'opérateur AND. Avec tous les filtres prédéfinis dans le navigateur d'objets gérés, les administrateurs assistants peuvent effectuer l'opération de recherche.

REMARQUE

- Seuls les attributs mis en cache peuvent être utilisés pour définir des filtres.
- Si vous créez un gestionnaire personnalisé en utilisant un script personnalisé pour le filtre personnalisé, vous devez également définir le filtre personnalisé manuellement dans l'onglet **Option du navigateur d'objets gérés** pour que le gestionnaire personnalisé fonctionne.

Créer une nouvelle page de propriété de l'objet

Pour créer une nouvelle page de propriété de l'objet :

1 Connectez-vous à la console Web en tant qu'administrateur DRA.

2 Accédez à **Administration** > **Customization** > **Property Pages** (Administration > Personnalisation > Pages des propriétés).

3 Cliquez sur + **Create** (Créer).

4 Créez le formulaire initial des propriétés de l'objet en définissant le nom de l'action, son icône, son type d'objet et la configuration de l'opération.

   Les actions Créer sont ajoutées au menu déroulant Créer tandis que les actions Propriété s'affichent sous forme d'objet lorsque l'utilisateur sélectionne et modifie un objet dans la liste de recherche.

5 Personnalisez le nouveau formulaire selon vos besoins. Veuillez consulter la rubrique Personnalisation d'une page des propriétés de l'objet.

Personnalisation des formulaires de requête

Les formulaires de requête sont enregistrés sur le serveur Web lorsqu'ils sont créés ou modifiés. L'administrateur DRA les gère à partir de **Administration** > **Customization** > **Requests** (Administration > Personnalisation > Requêtes). Les administrateurs assistants les gèrent à partir de **Tasks** > **Requests** (Tâches > Demandes). Ces formulaires permettent de soumettre des processus de travail automatisés créés dans le serveur de Workflow Automation. Les créateurs de formulaires utilisent ces demandes pour automatiser et améliorer davantage les tâches de gestion des objets.

Vous pouvez ajouter et modifier des propriétés de formulaire existantes et des gestionnaires personnalisés. Le comportement de l'interface pour l'ajout et la personnalisation des propriétés est généralement le même dans un formulaire de Workflow Automation que pour la personnalisation des propriétés des objets, à l'exception des options de configuration du processus de travail et des contrôles permettant de savoir qui peut utiliser le formulaire. Reportez-vous aux rubriques ci-dessous pour de l'information sur l'ajout et la modification de propriétés, l'ajout de gestionnaires personnalisés et le fonctionnement de Workflow Automation.

- Personnaliser les pages des propriétés(Client Web)
- Ajouter des gestionnaires personnalisés
- Processus de travail automatisé

Ajouter des gestionnaires personnalisés

Les gestionnaires personnalisés sont utilisés dans DRA pour que les attributs de propriété puissent interagir entre eux afin d'accomplir une tâche de processus de travail et pour les personnalisations de chargement et de soumission dans un processus de travail, une propriété ou un formulaire.

Gestionnaires personnalisés de propriété

Voici quelques exemples de gestionnaires personnalisés de propriété :

- interroger la valeur d'autres champs
- mettre à jour les valeurs de champ
- basculer l'état d'un champ en lecture seule
- afficher ou masquer des champs en fonction des variables configurées

Gestionnaires de chargement de page

Les gestionnaires de chargement de page effectuent généralement l'initialisation et sont surtout utilisés dans les pages de propriétés personnalisées. Ils ne sont exécutés que la première fois qu'une page est sélectionnée et, dans le cas des pages de propriété, ils sont exécutés après le chargement des données depuis le serveur.

Gestionnaires de chargement de formulaire

Les gestionnaires de chargement de formulaire effectuent généralement des contrôles d'initialisation. Ils ne sont exécutés qu'une seule fois lors du chargement initial du formulaire. Dans le cas des pages de propriétés, ils sont exécutés avant que la requête sur les propriétés de l'objet sélectionné ne soit lancée sur le serveur.

Gestionnaires de soumission du formulaire

Les gestionnaires de soumission de formulaire permettent aux utilisateurs d'effectuer certaines validations et éventuellement d'annuler la soumission du formulaire si un problème survient.

REMARQUE : La meilleure pratique consiste à éviter de configurer des gestionnaires de changement sur les pages et les formulaires qui modifient les valeurs des champs qui se trouvent sur des pages (onglets) différentes de celles où vous créez le gestionnaire. Dans ce scénario, les données figurant sur une page différente de celle du gestionnaire ne seront pas chargées avant que l'administrateur assistant n'accède à cette page, ce qui peut entrer en conflit avec la valeur définie par le gestionnaire de changement.

Pour obtenir des exemples détaillés de l'utilisation des gestionnaires personnalisés et des personnalisations dans la console Web, consultez les rubriques « Personnalisation de la console Web » et « Personnalisation du processus de travail » du document de référence *Personnalisation du produit* sur la page Documentation de DRA.

Consultez les rubriques suivantes pour en savoir plus sur le comportement des gestionnaires personnalisés et sur la façon de les créer :

- « Étapes de base pour créer un gestionnaire personnalisé » page 216
- « Activer le JavaScript personnalisé » page 219
- « Utiliser l'éditeur de script » page 219
- « À propos de l'exécution du gestionnaire personnalisé » page 220

Étapes de base pour créer un gestionnaire personnalisé

Avant d'essayer de créer un gestionnaire personnalisé, assurez-vous que le JavaScript personnalisé est activé dans la configuration de la console. Pour en savoir plus, consultez Activer le JavaScript personnalisé.

Les étapes peuvent être utilisées à partir d'une page de gestionnaire personnalisé présélectionnée. Pour arriver à ce point, naviguez vers différents gestionnaires en procédant comme suit :

- Gestionnaires personnalisés de propriétés d'objets : cliquez sur l'icône d'édition sur un champ de propriété.

- Gestionnaires de chargement de page : sélectionnez les propriétés de la page. Par exemple, **Général** > **Plus d'options** > **Propriétés**.
- Gestionnaires de chargement de formulaire ou de soumission du formulaire : cliquez sur le bouton **Form Properties** (Propriétés du formulaire) sur un formulaire de processus de travail sélectionné, une page Créer un objet ou une page Éditer les propriétés.

Créer un gestionnaire personnalisé :

1. Sélectionnez l'onglet du gestionnaire applicable en fonction de la propriété ou de la page que vous personnalisez :
   - Gestionnaires personnalisés
   - Gestionnaires de chargement de page
   - Gestionnaires de chargement du formulaire
   - Gestionnaires de soumission du formulaire
2. Activez la page du gestionnaire  et effectuez l'une des opérations suivantes :
   - **Gestionnaire personnalisé de champ de propriété :**
     1. Sélectionnez une heure d'exécution. Normalement, vous devriez utiliser la deuxième option.

        Le temps d'exécution contrôle le moment où les gestionnaires de changement sont exécutés en réponse à l'entrée de l'utilisateur. Notez que ce paramètre ne s'applique pas lorsque la valeur du champ est mise à jour par un autre gestionnaire personnalisé utilisant l'interface draApi.fieldValues.
     2. Cliquez sur **+ Add** (+ Ajouter) et choisissez un gestionnaire personnalisé dans le menu **Add Custom Handler** (Ajouter un gestionnaire personnalisé).
   - **Gestionnaire de page ou de formulaire :** cliquez sur **+ Add** (+ Ajouter) et choisissez un gestionnaire personnalisé dans le menu **Add Custom Handler** (Ajouter un gestionnaire personnalisé).

   REMARQUE : En règle générale, vous n'avez besoin que d'un seul gestionnaire, mais vous pouvez en utiliser plusieurs. Plusieurs gestionnaires sont exécutés séquentiellement dans l'ordre indiqué. Si vous voulez changer l'ordre des gestionnaires ou ignorer un gestionnaire qui n'est pas nécessaire, vous pouvez ajouter des API de contrôle de flux dans le script.

   ---
3. Vous devez configurer chaque gestionnaire personnalisé que vous ajoutez à la page. Les options de configuration varient selon le type de gestionnaire. L'éditeur de script dispose d'une aide intégrée et d'une assistance dynamique à la saisie de code Intellisense qui fait également référence à des extraits de l'aide. Pour en savoir plus sur l'utilisation de ces fonctionnalités, consultez la rubrique Utiliser l'éditeur de script.

   Vous pouvez créer vos propres types de gestionnaires.

   - **Gestionnaires de requêtes LDAP ou REST :**
     1. Si vous souhaitez que votre requête soit basée sur des valeurs statiques, définissez les **renseignements de connexion** et les **paramètres de requête**.

        REMARQUE : Pour les requêtes LDAP, vous pouvez exiger un type d'authentification spécifique dans les paramètres des informations de connexion :

        - **Compte par défaut :** s'authentifie avec une connexion au serveur DRA.

- **Compte de remplacement de domaine géré :** s'authentifie auprès d'Active Directory par l'intermédiaire du compte existant Remplacement du domaine géré.
- **Compte de remplacement LDAP :** authentifie par le biais d'un compte de remplacement LDAP, par opposition à un compte de domaine d'un domaine géré. Pour utiliser cette option, le compte doit d'abord être activé dans la console de délégation et de configuration. Pour en savoir plus, consultez Activer l'authentification de remplacement LDAP.

Si vous souhaitez que votre requête soit dynamique, entrez des marques de réservation dans les champs obligatoires. Cela est nécessaire pour que le gestionnaire s'exécute. Le script remplacera les valeurs de réservation.

REMARQUE : Vous pouvez également configurer les en-têtes et les témoins pour la requête REST.

---

2. Dans l'action de pré-requête, utilisez l'éditeur de script pour écrire un code JavaScript personnalisé qui s'exécutera avant que la requête ne soit soumise. Ce script a accès à toutes les informations de connexion et aux paramètres de requête et peut modifier n'importe lequel d'entre eux pour personnaliser la requête. Par exemple, la définition de paramètres d'interrogation basés sur les valeurs que l'utilisateur a saisies dans le formulaire.
3. Dans l'action post-requête, inclure un script pour traiter les résultats de la requête. Les tâches courantes comprennent la vérification des erreurs, la mise à jour des valeurs des formulaires en fonction des résultats renvoyés et la validation de l'unicité des objets en fonction du nombre d'objets renvoyés par la requête.

- **Script :** Insérez du code JavaScript personnalisé pour créer le script.
- **Requête DRA :** Spécifiez la charge utile JSON dans l'onglet Paramètres de la requête. Le format de la charge utile doit correspondre à la clé VarSet ou aux paires de valeurs qui seront envoyées au serveur DRA. Comme pour les requêtes REST et LDAP, vous pouvez spécifier une action de pré-requête qui peut être utilisée pour modifier la charge utile avant qu'elle ne soit soumise au serveur et une action de post-requête pour traiter les résultats.
- **Gestionnaires de boîte de message :** Après avoir défini les propriétés de la boîte de message elle-même, vous pouvez également écrire les segments JavaScript pour **Before-Show Action** (Action avant affichage) et **After-Close Action** (Action après fermeture).

  Ces actions sont facultatives. L'action Avant affichage est utilisé pour personnaliser l'une des propriétés de la boîte de message avant qu'elle ne soit affichée à l'utilisateur et l'action Après fermeture est utilisée pour traiter la sélection de bouton de l'utilisateur et effectuer toute logique supplémentaire en fonction de celle-ci.

4 Cliquez sur **OK** pour enregistrer le gestionnaire.

Pour obtenir des exemples détaillés de l'utilisation des gestionnaires personnalisés et des personnalisations dans la console Web, consultez les rubriques « Personnalisation de la console Web » et « Personnalisation du processus de travail » du document de référence *Personnalisation du produit* sur la page Documentation de DRA

Activer le JavaScript personnalisé

Pour des raisons de sécurité, le JavaScript personnalisé est désactivé par défaut. L'activation de JavaScript personnalisé permet aux administrateurs d'écrire des extraits de code JavaScript que la console Web exécutera tels quels. Vous ne devez autoriser cette exception que si vous comprenez et acceptez les risques.

Pour permettre aux personnalisations d'inclure du code JavaScript personnalisé :

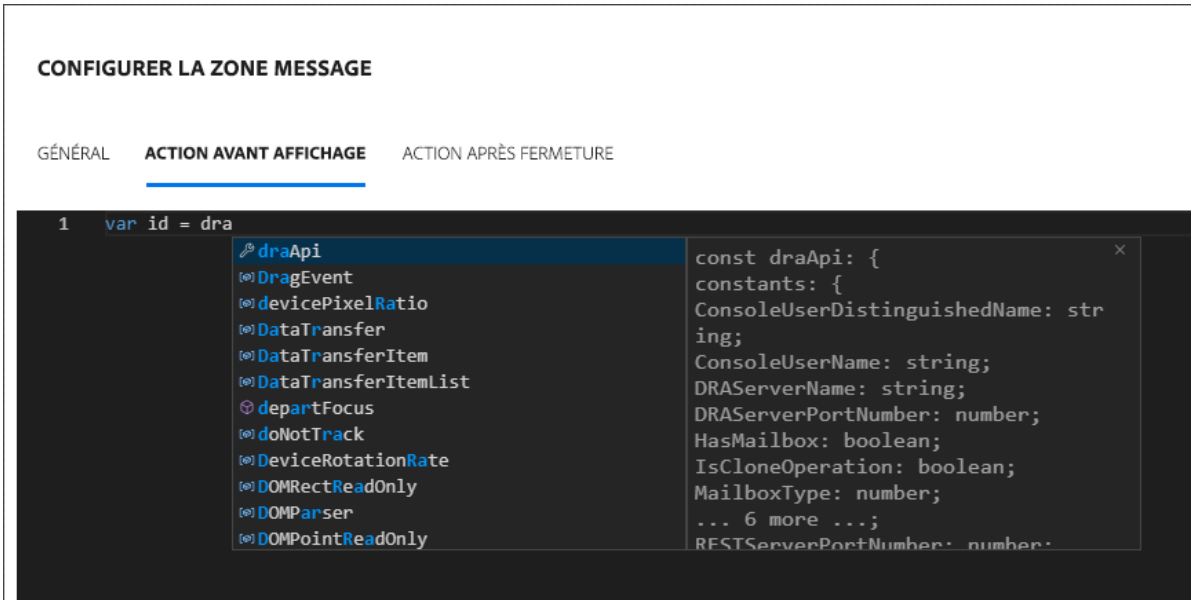
1. Accédez à l'emplacement `C:\ProgramData\NetIQ\DRARESTProxy`.
2. Ouvrez le fichier `restProxy.config`.
3. Ajoutez `allowCustomJavaScript="true"` à l'élément `<configuration_console>`.

Utiliser l'éditeur de script

L'éditeur de script permet de taper et de coller librement des méthodes JavaScript utilisant les API de DRA pour créer des gestionnaires personnalisés dans DRA. L'éditeur offre une assistance dynamique à la saisie de code Intellisense ainsi qu'un panneau d'aide contextuel pour vous aider à écrire le script.

Assistance à la saisie de code Intellisense

Dans l'éditeur de scripts, Intellisense fournit des extraits pour l'assistance à la saisie de code sélectionnables, des compléments de tabulation et des panneaux déroulants de résumés d'API avec des descriptions des API.



REMARQUE : L'assistance à la saisie de code Intellisense est dynamique. Cela signifie qu'elle peut vous fournir des options syntaxiques basées sur le type de gestionnaire pour lequel vous définissez le script, mais elle stocke également les chaînes précédemment saisies par l'utilisateur et fournit également ces invites.

Aide de l'éditeur de scripts

Lorsque vous cliquez sur l'option ⓘ AIDE dans l'éditeur de scripts, un panneau s'ouvre et explique l'objectif général des API de gestionnaires personnalisés, où ils sont utilisés et donne également la liste des API avec des descriptions de leurs fonctions par type d'API :

- Les API globales comprennent :
  - Accès au formulaire
  - Contrôle de flux
  - Constants
- Les API de la boîte à messages comprennent :
  - Opération avant-afficher
  - Opération après-fermer
- Les API d'interrogation comprennent :
  - Résultats de requête
  - Requête DRA
  - Requête LDAP
  - Requête REST

À propos de l'exécution du gestionnaire personnalisé

DRA permet de personnaliser le comportement des formulaires Web à plusieurs moments du cycle de vie des formulaires grâce à des gestionnaires personnalisés. Chaque type de gestionnaire personnalisé a une fenêtre d'exécution spécifique qui, à son tour, affecte la portée des données d'objet disponibles pendant l'exécution de la personnalisation, comme suit :

1. *Gestionnaires de chargement de formulaire*. Exécuté lorsque le formulaire se charge avant la collecte des attributs de l'objet auquel le formulaire est connecté. Ces gestionnaires n'ont pas accès aux valeurs des attributs de l'objet cible.
2. *Gestionnaires de chargement de page*. DRA exécute les gestionnaires de chargement de page lors du premier accès à une page d'un formulaire. Ces gestionnaires ont un accès garanti aux valeurs d'attributs de l'objet cible qui sont contenues dans cette page.
3. *Gestionnaires d'attributs*. DRA exécute les gestionnaires d'attributs lorsqu'on accède à une valeur d'attribut du formulaire. En outre, chaque attribut de formulaire peut être configuré pour exécuter ses gestionnaires personnalisés à l'un des trois moments spécifiques de l'interaction avec l'utilisateur : (1) immédiatement (lorsque l'attribut devient la cible), (2) lorsque l'attribut n'est plus la cible, ou (3) un laps de temps spécifique après que l'attribut n'est plus la cible.
4. *Gestionnaires de soumission du formulaire*. Les gestionnaires de soumission de formulaire sont exécutés lorsque le formulaire est enregistré ou que des modifications sont appliquées au formulaire.

Personnaliser la marque sur l'interface utilisateur

Vous pouvez personnaliser la barre de titre de la console Web de DRA avec votre propre titre et votre propre logo. L'emplacement est directement à droite du nom du produit DRA. Étant donné que cet emplacement est également utilisé pour la navigation de niveau supérieur, il sera masqué par les liens de navigation de DRA de niveau supérieur après l'ouverture de session. Toutefois, l'onglet du navigateur continuera d'afficher le titre personnalisé.

Pour personnaliser l'image de marque de la console Web de DRA :

1. Connectez-vous à la console Web en tant qu'administrateur DRA.
2. Accédez à **Administration** > **Configuration** > **Branding** (Administration > Configuration > Image de marque).
3. Si vous ajoutez une image de logo d'entreprise, enregistrez l'image du logo sur le serveur Web dans `inetpub\wwwroot\DRAClient\assets`.
4. Mettez à jour la configuration, le cas échéant, pour les vignettes Masthead et Login.

   Si vous voulez ajouter une notification pour les administrateurs assistants lors de la connexion, activez le bouton **Show a notification modal at login** (Afficher une modale de notification lors de la connexion). Mettez à jour la configuration de cette notification et cliquez sur **PREVIEW** (APPERÇU) pour voir à quoi ressemblera cette notification lors de la connexion.
5. Lorsque tous les changements sont terminés, cliquez sur **Save** (Enregistrer).

IX Outils et utilitaires

Ces sections fournissent de l'information sur l'utilitaire Analyseur d'ActiveView, l'utilitaire de diagnostic, l'utilitaire d'objets supprimés, l'utilitaire de contrôle de l'intégrité et l'utilitaire de la Corbeille fournis avec DRA.

25 Utilitaire Analyseur d'ActiveView

Chaque ActiveView de DRA contient une ou plusieurs règles, qui s'appliquent aux objets Active Directory (AD) gérés par un ensemble multimaîtres de DRA. L'utilitaire Analyseur d'ActiveView sert à surveiller le temps de traitement de chaque règle ActiveView de DRA telle qu'elle est appliquée aux objets AD au sein d'une opération DRA spécifique. Lors d'une opération DRA, le serveur DRA compare les objets cibles de cette opération à chaque règle de chaque ActiveView. DRA crée ensuite une liste de résultats contenant toutes les règles correspondantes. L'analyseur d'ActiveView calcule le temps passé à traiter chaque règle telle qu'elle est appliquée à une opération de DRA.

Grâce à ces informations, vous pouvez diagnostiquer les problèmes liés à ActiveView en vérifiant les anomalies dans le temps de traitement ActiveView, y compris le temps passé à traiter des ActiveViews inutilisées. L'utilitaire simplifie également la recherche des ActiveViews en double.

Après avoir effectué une collecte de données et consulté un rapport, il peut s'avérer nécessaire de modifier les règles d'une ou plusieurs ActiveViews.

Vous pouvez accéder à l'utilitaire Analyseur d'ActiveView à partir de n'importe quel serveur d'administration DRA. Cependant, vous devez exécuter l'utilitaire d'ActiveView sur le serveur d'administration où vous rencontrez le problème.

Pour accéder à l'utilitaire Analyseur d'ActiveView, connectez-vous au serveur d'administration avec les privilèges du rôle d'administration de DRA et accédez à **NetIQ Administration** > **ActiveView Analyzer Utility** (Administration NetIQ > Utilitaire Analyseur d'ActiveView) dans le menu Démarrer. Vous pouvez également lancer `ActiveViewAnalyzer.exe` à partir du chemin d'accès `Program Files (x86)\NetIQ\DRA\X64` installé par DRA.

Utilisez cet utilitaire pour effectuer les opérations suivantes :

- Collecter des données sur ActiveViews
- Pour générer un rapport d'analyseur

Exemple

Paul, qui est un administrateur assistant, informe Robert, un administrateur de DRA, que la création d'utilisateurs semble prendre plus de temps que d'habitude. Robert décide de lancer l'analyseur ActiveView sur l'objet utilisateur de Paul et demande ensuite à Paul de créer un utilisateur. Après la collecte, Robert génère un rapport d'analyse et remarque qu'une règle appelée Share MBX prend 50 ms pour être énumérée. Robert identifie l'ActiveView qui contient la règle et, après avoir modifié la règle, observe que le problème est résolu.

Démarrer une collecte de données d'ActiveView

Avec l'analyseur d'ActiveView, vous pouvez collecter des données sur les ActiveViews à partir d’actions effectuées sur ceux-ci par des administrateurs assistants. Ces données peuvent ensuite être visualisées dans un rapport d'analyseur. Pour collecter les données, vous devez spécifier l'administrateur assistant sur lequel collecter les données, puis démarrer une collection ActiveView.

REMARQUE : L'administrateur assistant sur lequel vous souhaitez collecter des données doit être connecté au même serveur DRA que celui sur lequel l'analyseur est exécuté.

Pour démarrer une collecte ActiveView :

1. Cliquez sur **Start** > **NetIQ Administration** > **ActiveView Analyzer Utility** (Démarrer > Administration NetIQ > Utilitaire Analyseur d'ActiveView).
2. Sur la page Analyseur d'ActiveView, indiquez les renseignements suivants :
   - 2a **Serveur DRA cible :** Le serveur DRA qui collecte les données de performance sur les opérations de l'administrateur assistant.
   - 2b **Administrateur assistant cible :** Cliquez sur Parcourir et sélectionnez un administrateur assistant sur lequel vous souhaitez collecter des données.
   - 2c **Contrôle de la durée :** Spécifiez le nombre total d'heures nécessaires à la collecte des données de l'analyseur. Après avoir dépassé le délai fixé, la collecte de données sera arrêtée.
3. Cliquez sur **Start Collection** (Démarrer la collecte) pour collecter les données d'ActiveView.

   Après avoir lancé la collecte de données ActiveView, l'utilitaire efface les données existantes et affiche le dernier état.
4. (Facultatif) Vous pouvez arrêter la collecte de données manuellement avant la fin de la durée planifiée et continuer à générer un rapport. Cliquez sur **Stop Collection** (Arrêter la collecte) pour cesser d'enregistrer les opérations de l'administrateur assistant dans les ActiveViews.
5. (Facultatif) Pour obtenir le dernier état, cliquez sur **Collection Status** (État de la collecte).

IMPORTANT : Si vous arrêtez la collecte et changez l'administrateur assistant ou relancez une collecte de données pour le même administrateur assistant, l'analyseur ActiveView efface les données existantes. Vous ne pouvez avoir les données de l'analyseur que pour un administrateur assistant de la base de données à la fois.

Générer un rapport d'analyseur

Avant de générer un rapport d'analyseur, assurez-vous que vous avez cessé de collecter des données.

Dans la page Analyseur d'ActiveView, la liste des opérations effectuées par l'administrateur assistant est affichée. Pour générer un rapport d'analyseur :

1. Cliquez sur **Select Report** (Sélectionner le rapport), puis choisissez le rapport que vous souhaitez consulter.
2. Cliquez sur **Generate Report** (Générer un rapport) pour générer un rapport d'analyse avec les détails de l'opération ActiveView tels que les objets AD affectés par l'opération, la gestion par ActiveView des objets répertoriés, les objets correspondants, non correspondants et la durée de traitement de chaque règle ActiveView individuelle.

À l'aide du rapport, vous pouvez analyser les règles qui prennent plus de temps pour effectuer des opérations, puis décider si certaines d'entre elles doivent être modifiées ou supprimées de leurs ActiveViews respectives.

3 (Facultatif) Passez la souris sur la grille, faites un clic droit, puis utilisez le menu de copie pour copier le rapport dans un presse-papiers. À partir du presse-papiers, les en-têtes de colonne et les données peuvent être collés dans une autre application telle que Notepad ou Excel.

Identification de la performance des objets

Pour identifier la performance de tous les objets gérés par un ActiveView ou une règle :

1 Launch th ·Delega io ·and·Confi ur ti n·Console.

2 Accédez à **Delegation Management** (Gestion des délégations) et cliquez sur **Manage ActiveViews** (Gérer les ActiveViews).

3 Lancez une recherche pour localiser un ActiveView spécifique.

   À partir de là, vous pouvez trouver la règle ou l'objet qui pose problème et y apporter des modifications.

   - Double-cliquez sur l'ActiveView et sélectionnez **Règles** pour énumérer les règles. Vous pouvez modifier une règle spécifique à partir du menu contextuel.
   - Cliquez à l'aide du bouton droit de la souris sur l'ActiveView et sélectionnez **Show Managed Objects** (Montrer les objets gérés) pour répertorier les objets. Vous pouvez modifier un objet à l'aide du menu contextuel (clic droit) > **Properties** (Propriétés).

4 Apporter des modifications à la règle ou à l'objet géré et vérifier si ces modifications résolvent le problème.

26 Utilitaire de diagnostic

L'utilitaire de diagnostic recueille des informations sur votre serveur d'administration pour vous aider à diagnostiquer les problèmes liés à DRA. Utilisez cet utilitaire pour fournir des fichiers journaux à votre représentant d'assistance technique. L'utilitaire de diagnostic fournit une interface d'assistant qui vous guide dans la définition des niveaux de journal et la collecte des informations de diagnostic.

Vous pouvez accéder à l'utilitaire de diagnostic à partir de n'importe quel ordinateur du serveur d'administration. Cependant, vous devez exécuter l'utilitaire de diagnostic sur le serveur d'administration où vous rencontrez le problème.

Pour accéder à l'utilitaire de diagnostic, connectez-vous à l'ordinateur du serveur d'administration en utilisant un compte d'administrateur qui a des droits d'administrateur locaux et ouvrez l'utilitaire à partir du groupe de programmes d'administration de NetIQ dans le menu Démarrer de Windows.

Pour obtenir de plus amples renseignements sur l'utilisation de cet utilitaire, contactez le service d'assistance technique.

27 Utilitaire d'objets supprimés

Cet utilitaire vous permet d'activer la prise en charge de l'actualisation du cache des comptes incrémentiels pour un domaine particulier lorsque le compte d'accès au domaine n'est pas un administrateur. Si le compte d'accès au domaine ne dispose pas d'autorisations de lecture sur le conteneur Objets supprimés du domaine, DRA ne peut pas actualiser le cache des comptes incrémentiels.

Vous pouvez utiliser cet utilitaire pour effectuer les tâches suivantes :

- Vérifiez que le compte d'utilisateur ou le groupe spécifié possède des autorisations de lecture sur le conteneur Objets supprimés du domaine spécifié
- Déléguer ou supprimer des autorisations de lecture sur un compte d'utilisateur ou un groupe spécifié
- Déléguer ou supprimer le droit d'utilisateur Synchroniser des données du service d'annuaire sur un compte d'utilisateur
- Afficher les paramètres de sécurité du conteneur Objets supprimés

Vous pouvez exécuter le fichier utilitaire d'objets supprimés (`DraDelObjsUtil.exe`) à partir du dossier `Program Files (x86)\NetIQ\DRA` de votre serveur d'administration.

Autorisations requises pour l'utilitaire d'objets supprimés

Pour utiliser cet utilitaire, vous devez disposer des autorisations suivantes :

Si vous souhaitez…	**Vous avez besoin de l'autorisation…**
Vérifier les autorisations du compte	Accès à l'autorisation de lecture dans le conteneur Objets supprimés
Déléguer les autorisations de lecture sur le conteneur Objets supprimés	Autorisations d'administrateur dans le domaine où se trouve le conteneur Objets supprimés
Déléguer le droit d'utilisateur Synchroniser des données du service d'annuaire	Autorisations d'administrateur dans le domaine où se trouve le conteneur Objets supprimés
Supprimer les autorisations précédemment déléguées	Autorisations d'administrateur dans le domaine où se trouve le conteneur Objets supprimés
Afficher les paramètres de sécurité du conteneur Objets supprimés	Accès à l'autorisation de lecture dans le conteneur Objets supprimés

Syntaxe pour l'utilitaire d'objets supprimés

```
DRADELOBJSUTIL /DOMAIN:DOMAINNAME [/DC:COMPUTERNAME] {/
DELEGATE:ACCOUNTNAME | /VERIFY:ACCOUNTNAME | /REMOVE:ACCOUNTNAME | /
DISPLAY [/RIGHT]}
```

Options pour l'utilitaire d'objets supprimés

Vous pouvez spécifier les options suivantes :

/DOMAIN:*domain*	Spécifie le nom NETBIOS ou DNS du domaine dans lequel se trouve le conteneur Objets supprimés.
/SERVER:*computername*	Spécifie le nom ou l'adresse IP du contrôleur de domaine pour le domaine spécifié.
/DELEGATE:*accountname*	Délègue des autorisations au compte d'utilisateur ou au groupe spécifié.
/REMOVE:*accountname*	Supprime les autorisations précédemment déléguées au compte d'utilisateur ou au groupe spécifié.
/VERIFY:*accountname*	Vérifie des autorisations du compte d'utilisateur ou du groupe spécifié.
/DISPLAY	Affiche les paramètres de sécurité du conteneur Objets supprimés dans le domaine spécifié.
/RIGHT	Vérifie que le compte d'utilisateur ou le groupe spécifié dispose du droit d'utilisateur Synchroniser des données du service d'annuaire. Vous pouvez utiliser cette option pour déléguer ou vérifier ce droit. Le droit d'utilisateur Synchroniser des données du service d'annuaire permet au compte de lire tous les objets et propriétés d'Active Directory.

REMARQUE

- Si le nom du compte d'utilisateur ou du groupe que vous souhaitez spécifier contient un espace, placez-le entre guillemets. Par exemple, si vous souhaitez spécifier le groupe Houston IT, tapez "Houston IT".
- Lorsque vous spécifiez un groupe, utilisez le nom antérieur à Windows 2000 pour ce groupe.

Exemple pour l'utilitaire d'objets supprimés

Les exemples suivants illustrent des exemples de commandes pour des scénarios courants.

Exemple 1

Pour vérifier que le compte d'utilisateur `MYCOMPANY\JSmith` dispose des autorisations de lecture sur le conteneur Objets supprimés du domaine `hou.mycompany.com`, saisissez :

```
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` du 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 d'utilisateur Synchroniser des données du service d'annuaire dans le domaine MYCOMPANY du compte d'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 du groupe MYCOMPANY\DraAdmins, entrez :

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

28 Utilitaire de contrôle de l'intégrité

L'utilitaire de contrôle de l'intégrité de DRA est une application autonome fournie avec l'ensemble d'installation de DRA. Vous pouvez utiliser l'utilitaire de contrôle de l'intégrité après l'installation, ainsi qu'avant et après la mise à niveau, pour vérifier, valider et obtenir de l'information sur l'état des composants et des processus du serveur DRA, du site Web DRA et des clients DRA. Vous pouvez également l'utiliser pour installer ou mettre à jour une licence de produit, pour sauvegarder l'instance AD LDS avant une mise à niveau du produit, pour afficher la description des vérifications et pour résoudre les problèmes ou identifier les actions à entreprendre pour résoudre les problèmes, puis les revalider.

L'utilitaire de contrôle de l'intégrité est accessible à partir du dossier du programme DRA après l'exécution du programme d'installation `NetIQAdminInstallationKit.msi`.

Vous pouvez exécuter l'utilitaire de contrôle de l'intégrité à tout moment en exécutant le fichier `NetIQ.DRA.HealthCheckUI.exe`. Lorsque l'application s'ouvre, vous pouvez choisir d'effectuer une opération précise, d'exécuter des contrôles sur des composants précis ou d'exécuter des contrôles sur tous les composants. Reportez-vous aux fonctions utiles ci-dessous pour en savoir plus sur l'utilitaire de contrôle de l'intégrité :

Fonction	Actions utilisateur
Sélectionner tout ou Désélectionner tout	Utilisez les options de la barre d'outils ou du menu Fichier pour **Sélectionner** ou **Désélectionner** tous les éléments à cocher ou pour cocher des cases individuelles afin d'effectuer des contrôles précis.
Exécuter les contrôles sélectionnés	Utilisez cette option de la barre d'outils ou du menu Fichier pour exécuter les contrôles sélectionnés (tous ou certains).
Enregistrer ou écrire des résultats	Utilisez cette option de la barre d'outils ou du menu Fichier pour créer et enregistrer un rapport détaillé sur le contrôle effectué.
Exécuter cette vérification	Sélectionnez un titre d'élément pour voir 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 : ◆ Validation de la licence (installation ou mise à jour d'une licence de produit) ◆ Sauvegarde de l'instance AD LDS (Sauvegarder l'instance AD LDS) ◆ Réplication (Valider la base de données de réplication)
Résoudre ce problème	Sélectionnez un titre d'élément, puis utilisez cette option de la barre d'outils lorsqu'un contrôle a échoué. Si exécuter à nouveau le contrôle ne résout pas le problème, la description doit inclure des informations ou des actions à entreprendre pour résoudre le problème.

29 Utilitaire 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 n'a pas d'autorisations sur le conteneur NetIQRecycleBin caché dans le domaine spécifié, DRA ne peut pas déplacer les comptes supprimés dans la Corbeille.

REMARQUE : Après avoir utilisé cet utilitaire pour activer la Corbeille, effectuez une actualisation complète du cache des comptes pour vous assurer que le serveur d'administration applique cette modification.

Vous pouvez utiliser cet utilitaire pour effectuer les tâches suivantes :

- vérifier que le compte possède des autorisations de lecture sur le conteneur NetIQRecycleBin du domaine spécifié
- déléguer des autorisations de lecture sur un compte spécifié
- afficher les paramètres de sécurité du conteneur NetIQRecycleBin

Autorisations requises pour l'utilitaire de la Corbeille

Pour utiliser cet utilitaire, vous devez disposer des autorisations suivantes :

Si vous souhaitez…	**Vous avez besoin de l'autorisation…**
Vérifier les autorisations du compte	Accès à l'autorisation de lecture dans le conteneur NetIQRecycleBin
Déléguer les autorisations de lecture sur le conteneur NetIQRecycleBin	Autorisations d'administrateur dans le domaine spécifié
afficher les paramètres de sécurité du conteneur NetIQRecycleBin	Accès à l'autorisation de lecture dans le conteneur NetIQRecycleBin

Syntaxe de l'utilitaire de la Corbeille

```
DRARECYCLEBINUTIL /DOMAIN:DOMAINNAME [/DC:COMPUTERNAME] {/
DELEGATE:ACCOUNTNAME | /VERIFY:ACCOUNTNAME | /DISPLAY}
```

Options de l'utilitaire de la Corbeille

Les options suivantes vous permettent de configurer l'utilitaire de la Corbeille :

/DOMAIN:domain	Spécifie le nom NETBIOS ou DNS du domaine dans lequel se trouve la Corbeille.
/SERVER:*computername*	Spécifie le nom ou l'adresse IP du contrôleur de domaine pour le domaine spécifié.
/DELEGATE:*accountname*	Délègue les autorisations au compte spécifié.
/VERIFY:*accountnam*e	Vérifie les autorisations du compte spécifié.
/DISPLAY	Affiche les paramètres de sécurité du conteneur NetIQRecycleBin dans le domaine spécifié.

Exemples pour l'utilitaire de la Corbeille

Les exemples suivants illustrent des exemples de commandes pour des scénarios courants.

Exemple 1

Pour vérifier que le compte d'utilisateur `MYCOMPANY\JSmith` dispose des autorisations de lecture sur le conteneur NetIQRecycleBin du domaine `hou.mycompany.com`, saisissez :

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Exemple 2

Pour déléguer des autorisations de lecture sur le conteneur NetIQRecycleBin dans le domaine `MYCOMPANY` du 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
```

A Annexe

Cette annexe fournit des informations sur les services DRA et sur la manière de résoudre les problèmes avec le service REST DRA.

Services DRA

Ce tableau fournit des informations sur les services DRA. Cela aide les administrateurs de DRA à décider s'ils peuvent désactiver un service en toute sécurité sans affecter aucune fonctionnalité de DRA.

Service DRA	Description	Désactivable en toute sécurité
Service d'administration NetIQ	Ce service effectue toutes les opérations du DRA et gère les processus internes du serveur du DRA.	Non
Service d'audit NetIQ DRA	Ce service traite les requêtes de l'historique des modifications unifié provenant de la console Web. Lorsque vous désactivez ce service : ◆ La fonctionnalité de DRA n'est pas affectée. ◆ Vous pourrez générer des rapports sur l'historique des modifications unifié à partir de la console de délégation et de configuration. ◆ Vous ne pourrez pas générer des rapports sur l'historique des modifications unifié à partir de la console Web.	Oui
Service de cache de BD NetIQ DRA	Ce service gère la base de données du cache de NetIQ DRA.	Non
Service de cache NetIQ DRA	Ce service agit comme un cache persistant pour le serveur d'administration de NetIQ.	Non
Service de base NetIQ DRA	Ce service génère des rapports pour les consoles DRA et planifie les tâches Active Directory, Office365, DRA et Resource Collector. Lorsque vous désactivez ce service : ◆ La fonctionnalité de DRA n'est pas affectée. ◆ Les tâches de collecte ne seront pas exécutées et les données pour les rapports de NRC ne seront pas collectées. ◆ Vous ne pourrez pas générer des rapports sur l'historique des modifications unifié à partir d'une console DRA.	Oui

Service DRA	Description	Désactivable en toute sécurité
Archivage des journaux NetIQ DRA	Ce service stocke tous les événements d'audit de DRA d'une manière sécurisée pour soutenir les rapports d'audit.	Non
Service de réplication NetIQ DRA	Ce service prend en charge la fonction d'affectation de groupe temporaire (TGA) du DRA. Les TGA ne seront pas disponibles sur un serveur DRA où ce service est supprimé ou arrêté.	Oui
Service Rest NetIQ DRA	Les clients de la console Web et de PowerShell utilisent ce service pour communiquer avec le serveur d'administration de NetIQ.	Non
Stockage sécurisé NetIQ DRA	Ce service gère l'instance AD LDS de DRA qui stocke la configuration de DRA. Il réplique également ces données de configuration à travers la configuration du MMS.	Non
Service Skype NetIQ DRA	Ce service gère toutes les tâches de Skype. Lorsque vous désactivez ce service : ◆ La fonctionnalité de DRA n'est pas affectée. ◆ Les opérations Skype ne seront pas traitées.	Oui

Dépannage des services REST de DRA

Cette section contient des informations de dépannage pour les sujets suivants :

- « Gestion des certificats pour les extensions REST de DRA » page 240
- « Gestion des erreurs du serveur DRA » page 241
- « Chaque commande PowerShell entraîne l'erreur PSInvalidOperation » page 242
- « Journalisation de suivi WCF » page 242

Gestion des certificats pour les extensions REST de DRA

Le service de nœud d'extrémité de DRA exige une liaison par certificat sur le port de communication. Pendant l'installation, le programme d'installation exécutera les commandes pour relier le port au certificat. L'objectif de cette section est de décrire comment valider la liaison et comment ajouter ou supprimer une liaison, si nécessaire.

Informations de base

Port de service par défaut du nœud d'extrémité : 8755

ID de l'application pour les extensions REST de DRA : 8031ba52-3c9d-4193-800a-d620b3e98508

Hachage du certificat : affiché sur la page des certificats SSL de l'IIS Manager.

Vérification des liaisons existantes

Dans une fenêtre CMD, exécutez la commande suivante : `netsh http show sslcert`

Cela affichera une liste des liaisons de certificats pour cet ordinateur. Recherchez dans la liste l'ID de l'application des extensions REST de DRA. Le numéro de port doit correspondre au port de configuration. Le hachage du certificat doit correspondre au hachage du certificat affiché dans IIS Manager.

```
IP:port                 : 0.0.0.0:8755
Certificate Hash        : d095304df3d3c8eecf64c25df7931414c9d8802c
Application ID          : {8031ba52-3c9d-4193-800a-d620b3e98508}
Certificate Store Name  : (null)
Verify Client Certificate Revocation    : Enabled
Verify Revocation Using Cached Client Certificate Only    : Disabled
Usage Check             : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout   : 0
Ctl Identifier          : (null)
Ctl Store Name          : (null)
DS Mapper Usage         : Disabled
Negotiate Client Certificate    : Disabled
```

Supprimer une liaison

Pour supprimer une liaison existante, saisissez cette commande dans une fenêtre CMD :

```
netsh http delete sslcert ipport=0.0.0.0:9999
```

Où 9999 est le numéro du port à supprimer. La commande `netsh` affichera un message indiquant que le certificat SSL a été supprimé avec succès.

Ajouter une liaison

Pour ajouter une nouvelle liaison, saisissez la commande suivante dans une fenêtre CMD :

```
netsh http add sslcert ipport=0.0.0.0:9999 certhash=[HashValue]
appid={8031ba52-3c9d-4193-800a-d620b3e98508}
```

Où 9999 est le numéro de port du service de nœud d'extrémité et `[HashValue]` est la valeur de hachage du certificat affichée dans IIS Manager.

Gestion des erreurs du serveur DRA

Si vous obtenez une erreur lors de la création d'un objet compatible avec le courrier, consultez les rubriques suivantes :

L'opération EnableEmail a échoué

Lorsque vous créez un objet compatible avec le courriel ou que vous appelez l'un des nœuds d'extrémité EnableEmail, il se peut que le serveur DRA vous renvoie une erreur du type *« Le serveur n'a pas réussi à mener à bien le processus de travail demandé. L'opération UserEnableEmail a échoué »*. Cela peut être causé par l'inclusion d'une propriété `mailNickname` dans les données utiles qui n'est pas conforme à la stratégie définie sur le serveur.

Supprimez la propriété `mailNickname` de la charge utile et laissez le serveur DRA générer la valeur de l'alias du courriel conformément à la stratégie définie.

Chaque commande PowerShell entraîne l'erreur PSInvalidOperation

Lorsque le service REST de DRA est lié à un certificat auto-signé, les cmdlets de PowerShell renverront l'erreur suivante :

```
Get-DRAServerInfo: One or more errors occurred.
An error occurred while sending the request.
The underlying connection was closed: Could not establish trust
relationship for the SSL/TLS secure channel.
The remote certificate is invalid according to the validation procedure.
```

Sur chaque commande, vous devrez inclure le paramètre `-IgnoreCertificateErrors`. Pour supprimer également le message de confirmation, ajoutez le paramètre `-Force`.

Journalisation de suivi WCF

Si vos requêtes REST provoquent des erreurs qui ne peuvent pas être résolues en consultant les journaux du service REST, vous devrez peut-être augmenter le niveau de journalisation de suivi WCF pour voir les détails sur la façon dont la requête voyage à travers la couche WCF. Le volume de données généré par ce niveau de suivi peut être important, c'est pourquoi le niveau de journalisation expédié est réglé sur « Critique, erreur ».

Par exemple, si les requêtes donnent lieu à des exceptions de valeur nulle alors que vous envoyez les objets dans la charge utile, cela peut s'avérer utile. Un autre cas de figure serait celui où le REST ne répond plus.

Pour augmenter la journalisation de suivi WCF, vous devez modifier le fichier de configuration pour le service qui est sous surveillance. Les exceptions de charge utile sont susceptibles d'être évidentes en examinant le journal de suivi WCF pour le service REST.

Étapes pour activer la journalisation détaillée

1. Dans l'Explorateur de fichiers de Windows, accédez au dossier d'installation des extensions de DRA. En général, il s'agit de `C:\Program Files (x86)\NetIQ\DRA`.
2. Ouvrez le fichier `NetIQ.DRA.RestService.exe.config`.
3. Localisez l'élément `<source>` dans le chemin xml suivant : `<system.diagnostics><sources>`.

4 Dans l'élément source, modifiez la valeur de l'attribut `switchValue` de « `Critical, Error` » (Critique, erreur) à « `Verbose, ActivityTracing` » (Verbeux, suivi d'activité).

5 Enregistrez le fichier et redémarrez le service DRA Rest de NetIQ.

L'opération EnableEmail a échoué

Les données de suivi de WCF sont écrites dans un format propriétaire. Vous pouvez lire le fichier traces.svslog en utilisant l'utilitaire SvcTraceViewer.exe. Vous pouvez trouver plus d'informations sur cet utilitaire ici :