

NetIQ Directory and Resource Administrator 10.2

Guide de l'utilisateur

Mai 2022

Mentions légales

Pour plus d'informations sur les mentions légales, les marques, les exclusions de garantie, les garanties, les limitations en matière d'exportation et d'utilisation, les droits du gouvernement américain, la politique relative aux brevets et la compatibilité avec la norme FIPS, rendez-vous sur <https://www.microfocus.com/fr-fr/legal>.

© Copyright 2007 - 2022 Micro Focus ou l'une de ses filiales.

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

Table des matières

À propos de ce guide	7
1 Mise en route	9
Qu'est-ce que Directory and Resource Administrator ?	9
Présentation des composants de Directory and Resource Administrator (DRA)	10
Serveur d'administration DRA	10
Gestion des comptes et des ressources	11
Console Web	11
Composants de création de rapports	12
Moteur de workflow	12
Architecture du produit	13
2 Utilisation des interfaces utilisateur	15
Console Web	15
Démarrage de la console Web	15
Configuration de la console Web	16
Personnalisation de la console Web	20
Gestion des objets dans la console Web	21
Génération de rapports de l'historique des modifications	22
Utilisation de Workflow Automation	23
Gestion des comptes et des ressources	24
Connexion à un serveur d'administration ou à un domaine géré	25
Modification du titre de la console	25
Personnalisation des colonnes de la liste	26
Gestion des objets dans le nœud de gestion des comptes et des ressources	26
Exécution de requêtes avancées enregistrées	27
Restauration des paramètres de la console	27
Restrictions relatives aux caractères spéciaux	28
Utilisation de caractères joker	29
Affichage des pouvoirs et des rôles qui vous sont assignés	30
Affichage du numéro de version du produit et des correctifs installés	30
Affichage de votre licence actuelle	31
Récupération d'un mot de passe BitLocker	31
DRA Reporting	32
Présentation de DRA Reporting	34
Mode d'utilisation des archives de journaux par DRA	35
Présentation des dates et heures	36
Tâches de création de rapports DRA	36
3 Gestion des objets Active Directory	41
Gestion des comptes utilisateur	41
Comptes utilisateur dans des domaines approuvés	42
Tâches de gestion des comptes utilisateur	42
Transformation des comptes utilisateur	45
Gestion des groupes	48

Tâches de gestion des groupes	48
Gestion des assignations de groupes temporaires dans la console de délégation et de configuration	51
Gestion des assignations de groupes temporaires dans la console Web	52
Gestion des groupes de distribution dynamiques	54
Gestion des groupes dynamiques	56
Exemple de scénario	56
Préparation du scénario	57
Tâches de groupe dynamique	58
Gestion des contacts	61
Gestion des comptes de service administrés de groupe	62
4 Recherche d'objets	65
Recherche	65
Utilisation des caractères joker	65
Recherche à plusieurs champs	66
Ajout et tri de colonnes	67
Exportation des résultats d'une recherche	67
Recherche avancée	68
Requêtes de recherche avancée	68
Gestion des requêtes avancées	69
Exportation des résultats d'une recherche avancée	70
5 Gestion des objets Azure	71
Gestion des comptes utilisateur Azure	71
Gestion des comptes utilisateur invité Azure	73
Gestion des groupes Azure	74
Gestion des contacts Azure	75
6 Gestion des dossiers publics et des boîtes aux lettres Exchange	77
Tâches de gestion des boîtes aux lettres utilisateur	77
Tâches de gestion des boîtes aux lettres Office 365	80
Tâches de gestion des boîtes aux lettres de ressources	81
Tâches de gestion des boîtes aux lettres partagées	83
Tâches de gestion des boîtes aux lettres liées	84
Tâches de gestion des dossiers publics	85
7 Gestion des ressources	87
Gestion des unités organisationnelles	87
Gestion des ordinateurs	88
Gestion des services	90
Gestion des imprimantes et des travaux d'impression	91
Tâches de gestion des imprimantes	92
Tâches de gestion des travaux d'impression	93
Tâches de gestion de l'imprimante publiée	93
Tâches de gestion des travaux d'impression des imprimantes publiées	94
Gestion des partages	95
Gestion des utilisateurs connectés	96

Gestion des périphériques	96
Gestion des journaux d'événements	97
Types de journaux d'événements	97
Tâches de gestion des journaux d'événements	98
Gestion des fichiers ouverts	99

8 Gestion de la corbeille **101**

À propos de ce guide

Le *Guide de l'utilisateur* fournit des informations conceptuelles concernant le produit NetIQ Directory and Resource Administrator (DRA). Il définit la terminologie ainsi que différents concepts associés.

Public

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

Documentation supplémentaire

Ce guide fait partie de la documentation consacrée à Directory and Resource Administrator. Pour obtenir la version la plus récente de ce guide et des autres ressources de documentation DRA, rendez-vous sur le [site Web de documentation relative à NetIQ DRA \(https://www.netiq.com/documentation/directory-and-resource-administrator/index.html\)](https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Coordonnées

Nous sommes à l'écoute de vos commentaires et suggestions concernant ce guide et les autres documents fournis avec ce produit. À cette fin, vous pouvez utiliser le lien [comment on this topic](#) (Ajouter un commentaire sur cette rubrique) situé au bas de chaque page de la documentation en ligne ou envoyer un message électronique à l'adresse Documentation-Feedback@microfocus.com.

En cas de problème spécifique concernant le produit, contactez le service clients Micro Focus à l'adresse <https://www.microfocus.com/support-and-services/>.

1 Mise en route

Avant de commencer à gérer les objets Active Directory à l'aide de NetIQ Directory and Resource Administrator (DRA), vous devez comprendre les principes de base du fonctionnement de DRA au sein de votre entreprise et le rôle des composants DRA dans l'architecture du produit.

- ♦ « [Qu'est-ce que Directory and Resource Administrator ?](#) » page 9
- ♦ « [Présentation des composants de Directory and Resource Administrator \(DRA\)](#) » page 10

Qu'est-ce que Directory and Resource Administrator ?

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

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

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

- ♦ **Prise en charge d'Azure et des environnements locaux Active Directory, Exchange et Skype Entreprise** : assure la gestion administrative d'Azure et des environnements locaux Active Directory, Exchange et Skype Entreprise, ainsi que d'Exchange Online et de Skype Entreprise Online.
- ♦ **Contrôles granulaires de l'accès aux privilèges utilisateur et administrateur** : la technologie brevetée ActiveView délègue uniquement les privilèges nécessaires à l'exécution de responsabilités spécifiques et empêche la réaffectation des privilèges.
- ♦ **Console Web personnalisable** : une approche intuitive permet à du personnel sans formation technique de réaliser facilement et en toute sécurité des tâches administratives au moyen d'un accès limité et d'un minimum de fonctionnalités (assignées).
- ♦ **Audit approfondi des activités et création de rapports** : fournit un enregistrement d'audit complet de toutes les activités réalisées avec le produit. Stocke en toute sécurité les données à long terme et démontre aux auditeurs (par exemple, PCI DSS, FISMA, HIPAA et NERC CIP) que des processus sont en place pour contrôler l'accès à Active Directory.

- ♦ **Automatisation des processus informatiques** : automatise les workflows pour des tâches aussi diverses que le provisioning et le déprovisioning, les actions des utilisateurs et des boîtes aux lettres, l'application de stratégies et les tâches en self-service contrôlées. Renforce l'efficacité de l'entreprise et réduit les tâches administratives manuelles et répétitives.
- ♦ **Intégrité opérationnelle** : empêche les modifications malintentionnées ou incorrectes qui affectent les performances et la disponibilité des systèmes et services en fournissant un contrôle d'accès granulaire aux administrateurs et en gérant l'accès aux systèmes et aux ressources.
- ♦ **Application des processus** : préserve l'intégrité des processus de gestion des modifications clés qui vous aident à améliorer la productivité, réduire les erreurs, gagner du temps et augmenter l'efficacité de l'administration.
- ♦ **Intégration avec Change Guardian** : permet d'améliorer l'audit des événements générés dans Active Directory en dehors de DRA et de l'automatisation du workflow.

Présentation des composants de Directory and Resource Administrator (DRA)

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

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

Type d'utilisateur de DRA	Interfaces utilisateur	Serveur d'administration
Administrateur DRA (Personne en charge de la configuration du produit)	Console de délégation et de configuration	Serveur primaire
Administrateur avancé	DRA Reporting PowerShell CLI Fournisseur ADSI DRA	N'importe quel serveur DRA
Administrateur occasionnel du service d'assistance	Nœud Gestion des comptes et des ressources de la console de délégation et de configuration Console Web	N'importe quel serveur DRA

Serveur d'administration DRA

Le serveur d'administration DRA stocke les données de configuration (environnementales, accès délégué et stratégie), exécute les tâches de l'opérateur et d'automatisation et audite l'activité de l'ensemble du système. Tout en prenant en charge plusieurs clients au niveau de la console et de

L'API, le serveur est conçu pour offrir une haute disponibilité pour la redondance et l'isolement géographique via un modèle d'évolutivité d'ensemble multi-maître (MMS, Multi-Master Set). Dans ce modèle, chaque environnement DRA nécessite un serveur d'administration DRA primaire qui se synchronise avec un certain nombre de serveurs d'administration DRA secondaires supplémentaires.

Nous recommandons vivement de ne pas installer les serveurs d'administration sur les contrôleurs de domaine Active Directory. Pour chaque domaine géré par DRA, assurez-vous qu'il existe au moins un contrôleur de domaine sur le même site que le serveur d'administration. Par défaut, le serveur d'administration accède au contrôleur de domaine le plus proche pour toutes les opérations de lecture et d'écriture. Lors de l'exécution de tâches spécifiques à un site, telles que les réinitialisations de mots de passe, vous pouvez spécifier un contrôleur de domaine spécifique du site pour traiter l'opération. Il est conseillé d'envisager de consacrer un serveur d'administration secondaire à la création de rapports, au traitement par lots et aux workloads automatisés.

Gestion des comptes et des ressources

Le nœud Account and Resource Management (Gestion des comptes et des ressources) de la console de délégation et de configuration permet aux assistants administrateur DRA de consulter et de gérer les objets délégués des domaines et des services connectés.

Console Web

La console Web est une interface utilisateur Web qui fournit un accès rapide et simple aux assistants administrateur DRA pour afficher et gérer les objets délégués des domaines et des services connectés.

Les administrateurs peuvent personnaliser l'apparence et l'utilisation de la console Web afin d'inclure une image de marque d'entreprise personnalisée et des propriétés d'objet personnalisées. Ils peuvent également configurer l'intégration avec les serveurs Change Guardian pour permettre l'audit des modifications effectué en dehors de DRA.

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

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

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

Composants de création de rapports

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

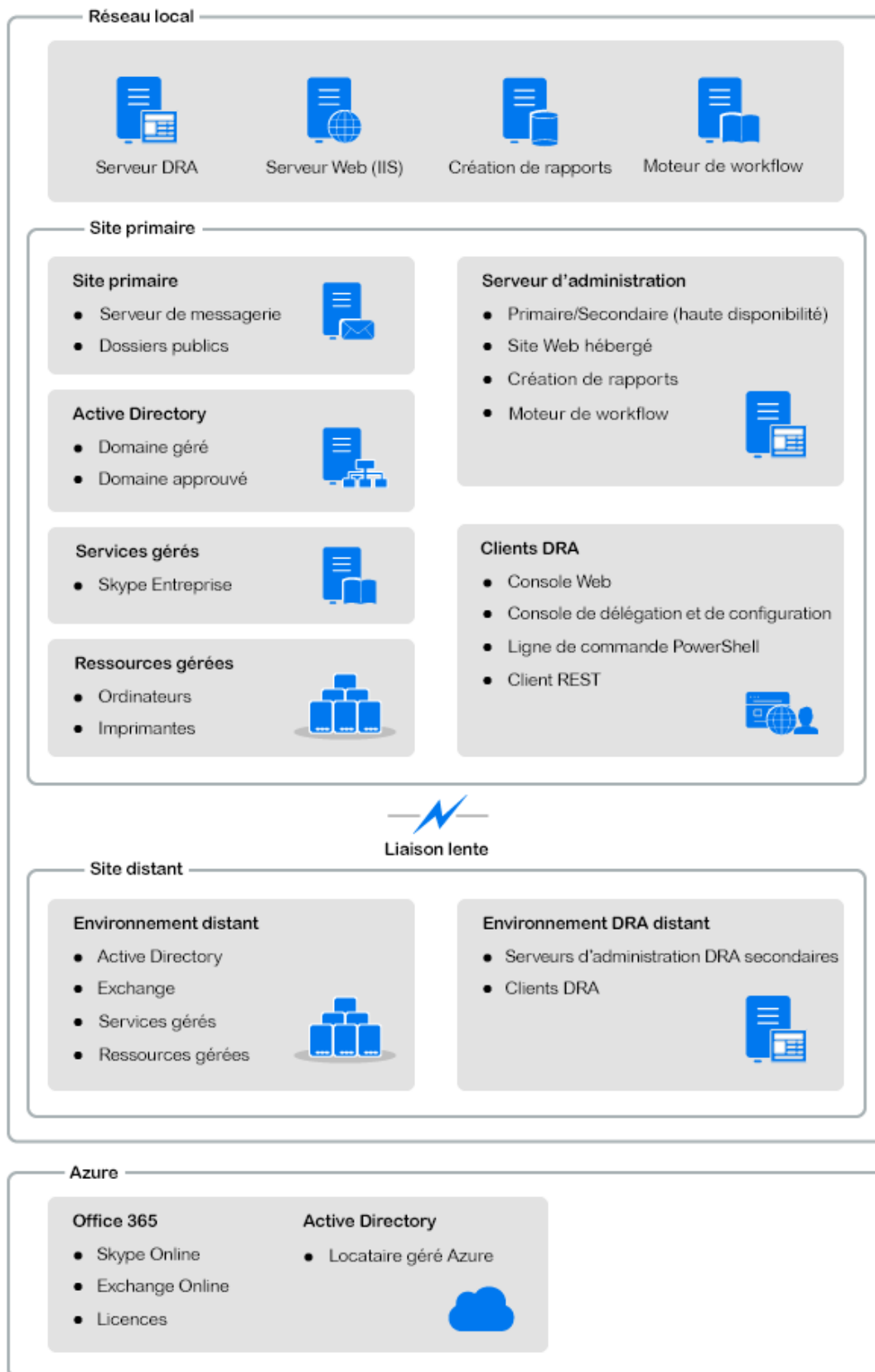
- ♦ Rapports sur les ressources pour les objets Active Directory
- ♦ Rapports sur les données d'objet Active Directory
- ♦ Rapports récapitulatifs Active Directory
- ♦ Rapports sur la configuration de DRA
- ♦ Rapports sur la configuration d'Exchange
- ♦ Rapports sur Office 365 Exchange Online
- ♦ Rapports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

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

Moteur de workflow

DRA s'intègre au moteur de workflow pour automatiser les tâches de workflow via la console Web dans laquelle les assistants administrateur peuvent configurer le serveur de workflow et exécuter des formulaires d'automatisation de workflow personnalisés, puis afficher l'état de ces workflows. Pour plus d'informations sur le moteur de workflow, reportez-vous à la documentation relative à Workflow Automation sur le [site de documentation NetIQ DRA](#).

Architecture du produit



2 Utilisation des interfaces utilisateur

Les interfaces utilisateur DRA apportent une solution à divers besoins d'administration. Ces interfaces sont les suivantes :

Console Web

Elle permet d'exécuter des tâches d'administration courantes sur les ressources et les comptes par le biais d'une interface Web. Vous pouvez accéder à la console Web à partir de tout ordinateur qui exécute Internet Explorer, Chrome ou Firefox.

PowerShell

Le module PowerShell permet aux clients non-DRA de demander des opérations DRA à l'aide d'applets de commande PowerShell.

Console NetIQ Reporting Center

Elle permet d'afficher et de déployer des rapports de gestion pour vous permettre d'auditer la sécurité de votre entreprise et d'effectuer le suivi des activités d'administration. Les rapports de gestion incluent les rapports d'activités, de configuration et de résumé. La plupart de ces rapports peuvent être affichés sous forme de graphique.

Console Web

La console Web est une interface utilisateur Web qui fournit un accès simple et rapide à de nombreux comptes utilisateur, groupes, ordinateurs, ressources et tâches de boîte aux lettres Microsoft Exchange. Vous pouvez personnaliser des propriétés d'objet pour améliorer l'efficacité des tâches de routine. Vous pouvez également gérer les propriétés générales de votre propre compte utilisateur, telles que votre adresse postale ou votre numéro de téléphone portable.

La console Web n'affiche une tâche que si vous avez le pouvoir de l'effectuer.

- ♦ [« Démarrage de la console Web » page 15](#)
- ♦ [« Configuration de la console Web » page 16](#)
- ♦ [« Personnalisation de la console Web » page 20](#)
- ♦ [« Gestion des objets dans la console Web » page 21](#)
- ♦ [« Génération de rapports de l'historique des modifications » page 22](#)
- ♦ [« Utilisation de Workflow Automation » page 23](#)

Démarrage de la console Web

Vous pouvez démarrer la console Web à partir de tout ordinateur qui exécute Internet Explorer. Pour démarrer la console Web, indiquez l'URL appropriée 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.entDomain.com/draclient` dans le champ d'adresse de votre navigateur Web.

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

Connexion à un serveur DRA

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

Écran de connexion - Options	Description des options de connexion
Utiliser la découverte automatique	Recherche un serveur DRA automatiquement ; aucune option de configuration n'est disponible.
Connecter au serveur DRA par défaut	Les détails préconfigurés du serveur et du port sont utilisés. REMARQUE : cette option n'est disponible que si vous avez configuré le serveur DRA par défaut dans la console Web. En outre, si vous indiquez que le client doit toujours se connecter au serveur DRA par défaut, seule l'option Connecter au serveur DRA par défaut est affichée sur l'écran de connexion.
Connecter à un serveur DRA spécifique	L'utilisateur configure le serveur et le port.
Connecter à un serveur DRA qui gère un domaine spécifique	L'utilisateur spécifie un domaine géré et choisit une option de connexion : <ul style="list-style-type: none">♦ Utiliser la découverte automatique (dans le domaine spécifié)♦ Serveur primaire pour ce domaine♦ Rechercher un serveur DRA (dans le domaine spécifié)

Configuration de la console Web

Si vous disposez des pouvoirs d'administration DRA, vous pouvez configurer Advanced Authentication, les paramètres de marque et de session du client, ainsi que toutes les connexions serveur requises pour la console Web. Pour accéder à l'un de ces paramètres, connectez-vous à la console Web et sélectionnez **Administration** > **Configuration**.

REMARQUE : l'onglet **Administration** du bloc générique ne s'affiche pas si vous ne disposez pas des pouvoirs d'administration requis.

- ♦ « [Advanced Authentication](#) » page 17
- ♦ « [Image de marque de la console Web](#) » page 17
- ♦ « [Paramètres de session client](#) » page 19
- ♦ « [Connexion au serveur](#) » page 19

Advanced Authentication

Advanced Authentication vous permet de passer à une méthode davantage sécurisée qu'un simple nom d'utilisateur et mot de passe pour protéger vos informations sensibles, à savoir l'authentification multi-critères. Cette authentification est une méthode de contrôle d'accès à l'ordinateur qui implique plusieurs méthodes d'authentification issues de différentes catégories d'informations d'identification afin de vérifier l'identité d'un utilisateur.

Lorsque l'administrateur DRA configure des chaînes et des événements, si vous possédez les pouvoirs requis, vous pouvez vous connecter à la console Web et activer Advanced Authentication. Une fois l'authentification activée, tous les utilisateurs devront s'authentifier par le biais d'Advanced Authentication avant de se voir octroyer l'accès à la console Web.

Pour activer Advanced Authentication, sélectionnez **Advanced Authentication** dans l'onglet Configuration, cliquez sur **Activer Advanced Authentication**, puis configurez le formulaire conformément aux instructions fournies pour chaque champ.

Pour plus d'informations sur Advanced Authentication, reportez-vous à la section « [Authentification](#) » du *Guide de l'administrateur de DRA*.

Image de marque de la console Web

Vous pouvez personnaliser l'écran de connexion et le bloc générique de la console Web de DRA, comme suit :

- ♦ **Bloc générique** : barre de navigation principale située dans la partie supérieure de la console Web après la connexion.
 - ♦ *Image du logo ou texte de remplacement* : élément affiché à l'extrême gauche de la barre du bloc générique. Vous pouvez afficher une image du logo ou un texte de remplacement, mais pas les deux.
 - ♦ *Couleur du bloc générique* : couleur appliquée à tout le bloc générique, à l'exception de la zone de l'image du logo.
- ♦ **Écran de connexion avec thème** : aspect de la page de connexion lorsque vous accédez à l'URL de la console Web dans votre navigateur. Le thème DRA est configuré et activé par défaut.
 - ♦ *Image du logo ou texte de remplacement* : élément affiché au-dessus des champs de titre du produit et d'informations d'identification. Vous pouvez afficher une image du logo ou un texte de remplacement, mais pas les deux.
 - ♦ *Titre de l'application* : élément affiché entre les champs d'informations d'identification et l'image du logo.
 - ♦ *Boîte de dialogue modale de notification* : zone de message qui recouvre et masque la page de connexion jusqu'à ce que l'utilisateur clique sur **OK**. Elle sert généralement à informer l'utilisateur que l'accès à la console implique le respect d'une stratégie de sécurité de l'entreprise. Une fois activée, cette invite est affichée pour tous les utilisateurs qui accèdent à la console Web.

Configurer le bloc générique

Pour configurer le bloc générique :





- 1 Connectez-vous à la console Web, puis accédez à **Administration > Configuration > Image de marque**.
- 2 Effectuez l'une des opérations ci-dessous. Si vous ajoutez du texte et un fichier image, seule l'image sera affichée.
 - ♦ Mettez à jour l'image du logo :
 1. Ajoutez le nom du fichier image enregistré, y compris l'extension du fichier, dans le champ Image du logo de la vignette **Bloc générique**.
 2. Enregistrez l'image du logo dans le répertoire « assets » sur le serveur Web.
Exemple :
`C:\inetpub\wwwroot\DRAClient\assets`
La taille optimale de l'image est de 56 x 56 pixels.
 - ♦ Saisissez ou écrasez le texte existant dans le champ Texte de remplacement de l'image du logo de la vignette **Bloc générique**, si nécessaire.
- 3 Cliquez sur **Enregistrer** au bas de la page pour appliquer les modifications apportées à la configuration.

Configurer l'écran de connexion

La procédure ci-dessous fournit des informations permettant de modifier les trois options configurables : le logo de la société, le titre de l'application et la boîte de dialogue modale de notification. Vous pouvez modifier autant d'options que vous souhaitez.

Pour modifier le thème par défaut dans l'écran de connexion :

- 1 Enregistrez le logo de votre société dans le dossier « assets » sur le serveur Web. Exemple :
`C:\inetpub\wwwroot\DRAClient\assets`
La taille optimale de l'image est de 115 x 28 pixels.
- 2 Connectez-vous à la console Web, puis accédez à **Administration > Configuration > Image de marque**.
- 3 Remplacez le nom de fichier dans le champ Image du logo de la société de la vignette **Connexion** par le nom du fichier image enregistré, y compris l'extension de fichier.
- 4 Modifiez le texte dans le champ **Titre de l'application**, si nécessaire.
- 5 Cliquez sur **Afficher une boîte de dialogue modale de notification lors de la connexion** pour activer ce paramètre, puis saisissez un titre pour l'invite de notification. Saisissez ou collez le contenu du message qui doit s'afficher pour les utilisateurs dans le champ **Contenu**. Exemple :
Vous vous connectez à un réseau sécurisé. En vous connectant à ce système, vous consentez à respecter les stratégies de sécurité de l'entreprise en matière d'accès au réseau.
- 6 Sélectionnez le style du message. Le style modifie l'indicateur d'image joint à la zone de message (voir ci-dessous). Si vous le souhaitez, vous pouvez cliquer sur **Aperçu** pour afficher le message.

	Information		Erreur
	Avertissement		Question

- 7 Cliquez sur **Enregistrer** dans le bas de la page pour appliquer les modifications apportées à la configuration.

Paramètres de session client

Dans les paramètres de session client, vous pouvez définir un délai d'inactivité à l'issue duquel la console Web se déconnecte automatiquement ou indiquer qu'elle ne se déconnecte jamais automatiquement.

Pour configurer la déconnexion automatique au niveau de la console Web, accédez à **Administration > Configuration > Paramètres de session client**. Activez la fonction de déconnexion automatique à l'aide du commutateur et, si nécessaire, modifiez le paramètre de durée d'inactivité, en minutes.

Connexion au serveur

Lorsque vous accédez à la page de connexion de la console Web dans votre navigateur, vous pouvez configurer des paramètres **Options** afin de définir le mode de connexion à DRA. Ces paramètres sont également accessibles via l'option **Connexion au serveur** du menu de profil utilisateur de la console Web. Le port de service par défaut du serveur DRA est 8775. Vous pouvez définir un nouveau paramètre par défaut pour le serveur DRA dans le profil utilisateur ou les options d'écran de connexion si aucune option par défaut n'est activée. Les paramètres de connexion de la configuration de la connexion au serveur sont conservés avec votre profil utilisateur Windows.

Vous trouverez ci-dessous des informations sur les paramètres que vous pouvez modifier à partir de la configuration de la **connexion au serveur**, soit à partir du menu Options de l'écran de connexion, soit à partir du menu de profil utilisateur après la connexion :

Paramètres du serveur DRA	Description
Utiliser la découverte automatique	Recherche un serveur DRA automatiquement ; aucune option de configuration n'est disponible.
Connecter au serveur DRA par défaut (Accessible uniquement si la valeur par défaut est activée dans la configuration de la connexion au serveur.)	Utilise le paramètre par défaut de la configuration de la connexion au serveur (si elle est activée). Aucune option de configuration n'est disponible.
Connecter à un serveur DRA spécifique	L'utilisateur configure le serveur et le port.

Si vous le souhaitez, vous pouvez configurer un emplacement, un serveur et un domaine par défaut pour le serveur DRA à partir de la configuration de la **connexion au serveur** dans la console Web.

Pour activer les paramètres par défaut, connectez-vous à la console Web, puis accédez à **Administration > Configuration > Connexion au serveur DRA**. Activez les paramètres de connexion à utiliser, puis cliquez sur **Enregistrer**.

Connexion à un serveur DRA

La configuration de la connexion au serveur DRA inclut la définition d'un emplacement de serveur par défaut, la modification du port (si nécessaire) et la détermination d'un timeout de connexion, en secondes. Vous pouvez également désactiver le paramètre avec le commutateur.

Lorsque vous fournissez l'emplacement du serveur DRA, utilisez le format illustré dans l'exemple ci-dessous :

```
nom_serveur.nom_domaine.com
```

Personnalisation de la console Web

Vous pouvez personnaliser les propriétés d'objet dans la console Web. Lorsqu'elles sont implémentées correctement, les personnalisations de propriété vous aident à automatiser les tâches de gestion des objets.

Personnalisation de pages de propriétés

Si vous disposez des pouvoirs d'administration DRA, vous pouvez personnaliser les formulaires de propriétés d'objet que vous utilisez dans votre rôle de gestion Active Directory par type d'objet. Cela comprend la création et la personnalisation de nouvelles pages d'objet basées sur des types d'objet intégrés à DRA. Vous pouvez également modifier les propriétés des types d'objet intégrés.

Les objets de propriétés sont clairement définis dans la liste Pages de propriétés de la console Web pour vous permettre d'identifier facilement les pages d'objet intégrées, les pages intégrées personnalisées et les pages non intégrées qui ont été créées par un administrateur.





Personnalisation d'une page de propriétés d'un objet

Vous pouvez personnaliser les formulaires de propriétés d'objet en ajoutant ou en supprimant des pages, en modifiant les pages et 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 également possible de configurer le moment d'exécution. Ainsi, l'administrateur peut spécifier si les gestionnaires doivent être exécutés immédiatement (à chaque pression sur une touche), lorsque le champ perd le focus ou après un délai spécifié.

La liste d'objets dans les pages de propriétés propose les types d'opération pour chaque type d'objet : Créer un objet et Éditer les propriétés. Il s'agit des opérations principales que les assistants administrateur effectuent dans la console Web. Pour y accéder, ils sélectionnent **Management** (Gestion) > **Search** (Rechercher) ou **Advanced Search** (Recherche avancée). Ils peuvent y créer des objets dans le menu déroulant Create (Créer) ou éditer des objets existants sélectionnés dans le tableau des résultats de la recherche à l'aide de l'icône Properties (Propriétés).

Pour personnaliser une page de propriétés d'objet au niveau de la console Web :

- 1 Connectez-vous à la console Web avec des privilèges d'administration DRA.
- 2 Accédez à **Administration > Personnalisation > Pages de propriétés**.

- 3 Sélectionnez un objet et un type d'opération (Créer un objet ou Éditer l'objet) dans la liste des pages de propriétés.
- 4 Cliquez sur l'icône **Propriétés** (Propriétés) .
- 5 Personnalisez le formulaire de propriétés d'objet en effectuant une ou plusieurs des opérations suivantes, puis appliquez les modifications apportées :
 - ♦ Ajouter une nouvelle page de propriétés : **+ Add Page** (+ Ajouter une page)
 - ♦ Réorganiser et supprimer des pages de propriétés
 - ♦ Sélectionner une page de propriétés et la personnaliser :
 - ♦ Réorganiser les champs de configuration sur la page :  
 - ♦ Modifier les champs ou les sous-champs : 
 - ♦ Ajouter un ou plusieurs champs : **+** ou **Insert a new Field** (Insérer un nouveau champ)
 - ♦ Supprimer un ou plusieurs champs : **×**
 - ♦ Créer des questionnaires personnalisés pour les propriétés à l'aide de scripts, de fenêtres de messages ou de requêtes (LDAP, DRA ou REST)

Pour plus d'informations sur l'utilisation de questionnaires personnalisés, reportez-vous à la section « [Ajout de questionnaires personnalisés](#) » dans le *Guide de l'administrateur de DRA*.

Création d'une nouvelle page de propriétés d'objet


Pour créer une nouvelle page de propriétés d'objet :

- 1 Connectez-vous à la console Web avec les pouvoirs d'administration DRA, accédez à **Administration > Personnalisation > Pages de propriétés**, puis cliquez sur **+ Créer**.
- 2 Créez le formulaire initial de propriétés d'objet en définissant son nom, son icône, son type d'objet et la configuration de l'opération.
Après que vous avez cliqué sur OK, les opérations de création sont ajoutées au menu déroulant Créer et les opérations liées aux propriétés s'affichent dans le formulaire d'objet lorsque l'utilisateur sélectionne et édite un objet de la liste de recherche.
- 3 Personnalisez le nouveau formulaire en fonction de vos besoins. Reportez-vous à la section [Personnalisation d'une page de propriétés d'un objet](#).

Gestion des objets dans la console Web

Pour gérer les objets dans la console Web, accédez au bloc générique Management (Gestion). Vous pouvez y rechercher des objets par type dans les domaines gérés, les locataires Azure, les conteneurs et la corbeille. Au sein d'un domaine ou d'un locataire Azure, vous pouvez gérer les objets Active Directory et Azure Active Directory à l'aide de DRA, ainsi qu'effectuer des opérations sur ces objets.

Si vous sélectionnez un objet dans la liste des résultats de la recherche, toutes les opérations que vous pouvez effectuer sur cet objet sont disponibles dans la barre des tâches située au-dessus de la grille. Les options disponibles dépendent du type d'objet sélectionné, des composants actuellement configurés pour DRA et des privilèges d'administrateur qui vous sont assignés.

Pour éditer les propriétés d'un objet, placez le pointeur de la souris sur l'objet en question, puis cliquez sur l'icône **Properties** (Propriétés)  qui s'affiche sur la ligne de l'objet. Vous pouvez alors accéder à toutes les pages de propriétés de l'objet dans le volet de navigation de gauche.

IMPORTANT : si vous souhaitez **protéger un objet d'une suppression accidentelle**, faites défiler la page de propriétés **générales** jusqu'en bas, activez la case à cocher correspondante pour activer cette fonctionnalité, puis **appliquez** les modifications apportées.

Pour plus d'informations sur les opérations que vous pouvez effectuer sur les objets, reportez-vous aux rubriques suivantes :


- ♦ [Gestion des objets Active Directory](#)
- ♦ [Gestion des dossiers publics et des boîtes aux lettres Exchange](#)
- ♦ [Gestion des ressources](#)

Génération de rapports de l'historique des modifications

Si l'historique des modifications est configuré par votre administrateur DRA et que vous disposez du pouvoir **Generate UI Reports** (Générer des rapports d'interface utilisateur), vous pouvez générer des rapports de l'historique des modifications pour les objets gérés dans DRA et exporter ces rapports. Cela concerne notamment les modifications effectuées dans DRA et en dehors de DRA. Vous ne pouvez générer des rapports de l'historique des modifications qu'à partir de la console Web, qui inclut les types de rapports suivants :

- ♦ Modifications apportées par l'utilisateur
- ♦ Modifications apportées à l'utilisateur
- ♦ Boîtes aux lettres utilisateur créées par l'utilisateur
- ♦ Boîtes aux lettres utilisateur supprimées par l'utilisateur
- ♦ Adresses électroniques de groupes et de contacts créées par l'utilisateur
- ♦ Adresses électroniques de groupes et de contacts supprimées par l'utilisateur
- ♦ Attributs virtuels créés ou désactivés par l'utilisateur
- ♦ Objets déplacés par l'utilisateur



Pour générer des rapports de l'historique des modifications unifiées (UCH) :

- 1 Lancez la console Web.
- 2 Accédez à **Gestion > Rechercher**.
- 3 Définissez les critères de recherche à l'aide des options **Rechercher par**, **Terme à rechercher**, **OBJETS** et **ÉTENDUE**.
- 4 Cliquez sur le bouton **Rechercher** pour afficher les résultats de la recherche.
- 5 Sélectionnez les objets pour lesquels vous souhaitez générer des rapports.
- 6 Cliquez sur l'icône **Afficher les rapports de l'historique des modifications** .

Dans le formulaire Rapport de l'historique des modifications unifiées, vous pouvez éditer et générer vos critères de rapport à l'aide des options **Type**, **Objet(s) cible(s)**, **Plage de dates** et **Nombre maximal de lignes** pour inclure la définition des serveurs sur lesquels les modifications sont détectées (DRA et Change Guardian).

- 7 Cliquez sur **Générer** pour récupérer les données d'audit et générer un rapport UCH.
- 8 Vous pouvez trier et exporter le rapport au format requis, par exemple, CSV ou HTML.

Pour créer un fichier CSV du rapport affiché, vous pouvez exporter toutes les modifications générées ou uniquement celles qui sont affichées sur la page actuelle en exécutant l'une des options suivantes après avoir généré le rapport à l'aide des étapes ci-dessus :

- ♦ Cliquez sur **Exporter tout**  et enregistrez le rapport exporté.
 - ♦ Cliquez sur **Exporter la page actuelle**  et enregistrez le rapport exporté.
- Si nécessaire, modifiez le nombre de modifications affichées sur la page (maximum 200 éléments).

Utilisation de Workflow Automation

Workflow Automation permet d'automatiser les processus informatiques en lançant des formulaires de workflow qui s'exécutent lors de l'exécution d'un workflow ou lorsqu'ils sont déclenchés par un événement de workflow nommé, créé sur le serveur d'automatisation de workflow.

Une fois créés ou modifiés, les formulaires de workflow sont enregistrés sur le serveur Web. Lorsque vous vous connectez à la console Web de ce serveur, vous aurez accès aux formulaires en fonction des pouvoirs qui vous ont été délégués et de la configuration des formulaires. Les formulaires sont généralement accessibles à tous les utilisateurs possédant des informations d'identification pour le serveur Web. Des pouvoirs appropriés sont nécessaires pour soumettre le formulaire.

Lancement d'un formulaire de workflow : les workflows sont créés sur le serveur d'automatisation de workflow qui doit être intégré à DRA via la console Web. Pour pouvoir enregistrer un nouveau formulaire, l'option **Lancer le workflow spécifique** ou **Déclencher le workflow par événement** doit être configurée dans les propriétés de formulaire. Vous trouverez plus d'informations sur ces options ci-dessous :

- ♦ **Lancer le workflow spécifique** : cette option répertorie tous les workflows disponibles en production sur le serveur de workflow pour DRA. Pour que les workflows viennent remplir cette liste, ils doivent être créés dans le dossier `DRA_Workflows` du serveur d'automatisation de workflow.
- ♦ **Déclencher le workflow par événement** : cette option permet d'exécuter des workflows avec des déclencheurs prédéfinis. Les workflows avec des déclencheurs sont également créés sur le serveur d'automatisation de workflow.

REMARQUE : seuls les formulaires de workflow configurés avec l'option Launch Specific Workflow (Lancer le workflow spécifique) auront un historique d'exécution consultable dans le volet de recherche principal sous **Tasks** (Tâches) > **Requests** (Requêtes).

Pour plus d'informations sur Workflow Automation, reportez-vous aux guides suivants disponibles sur le [site de documentation relative à DRA](#) :

- ♦ *Guide de l'administrateur de DRA*
- ♦ *Guide de l'administrateur de WFA*
- ♦ *Guide de l'utilisateur de WFA*
- ♦ *Guide sur la création de processus WFA*

Gestion des comptes et des ressources

Le nœud Account and Resource Management (Gestion des comptes et des ressources) de la console de délégation et de configuration permet d'accéder à la plupart des tâches des assistants administrateur de DRA, qui pourvoient aux besoins de gestion de l'entreprise depuis les problèmes d'administration de base jusqu'à ceux plus complexes adressés au service d'assistance. Grâce au nœud de gestion des comptes et des ressources, vous pouvez effectuer des tâches correspondantes et gérer les boîtes aux lettres Microsoft Exchange.

Le nœud de gestion des comptes et des ressources contient les nœuds suivants :

Tous mes objets gérés

Permet de gérer des objets, tels que des comptes utilisateur, groupes, contacts, ressources, groupes dynamiques, groupes de distribution dynamiques, boîtes aux lettres de ressources et dossiers publics pour chaque domaine sur lequel vous disposez de certains pouvoirs.

Assignations temporaires à des groupes

Permet de gérer les adhésions à des groupes d'utilisateurs qui ont uniquement besoin d'une adhésion à un groupe pour une période spécifique.

Requêtes avancées

Permet de gérer les requêtes avancées disponibles sur le serveur d'administration.

Corbeille

Permet de gérer les comptes utilisateur, groupes, ressources et contacts supprimés pour tout domaine Microsoft Windows pour lequel la corbeille est activée.

Pour accéder au nœud Account and Resource Management (Gestion des comptes et des ressources), cliquez sur **Delegation and Configuration** (Délégation et configuration) dans le dossier de programmes d'administration NetIQ, puis développez le nœud Delegation and Configuration (Délégation et configuration) de la console.

Lorsque vous démarrez la console de délégation et de configuration, vous vous connectez au meilleur serveur d'administration disponible dans le domaine local. Le meilleur serveur d'administration disponible est le serveur le plus proche, à savoir généralement un serveur du site réseau. Lors de la recherche du meilleur serveur d'administration disponible, DRA fournit une connexion plus rapide et des performances améliorées.

Pour plus d'informations sur l'utilisation du nœud de gestion des comptes et des ressources, reportez-vous aux rubriques suivantes :

- ♦ [« Connexion à un serveur d'administration ou à un domaine géré » page 25](#)
- ♦ [« Modification du titre de la console » page 25](#)
- ♦ [« Personnalisation des colonnes de la liste » page 26](#)
- ♦ [« Gestion des objets dans le nœud de gestion des comptes et des ressources » page 26](#)
- ♦ [« Exécution de requêtes avancées enregistrées » page 27](#)
- ♦ [« Restauration des paramètres de la console » page 27](#)
- ♦ [« Restrictions relatives aux caractères spéciaux » page 28](#)
- ♦ [« Utilisation de caractères joker » page 29](#)
- ♦ [« Affichage des pouvoirs et des rôles qui vous sont assignés » page 30](#)

- ♦ « Affichage du numéro de version du produit et des correctifs installés » page 30
- ♦ « Affichage de votre licence actuelle » page 31
- ♦ « Récupération d'un mot de passe BitLocker » page 31

Connexion à un serveur d'administration ou à un domaine géré

Par défaut, DRA se connecte au meilleur serveur d'administration disponible d'un ordinateur ou domaine géré. Le meilleur serveur d'administration disponible est le serveur le plus proche, à savoir généralement un serveur du site réseau. En l'absence de serveur d'administration sur le site, DRA se connecte au serveur disponible suivant dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également spécifier le serveur d'administration ou le domaine auquel vous souhaitez vous connecter.

Au premier démarrage des interfaces utilisateur, DRA se connecte d'abord au domaine de votre compte de connexion. Si vous êtes connecté à un domaine qui n'est pas géré par un serveur d'administration, ou si DRA ne parvient pas à se connecter au serveur d'administration de ce domaine, DRA risque d'afficher un message d'erreur. Vérifiez que le serveur d'administration est disponible, puis réessayez.

Pour vous connecter à un serveur d'administration :

- 1 Dans le menu Fichier, cliquez sur **Connecter au serveur**.
- 2 Cliquez sur **Connecter à un serveur DRA spécifique**.
- 3 Entrez le nom du serveur d'administration à l'aide du format suivant : *NomOrdinateur*.
- 4 Cliquez sur **OK**.

Pour vous connecter à un ordinateur ou à un domaine géré :

- 1 Dans le menu Fichier, cliquez sur **Connecter au serveur**.
- 2 Sélectionnez l'option appropriée, puis entrez le nom du domaine ou de l'ordinateur géré.
- 3 Par exemple, pour vous connecter au domaine HOULAB, cliquez sur **Connecter à un serveur DRA qui gère un domaine spécifique**, puis tapez HOULAB.
- 4 Pour spécifier un serveur d'administration pour le domaine ou l'ordinateur géré, cliquez sur **Avancé**, puis sélectionnez l'option appropriée.
- 5 Cliquez sur **OK**.

Modification du titre de la console

Vous pouvez modifier les informations affichées dans la barre de titre de la console de délégation et de configuration. Pour une plus grande clarté et pour des raisons de commodité, vous pouvez ajouter le nom d'utilisateur avec lequel la console a été lancée et le serveur d'administration auquel la console est connectée. Dans les environnements complexes nécessitant une connexion à plusieurs serveurs d'administration à l'aide de différentes informations d'identification, cette fonctionnalité vous permet de déterminer rapidement quelle console utiliser.

Pour modifier la barre de titre de la console :

- 1 Démarrez la console de délégation et de configuration.
- 2 Cliquez sur **View** (Afficher) > **Options**.

- 3 Sélectionnez l'onglet Titre de la fenêtre.
- 4 Spécifiez les options appropriées, puis cliquez sur **OK**.

Personnalisation des colonnes de la liste

Vous pouvez sélectionner les propriétés d'objet que DRA affiche dans les colonnes de la liste. Cette fonctionnalité flexible vous permet de personnaliser l'interface utilisateur, notamment les listes des résultats de recherche, pour mieux répondre aux besoins d'administration spécifiques de votre entreprise. Par exemple, vous pouvez définir des colonnes pour afficher le nom de connexion de l'utilisateur ou le type de groupe, afin de retrouver rapidement et efficacement les données dont vous avez besoin et de les trier.

Pour personnaliser les colonnes de la liste :

- 1 Sélectionnez le noeud approprié. Par exemple, pour choisir les colonnes à afficher lorsque vous parcourez les résultats de la recherche d'objets gérés, sélectionnez **All My Managed Objects** (Tous mes objets gérés).
- 2 Dans le menu View (Afficher), cliquez sur **Choose Columns** (Sélectionner des colonnes).
- 3 Dans la liste des propriétés disponibles pour ce noeud, sélectionnez les propriétés d'objet que vous souhaitez afficher.
- 4 Pour modifier l'ordre des colonnes, sélectionnez une colonne, puis cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas).
- 5 Pour spécifier la largeur des colonnes, sélectionnez une colonne, puis entrez le nombre de pixels approprié dans le champ prévu à cet effet.
- 6 Cliquez sur **OK**.

Gestion des objets dans le nœud de gestion des comptes et des ressources

Pour gérer les objets dans le nœud de gestion des comptes et des ressources, sélectionnez **All My Managed Objects** (Tous mes objets gérés) ou un sous-nœud de l'arborescence. Vous pouvez y rechercher des objets par type dans les domaines, les conteneurs et les unités organisationnelles.

Si vous sélectionnez un objet dans la liste des résultats de la recherche, toutes les opérations que vous pouvez effectuer sur cet objet sont disponibles dans le menu **Tasks** (Tâches) de la barre d'outils ou dans le menu contextuel. Les options disponibles dépendent du type d'objet sélectionné, des composants actuellement configurés pour DRA et des privilèges d'administrateur qui vous sont assignés.

Pour éditer les propriétés d'un objet, sélectionnez l'objet en question, puis cliquez sur **Properties** (Propriétés) dans le menu **Tasks** (Tâches). Vous pouvez alors accéder à toutes les pages de propriétés de l'objet à l'aide des liens situés dans le volet de navigation de gauche.

IMPORTANT : si vous souhaitez **protéger un objet d'une suppression accidentelle**, sélectionnez l'objet en question, ouvrez **Properties** (Propriétés), sélectionnez **General** (Général), activez la case à cocher correspondante pour activer cette fonctionnalité, puis **appliquez** les modifications apportées.

Pour plus d'informations sur les opérations que vous pouvez effectuer sur les objets, reportez-vous aux rubriques suivantes :

- ♦ [Gestion des objets Active Directory](#)
- ♦ [Gestion des dossiers publics et des boîtes aux lettres Exchange](#)
- ♦ [Gestion des ressources](#)

Exécution de requêtes avancées enregistrées

Les requêtes avancées permettent de rechercher des utilisateurs, contacts, groupes, ordinateurs, imprimantes, unités organisationnelles et tout autre objet pris en charge par DRA. Si vous possédez le pouvoir *Execute Saved Advanced Queries* (Exécuter des requêtes avancées enregistrées), vous pouvez exécuter les requêtes avancées disponibles dans la liste **Saved Queries** (Requêtes enregistrées) pour tout conteneur du noeud de gestion des comptes et des ressources. Pour plus d'informations sur vos pouvoirs assignés, reportez-vous à la section [Affichage des pouvoirs et des rôles qui vous sont assignés](#).

Pour exécuter des requêtes avancées enregistrées :

- 1 Développez **Account and Resource Management** (Gestion des comptes et des ressources) > **All My Managed Objects** (Tous mes objets gérés).
- 2 Sélectionnez le conteneur approprié. Par exemple, si vous souhaitez que DRA recherche les informations d'un compte utilisateur, sélectionnez **Utilisateurs**.
- 3 Pour afficher le volet de recherche avancée, cliquez sur **Recherche avancée**.
- 4 Dans le volet de recherche avancée, sélectionnez une requête de recherche avancée dans la liste **Saved Queries** (Requêtes enregistrées).
- 5 Cliquez sur **Load Query** (Charger la requête), puis sur **Find Now** (Rechercher maintenant).

Restauration des paramètres de la console

DRA vous permet de redimensionner les fenêtres et de conserver leur nouvelle taille par la suite. DRA conserve également de nombreux autres paramètres, y compris le dernier serveur d'administration auquel vous vous êtes connecté, les colonnes ajoutées ou supprimées des résultats de la liste de même que la largeur des colonnes. Si vous souhaitez restaurer ces paramètres sur le paramètre d'origine avec lequel vous avez installé DRA, l'option de restauration des paramètres par défaut vous permet de le faire.

Pour restaurer les paramètres par défaut de la console :

- 1 Cliquez sur **View** (Afficher) > **Options**.
- 2 Sélectionnez l'onglet **Saved Settings** (Paramètres enregistrés).
- 3 Passez en revue les informations renseignées dans la fenêtre, puis cliquez sur **Restore Default Settings** (Restaurer les paramètres par défaut).

Restrictions relatives aux caractères spéciaux

Les caractères spéciaux suivants sont interdits lorsque vous assignez un nom à des comptes utilisateur, groupes, contacts, unités organisationnelles, ordinateurs, instances Active Views, groupes AA, rôles, stratégies ou déclencheurs d'automatisation. Ces restrictions de dénomination s'appliquent au nom de l'objet, ainsi qu'au nom de la règle qui définit l'objet.

Assignation d'un nom à des comptes utilisateur, groupes et ordinateurs

Lorsque vous spécifiez un nom issu d'un système d'exploitation antérieur à Windows 2000, vous ne pouvez pas utiliser les caractères spéciaux suivants :

Barre oblique inverse	\
Deux-points	:
Virgule	,
Guillemets	"
Signe égal	=
Barre oblique	/
Signe supérieur à	>
Crochet ouvrant	[
Signe inférieur à	<
Signe plus	+
Crochet fermant]
Point-virgule	;
Barre verticale	

IMPORTANT : la gestion des dossiers publics ne prend pas en charge la barre oblique inverse (\).

Lorsque vous assignez un nom à des comptes utilisateur, groupes et ordinateurs dans des domaines Microsoft Windows, vous pouvez utiliser n'importe quel caractère spécial.

Assignation d'un nom à des contacts et à des unités organisationnelles

Lorsque vous assignez un nom à des contacts et à des unités organisationnelles, vous pouvez utiliser n'importe quel caractère spécial.

Assignation d'un nom à des instances Active Views, à des rôles et à des groupes AA

Lorsque vous assignez un nom à des instances Active Views, à des rôles et à des groupes AA, vous ne pouvez pas utiliser la barre oblique inverse (\).

Assignation d'un nom à des stratégies et à des déclencheurs d'automatisation

Lorsque vous assignez un nom à des stratégies et à des déclencheurs d'automatisation, vous ne pouvez pas utiliser la barre oblique inverse (\).

Caractères non valides dans Azure

Des caractères non valides entraînent l'échec de la synchronisation entre Azure Active Directory et votre annuaire local. Pour plus d'informations sur ces caractères non valides, reportez-vous à la sous-rubrique « [Directory object and attribute preparation](#) » (Préparation des objets et des attributs d'annuaire) sur le site Web de support de Microsoft Office.

Pour vous assurer que ces caractères ne sont pas utilisés dans les propriétés de boîte aux lettres en ligne, procédez comme suit :

1. Cliquez sur le nœud Configuration Management (Gestion de la configuration) de la console de délégation et de configuration, puis sélectionnez **Update Administration Server Options** (Mettre à jour les options du serveur d'administration).
2. Cliquez sur **Azure Sync** dans le menu de l'onglet.
3. Cliquez sur **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 de caractères), puis sur **OK**.

Utilisation de caractères joker

DRA prend en charge les caractères joker dans de nombreux champs dans les consoles DRA et les commandes de l'interface de ligne de commande. Les caractères joker permettent de définir des règles qui correspondent à plusieurs objets sur une condition ou une norme spécifique, par exemple une convention de dénomination. Vous pouvez utiliser des caractères joker à la place d'expressions régulières pour réduire ou élargir l'étendue de la règle. La concordance des caractères joker n'est pas sensible à la casse. Vous pouvez également utiliser le point d'interrogation (?), l'astérisque (*) ou le caractère joker dièse (#) en tant que caractères normaux en les faisant précéder d'une barre oblique inverse (\) pour le caractère joker spécifique. Par exemple, pour rechercher abc*, entrez le texte abc*.

DRA prend en charge les caractères joker suivants. Vous ne pouvez pas utiliser de caractères joker dans les noms.

Élément de concordance	Caractère	Définition
Tout caractère	Point d'interrogation ?	Correspond précisément à un caractère
Tout chiffre	Signe dièse #	Correspond à un chiffre
Correspond à n'importe quel caractère, 0 ou plusieurs correspondances	Astérisque *	Ne remplace aucun caractère ou en remplace plusieurs

Le tableau suivant fournit des exemples de spécifications de caractères joker et ce à quoi ils correspondent et ne correspondent pas.

Exemple	Correspond à	Ne correspond pas à
Den???	Denton et Dennis	Denison
El ????o	El Campo et El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA ne prend pas en charge les spécifications de caractères joker qui contiennent des opérations logiques.

Affichage des pouvoirs et des rôles qui vous sont assignés

Les rôles et pouvoirs définissent la façon dont vous gérez des objets. Un rôle représente un ensemble de pouvoirs qui fournit les autorisations requises pour effectuer une tâche d'administration spécifique, comme créer un compte utilisateur ou déplacer des répertoires partagés.

L'administrateur DRA assigne des rôles, vous ajoute à des groupes AA spécifiques et vous associe à des instances Active Views (ensembles d'objets Domaine que vous pouvez gérer). Vous pouvez afficher ces assignations via la console de délégation et de configuration. Vous n'avez besoin d'aucun pouvoir auxiliaire pour afficher les rôles et pouvoirs qui vous sont assignés.

Pour afficher vos pouvoirs et rôles assignés :

- 1 Dans le menu File (Fichier), cliquez sur **DRA Properties** (Propriétés DRA).
- 2 Cliquez sur **Powers** (Pouvoirs).
- 3 Sélectionnez la vue appropriée. Par exemple, cliquez sur **Flat View** (Vue à plat) pour afficher un tableau de vos adhésions au groupe AA, des pouvoirs et des rôles qui vous sont assignés, et des instances Active Views associées.
- 4 Développez l'élément approprié. Par exemple, sous la colonne **Has Power** (Possède le pouvoir), développez **Roles and Powers** (Rôles et pouvoirs) pour afficher les pouvoirs ou rôles individuels qui vous sont assignés.
- 5 Cliquez sur **OK**.

Affichage du numéro de version du produit et des correctifs installés

Vous pouvez afficher le numéro de version du produit et les correctifs installés à partir de la fenêtre DRA Properties (Propriétés DRA). Cette fenêtre indique les numéros de version et répertorie les correctifs installés pour le serveur d'administration et l'ordinateur du client DRA.

Pour afficher le numéro de version du produit et les correctifs installés :

- 1 Dans le menu File (Fichier), cliquez sur **DRA Properties** (Propriétés DRA).
- 2 Cliquez sur **Général**.

- 3 Affichez les informations dont vous avez besoin.
- 4 Cliquez sur **OK**.

Affichage de votre licence actuelle

DRA nécessite un fichier de clé de licence. Vous pouvez afficher votre licence produit à partir de n'importe quel ordinateur du serveur d'administration. Vous n'avez besoin d'aucun pouvoir auxiliaire pour afficher la licence produit.

Pour afficher votre licence :

- 1 Dans le menu File (Fichier), cliquez sur **DRA Properties** (Propriétés DRA).
- 2 Cliquez sur **License** (Licence).
- 3 Passez en revue les propriétés de la licence, puis cliquez sur **OK**.

Récupération d'un mot de passe BitLocker

Microsoft BitLocker stocke ses mots de passe de récupération dans Active Directory. Si vous disposez des pouvoirs requis, vous pouvez utiliser la fonctionnalité de récupération BitLocker DRA pour rechercher et récupérer les mots de passe BitLocker oubliés par les utilisateurs finaux.

IMPORTANT : Avant d'utiliser la fonction de mot de passe de récupération BitLocker, assurez-vous que votre ordinateur est assigné à un domaine et que BitLocker est activé.

Affichage et copie d'un mot de passe de récupération BitLocker

En cas d'oubli d'un mot de passe BitLocker pour un ordinateur, il peut être réinitialisé à l'aide de la clé du mot de passe de récupération à partir des propriétés de l'ordinateur dans Active Directory. Copiez la clé du mot de passe et fournissez-la à l'utilisateur.

Pour afficher et copier le mot de passe de récupération :

- 1 Lancez la console de délégation et de configuration, puis accédez à **Account and Resource Management** (Gestion des comptes et des ressources) > **All My Managed Objects** (Tous mes objets gérés).
- 2 Sélectionnez le domaine souhaité, puis lancez une recherche pour afficher la liste de tous les ordinateurs du domaine.
- 3 Dans la liste des ordinateurs, cliquez avec le bouton droit sur l'ordinateur souhaité, puis sélectionnez **Properties** (Propriétés) > **BitLocker Recovery Password** (Mot de passe de récupération BitLocker).
- 4 À l'aide d'un clic droit, copiez le mot de passe de récupération BitLocker, puis collez le texte du mot de passe dans un fichier texte.

Recherche d'un mot de passe de récupération

Si le nom d'un ordinateur a été modifié, vous devez rechercher le mot de passe de récupération dans le domaine à l'aide des huit premiers caractères de l'ID de mot de passe.

REMARQUE : Pour rechercher le mot de passe de récupération, l'assistant administrateur doit disposer du pouvoir **View BitLocker recovery password** (Afficher le mot de passe de récupération BitLocker) sur le domaine contenant les objets Ordinateur délégués.

Pour rechercher un mot de passe de récupération à l'aide d'un ID de mot de passe :

- 1 Lancez la console de délégation et de configuration, puis accédez à **Account and Resource Management** (Gestion des comptes et des ressources) > **All My Managed Objects** (Tous mes objets gérés).
- 2 Cliquez avec le bouton droit sur **Domaine géré**, puis cliquez sur **Rechercher un mot de passe de récupération BitLocker**.

Pour trouver les huit premiers caractères du mot de passe de récupération, reportez-vous à la section **Affichage et copie d'un mot de passe de récupération BitLocker**.
- 3 Sur la page **Rechercher un mot de passe de récupération BitLocker**, collez les caractères copiés dans le champ de recherche, puis cliquez sur **Rechercher**.

DRA Reporting

DRA Reporting fournit des rapports intégrés et prêts à l'emploi qui vous permettent d'effectuer rapidement le suivi des comptes en double, des dernières connexions au compte, des détails de boîte aux lettres Microsoft Exchange, etc. Il fournit également des informations en temps réel sur les modifications apportées à votre environnement, y compris les anciennes et les nouvelles valeurs des propriétés modifiées. Vous pouvez exporter, imprimer, ou afficher des rapports ou les publier sur SQL Server Reporting Services.

DRA propose deux méthodes de génération de rapports qui vous permettent de collecter et de passer en revue les définitions des comptes utilisateur, des groupes et ressources dans votre domaine : **rapports de détail des activités** et **rapports de gestion DRA**. Accessibles au moyen de la console de délégation et de configuration, les rapports de détail des activités fournissent des informations en temps réel sur les modifications apportées aux objets de votre domaine. Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'un laps de temps spécifié à l'aide des rapports de détail des activités.

L'illustration suivante affiche un exemple de rapport de détail des activités :

Changes made to 'Kathy R. Johnson' - Change History

File

Displays the activity details for the following object(s) :
Kathy R. Johnson

Drag a column header here to group by that column

Operation Status	UTC Date a...	Assistant Admi...	Operation Name	Action	Object Type
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	QUIMoveHere	MoveHere	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User

Total number o...

Les **rapports de gestion DRA** facultatifs consultés via NetIQ Reporting Center (centre de création de rapports) fournissent des informations relatives aux activités et à la configuration ainsi qu'un résumé des événements survenus dans vos domaines gérés. Certains rapports de gestion sont disponibles en tant que représentations graphiques des données. Ces rapports intégrés peuvent également être personnalisés pour vous fournir exactement les informations dont vous avez besoin.

Par exemple, vous pouvez afficher un graphique reprenant le nombre d'événements survenus dans chaque domaine géré au cours d'un laps de temps spécifié à l'aide de rapports de gestion.

DRA Reporting vous permet d'afficher les détails relatifs au modèle de sécurité DRA, tels que les définitions de groupe ActiveView et AA.

Vous devez installer et configurer les rapports de gestion facultatifs avant de pouvoir afficher ces rapports. Pour plus d'informations sur l'installation des composants de création de rapports, reportez-vous au *Guide d'installation*. Pour plus d'informations sur DRA Reporting, reportez-vous à la section « **DRA Reporting** » page 32.

Démarrez la console Reporting Center dans le groupe de programmes NetIQ > Reporting Center.

NetIQ Reporting Center

File View Report Tools Help

Back Refresh Home Reports Deploy Report... Execute Report

Navigation

- Reporting Center Home
 - Database Connections
 - Reports
 - DRA Management Reports
 - Activity Trends
 - AD Summary Reports
 - Data Reports(AD)
 - DRA Configurations Report
 - DRA Resources Reports
 - Exchange Configuration Report
 - Summarized Activity Report
 - AA Activity Details
 - Active View Events
 - Activity By Action
 - Activity By Action - Chart
 - Activity By Action - Table
 - Activity By ObjectType
 - Activity By ObjectType - Table
 - Event Summary By Table
 - Event Summary By Table - Table
 - Group Membership Change
 - Templates

Activity By Action - Chart
(NOTE - Cached Data. For live data, click Execute Report button.)

This report displays the number of DRA events that have been generated during the specified time period, grouped by action.

Report's date range: Last 7 Days (7/10/2009 to 7/9/2009)

Action	Count
Associate	21
Create	12
Delete	12
Disable	2
Enable	2
MemberAdd	3
MemberRemove	4
MoveHere	4
SendToRecycleBin	8
SetInfo	1
Copy	1

Database Connection

Database Connection:
DRA Reporting DataSource

Database Connection

- Time
- All changes
- Action
- Object Type
- Event type

Context Properties

Activity By Action - Chart

- ◆ « Présentation de DRA Reporting » page 34
- ◆ « Mode d'utilisation des archives de journaux par DRA » page 35
- ◆ « Présentation des dates et heures » page 36
- ◆ « Tâches de création de rapports DRA » page 36

DRA Reporting propose deux méthodes de génération de rapports qui vous permettent de consulter les derniers changements apportés à votre environnement, mais aussi de collecter et de passer en revue le compte utilisateur, le groupe et les définitions de ressources dans votre domaine.

Accessibles via le nœud Account and Resource Management (Gestion des comptes et des ressources) de la console de délégation et de configuration, ces rapports fournissent des informations en temps réel sur les modifications apportées aux objets de votre domaine.

Rapports de gestion DRA

Accessibles via NetIQ Reporting Center (centre de création de rapports), ces rapports fournissent des informations relatives aux activités et à la configuration ainsi qu'un résumé des événements survenus dans vos domaines gérés. Certains rapports sont disponibles sous forme de représentations graphiques des données.

Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'un laps de temps spécifié à l'aide des rapports de détail des activités. Vous pouvez également afficher un graphique reprenant le nombre d'événements survenus dans chaque domaine géré au cours d'un laps de temps spécifié à l'aide de rapports de gestion. DRA Reporting vous permet également d'afficher les détails relatifs au modèle de sécurité DRA, tels que les définitions de groupe ActiveView et AA.

DRA désactive les fonctions et les rapports qui ne sont pas pris en charge par votre licence. Vous devez également disposer des pouvoirs appropriés pour exécuter et afficher des rapports. Il se peut donc que vous n'ayez pas accès à certains rapports.

Les rapports de gestion DRA peuvent être installés et configurés en tant que fonction facultative et s'affichent 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 la 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 :

- ♦ des rapports d'activité mentionnant qui a fait quoi et quand ;
- ♦ des rapports de configuration indiquant l'état d'AD ou de DRA à un moment spécifique ;
- ♦ des rapports récapitulatifs reprenant le volume des activités.

Pour plus d'informations sur la configuration de la collecte de données pour les rapports de gestion, reportez-vous au *Guide de l'administrateur*.

Mode d'utilisation des archives de journaux par DRA

Pour vous permettre d'examiner les opérations des assistants administrateur et d'établir des rapports à leur sujet, DRA consigne toutes les opérations des utilisateurs dans l'archive de journal sur l'ordinateur du serveur d'administration. Les opérations des utilisateurs incluent toutes les tentatives de modification de définitions, telles que la mise à jour des comptes utilisateur, la suppression de groupes ou la redéfinition des instances ActiveView. DRA consigne également des opérations internes spécifiques, telles que l'initialisation du serveur d'administration et des informations associées au serveur. En plus de consigner ces événements d'audit, DRA consigne l'ancienne et la nouvelle valeur de l'événement afin que vous puissiez voir exactement ce qui a été modifié.

DRA utilise un dossier **NetIQLogArchiveData**, appelé une **archive de journal** afin de stocker en toute sécurité les données de journal archivées. DRA archive les journaux au fil du temps, puis supprime les données les plus anciennes afin de libérer de l'espace pour les données les plus récentes grâce à un processus dit de nettoyage.

DRA utilise les événements d'audit stockés dans les fichiers d'archivage des journaux pour afficher les rapports de détail des activités, notamment les modifications apportées à un objet au cours d'une période donnée. Vous pouvez également configurer DRA afin d'exporter les informations de ces fichiers d'archivage de journaux vers une base de données SQL Server qui permettra à NetIQ Reporting d'afficher les rapports de gestion.

DRA consigne systématiquement les événements d'audit dans l'archive de journal. Vous pouvez aussi activer ou désactiver l'écriture des événements DRA dans les journaux d'événements Windows.

Pour plus d'informations sur l'audit DRA, reportez-vous au *Guide de l'administrateur*.

Présentation des dates et heures

DRA utilise le **format de date abrégée** et le **style de l'heure** spécifié dans le cadre de l'application des paramètres régionaux du panneau de configuration pour l'affichage du rapport. Les rapports DRA affichent la date et l'heure au format du temps universel coordonné (UTC) ainsi que la date et l'heure locales des événements. Les rapports DRA prennent en charge les formats de date suivants :

- ♦ m/j/aa
- ♦ m-j-aa
- ♦ m/j/aaaa
- ♦ m-j-aaaa
- ♦ mm/jj/aa
- ♦ mm-jj-aa
- ♦ mm/jj/aaaa
- ♦ mm-jj-aaaa
- ♦ jj/mm/aa
- ♦ jj-mm-aa
- ♦ jj/mm/aaaa
- ♦ jj-mm-aaaa

Tâches de création de rapports DRA

Pour générer des rapports de gestion DRA, installez Reporting Center et activez la collecte des données dans DRA. Pour plus d'informations sur l'activation de la collecte des données, reportez-vous au *Guide de l'administrateur*. Pour générer des rapports de détail des activités, cliquez avec le bouton droit sur n'importe quel objet, puis cliquez sur **Création de rapports** pour afficher vos choix concernant les rapports sur cet objet. Les sections suivantes vous guident tout au long des différentes tâches de création de rapports.

Affichage des rapports de détail des activités

Les rapports de détail des activités affichent des informations sur les modifications apportées à votre environnement. Vous pouvez afficher ou imprimer un rapport, mais aussi enregistrer un rapport dans Excel, au format CSV ou TXT. Pour afficher ou imprimer des rapports, vous devez être associé au rôle d'administration de création de rapports.

Lorsque vous affichez des rapports, entrez des critères pour spécifier la durée pour laquelle vous souhaitez afficher des informations. Vous pouvez également choisir d'afficher un rapport se limitant aux modifications apportées à certains serveurs DRA, et vous pouvez limiter le nombre de lignes à inclure dans le rapport. Si la taille du rapport dépasse une des limites suivantes, DRA affiche un message indiquant que le rapport n'est pas complet :

- ♦ La taille est supérieure à 500 Mo.
- ♦ La durée d'interrogation nécessaire de tous les serveurs DRA dépasse 5 minutes.
- ♦ Le nombre de lignes à afficher est supérieur à 1000.

Vous avez la possibilité d'afficher le rapport contenant uniquement les informations récupérées avant d'atteindre une de ces limites, ou vous pouvez modifier les critères du rapport pour afficher un rapport qui correspond à ces limites.

Pour afficher un rapport :

- 1 Dans le volet de gauche, développez **Tous mes objets gérés**.
- 2 Pour spécifier l'objet pour lequel vous souhaitez afficher un rapport, procédez comme suit :
 - 2a **Si vous connaissez l'emplacement de l'objet**, sélectionnez le domaine et l'unité organisationnelle qui contient cet objet.
 - 2b Dans le volet de recherche, indiquez les attributs d'objet, puis cliquez sur **Find Now** (Rechercher maintenant).
- 3 Dans le volet de la liste, cliquez avec le bouton droit sur l'objet, puis cliquez sur **Reporting** (Création de rapports).
- 4 Sélectionnez le type de rapport, tel que **Modifications apportées à objectName** ou **Modifications apportées par objectName**. Les rapports disponibles varient en fonction du type d'objet sélectionné.
- 5 Sélectionnez les dates de début et de fin pour spécifier les modifications que vous souhaitez afficher.
- 6 **Si vous souhaitez modifier le nombre de lignes à afficher**, entrez un nombre à la place de 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 que vous utilisez la valeur par défaut de 250 lignes à afficher, le rapport peut afficher jusqu'à 750 lignes.

- 7 **Si vous souhaitez que le rapport inclue uniquement certains serveurs d'administration**, sélectionnez **Restrict query to these DRA servers** (Limiter la requête à ces serveurs DRA) et tapez le nom du serveur ou les noms que vous souhaitez voir figurer dans le rapport. Séparez le nom des différents serveurs par une virgule.
- 8 Cliquez sur **OK**.

REMARQUE : DRA peut mettre jusqu'à 5 secondes avant d'afficher les modifications récentes apportées aux rapports. Par conséquent, patientez au moins 5 secondes après avoir apporté une modification avant de tenter d'afficher un rapport qui la contient.

Exportation des rapports de détail des activités

Les rapports de détail des activités peuvent être exportés aux formats suivants : XLS, CSV et TXT. Le format par défaut est Microsoft Excel.

Pour exporter les rapports de détail des activités :

- 1 Dans la fenêtre Report (Rapport), dans le menu File (Fichier), cliquez sur **Preview and Export** (Aperçu et Exporter).
- 2 Dans la fenêtre Preview (Aperçu), dans le menu File (Fichier), cliquez sur **Export Document** (Exporter le document) > **Excel File** (Fichier Excel).
- 3 Sélectionnez vos options d'exportation, puis cliquez sur **OK**.
- 4 Dans la fenêtre Enreg. sous, entrez un nom pour le fichier, puis cliquez sur **Enregistrer**.

Impression des rapports de détail des activités

Pour imprimer des rapports, vous devez être associé au rôle d'administration de création de rapports. Vous pouvez afficher ou imprimer des rapports de détail des activités, mais aussi enregistrer un rapport sous divers formats.

Pour imprimer des rapports de détail des activités :

- 1 Dans la fenêtre Report (Rapport), dans le menu File (Fichier), cliquez sur **Preview and Export** (Aperçu et Exporter).
- 2 Dans la fenêtre Preview (Aperçu), dans le menu File (Fichier), cliquez sur **Print** (Imprimer).

Affichage des rapports de gestion

Vous devez installer DRA Reporting et configurer les collecteurs de données DRA pour pouvoir afficher les rapports de gestion dans Reporting Center. Pour plus d'informations sur l'installation de DRA Reporting et la configuration des collecteurs DRA, reportez-vous au *Guide de l'administrateur*.

Lorsque vous vous connectez à Reporting Center, le service Web utilise IIS pour valider les informations d'identification du compte selon la façon dont vous avez configuré le service Web lors de l'installation.

Pour afficher les rapports de gestion :

- 1 Connectez-vous à l'ordinateur qui exécute la console Reporting Center.
- 2 Démarrez la **console Reporting Center** dans le groupe de programmes NetIQ > Reporting Center.
- 3 Fournissez les informations requises dans la boîte de dialogue de connexion, puis cliquez sur **Logon** (Connexion).
- 4 Dans le volet de navigation, développez **Reports** (Rapports) > **DRA Management Reports** (Rapports de gestion DRA).

- 5 Développez les catégories de rapport jusqu'à ce que vous trouviez un rapport que vous souhaitez afficher.
- 6 Cliquez sur son nom dans le volet de navigation pour que le rapport se charge dans le volet de résultats de Reporting Center et affiche les données mises en cache.
- 7 **Si vous souhaitez afficher les données les plus récentes du rapport**, cliquez sur **Execute Report** (Exécuter le rapport) dans le volet des résultats.

Vous pouvez modifier les paramètres de contexte par défaut pour afficher d'autres résultats de rapport. Pour plus d'informations sur les paramètres de contexte de Reporting Center, reportez-vous au *Guide de l'administrateur*.

Personnalisation des rapports de gestion

DRA contient plus de 60 rapports de gestion. Reporting Center vous offre la flexibilité de personnaliser et de déployer ces rapports de nombreuses manières. Pour plus d'informations sur la personnalisation et le déploiement de rapports de gestion dans Reporting Center, reportez-vous au *Guide de l'administrateur*.

Pour personnaliser un rapport de gestion :

- 1 Affichez un rapport similaire à celui que vous souhaitez créer. Pour plus d'informations, reportez-vous à la section [Affichage des rapports de gestion](#).
- 2 Personnalisez le rapport en modifiant ses propriétés et ses paramètres de contexte pour afficher les informations souhaitées.
- 3 Cliquez sur **Execute Report** (Exécuter le rapport).
- 4 Dans le menu Report (Rapports), cliquez sur **Save Report As** (Enregistrer le rapport sous), spécifiez un titre pour le rapport et l'emplacement auquel vous souhaitez l'enregistrer.
- 5 Cliquez sur **Save** (Enregistrer).

Pour plus d'informations sur l'utilisation des rapports de gestion dans Reporting Center, reportez-vous au *Guide de l'administrateur*.

3 Gestion des objets Active Directory

Ce chapitre contient des informations sur les concepts et les procédures de gestion des comptes utilisateur, groupes, groupes dynamiques, groupes de distribution dynamique et contacts au niveau du nœud Account and Resource Management (Gestion des comptes et des ressources) de la console de délégation et de configuration ainsi qu'au niveau de la console Web. Les informations relatives aux comptes utilisateur sont plus complètes afin de donner un exemple de méthode de gestion des objets en général dans les deux applications clientes.

- ♦ [« Gestion des comptes utilisateur » page 41](#)
- ♦ [« Gestion des groupes » page 48](#)
- ♦ [« Gestion des groupes de distribution dynamiques » page 54](#)
- ♦ [« Gestion des groupes dynamiques » page 56](#)
- ♦ [« Gestion des contacts » page 61](#)
- ♦ [« Gestion des comptes de service administrés de groupe » page 62](#)

Gestion des comptes utilisateur

Microsoft Windows se base sur le type de compte utilisateur pour déterminer les autorisations d'accès du compte utilisateur associé. Un compte utilisateur peut être global ou local. DRA prend également en charge des objets InetOrgPerson, mais les identifie comme de utilisateurs normaux.

Compte utilisateur global

Ce compte utilisateur peut être utilisé dans n'importe quel domaine qui approuve le domaine dans lequel le compte utilisateur a été créé. Vous pouvez accorder des autorisations spécifiques à un compte utilisateur. Vous pouvez également faire en sorte qu'un compte utilisateur devienne membre d'un groupe, puis assigner des autorisations à ce groupe. Le regroupement des comptes utilisateur vous aide à simplifier le processus de gestion des autorisations réseau pour de nombreux comptes utilisateur.

Compte utilisateur local

Un compte utilisateur local correspond à tout compte que vous employez pour vous connecter à un système d'exploitation Windows. Il vous permet d'accéder aux ressources du système situées dans votre propre espace utilisateur.

Pour plus d'informations sur la gestion des comptes utilisateur, reportez-vous aux rubriques suivantes :

- ♦ [« Comptes utilisateur dans des domaines approuvés » page 42](#)
- ♦ [« Tâches de gestion des comptes utilisateur » page 42](#)
- ♦ [« Transformation des comptes utilisateur » page 45](#)

Comptes utilisateur dans des domaines approuvés

Microsoft Windows stocke les définitions de groupe et de compte utilisateur dans le répertoire du domaine géré. Par conséquent, un serveur d'administration ne peut pas modifier les informations d'annuaire à partir d'un domaine approuvé, sauf si ce domaine est également géré par DRA.

Par exemple, au niveau du nœud de gestion des comptes et des ressources, certains groupes et comptes utilisateur affichés ne peuvent pas être modifiés. Ces groupes et comptes utilisateur sont définis dans des domaines approuvés par un des domaines gérés. Toutefois, vous pouvez ajouter des comptes et des groupes à partir d'un domaine approuvé à d'autres groupes dans le domaine géré.

Tâches de gestion des comptes utilisateur

Cette section vous guide tout au long de l'administration des comptes utilisateur dans le nœud Account and Resource Management (Gestion des comptes et des ressources) de la console de délégation et de configuration et dans la console Web. Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion sur le compte utilisateur, telles que la création et la suppression de comptes. Si vous sélectionnez plusieurs comptes utilisateur, vous pouvez effectuer certaines tâches en une seule opération, notamment supprimer, déplacer ou ajouter des utilisateurs à un groupe. Pour plus d'informations sur vos pouvoirs assignés, reportez-vous à la section [Affichage des pouvoirs et des rôles qui vous sont assignés](#).

Tâches liées aux comptes utilisateur dans le nœud de gestion des comptes et des ressources

Vous pouvez exécuter toutes les tâches applicables ci-dessous à partir du menu **Tâches** ou du menu contextuel. En règle générale, vous sélectionnez le nœud **Tous mes objets gérés** et exécutez une opération **Find Now** (Rechercher maintenant) pour rechercher et sélectionner l'objet Utilisateur de votre choix. Lors de la création d'un utilisateur, vous devez sélectionner l'unité organisationnelle ou le domaine dans lequel créer l'utilisateur. Le menu Tâches indique les tâches que vous pouvez effectuer lorsque vous sélectionnez un ou plusieurs comptes utilisateur.

Gestion de votre propre compte

Vous pouvez gérer votre propre compte en modifiant ses propriétés générales, telles que votre numéro de téléphone. Avant de gérer votre compte, vérifiez que vous disposez du pouvoir approprié.

Copie d'un compte utilisateur dans une autre instance Active View

Vous pouvez copier un compte utilisateur dans une autre instance Active View. Cette opération est appelée transfert d'un compte utilisateur. Pour copier un compte utilisateur dans une autre instance Active View, vous devez disposer du pouvoir Copy User to Another Active View (Copier l'utilisateur dans une autre instance Active View) dans les instances Active View source et cible. Le transfert d'un compte utilisateur vers une autre instance Active View ne supprime pas le compte utilisateur de l'instance Active View source.

REMARQUE : vous ne pouvez copier un compte utilisateur vers une autre instance ActiveView qu'à partir de la console de délégation et de configuration via le nœud Account and Resource Management (Gestion des comptes et des ressources).

Modification du nom d'un compte utilisateur

Vous pouvez renommer les comptes utilisateur dans le domaine géré ou dans la sous-arborescence gérée. La modification du nom de connexion de l'utilisateur modifie également le nom de la boîte aux lettres associée au compte utilisateur.

Tâches du compte utilisateur au niveau de la console Web

Vous pouvez exécuter la plupart des tâches ci-dessous à partir de l'onglet **Gestion** > **Rechercher** de la console Web. Exécutez une opération de recherche pour localiser et sélectionner l'objet Utilisateur de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches est activée avec les options de barre d'outils et les options de menu déroulant pour les **comptes** et **Exchange**. Passez le pointeur de la souris sur une icône de la barre d'outils ou cliquez sur un menu déroulant pour afficher les fonctions ou options correspondantes.

Création d'un compte utilisateur

Vous pouvez créer des comptes utilisateur dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier les propriétés, créer une boîte aux lettres, activer la messagerie électronique et spécifier des adhésions au groupe pour le nouveau compte.

REMARQUE

- ♦ Votre société peut avoir une convention de dénomination appliquée par une stratégie qui détermine le nom que vous pouvez assigner au nouveau compte utilisateur.
 - ♦ Par défaut, DRA place le nouveau compte utilisateur dans l'unité organisationnelle des utilisateurs du domaine géré.
 - ♦ Vous ne pouvez pas créer d'objets InetOrgPerson dans DRA.
-

Clonage d'un compte utilisateur

Lorsque vous clonez un compte utilisateur, tous les groupes dont l'utilisateur est membre sont automatiquement ajoutés au nouveau compte utilisateur vous permettant ainsi de gagner du temps lors de la configuration du nouveau compte. Vous pouvez ajouter ou supprimer des groupes à partir du nouveau compte, vous pouvez activer la messagerie électronique et configurer toutes les autres propriétés comme vous le feriez pour n'importe quel nouveau compte.

REMARQUE : lorsque vous clonez un objet InetOrgPerson, vous créez un compte utilisateur.

Modification des propriétés du compte utilisateur

Vous pouvez gérer les propriétés des comptes utilisateur dans le domaine géré ou dans la sous-arborescence gérée. Les pouvoirs en votre possession déterminent les propriétés que vous pouvez modifier pour un compte utilisateur. Si vous avez installé Exchange et activé la prise en charge de Microsoft Exchange, vous pouvez modifier les propriétés de boîte aux lettres associées lors de la gestion des comptes utilisateur.

REMARQUE : si les stratégies de répertoire privé sont activées, DRA modifie automatiquement le répertoire privé d'un compte utilisateur lorsque vous gérez ce compte. Par exemple, lorsque vous modifiez l'emplacement du répertoire privé, DRA tente de créer le répertoire privé spécifié

et déplace le contenu du répertoire privé précédent vers le nouvel emplacement. DRA applique également les listes de contrôle d'accès assignées du répertoire précédent au nouveau répertoire.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Activation d'un compte utilisateur

Vous pouvez activer un compte utilisateur dans le domaine géré ou dans la sous-arborescence gérée. Si vous gérez un compte Microsoft Windows, vous pouvez spécifier le contrôleur de domaine auquel DRA applique cette modification.

Lorsque vous appliquez cette modification à un contrôleur de domaine spécifique, DRA applique également cette modification au contrôleur de domaine par défaut de ce domaine géré. Pour vérifier quel contrôleur de domaine par défaut DRA utilise, affichez les propriétés du domaine.

Désactivation d'un compte utilisateur

Vous pouvez désactiver un compte utilisateur dans le domaine géré. Si vous gérez un compte Microsoft Windows, vous pouvez spécifier le contrôleur de domaine auquel DRA applique cette modification.

Lorsque vous appliquez cette modification à un contrôleur de domaine spécifique, DRA applique également cette modification au contrôleur de domaine par défaut de ce domaine géré. Pour vérifier quel contrôleur de domaine par défaut DRA utilise, affichez les propriétés du domaine.

Déverrouillage d'un compte utilisateur

Vous pouvez déverrouiller un compte utilisateur dans le domaine géré ou dans la sous-arborescence gérée.

Étant donné que DRA récupère l'état du compte utilisateur à partir du cache des comptes, l'interface utilisateur peut indiquer que le compte sélectionné est déverrouillé alors qu'il est verrouillé. DRA vous permet de déverrouiller un compte utilisateur, même si l'état du compte indique qu'il est actuellement déverrouillé. Vous pouvez également spécifier un contrôleur de domaine lorsque vous déverrouillez un compte utilisateur à l'aide de la console DRA sans devoir réinitialiser le mot de passe du compte utilisateur.

Réinitialisation du mot de passe d'un compte utilisateur

Vous pouvez réinitialiser le mot de passe d'un compte dans le domaine géré ou dans la sous-arborescence gérée. Les pouvoirs en votre possession déterminent les champs que vous pouvez modifier pour ce compte utilisateur.

Lorsque vous réinitialisez le mot de passe d'un compte utilisateur, DRA déverrouille automatiquement le compte. Vous pouvez indiquer si DRA doit générer un nouveau mot de passe pour le compte utilisateur. Vous pouvez également modifier plusieurs options de mot de passe pour le compte. Si vous gérez un compte Microsoft Windows, vous pouvez spécifier le contrôleur de domaine à partir duquel DRA applique ces modifications.

REMARQUE : lorsque vous appliquez cette modification à un contrôleur de domaine spécifique, DRA applique également cette modification au contrôleur de domaine par défaut de ce domaine géré. Pour vérifier quel contrôleur de domaine par défaut DRA utilise, affichez les propriétés du domaine.

Déplacement d'un compte utilisateur vers un autre conteneur

Vous pouvez déplacer un compte utilisateur vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Suppression d'un compte utilisateur

Vous pouvez supprimer un compte utilisateur du domaine géré ou de la sous-arborescence gérée. Si la corbeille est désactivée pour ce domaine, la suppression d'un compte utilisateur supprime définitivement ce compte d'Active Directory. Si la corbeille est activée pour ce domaine, lors de la suppression d'un compte utilisateur, celui-ci est déplacé vers la corbeille.

AVERTISSEMENT : lorsque vous créez un compte utilisateur, Microsoft Windows lui assigne un identificateur de sécurité (SID). Le SID n'est pas généré à partir du nom du compte. Microsoft Windows utilise des identificateurs de sécurité pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) pour chaque ressource. Si vous supprimez un compte utilisateur, vous ne pouvez pas restaurer les droits d'accès à ce compte en créant un nouveau compte utilisateur portant le même nom.

Spécification d'une adhésion à un groupe pour des comptes utilisateur

Vous pouvez ajouter des comptes utilisateur à partir d'un groupe spécifique du domaine géré ou de la sous-arborescence gérée ou en supprimer. Vous pouvez également afficher ou modifier les propriétés de groupes existants auxquels ce compte appartient.

Transformation des comptes utilisateur

DRA vous permet de transformer rapidement et efficacement des comptes utilisateur. Lorsque la personne associée à un compte utilisateur obtient de nouvelles responsabilités professionnelles, vous pouvez utiliser les fonctionnalités de transformation DRA. Les modèles de rôle professionnel vous permettent d'ajouter, de supprimer ou de mettre à jour rapidement les adhésions au groupe associées à un compte. Si une personne obtient une promotion, change de département ou quitte la société, la possibilité de transformer un compte utilisateur vous fera gagner du temps, de l'argent et vous évitera de devoir formuler d'hypothèses hasardeuses.

Présentation du processus de transformation

Vous pouvez utiliser les fonctionnalités de transformation d'un compte utilisateur pour répondre aux besoins suivants :

- ♦ supprimer des adhésions à un groupe à partir d'un compte utilisateur ;
- ♦ ajouter des adhésions à un groupe à un compte utilisateur ;
- ♦ modifier les propriétés d'un utilisateur ;
- ♦ supprimer des adhésions à un groupe donné tout en ajoutant des adhésions à d'autres groupes à un compte utilisateur.

Tenez compte des aspects suivants avant d'essayer de transformer un compte utilisateur :

- 1 Décidez si vous avez besoin d'ajouter, de supprimer ou d'ajouter et de supprimer des adhésions au groupe.
- 2 Passez en revue vos modèles de retrait et d'ajout actuels pour vérifier que vous disposez du modèle de comptes utilisateur nécessaire.
- 3 Au besoin, créez le modèle Comptes requis.
- 4 Effectuez les étapes de l'assistant de transformation d'un utilisateur.

Lorsque DRA transforme un utilisateur, les adhésions au groupe désignées par le modèle de retrait sont supprimées du compte utilisateur, tandis que les adhésions désignées par le modèle d'ajout sont assignées au compte utilisateur. DRA conserve intactes toutes les adhésions ne relevant pas des modèles de retrait ou d'ajout. Par exemple, une personne de votre service des ventes externe est transférée du département de vente américain vers le département de vente européen. Au sein de votre organisation, vous avez des groupes de distribution et des groupes de sécurité propres à ces équipes de vente ainsi qu'un numéro partagé par toutes les équipes de vente. L'équipe de vente américaine est associée aux groupes de distribution Listes de distribution Zones États-Unis et Listes de distribution Management Ventes États-Unis, tandis que l'équipe de vente européenne est associée aux groupes de distribution Zones Euro et Management Ventes Euro. Les deux équipes sont membres du groupe de sécurité des ventes à l'échelle mondiale, mais également des groupes de sécurité propres à leur site.

Votre modèle de retrait nommé Ventes États-Unis sera assigné aux adhésions au groupe suivantes :

- ♦ Listes de distribution Zones États-Unis
- ♦ Listes de distribution Management Ventes États-Unis
- ♦ Sécurité des ventes au niveau mondial
- ♦ Sécurité États-Unis

Votre modèle d'ajout nommé Ventes en euros sera assigné aux adhésions au groupe suivantes :

- ♦ Listes de distribution Zones Euro
- ♦ Listes de distribution Management Ventes Euro
- ♦ Sécurité des ventes au niveau mondial
- ♦ Sécurité Zone euro

Au cours du processus de transformation, le compte utilisateur du membre du personnel de vente transféré est d'abord supprimé de toutes les adhésions au groupe désignées par le modèle Ventes États-Unis, puis ajouté à toutes les adhésions au groupe désignées par le modèle Ventes Zone euro. Si cette personne était aussi membre du groupe de distribution Joueurs de poker, cette adhésion au groupe reste inchangée.

Les pouvoirs suivants permettent à un assistant administrateur de continuer à modifier un compte utilisateur pendant le processus de transformation :

- ♦ Modifier les propriétés de l'adresse lors de la transformation d'un compte utilisateur
- ♦ Modifier la description lors de la transformation d'un compte utilisateur
- ♦ Modifier le bureau lors de la transformation d'un compte utilisateur
- ♦ Modifier les propriétés du numéro de téléphone lors de la transformation d'un compte utilisateur

Vous pouvez également limiter la possibilité d'ajouter ou de supprimer des adhésions au groupe en n'accordant à un assistant administrateur qu'un seul des pouvoirs suivants :

- ♦ Ajouter un utilisateur à des groupes trouvés dans un modèle
- ♦ Supprimer un utilisateur de groupes trouvés dans un modèle

Vous pouvez utiliser une de ces options de limitation des pouvoirs pour créer un niveau de sécurité au sein de votre organisation. En donnant à certaines personnes le pouvoir de ne supprimer que les groupes trouvés dans un modèle, vous pouvez créer des comptes utilisateur temporaires. Ces comptes temporaires peuvent ensuite être examinés avant qu'un autre assistant administrateur utilise un modèle d'ajout Compte pour accorder de nouvelles adhésions au groupe.

Création de modèles de transformation de l'utilisateur

La transformation des comptes utilisateur est directement liée aux rôles et échelons des postes dans votre organisation. Envisagez de créer un modèle pour chaque rôle ou travail au sein de votre société. DRA ne fait aucune distinction entre un modèle de compte utilisateur utilisé pour l'ajout ou le retrait. Créez un seul modèle de compte utilisateur pour chaque rôle au sein de votre organisation. Au cours de la transformation, vous sélectionnez le modèle pour effectuer un ajout ou un retrait. La sélection d'un modèle de retrait n'empêche pas l'utilisation du même modèle pour un ajout lors d'une future transformation.

Pour créer un modèle de transformation de l'utilisateur, vous devez disposer de pouvoirs pour créer un compte utilisateur et l'assigner aux groupes appropriés. Ces pouvoirs peuvent être obtenus en associant votre compte avec les comptes de création et de suppression d'utilisateurs et les rôles d'administration de groupe dans les instances Active Views appropriées ou via l'assignation de pouvoirs individuels.

Transformation des comptes utilisateur

La transformation d'un compte utilisateur permet d'ajouter, de supprimer ou d'ajouter et de supprimer des adhésions au groupe du compte utilisateur. Ce workflow peut vous aider lorsque des utilisateurs changent de responsabilités pour occuper un autre poste au sein de votre organisation. Vous devez disposer du rôle de transformation d'un utilisateur d'un rôle qui contient des pouvoirs vous permettant de transformer des comptes utilisateur. Vous ne pouvez exécuter cette fonction qu'à partir de la console de délégation et de configuration via le nœud Account and Resource Management (Gestion des comptes et des ressources).

Pour transformer un compte utilisateur :

- 1 Dans le volet de gauche, développez **Tous mes objets gérés**.
- 2 Pour spécifier le compte utilisateur que vous souhaitez gérer, exécutez une opération **Find Now** (Rechercher maintenant) pour le localiser, puis sélectionnez l'objet Utilisateur.
- 3 Cliquez sur **Tasks** (Tâches) > **Transformation** (Transform).
- 4 Passez en revue la fenêtre Welcome (Bienvenue), puis cliquez sur **Next** (Suivant).
- 5 Dans la fenêtre Select User Template (Sélectionner un modèle utilisateur), utilisez l'option **Browse** (Parcourir) pour sélectionner le modèle utilisateur de retrait approprié.
- 6 Si vous souhaitez passer en revue les propriétés du modèle de retrait de compte utilisateur, cliquez sur **View** (Afficher).
- 7 Utilisez **Browse** (Parcourir) pour sélectionner le modèle d'ajout utilisateur approprié.

- 8 Si vous souhaitez passer en revue les propriétés du modèle d'ajout de compte utilisateur, cliquez sur **View** (Afficher).
- 9 Si vous possédez les pouvoirs appropriés, vous pouvez cocher la case **Change other properties of the user** (Modifier d'autres propriétés de l'utilisateur) et sélectionner des propriétés à modifier. Cliquez sur **Next** (Suivant) pour naviguer parmi les propriétés disponibles.
- 10 Cliquez sur **Next** (Suivant).
- 11 Passez en revue la fenêtre récapitulative, puis cliquez sur **Terminer**.

Gestion des groupes

En tant qu'assistant administrateur, vous pouvez utiliser DRA pour gérer les groupes et modifier leurs propriétés. Les groupes vous permettent de donner des autorisations spécifiques à un ensemble défini de comptes utilisateur. Les groupes vous permettent de contrôler les données et ressources accessibles à un compte utilisateur dans n'importe quel domaine.

Vous pouvez gérer des groupes quel que soit leur type et leur étendue. Par exemple, vous pouvez imbriquer des groupes, ce qui permet à un groupe d'hériter des autorisations d'un autre groupe. Vous pouvez aussi contrôler efficacement les adhésions aux groupes dans les différents domaines en ajoutant des groupes de domaines approuvés à d'autres groupes dans le domaine géré et en gérant les assignations temporaires à des groupes.

Pour plus d'informations sur la gestion des groupes, reportez-vous aux rubriques suivantes :

- ♦ « [Tâches de gestion des groupes](#) » page 48
- ♦ « [Gestion des assignations de groupes temporaires dans la console de délégation et de configuration](#) » page 51
- ♦ « [Gestion des assignations de groupes temporaires dans la console Web](#) » page 52

Tâches de gestion des groupes

Cette section vous guide tout au long de l'administration des groupes dans la console de délégation et de configuration via le nœud Account and Resource Management (Gestion des comptes et des ressources). Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion sur le groupe, telles que modifier les adhésions au groupe. Si vous sélectionnez plusieurs groupes, vous pouvez effectuer certaines tâches en une seule opération, notamment supprimer, déplacer ou ajouter des membres à un groupe. Le menu Tâches indique les tâches que vous pouvez effectuer lorsque vous sélectionnez un ou plusieurs groupes.

Ajout de comptes à des groupes

Vous pouvez ajouter des comptes utilisateur, des contacts et des ordinateurs à un groupe géré.

REMARQUE : cette tâche ajoute plusieurs comptes à un groupe sélectionné. Vous pouvez ajouter un seul compte à un groupe en sélectionnant le compte approprié, puis en cliquant sur Ajouter aux groupes dans le menu Tâches.

Si l'ajout d'un compte à un autre groupe augmente vos pouvoirs sur ce compte, DRA ne vous autorise pas à ajouter ce compte.

Ajout de groupes à d'autres groupes

Vous pouvez imbriquer des groupes en ajoutant un groupe à un autre groupe géré. Lorsqu'un groupe est imbriqué dans un autre groupe, le groupe enfant peut hériter des autorisations du groupe parent.

REMARQUE : si l'ajout d'un groupe à un autre groupe augmente vos pouvoirs sur le groupe source, DRA ne vous autorise pas à ajouter ce groupe.

Modification des propriétés de groupe

Vous pouvez modifier les propriétés des groupes locaux et globaux. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un groupe situé dans le domaine géré ou dans la sous-arborescence gérée. Si vous avez installé Exchange et activé la prise en charge de Microsoft Exchange, vous pouvez modifier les propriétés de liste de distribution dans le cadre de la gestion des groupes.

Création d'un groupe

Vous pouvez créer un groupe dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier des propriétés, telles que les membres du nouveau groupe.

REMARQUE

- ♦ Votre société peut avoir une convention de dénomination appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez assigner au nouveau groupe.
 - ♦ Par défaut, DRA place le nouveau groupe dans l'unité organisationnelle des utilisateurs du domaine géré.
-

Spécification des membres du groupe

Vous pouvez ajouter des comptes utilisateur, des contacts, des ordinateurs ou d'autres groupes à partir d'un groupe géré ou en supprimer. DRA vous autorise uniquement à supprimer les principaux de sécurité étrangère. Vous pouvez également afficher ou modifier les propriétés des membres du groupe existant, à l'exception des principaux de sécurité étrangère.

Lorsque vous supprimez des membres d'un groupe, DRA ne supprime pas les objets. Lorsque vous ajoutez des membres à un groupe, vous devez posséder le pouvoir de modifier les objets que vous souhaitez ajouter.

REMARQUE

- ♦ vous ne pouvez ajouter de comptes utilisateur ou de groupes à aucun des groupes spéciaux Windows (administrateurs, opérateurs de compte, opérateurs de sauvegarde ou opérateurs de serveur) à moins d'être administrateur Windows ou d'être membre de ce groupe spécial spécifique.
 - ♦ DRA vous permet d'exporter les résultats de type **Membres** dans un fichier CSV. Pour exporter les résultats de type **Membres** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membres**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.
-

Spécification d'une adhésion à un groupe pour des groupes

Vous pouvez ajouter ou supprimer un groupe à partir d'autres groupes du domaine géré ou de la sous-arborescence gérée. Vous pouvez également afficher ou modifier les propriétés de groupes existants auxquels ce groupe appartient.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Configuration des autorisations de sécurité de l'adhésion au groupe

Vous pouvez définir des autorisations de sécurité Active Directory pour les adhésions au groupe. Ces autorisations indiquent qui peut afficher (lecture) et modifier (écriture) les adhésions au groupe à l'aide de Microsoft Outlook. Ces paramètres vous permettent de sécuriser plus efficacement les listes de distribution et les groupes de sécurité dans votre environnement. Vous ne pouvez pas modifier des autorisations de sécurité héritées.

REMARQUE : lorsque vous gérez la sécurité de l'adhésion au groupe, des autorisations désactivées peuvent signaler qu'il s'agit d'autorisations héritées.

Configuration de la propriété du groupe

Vous pouvez définir la propriété de n'importe quels groupes de sécurité ou de distribution Microsoft Windows. Vous pouvez accorder l'autorisation de propriété du groupe à un compte utilisateur, un groupe ou un contact. L'octroi de la propriété d'un groupe permet au compte utilisateur, au groupe ou au contact spécifié de modifier l'adhésion de ce groupe.

REMARQUE : DRA désactive la case à cocher **Manager can update membership list** (Le gestionnaire peut mettre à jour la liste des membres) lorsque l'adhésion au groupe est masquée du serveur Microsoft Exchange. Pour cocher cette case, cliquez sur **Expose Group Membership** (Exposer l'adhésion au groupe) sous l'onglet Exchange de la fenêtre Group Properties (Propriétés de groupe).

Clonage d'un groupe

Vous pouvez cloner des groupes locaux et globaux dans les domaines gérés. Le clonage des groupes crée de nouveaux groupes du même type et avec les mêmes attributs que le groupe d'origine. DRA tente également d'ajouter tous les membres du groupe initial au nouveau groupe.

En clonant un groupe, vous pouvez créer rapidement des groupes en fonction d'autres groupes qui ont des propriétés similaires. Lorsque vous clonez un groupe, DRA complète les champs de l'assistant de clonage du groupe avec les valeurs du groupe sélectionné. Vous pouvez également modifier les propriétés du nouveau groupe.

REMARQUE

- ♦ Votre société peut avoir une convention de dénomination appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez assigner au nouveau groupe.
 - ♦ Par défaut, DRA place le nouveau groupe dans l'unité organisationnelle des utilisateurs du domaine géré.
-

Suppression d'un groupe

Vous pouvez supprimer des groupes locaux et globaux du domaine géré ou de la sous-arborescence gérée. Si la corbeille est désactivée pour ce domaine, la suppression d'un groupe supprime définitivement ce groupe d'Active Directory. Si la corbeille est activée pour ce domaine, lors de la suppression d'un groupe, celui-ci est déplacé vers la corbeille et les propriétés de ce groupe sont désactivées.

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

AVERTISSEMENT : lorsque vous créez un groupe, Microsoft Windows lui assigne un identificateur de sécurité (SID). Le SID n'est pas généré à partir du nom du groupe. Microsoft Windows utilise des identificateurs de sécurité pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) pour chaque ressource. Si vous supprimez un groupe, vous ne pouvez pas restaurer les droits d'accès à ce groupe en créant un nouveau groupe portant le même nom.

Déplacement d'un groupe vers un autre conteneur

Vous pouvez déplacer un groupe vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Exposition des adhésions au groupe dans les listes de distribution

Vous pouvez exposer les adhésions au groupe dans les listes de distribution des groupes du domaine géré ou de la sous-arborescence gérée.

Masquer les adhésions au groupe des listes de distribution

Vous pouvez masquer les adhésions au groupe dans les listes de distribution pour les groupes situés dans le domaine géré ou dans la sous-arborescence gérée.

Gestion des assignations de groupes temporaires dans la console de délégation et de configuration

Les assignations de groupes temporaires permettent de gérer les adhésions aux groupes des utilisateurs ayant uniquement besoin d'être membres d'un groupe pour une période spécifique. Cette section vous guide tout au long de l'administration des assignations de groupes temporaires dans la console de délégation et de configuration via le nœud **Account and Resource Management** (Gestion des comptes et des ressources). Si vous disposez des pouvoirs appropriés, vous pouvez effectuer des tâches telles que créer des assignations de groupes temporaires ou supprimer celles ayant expiré.

Un assistant administrateur ne peut afficher les assignations temporaires qu'aux groupes pour lesquels il a les pouvoirs de modifier l'adhésion (ajouter ou supprimer des membres).

Vous ne pouvez pas modifier le groupe associé ou modifier la liste d'utilisateurs tant que l'assignation de groupe temporaire est active. Si vous souhaitez modifier ces éléments, vous devez annuler l'assignation de groupe temporaire.

Gérer les propriétés d'attributions de groupes temporaires

Vous pouvez gérer les propriétés des attributions de groupes temporaires ou des attributions expirées enregistrées.

Si vous souhaitez reprogrammer une attribution de groupe temporaire, modifiez la planification dans les **propriétés** de l'attribution, puis enregistrez les modifications apportées.

Créer une attribution de groupe temporaire

Vous pouvez créer une attribution de groupe temporaire sur les serveurs d'administration primaire et secondaires.

Par défaut, lorsqu'une attribution de groupe temporaire arrive à expiration, elle est supprimée au bout de sept jours, sauf si vous avez sélectionné l'option **Keep this temporary group assignment for future use** (Conserver cette attribution de groupe temporaire pour une utilisation ultérieure). Pour modifier cette période de conservation, cliquez avec le bouton droit sur le nœud **Temporary Group Assignment** (Attribution de groupe temporaire) sous All My Managed Objects (Tous mes objets gérés), sélectionnez **Properties** (Propriétés), puis modifiez le nombre de jours de conservation des attributions de groupes temporaires.

Gérer les comptes utilisateur dans une attribution de groupe temporaire

Vous pouvez ajouter des comptes utilisateur aux attributions de groupes temporaires sur les serveurs d'administration primaire ou secondaires, ou en supprimer.

REMARQUE : vous pouvez uniquement gérer les comptes utilisateur des attributions de groupes temporaires qui ne sont pas encore actives.

Supprimer une attribution de groupe temporaire

Vous pouvez supprimer n'importe quelle attribution de groupe temporaire sur les serveurs d'administration primaire et secondaires.

Gestion des attributions de groupes temporaires dans la console Web

Les attributions de groupes temporaires permettent de gérer les adhésions aux groupes des utilisateurs ayant besoin d'être membres d'un groupe pour une période spécifique. Si Azure Active Directory est configuré par l'administrateur DRA, vous pouvez créer des attributions temporaires pour des groupes Azure et ajouter des utilisateurs Azure, des utilisateurs invité Azure et des utilisateurs synchronisés à une adhésion à un groupe Azure. Dans la console Web, vous pouvez créer et gérer des attributions à partir des serveurs DRA primaire et secondaires. Toutefois, les opérations que vous pouvez effectuer sur une attribution existante varient en fonction de l'état de cette attribution.

Un assistant administrateur ne peut afficher les attributions temporaires qu'aux groupes qu'il a les pouvoirs de modifier conformément aux attributions ActiveView, comme l'ajout ou la suppression de membres d'un groupe.

Pour gérer les attributions de groupes temporaires dans la console Web, accédez à **Tasks** (Tâches) > **Temporary Group Assignments** (Attributions de groupes temporaires).

Vous pouvez effectuer les opérations suivantes :

Créer une assignation de groupe temporaire

Vous pouvez créer des assignations de groupes temporaires en utilisant les groupes que vous avez les pouvoirs de modifier, ainsi que spécifier le contrôleur de domaine. Le groupe cible peut être un groupe d'un locataire géré Azure ou un groupe d'un domaine Active Directory. Lorsqu'une assignation de groupe temporaire arrive à expiration, DRA la supprime automatiquement au bout de sept jours, sauf si vous sélectionnez l'option de conservation de cette assignation pour une utilisation ultérieure.

REMARQUE : si l'assignation de groupe temporaire configurée avec l'adhésion à un groupe Azure est modifiée en dehors de DRA, cette assignation devient non valide.

Pour créer une assignation de groupe temporaire :

1. Accédez à **Tâches > Assignations de groupes temporaires**, puis cliquez sur **Créer**.
2. Cliquez sur **Sélectionner**, puis recherchez le groupe en exécutant une recherche dans le conteneur concerné.
3. Si vous devez ajouter des membres au groupe, cliquez sur **Ajouter** sous **Membres** sur la page Créer une assignation de groupe temporaire, puis recherchez et utilisez l'option **Ajouter +** dans la liste des résultats.
4. Configurez la planification.
5. Nommez l'assignation de groupe temporaire sous Informations générales, puis cliquez sur **Créer**.

Rechercher des assignations existantes

Lorsque vous recherchez des assignations de groupes temporaires existantes, ces dernières sont répertoriées dans les résultats en fonction de l'état de l'assignation. Les différents états sont les suivants :

- ♦ **Pending (En attente)** : l'assignation de groupe temporaire est planifiée pour un démarrage ultérieur. Vous pouvez effectuer les opérations suivantes : annuler, supprimer et replanifier.
- ♦ **Active (Actif)** : l'assignation de groupe temporaire a démarré et a ajouté les membres concernés au groupe. Vous pouvez effectuer les opérations suivantes : annuler et supprimer.
- ♦ **Active with Error (Actif avec erreur)** : l'assignation de groupe temporaire a démarré, mais n'est pas parvenue à ajouter tous les membres concernés au groupe. Vous pouvez effectuer les opérations suivantes : annuler et supprimer.
- ♦ **Completed (Terminé)** : l'assignation de groupe temporaire est arrivée à expiration et a supprimé tous les membres concernés du groupe. Vous pouvez effectuer les opérations suivantes : supprimer et replanifier.
- ♦ **Completed with Error (Terminé avec erreur)** : l'assignation de groupe temporaire est arrivée à expiration, mais n'est pas parvenue à supprimer tous les membres concernés du groupe. Vous pouvez effectuer les opérations suivantes : supprimer et replanifier.
- ♦ **Canceled (Annulé)** : l'assignation de groupe temporaire a été annulée par un utilisateur et a supprimé tous les membres concernés du groupe. Vous pouvez effectuer les opérations suivantes : supprimer et replanifier.

- ♦ **Canceled with Error (Annulé avec erreur)** : l'assignation de groupe temporaire a été annulée par un utilisateur, mais n'est pas parvenue à supprimer tous les membres concernés du groupe. Vous pouvez effectuer les opérations suivantes : supprimer et replanifier.
- ♦ **Error (Erreur)** : l'assignation de groupe temporaire n'est pas parvenue à ajouter ou à supprimer tous les membres. Vous pouvez effectuer les opérations suivantes : supprimer et replanifier.

Vous pouvez filtrer les résultats en fonction de ces états et d'autres critères, notamment le nom de l'assignation, le groupe cible, la durée et l'administrateur qui a créé l'assignation.

Afficher ou modifier les propriétés d'une assignation de groupe temporaire

Vous pouvez afficher ou modifier toutes les assignations de groupes temporaires définies lors de la création de l'assignation de groupe temporaire. Après avoir recherché des assignations de groupes temporaires, sélectionnez une assignation pour afficher ou modifier les propriétés correspondantes.

Si vous souhaitez replanifier une assignation de groupe temporaire, modifiez la planification dans les **propriétés** de l'assignation, puis enregistrez les modifications apportées. Si l'assignation est active, vous ne pouvez modifier que la date de fin.

IMPORTANT : vous ne pouvez pas modifier le groupe associé ou modifier la liste d'utilisateurs lorsque l'assignation de groupe temporaire est active. Si vous souhaitez modifier ces éléments, vous devez d'abord annuler l'assignation.

Annuler une assignation de groupe temporaire

Vous ne pouvez annuler une assignation de groupe temporaire que lorsqu'elle présente l'un des états suivants :

- ♦ Active (Actif)
- ♦ Active with Error (Actif avec erreur)
- ♦ Pending (En attente)

Supprimer une assignation de groupe temporaire

Vous pouvez sélectionner plusieurs assignations de groupes temporaires et les supprimer. Si l'état des assignations de groupes temporaires sélectionnées est Active (Actif), Active with Error (Actif avec erreur) ou Pending (En attente), l'option **Cancel** (Annuler) est également activée.

Gestion des groupes de distribution dynamiques

Un groupe de distribution dynamique est un objet Groupe Active Directory que vous pouvez créer pour faciliter l'envoi en masse de messages électroniques et d'autres informations.

La liste des membres d'un groupe de distribution dynamique est calculée lors de chaque envoi d'un message au groupe, en fonction des filtres et des conditions que vous définissez. Elle diffère d'un groupe de distribution standard, qui contient un ensemble défini de membres. Lorsqu'un message électronique est envoyé à un groupe de distribution dynamique, il est remis à tous les destinataires de l'organisation qui correspondent aux critères définis pour ce groupe.

DRA prend en charge les fonctionnalités suivantes :

- ♦ Audit et création de rapports concernant l'interface utilisateur

- ♦ Prise en charge de l'énumération des groupes de distribution dynamiques
- ♦ Rapport NetIQ Reporting Center (NRC) pour les groupes de distribution dynamiques
- ♦ Prise en charge de l'opération de déclenchement pour les groupes de distribution dynamiques
- ♦ Prise en charge de l'extension de l'interface utilisateur pour les groupes de distribution dynamiques Exchange

Tâches du groupe de distribution dynamique :

Création d'un groupe de distribution dynamique

Vous pouvez créer un groupe de distribution dynamique dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier des propriétés, telles que les membres du nouveau groupe de distribution dynamique.

REMARQUE

- ♦ Votre société peut avoir une convention de dénomination appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez assigner au nouveau groupe de distribution dynamique.
 - ♦ Par défaut, DRA place le nouveau groupe de distribution dynamique dans l'unité organisationnelle des utilisateurs du domaine géré.
-

Clonage d'un groupe de distribution dynamique

Vous pouvez cloner les groupes de distribution dynamiques locaux et globaux dans les domaines gérés. Le clonage des groupes de distribution dynamiques crée de nouveaux groupes de distribution dynamiques du même type et avec les mêmes attributs que le groupe de distribution dynamique d'origine.

En clonant un groupe de distribution dynamique, vous pouvez créer rapidement des groupes de distribution dynamiques en fonction d'autres groupes de distribution dynamiques qui ont des propriétés similaires. Lorsque vous clonez un groupe de distribution dynamique, DRA complète les champs de l'assistant de clonage du groupe de distribution dynamique avec les valeurs du groupe de distribution dynamique sélectionné. Vous pouvez également modifier les propriétés du nouveau groupe de distribution dynamique.

Déplacement d'un groupe de distribution dynamique vers un autre conteneur

Vous pouvez déplacer un groupe de distribution dynamique vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Suppression d'un groupe de distribution dynamique

Vous pouvez supprimer des groupes de distribution dynamiques locaux et globaux du domaine géré ou de la sous-arborescence gérée. Si la corbeille est désactivée pour ce domaine, la suppression d'un groupe de distribution dynamique supprime définitivement ce groupe d'Active Directory. Si la corbeille est activée pour ce domaine, lors de la suppression d'un groupe de distribution dynamique, celui-ci est déplacé vers la corbeille et les propriétés de ce groupe sont désactivées.

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

AVERTISSEMENT : lorsque vous créez un groupe de distribution dynamique, Microsoft Windows lui assigne un identificateur de sécurité (SID). Le SID n'est pas généré à partir du nom de groupe de distribution dynamique. Microsoft Windows utilise des identificateurs de sécurité pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) pour chaque ressource. Si vous supprimez un groupe de distribution dynamique, vous ne pouvez pas restaurer les droits d'accès à ce groupe en créant un nouveau groupe de distribution dynamique portant le même nom.

Modification des propriétés du groupe de distribution dynamique

Vous pouvez modifier les propriétés des groupes de distribution dynamiques locaux et globaux. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un groupe situé dans le domaine géré ou dans la sous-arborescence gérée.

Spécification d'un filtre

L'adhésion d'une liste de distribution dynamique est déterminée par son filtre, que vous pouvez définir.

Spécification de conditions

Les conditions définissent les critères auxquels doit répondre un objet pour être membre du groupe de distribution dynamique.

Gestion des groupes dynamiques

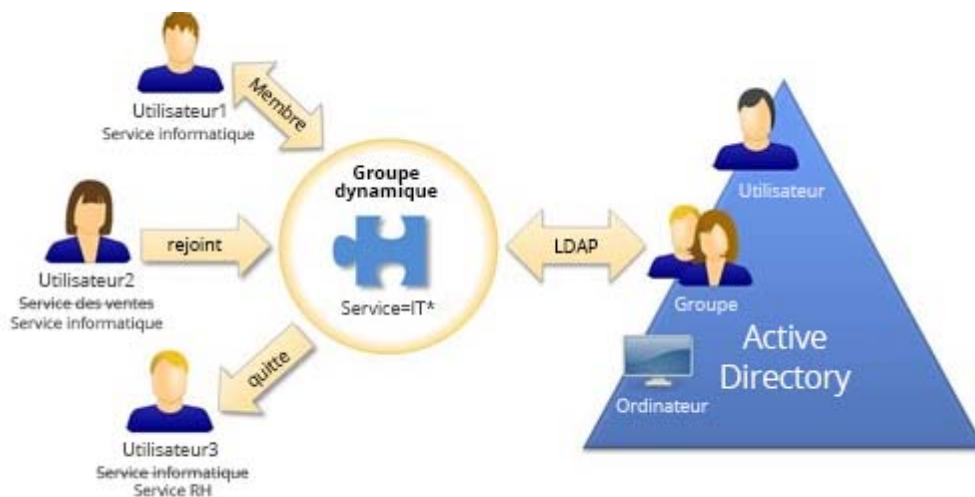
Un groupe dynamique est un groupe dont l'adhésion change en fonction d'un ensemble de critères défini. Dans DRA, vous pouvez créer des groupes dynamiques sans environnement Exchange. Les filtres d'adhésion utilisés pour gérer les groupes dynamiques dans Active Directory sont uniques à DRA.

L'administrateur DRA configure la planification de rafraîchissement du domaine pour les groupes dynamiques dans la console de délégation et de configuration. Les nouveaux membres sont ajoutés de façon dynamique au groupe lorsqu'une ou plusieurs propriétés utilisateur qui correspondent aux critères de filtre de membres du groupe sont mises à jour, puis qu'un rafraîchissement a lieu. De la même manière, un membre peut être supprimé de manière dynamique du groupe lorsque des propriétés correspondantes sont modifiées ou supprimées de l'utilisateur.

Exemple de scénario

Le graphique ci-dessous décrit une utilisation courante d'un groupe dynamique Active Directory. Le graphique contient trois groupes dynamiques. Chaque groupe comporte un ensemble de critères qui déterminent qui peut être ajouté au groupe et qui ne peut pas. Chaque groupe contrôle l'accès à un ensemble spécifique de fichiers, dossiers et applications.

SUGGESTION : vous pouvez créer une *liste de membres statiques* qui contient les membres permanents du groupe dynamique. Vous pouvez également créer une *liste des membres exclus* qui refuse à ces utilisateurs l'adhésion au groupe dynamique.



L'utilisateur 2 a rejoint le service informatique. Lors du rafraîchissement du groupe dynamique du service informatique, il sera ajouté au groupe. Lors du rafraîchissement du groupe dynamique du service des ventes, l'utilisateur 2 sera supprimé de la liste des membres.

L'utilisateur 3, qui a quitté le service informatique pour rejoindre le département RH, sera supprimé du groupe dynamique du service informatique et ajouté au groupe dynamique du service RH.

Préparation du scénario

Les informations ci-dessous fournissent un exemple des opérations que vous devez effectuer dans la console Web pour activer le scénario ci-dessus. Vous pouvez rendre un groupe existant dynamique ou en créer un. Pour des raisons de simplicité, nous n'ajouterons aucun membre statique ou exclu et nous rendrons trois groupes existants dynamiques : groupe RH, groupe Informatique et groupe Ventes.

Configuration du groupe dynamique :

- 1 Pour chaque groupe fourni ci-dessus, effectuez une opération de recherche avec le filtre de groupe activé pour localiser le groupe.
- 2 Ouvrez les **propriétés** du groupe et accédez à la page **Filtre de membres dynamiques**.
- 3 Cliquez sur le curseur **Rendre ce groupe dynamique** pour activer la fonction.
- 4 Cliquez sur **Modifier**, puis saisissez ou collez les critères du filtre de membres dans le champ Requête LDAP. Dans ce cas, nous recherchons des critères dans la propriété **User** (Utilisateur) > **Department** (Service). Les exemples ci-dessous indiquent les critères LDAP que nous utiliserons pour chaque groupe dans l'**exemple de scénario** :
 - ♦ Groupe RH : (&(objectClass=user)(objectCategory=person)(department=HR*))
 - ♦ Groupe informatique : (&(objectClass=user)(objectCategory=person)(department=IT*))
 - ♦ Groupe Ventes : (&(objectClass=user)(objectCategory=person)(department=Sales*))
- 5 Cliquez sur **Appliquer** pour enregistrer les modifications.

Opérations effectuées pour modifier dynamiquement l'affiliation des utilisateurs au groupe dans les propriétés de l'utilisateur sélectionné :

- ♦ Utilisateur 2 : remplacement de la propriété **Organization** (Organisation) > **Department** (Service) « Ventes » par « Informatique ».
- ♦ Utilisateur 3 : remplacement de la propriété **Organization** (Organisation) > **Department** (Service) « Informatique » par « RH ».

Les modifications dynamiques se produisent pendant le rafraîchissement de groupe dynamique planifié ou lors d'un rafraîchissement manuel par l'administrateur DRA.

Tâches de groupe dynamique

Les tâches de groupe dynamique que vous pouvez exécuter dans la console Web sont décrites ci-dessous.

Création d'un groupe dynamique

Vous pouvez créer un groupe dynamique dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier des propriétés, telles que les membres du nouveau groupe dynamique. Pour créer un groupe dynamique, accédez à **Créer** > **Groupe dynamique** dans le bloc générique de gestion.

REMARQUE : Votre société peut avoir une convention de dénomination appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez assigner au nouveau groupe dynamique.

Création d'un filtre

Le groupe dynamique utilise le **filtre de membres dynamiques** pour ajouter ou supprimer des utilisateurs de sa liste de membres lors de chaque rafraîchissement du groupe. Pour obtenir des exemples de création de requêtes LDAP et d'attribut virtuel pour le filtre, reportez-vous aux exemples illustrés dans les « requêtes de recherche avancée ». Bien que le filtre fasse office de critères d'adhésion au groupe et non de recherche, les exemples de requête restent applicables :

- ♦ [Exemples de requêtes LDAP](#)
- ♦ [Exemples de requêtes d'attribut virtuel](#)

Gestion de la liste des membres statiques

Les utilisateurs placés dans la liste des membres statiques d'un groupe dynamique deviennent membres permanents du groupe jusqu'à ce que vous les supprimiez manuellement. Vous pouvez modifier cette liste à partir de la page de propriétés Filtre de membres dynamiques correspondant à l'utilisateur sélectionné.

Lorsque vous supprimez des membres d'un groupe dynamique, DRA ne supprime pas les objets. Lorsque vous ajoutez des membres à un groupe dynamique, vous devez pouvoir modifier les objets que vous souhaitez ajouter.


Gestion de la liste des membres exclus

Les utilisateurs placés dans la liste des membres exclus d'un groupe dynamique ne pourront pas rejoindre le groupe tant que vous ne les aurez pas supprimés manuellement de cette liste. Vous pouvez modifier cette liste à partir de la page de propriétés Filtre de membres dynamiques correspondant à l'utilisateur sélectionné.

Clonage d'un groupe dynamique


Vous pouvez cloner des groupes dynamiques locaux et globaux dans des domaines gérés. Le clonage des groupes dynamiques crée de nouveaux groupes dynamiques du même type et avec les mêmes attributs que le groupe dynamique d'origine.

En clonant un groupe dynamique, vous pouvez créer rapidement des groupes dynamiques en fonction d'autres groupes dynamiques qui ont des propriétés similaires. Lorsque vous clonez un groupe dynamique, DRA complète les champs de l'assistant de clonage du groupe de distribution dynamique avec les valeurs du groupe dynamique sélectionné. Vous pouvez également modifier les propriétés du nouveau groupe dynamique.

Pour cloner un groupe dynamique, sélectionnez-le dans le volet des résultats de la recherche, puis cliquez sur **Cloner**  dans la barre d'outils.

Déplacement d'un groupe dynamique vers un autre conteneur

Vous pouvez déplacer un groupe dynamique vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.


Pour déplacer un groupe dynamique, sélectionnez-le dans le volet des résultats de la recherche, puis cliquez sur **Déplacer les objets**  dans la barre d'outils.

Suppression d'un groupe dynamique

Vous pouvez supprimer des groupes dynamiques locaux et globaux du domaine géré ou de la sous-arborescence gérée.

Si la Corbeille est désactivée pour ce domaine, la suppression d'un groupe dynamique supprime définitivement ce groupe d'Active Directory.


Si la corbeille est activée pour ce domaine, lors de la suppression d'un groupe dynamique, celui-ci est déplacé vers la corbeille et les propriétés de ce groupe sont désactivées. Pour plus d'informations sur la corbeille, reportez-vous à la section [Gestion de la corbeille](#).

Pour supprimer un groupe dynamique, sélectionnez-le dans le volet des résultats de la recherche, puis cliquez sur **Supprimer**  dans la barre d'outils.

AVERTISSEMENT : lorsque vous créez un groupe dynamique, Microsoft Windows lui assigne un identificateur de sécurité (SID). Le SID n'est pas généré à partir du nom de groupe dynamique. Microsoft Windows utilise des identificateurs de sécurité pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) pour chaque ressource. Si vous supprimez un groupe dynamique, vous ne pouvez pas restaurer les droits d'accès à ce groupe en créant un nouveau groupe dynamique portant le même nom.

Modification des propriétés du groupe dynamique

Vous pouvez modifier les propriétés des groupes dynamiques locaux et globaux. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un groupe situé dans le domaine géré ou dans la sous-arborescence gérée.


Pour modifier les propriétés d'un groupe dynamique, sélectionnez-le dans le volet des résultats de la recherche, puis cliquez sur **Propriétés**  dans la barre d'outils.

REMARQUE : DRA vous permet d'exporter les résultats des types **Membres** et **Membre de** dans un fichier CSV. Pour exporter les résultats des types **Membres** et **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet

Membres ou **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Ajout de groupes dynamiques à d'autres groupes dynamiques

Vous pouvez imbriquer des groupes dynamiques en ajoutant un groupe dynamique à un autre groupe dynamique géré. Lorsqu'un groupe dynamique est imbriqué dans un autre groupe dynamique, le groupe dynamique enfant peut hériter des autorisations du groupe parent.

Pour ajouter un groupe dynamique à un autre groupe dynamique, sélectionnez-le dans le volet des résultats de la recherche, puis cliquez sur **Ajouter aux groupes**  dans la barre d'outils.

REMARQUE : si l'ajout d'un groupe dynamique à un autre groupe dynamique augmente vos pouvoirs sur le groupe dynamique source, DRA ne vous autorise pas à ajouter ce groupe.

Configuration des autorisations de sécurité de l'adhésion au groupe

Vous pouvez définir des autorisations de sécurité Active Directory pour les adhésions au groupe dynamique. Ces autorisations indiquent qui peut afficher (lecture) et modifier (écriture) les adhésions au groupe dynamique à l'aide de Microsoft Outlook. Ces paramètres vous permettent de sécuriser plus efficacement les listes de distribution et les groupes dynamiques de sécurité dans votre environnement. Vous ne pouvez pas modifier des autorisations de sécurité héritées.

Vous pouvez mettre à jour ces paramètres à partir de la page de propriétés **Sécurité d'adhésion** correspondant au groupe dynamique sélectionné.

REMARQUE : lorsque vous gérez la sécurité de l'adhésion au groupe dynamique, des autorisations désactivées peuvent signaler qu'il s'agit d'autorisations héritées.

Configuration de la propriété du groupe dynamique

Vous pouvez accorder l'autorisation de propriété du groupe dynamique à un compte utilisateur, un groupe ou un contact. L'octroi de la propriété d'un groupe dynamique permet au compte utilisateur, au groupe ou au contact spécifié de modifier l'adhésion de ce groupe.

Vous pouvez mettre à jour ces paramètres à partir de la page de propriétés **Géré par** correspondant au groupe dynamique sélectionné.

Exposition des adhésions au groupe dynamique dans les listes de distribution

Vous pouvez exposer les adhésions au groupe dynamique dans les listes de distribution des groupes du domaine géré ou de la sous-arborescence gérée.

Vous pouvez accéder à cette option à partir du menu déroulant **Exchange** de la barre d'outils correspondant au groupe dynamique sélectionné.

Masquer les adhésions au groupe dynamique des listes de distribution

Vous pouvez masquer les adhésions au groupe dynamique dans les listes de distribution des groupes du domaine géré ou de la sous-arborescence gérée.

Vous pouvez accéder à cette option à partir du menu déroulant **Exchange** de la barre d'outils correspondant au groupe dynamique sélectionné.

REMARQUE : L'option **Hide Group Membership** (Masquer l'adhésion au groupe) est désactivée pour les listes de distribution Microsoft Exchange 2007.

Gestion des contacts

DRA permet de gérer de nombreux objets Réseau, y compris des contacts et les adresses électroniques associées. Les contacts sont disponibles uniquement dans les domaines Microsoft Windows en mode mixte ou natif. Contrairement aux comptes utilisateur et aux groupes, les contacts n'ont pas d'identificateur de sécurité (SID). Utilisez les contacts pour ajouter des membres aux groupes ou listes de distribution sans leur donner accès aux services réseau.

Vous pouvez ajouter des contacts à des groupes de sécurité ou de distribution dans des domaines en modes mixte et natif. Dans la mesure où les groupes de sécurité peuvent être utilisés en tant que listes de distribution dans Microsoft Windows, vous souhaitez peut-être ajouter des contacts à ces groupes. Le fait d'avoir un contact dans un groupe de sécurité global n'empêche pas le groupe d'être converti en groupe de sécurité universel lorsque vous migrez vers un domaine Microsoft Windows en mode natif.

Modification des propriétés d'un contact

Vous pouvez modifier les propriétés d'un contact. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un contact situé dans le domaine géré. Si vous avez installé et activé la prise en charge d'Exchange, vous pouvez modifier les propriétés d'adresse électronique dans le cadre de la gestion des contacts.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Création d'un contact

Vous pouvez créer des contacts dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier les propriétés, activer la messagerie électronique, indiquer des adresses électroniques et spécifier à quels groupes appartient le nouveau contact.

Pour créer un contact, accédez à **Gestion > Rechercher**, puis sélectionnez **Contact** dans le menu déroulant Créer.

Clonage d'un contact

En clonant un contact, vous pouvez créer rapidement des contacts en fonction d'autres contacts qui ont des propriétés similaires. Lorsque vous clonez un contact, DRA complète les champs de l'assistant de clonage du contact avec les valeurs du contact sélectionné. Vous pouvez également modifier les propriétés, activer la messagerie électronique, indiquer des adresses électroniques et spécifier à quels groupes appartient le nouveau contact.

Gestion des adhésions aux groupes du contact

Vous pouvez ajouter des contacts à partir d'un groupe spécifique du domaine géré ou de la sous-arborescence gérée ou en supprimer. Vous pouvez également afficher ou modifier les propriétés de groupes existants auxquels ce contact appartient.

Déplacement d'un contact vers une autre unité organisationnelle

Vous pouvez déplacer un contact vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Suppression d'un contact

Vous pouvez supprimer un contact du domaine géré ou de la sous-arborescence gérée. Si la corbeille est désactivée pour ce domaine, la suppression d'un contact supprime définitivement ce contact d'Active Directory. Si la corbeille est activée pour ce domaine, lors de la suppression d'un contact, celui-ci est déplacé vers la corbeille.

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

Gestion des comptes de service administrés de groupe

Un compte de service administré de groupe (gMSA) est un compte de domaine géré que vous pouvez assigner à des services sur des ressources informatiques. Il n'est pas nécessaire de mettre à jour manuellement le mot de passe de ces comptes dans Active Directory, car il est automatiquement géré par Windows Server.

Vous pouvez créer et gérer un compte gMSA à partir de la console Web DRA. Un compte de service administré de groupe peut être utilisé avec plusieurs ordinateurs pour exécuter des services. Les ordinateurs qui utilisent un compte gMSA demandent le mot de passe actuel à Active Directory pour démarrer des services.

Si vous disposez des pouvoirs appropriés, vous pouvez effectuer diverses tâches liées aux comptes de service administrés de groupe. Exécutez une opération de recherche pour localiser et sélectionner l'objet Compte gMSA de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches est activée avec des options permettant de supprimer des objets, d'ajouter des objets à des groupes, de supprimer des objets de groupes, de déplacer des objets d'un conteneur à l'autre, ainsi que de modifier les propriétés d'un compte gMSA. Vous pouvez également télécharger les résultats de la recherche dans un fichier CSV. Cliquez sur une option pour afficher la fonction correspondante.

Créer un compte gMSA

Lorsque vous créez un compte gMSA, vous devez spécifier l'hôte sur lequel ce compte est utilisé et les objets Ordinateurs qui peuvent l'utiliser. Les objets Ordinateur définis dans la stratégie d'adhésion peuvent utiliser le compte gMSA pour exécuter des services. Vous pouvez également spécifier un groupe de sécurité qui contient une liste d'objets Ordinateur.

Pour créer un compte gMSA, accédez à **Gestion > Rechercher**, puis sélectionnez **Compte de service géré de groupe** dans le menu déroulant Créer.

Modifier les propriétés d'un compte gMSA

Vous pouvez modifier les propriétés d'un compte gMSA. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un compte gMSA situé dans le domaine géré.

Activer un compte gMSA

L'activation d'un compte gMSA vous permet d'utiliser ce compte en tant qu'informations d'identification de connexion pour un service informatique. Vous pouvez activer ou désactiver un compte gMSA à partir de l'onglet Comptes.

Gérer les adhésions aux groupes d'un compte gMSA

Vous pouvez ajouter ou supprimer des comptes de service administrés de groupe à partir d'un groupe spécifique du domaine géré ou de la sous-arborescence gérée.

Déplacer un compte gMSA vers un autre conteneur

Un compte gMSA est créé par défaut sous le conteneur Compte de service administré dans Active Directory. Vous pouvez déplacer un compte de service administré de groupe du conteneur par défaut vers un autre conteneur, tel qu'une unité organisationnelle, situé dans le domaine géré ou dans la sous-arborescence gérée.

Supprimer un compte gMSA

Vous pouvez supprimer définitivement un compte de service administré de groupe du domaine géré ou de la sous-arborescence gérée.

4 Recherche d'objets

Ce chapitre contient des informations sur les concepts et les procédures relatifs aux fonctionnalités de recherche et de recherche avancée (recherche LDAP).

- ♦ « Recherche » page 65
- ♦ « Recherche avancée » page 68

Recherche

DRA vous permet de rechercher des objets dans les domaines Active Directory locaux, Microsoft Exchange et les locataires Azure. Vous pouvez rechercher des utilisateurs, des utilisateurs invité, des groupes et des contacts dans vos locataires Azure, des objets tels que des utilisateurs, des groupes, des contacts, des ordinateurs, des imprimantes, des unités organisationnelles et des comptes de service administrés de groupe (gMSA) dans vos domaines Active Directory, ainsi que des objets tels que des boîtes aux lettres de salle, des boîtes aux lettres de ressource, des boîtes aux lettres partagées et des groupes de distribution dynamique dans Exchange. Vous pouvez utiliser les différentes options de recherche pour effectuer des recherches plus efficaces. DRA tronque automatiquement les espaces de début ou de fin de l'entrée de recherche et renvoie les résultats de la recherche.

REMARQUE : pour obtenir des résultats d'objets recherchés précis lors de l'utilisation de filtres de types d'objets, toute modification apportée à la pagination doit être effectuée avant l'application des filtres de types d'objets et l'exécution de la recherche. En effet, la modification du paramètre **Items per page** (Éléments par page) au bas de la console Web n'est pas prise en charge lors de l'application des filtres de types d'objet.

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

- ♦ « Utilisation des caractères joker » page 65
- ♦ « Recherche à plusieurs champs » page 66
- ♦ « Ajout et tri de colonnes » page 67
- ♦ « Exportation des résultats d'une recherche » page 67

Utilisation des caractères joker

DRA prend en charge les caractères joker tels que le point d'interrogation (?), l'astérisque (*) et le signe dièse (#) pour optimiser vos résultats de recherche. La concordance des caractères joker n'est pas sensible à la casse.

Le tableau suivant fournit des exemples de spécifications de caractères joker et ce à quoi ils correspondent et ne correspondent pas.

Caractère	Élément de concordance
Point d'interrogation ?	Un caractère ou un chiffre
Signe dièse #	Un chiffre
Astérisque *	Un ou plusieurs caractères ou chiffres

Recherche à plusieurs champs

L'option Multi-Field Match (Correspondance de plusieurs champs) vous permet de rechercher des correspondances de plusieurs attributs dans une seule recherche. Lorsque vous effectuez une recherche à l'aide de la correspondance de plusieurs champs, la chaîne de recherche est comparée à plusieurs attributs, tels le nom d'affichage, le prénom et le nom. Si la chaîne de recherche correspond à l'un de ces attributs, l'objet est renvoyé dans les résultats de la recherche.

L'option Multi-Field Match (Correspondance de plusieurs champs) ne prend en charge que les critères de recherche « **begins with** » (commence par).

Par exemple, vous avez deux utilisateurs : l'un dont le *nom d'affichage* est « Fabien Sarrot » et l'autre dont le nom principal est `fabrice.durand@acme.com`. Si vous effectuez une recherche à l'aide de la chaîne « Fab », ces deux utilisateurs sont renvoyés dans les résultats de la recherche.

Le tableau ci-dessous répertorie les attributs recherchés pour chaque type d'objet :

Type d'objet	Attributs recherchés
Contact Azure	displayName, givenName, mail, mailNickname, surname
Groupe Azure	displayName, mail
Utilisateur Azure	displayName, employeeId, givenName, mail, surname, userPrincipalName
Ordinateur	displayName, name, sAMAccountName
Contact	displayName, employeeId, givenName, mail, mailNickname, name, surname
Groupe de distribution dynamique	displayName, mail, mailNickname, name
Groupe	displayName, mail, mailNickname, name, sAMAccountName
Compte de service administré de groupe	displayName, name, sAMAccountName
Unité organisationnelle	name
Corbeille	name, sAMAccountName
Utilisateur	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

REMARQUE : la fonction de concordance multiple n'est pas prise en charge dans les recherches du sélecteur d'objet dans la console de délégation et de configuration lors de l'ajout de délégués ou d'autorisations pour les objets Exchange répertoriés ci-dessous :

- ♦ Boîte aux lettres utilisateur
 - ♦ Utilisateur à extension messagerie
 - ♦ Groupe à extension messagerie
 - ♦ Contact à extension messagerie
 - ♦ Groupe de distribution dynamique
 - ♦ Boîte aux lettres partagée
 - ♦ Boîte aux lettres de ressources
-

Ajout et tri de colonnes

Vous pouvez trier les objets figurant dans les résultats de la recherche en fonction de l'un des attributs suivants. Pour cela, cliquez sur l'en-tête de colonne correspondant :

- ♦ Alias
- ♦ Nom d'affichage
- ♦ Adresse électronique
- ♦ ID d'employé
- ♦ Prénom
- ♦ Nom
- ♦ Emplacement
- ♦ Nom
- ♦ Nom antérieur à Windows 2000
- ♦ Nom principal de l'utilisateur

Pour ajouter ou supprimer des colonnes d'attributs, cliquez sur l'icône de colonne.

Exportation des résultats d'une recherche

DRA permet aux assistants administrateur d'exporter les résultats d'une **recherche** vers un fichier CSV. Pour exporter les résultats de la **recherche** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur l'icône **Télécharger**.

REMARQUE : seules les colonnes sélectionnées sont exportées. Si vous souhaitez inclure des données supplémentaires qui ne sont pas affichées, ajoutez d'abord les colonnes concernées, puis exportez les résultats de la **recherche**.

Recherche avancée

DRA vous permet d'effectuer des requêtes LDAP et d'attribut virtuel dans vos domaines Active Directory locaux à partir de la page de recherche avancée. Vous pouvez effectuer une recherche en utilisant une requête existante, modifier une requête existante, créer une requête, ainsi qu'enregistrer les requêtes nouvelles et modifiées pour pouvoir les utiliser ultérieurement en tant que requêtes publiques ou privées. Utilisez les filtres de recherche pour effectuer des recherches plus efficaces.

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

- ♦ [« Requêtes de recherche avancée » page 68](#)
- ♦ [« Gestion des requêtes avancées » page 69](#)
- ♦ [« Exportation des résultats d'une recherche avancée » page 70](#)

Requêtes de recherche avancée

DRA prend en charge les requêtes d'attribut virtuel et LDAP pour rechercher des objets DRA et Active Directory. Les attributs virtuels peuvent être associés à des types d'objets Active Directory tels que des utilisateurs, des groupes, des groupes de distribution dynamique, des contacts, des ordinateurs et des unités organisationnelles. Grâce à une requête d'attribut virtuel, vous pouvez filtrer les résultats renvoyés par la requête LDAP pour obtenir uniquement ceux qui correspondent à la requête correspondante. Les chaînes de requête d'attribut virtuel doivent commencer par `(objectCategory=<type_objet>)`. Pour effectuer une requête d'attribut virtuel, vous devez spécifier des chaînes pour les requêtes LDAP et d'attribut virtuel.

Exemples de requêtes LDAP :

- ♦ Pour rechercher « tous les objets Ordinateur » dans DRA :
Requête LDAP : `(objectCategory=computer)`
- ♦ Pour rechercher les objets Utilisateur dont la description est « East\West Sales » dans DRA :
Requête LDAP : `(&(objectCategory=user)(description=East\5CWest Sales))`
- ♦ Pour rechercher « tous les objets Ordinateur » dans DRA :
Requête LDAP : `(objectCategory=computer)`

IMPORTANT : la barre oblique inverse doit être placée dans une séquence d'échappement dans les filtres LDAP. Vous devez la substituer par `\5C`.

- ♦ Pour « afficher la liste de tous les objets Utilisateur désactivés » dans DRA :

Requête LDAP :

```
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))
```

La chaîne 1.2.840.113556.1.4.803 spécifie LDAP_MATCHING_RULE_BIT_AND. Il s'agit d'un élément AND au niveau du bit d'un attribut de drapeau (nombre entier), comme userAccountControl, groupType ou systemFlags, et d'un masque de bits (comme 2, 32 ou 65536). La clause a la valeur True si l'élément AND au niveau du bit de la valeur d'attribut et du masque de bits est différent de zéro, ce qui indique que le bit est défini.

Exemples de requêtes d'attribut virtuel :

- ♦ Pour rechercher tous les utilisateurs dont le nom de la société est ABC :

Requête : (&(objectCategory=User)(CompanyName=ABC))

L'objet DRA est « User » et l'attribut virtuel est « CompanyName » (associé à l'utilisateur).

- ♦ Pour rechercher tous les utilisateurs dont le nom de société est ABC dans le domaine Storage :

Requête : (&(objectCategory=User)(CompanyName=ABC)(Domain=Storage))

L'objet DRA est « User » et les attributs virtuels sont « CompanyName » et « Domain » (associés à l'utilisateur).

- ♦ Pour rechercher tous les groupes dont le nom de produit est DRA ou tous les utilisateurs dont le nom de société est ABC :

Requête :

```
( | (&(objectCategory=Group)(ProductGroupName=DRA)) (&(objectCategory=User)(CompanyName=ABC)) )
```

Les objets DRA sont « Group » et « User » et les attributs virtuels sont CompanyName (associé à l'utilisateur) et ProductGroupName (associé au groupe).

- ♦ Pour rechercher tous les groupes dont le nom de produit est DRA ou tous les utilisateurs dont le nom de société est ABC dans le domaine Storage :

Requête :

```
( | (&(objectCategory=Group)(ProductGroupName=DRA)) (&(objectCategory=User)(CompanyName=ABC)(Domain=Storage)) )
```

Les objets DRA sont « Group » et « User » et les attributs virtuels sont CompanyName (associé à l'utilisateur), ProductGroupName (associé au groupe) et Domain (associé à l'utilisateur).

Gestion des requêtes avancées

DRA utilise LDAP pour assurer la prise en charge de la fonction de requêtes de recherche avancées. Grâce aux requêtes avancées, vous pouvez rechercher des utilisateurs, contacts, groupes, ordinateurs, unités organisationnelles et tout autre objet pris en charge par DRA. Si vous disposez du pouvoir Execute Saved Advanced Queries (Exécuter les requêtes avancées enregistrées), vous pouvez exécuter les requêtes avancées disponibles dans les listes **My Searches** (Mes recherches) et **Public Searches** (Recherches publiques) pour n'importe quel conteneur.

Outre l'exécution d'une recherche avec une requête avancée enregistrée et l'affichage des détails correspondant, avec les autorisations applicables, vous pouvez également effectuer les opérations suivantes en ce qui concerne les requêtes avancées de la page de recherche avancée :

Créer une requête

Créez une requête avancée sur le serveur d'administration primaire ou secondaire en fournissant la chaîne de requête (LDAP et, le cas échéant, l'attribut virtuel) pour la nouvelle requête avancée. Après avoir exécuté la recherche, développez le menu déroulant **Search** (Rechercher) pour enregistrer la requête dans la liste My Searches (Mes recherches) ou Public Searches (Recherches publiques).


Modifier une requête

Sélectionnez une requête avancée dans la liste My Searches (Mes recherches) ou Public Searches (Recherches publiques) et utilisez l'option **Modify** (Modifier) pour modifier les critères de recherche. Après avoir exécuté la recherche avec les critères de recherche mis à jour, vous pouvez, si vous le souhaitez, développer le menu déroulant **Search** (Rechercher) et sélectionner **Save** (Enregistrer) pour enregistrer les modifications apportées à cette requête.

Copier une requête

Sélectionnez une requête avancée dans la liste My Searches (Mes recherches) ou Public Searches (Recherches publiques), puis exécutez la recherche. Ensuite, vous pouvez développer le menu déroulant **Search** (Rechercher) et sélectionner **Save As** (Enregistrer sous) pour enregistrer la requête sous un autre nom.

Personnaliser les résultats d'une requête

DRA vous fournit un ensemble de colonnes par défaut dans la liste des résultats de recherche. Pour personnaliser les résultats de recherche à partir d'une requête enregistrée ou non, cliquez sur l'icône **Add/Remove Columns** (Ajouter/Supprimer des colonnes)  à droite de la page pour modifier le mode d'affichage des résultats de la recherche.

Supprimer une requête

Vous pouvez supprimer n'importe quelle requête avancée figurant dans la liste **My Searches** (Mes recherches). Si vous disposez des autorisations applicables, vous pouvez également supprimer des requêtes avancées de la liste **Public Searches** (Recherches publiques). Pour supprimer une requête avancée enregistrée, sélectionnez-la dans la liste correspondante, puis cliquez sur **Supprimer** dans le menu déroulant Rechercher.

Effacer une requête

Dans la console Web, vous pouvez effacer les champs de formulaire d'une requête enregistrée ou non pour effectuer des modifications à partir d'un formulaire vierge. Pour effacer les champs d'une requête, sélectionnez **Clear** (Effacer) dans le menu déroulant Search (Rechercher).

Exportation des résultats d'une recherche avancée

DRA permet aux assistants administrateur d'exporter les résultats d'une **recherche avancée** vers un fichier CSV. Pour exporter les résultats de la **recherche avancée** à partir de la console Web, accédez à **Gestion > Recherche avancée**, puis cliquez sur l'icône **Télécharger**.

REMARQUE : seules les colonnes sélectionnées sont exportées. Si vous souhaitez inclure des données supplémentaires qui ne sont pas affichées, ajoutez d'abord les colonnes concernées, puis exportez les résultats de la **recherche avancée**.

5 Gestion des objets Azure

Ce chapitre contient des informations sur les concepts et les procédures de gestion des comptes utilisateur, des contacts et des groupes Azure dans la console Web. Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion des objets Azure, comme créer et supprimer des objets Compte utilisateur Azure.


Vous pouvez exécuter la plupart des tâches liées aux objets Azure à partir de l'onglet **Management** (Gestion) > **Search** (Rechercher) de la console Web en recherchant des objets dans l'un des nœuds suivants :

- ♦ All My Managed Objects (Tous mes objets gérés)
- ♦ All My Managed Tenants (Tous mes locataires gérés)
- ♦ Un sous-nœud de All My Managed Tenants (Tous mes locataires gérés)

Les rubriques sont, notamment, les suivantes :

- ♦ « [Gestion des comptes utilisateur Azure](#) » page 71
- ♦ « [Gestion des comptes utilisateur invité Azure](#) » page 73
- ♦ « [Gestion des groupes Azure](#) » page 74
- ♦ « [Gestion des contacts Azure](#) » page 75

Gestion des comptes utilisateur Azure

En tant qu'assistant administrateur, vous pouvez utiliser DRA pour gérer les comptes utilisateur Azure et modifier les propriétés d'un de ces comptes lorsqu'Azure Active Directory est configuré par l'administrateur DRA. L'icône  indique un compte utilisateur Azure dans la console Web.

Exécutez une opération de recherche pour localiser et sélectionner l'objet Utilisateur Azure de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches est activée avec des options telles que la suppression, l'autorisation, le blocage, la réinitialisation de mot de passe et la modification des propriétés. Vous pouvez également télécharger les résultats de la recherche dans un fichier CSV. Cliquez sur une option pour afficher la fonction correspondante.

Créer un compte utilisateur Azure

Vous pouvez créer des comptes utilisateur Azure dans Azure Active Directory. Vous pouvez également activer la messagerie et spécifier des adhésions aux groupes pour le nouveau compte.

Modifier les propriétés d'un compte utilisateur Azure

Vous pouvez gérer les propriétés des comptes utilisateur Azure dans Azure Active Directory. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un compte utilisateur Azure. Si le compte utilisateur Azure dispose d'une boîte aux lettres Office 365 ou s'il est à extension messagerie, vous pouvez gérer les propriétés liées à la boîte aux lettres et à la messagerie pour ce compte. Vous pouvez gérer les stratégies de boîte aux

lettres, définir des restrictions et des options de distribution, définir des limites de stockage, déléguer des autorisations de boîte aux lettres, mettre en attente des litiges, gérer les adresses électroniques, etc.

REMARQUE

- ♦ Vous ne pouvez mettre à jour les propriétés de téléphone mobile, de téléphone professionnel et d'autre adresse électronique que pour les utilisateurs Azure qui ne sont pas administrateurs. Pour plus d'informations, reportez-vous à l'article [Mettre à jour un utilisateur](#) sur le site de documentation Microsoft.
- ♦ DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Autoriser la connexion d'un compte utilisateur Azure

Vous pouvez autoriser un compte utilisateur Azure à se connecter à Azure Active Directory.

Bloquer la connexion d'un compte utilisateur Azure

Vous pouvez empêcher un compte utilisateur Azure de se connecter à Azure Active Directory.

Réinitialiser le mot de passe d'un compte utilisateur Azure

Vous pouvez réinitialiser le mot de passe d'un compte utilisateur Azure dans Azure Active Directory et indiquer si DRA doit générer un nouveau mot de passe pour le compte.

Supprimer un compte utilisateur Azure

Vous pouvez supprimer un compte utilisateur Azure d'Azure Active Directory, mais vous ne pouvez pas le restaurer à partir de DRA.

REMARQUE : vous ne pouvez supprimer que les utilisateurs Azure qui ne sont pas administrateurs. Pour plus d'informations, reportez-vous à l'article [Supprimer un utilisateur](#) sur le site de documentation Microsoft.

Spécifier une adhésion à un groupe Azure pour un compte utilisateur Azure


Vous pouvez ajouter ou supprimer des comptes utilisateur Azure d'un groupe Azure donné dans Azure Active Directory.

Gestion des comptes utilisateur invité Azure

En tant qu'assistant administrateur, vous pouvez inviter des utilisateurs externes ou invité à collaborer et partager des applications dans Azure Active Directory. Les utilisateurs invité peuvent se connecter à Azure Active Directory à l'aide de leurs informations d'identification pour accéder aux applications que vous avez partagées avec eux.

Exécutez une opération de recherche pour localiser et sélectionner l'objet Utilisateur invité Azure de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches devient active avec des options telles que Supprimer, Bloquer la connexion, Ajouter aux groupes, Renvoyer l'invitation et Modifier les propriétés.

Inviter un utilisateur invité Azure

Pour inviter un utilisateur invité à rejoindre Azure Active Directory, accédez à **Créer > Inviter un utilisateur Azure** dans le bloc générique Gestion. Lorsque vous invitez un utilisateur invité à rejoindre Azure Active Directory, DRA lui envoie une invitation par message électronique et crée un compte utilisateur pour cet utilisateur dans Azure Active Directory. L'icône  indique un compte utilisateur invité Azure dans la console Web.

REMARQUE : L'URL de redirection et le message d'invitation sont configurés par l'administrateur DRA dans la console de délégation et de configuration pour chaque locataire géré. Vous pouvez personnaliser ce message si nécessaire lorsque vous invitez l'utilisateur.

Un utilisateur invité Azure doit accepter l'invitation pour commencer à accéder aux applications que vous avez partagées. Vous pouvez consulter l'état de l'invitation dans l'onglet **Informations sur l'invité**. Lorsqu'il accepte l'invitation, l'utilisateur est redirigé vers l'URL spécifiée dans le champ **URL de redirection**, qui permet à l'utilisateur invité Azure de se connecter à l'aide de ses informations d'identification.

Réinviter un utilisateur invité Azure

Si un utilisateur invité n'a pas accepté l'invitation, vous pouvez renvoyer l'invitation.

Pour réinviter un utilisateur invité :

1. Exécutez une opération de recherche pour localiser et sélectionner l'objet Utilisateur invité Azure de votre choix.
2. Sélectionnez **Compte > Renvoyer l'invitation**.

Modifier les propriétés d'un compte utilisateur invité Azure

Vous pouvez gérer les propriétés des comptes utilisateur invité Azure dans Azure Active Directory. Vous pouvez indiquer si l'adresse électronique doit être masquée dans la liste d'adresses et ajouter d'autres adresses électroniques.

Autoriser la connexion pour un compte utilisateur invité Azure

Vous pouvez autoriser un compte utilisateur invité Azure à se connecter à Azure Active Directory.

Bloquer la connexion pour un compte utilisateur invité Azure

Vous pouvez empêcher un compte utilisateur invité Azure de se connecter à Azure Active Directory.

Supprimer un compte utilisateur invité Azure

Vous pouvez supprimer un compte utilisateur invité Azure d'Azure Active Directory, mais vous ne pouvez pas le restaurer à partir de DRA.

Spécifier une adhésion à un groupe Azure pour un compte utilisateur invité Azure

Vous pouvez ajouter ou supprimer des comptes utilisateur invité Azure d'un groupe Azure donné dans Azure Active Directory.

Assigner des licences à des comptes utilisateur invité Azure

Lorsque vous ajoutez un compte utilisateur invité Azure à un groupe associé à une stratégie Office 365, DRA assigne automatiquement la licence Office 365 appropriée à l'utilisateur invité Azure.

Ajouter des comptes utilisateur invité Azure à des assignations temporaires à des groupes

Vous pouvez ajouter ou supprimer des comptes utilisateur invité Azure d'assignations temporaires à des groupes à partir de l'onglet **Tâches** du bloc générique sur les serveurs d'administration primaires et secondaires.

Gestion des groupes Azure

En tant qu'assistant administrateur, vous pouvez utiliser DRA pour gérer les groupes Azure lorsqu'Azure Active Directory est configuré par l'administrateur DRA. Grâce aux groupes Azure, vous pouvez donner des autorisations spécifiques à un ensemble défini de comptes utilisateur. Les groupes Azure vous permettent de déterminer les données et ressources accessibles à un compte utilisateur dans n'importe quel locataire.

Exécutez une opération de recherche pour localiser et sélectionner l'objet Groupe Azure de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches est activée avec des options permettant de supprimer des objets, d'ajouter des objets à des groupes, de supprimer des objets de groupes, d'ajouter des groupes à d'autres groupes, de supprimer des groupes existants et de modifier les propriétés d'un groupe. Cliquez sur une option pour afficher la fonction correspondante.

REMARQUE : les membres de groupe Azure pris en charge peuvent être des utilisateurs, des groupes et des contacts Azure, ainsi que des utilisateurs, des contacts et des groupes synchronisés.

Les types de groupes Azure suivants sont pris en charge :

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

Ajouter des comptes à des groupes Azure

Vous pouvez ajouter des comptes utilisateur, des contacts et des groupes (locaux et Azure) à un groupe Azure géré.

Cette tâche ajoute plusieurs comptes à un groupe sélectionné. Pour ajouter un seul compte à un groupe, sélectionnez le compte correspondant. Si l'ajout d'un compte à un autre groupe augmente vos pouvoirs sur le compte, DRA ne vous autorise pas à ajouter ce compte.

Imbriquer des groupes dans Azure

Vous pouvez imbriquer des groupes en ajoutant d'autres groupes (locaux et Azure) à un groupe Azure géré. Lorsqu'un groupe est imbriqué dans un groupe Azure, le groupe enfant hérite des autorisations du groupe parent.

Si l'ajout d'un domaine ou d'un groupe Azure à un autre groupe augmente vos pouvoirs sur le groupe source, DRA ne vous autorise pas à ajouter ce groupe.

Créer un groupe Azure

Vous pouvez créer un groupe Azure dans Azure Active Directory. Vous pouvez également modifier des propriétés, tel l'ajout de membres de groupe Azure au nouveau groupe.

Si vous n'indiquez aucun propriétaire, DRA utilise par défaut le compte d'accès au locataire Azure.

Modifier les propriétés d'un groupe Azure

Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un groupe dans Azure Active Directory. Si la stratégie Exchange est activée, vous pouvez gérer les propriétés Exchange des groupes Azure à extension messagerie, tels que le groupe Office 365, le groupe de sécurité à extension messagerie et la liste de distribution. En fonction du type de groupe, vous pouvez gérer les adresses électroniques du groupe, déterminer les utilisateurs autorisés à envoyer des messages électroniques au groupe ou de la part du groupe, définir des options d'approbation des messages électroniques, etc.

REMARQUE : DRA vous permet d'exporter les résultats des types **Membres** et **Membre de** dans un fichier CSV. Accédez à l'onglet **Membres** ou **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Configurer la propriété d'un groupe Azure

Vous pouvez définir la propriété de n'importe quel groupe. Vous pouvez accorder l'autorisation de propriété du groupe à un compte utilisateur ou à un groupe. La propriété d'un groupe permet au compte utilisateur ou au groupe spécifié de gérer le groupe, notamment les membres.

Supprimer un groupe Azure

Vous pouvez supprimer des groupes Azure d'Azure Active Directory, mais vous ne pouvez pas les restaurer à partir de DRA.

Gestion des contacts Azure

Les contacts Azure sont des objets à extension messagerie qui contiennent une adresse électronique externe. En tant qu'assistant administrateur, vous pouvez utiliser DRA pour gérer les contacts Azure et modifier les propriétés d'un de ces contacts lorsqu'Azure Active Directory est configuré par l'administrateur DRA.

Exécutez une opération de recherche pour localiser et sélectionner l'objet Contact Azure de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches est activée avec des options permettant de supprimer des objets, d'ajouter des objets à des groupes, de

supprimer des objets de groupes, ainsi que de modifier les propriétés d'un contact. Vous pouvez également télécharger les résultats de la recherche dans un fichier CSV. Cliquez sur une option pour afficher la fonction correspondante.

Créer un contact Azure

Vous pouvez créer un contact Azure dans le locataire géré et spécifier les coordonnées et l'adresse électronique de ce nouveau contact.

Modifier les propriétés d'un contact Azure

Vous pouvez modifier les propriétés d'un contact Azure. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un contact Azure situé dans le locataire géré. Si la stratégie Exchange est activée, vous pouvez gérer les propriétés liées à la messagerie, telles que définir des restrictions de distribution des messages, déterminer les utilisateurs autorisés à envoyer des messages électroniques de la part de ce contact Azure, indiquer si le contact Azure est visible dans la liste d'adresses, etc.

Activer la modération des messages

Vous pouvez définir les options relatives à la modération des messages envoyés à un contact Azure. Lorsque vous activez la modération, les messages envoyés au contact Azure concerné sont approuvés par un modérateur que vous définissez avant la distribution des messages. Vous pouvez également spécifier les utilisateurs et les groupes qui sont exclus du processus d'approbation.

Gérer les adhésions aux groupes des contacts Azure

Vous pouvez ajouter ou supprimer des contacts Azure dans les listes de distribution et les groupes de sécurité à extension messagerie.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger l'adhésion enregistrée**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Supprimer un contact Azure

Vous pouvez supprimer des contacts Azure d'Azure Active Directory, mais vous ne pouvez pas les restaurer à partir de DRA.

6 Gestion des dossiers publics et des boîtes aux lettres Exchange

DRA vous permet de gérer des boîtes aux lettres Microsoft Exchange en tant qu'extension de propriétés du compte utilisateur. Cette intégration vous permet de simplifier vos workflows d'administration pour que vous puissiez administrer efficacement les propriétés Exchange. Vous pouvez également lier des boîtes aux lettres à partir d'un compte utilisateur et de forêts de comptes Exchange et gérer des boîtes aux lettres de ressources, des boîtes aux lettres partagées ainsi que des dossiers publics.

Gestion des tâches liées aux boîtes aux lettres dans la console de délégation et de configuration

Lorsque vous utilisez le nœud ARM, vous exécutez les tâches de boîte aux lettres applicables sous l'onglet **Exchange Tasks** (Tâches Exchange) des propriétés de l'objet, qui est également accessible à partir du menu **Tasks** (Tâches) ou du menu contextuel d'un objet sélectionné. En règle générale, vous sélectionnez le nœud **Tous mes objets gérés** et exécutez une opération **Find Now** (Rechercher maintenant) pour rechercher et sélectionner l'objet de votre choix.

Gestion des tâches de boîte aux lettres au niveau de la console Web

Lorsque vous utilisez la console Web, vous pouvez exécuter les tâches de boîte aux lettres applicables ci-dessous à partir de l'onglet **Gestion > Rechercher**. En règle générale, vous exécutez une opération de recherche pour localiser et sélectionner l'objet Boîte aux lettres de votre choix. Une fois que vous avez sélectionné un ou plusieurs objets de la liste, la barre des tâches est activée. Cliquez sur une option pour afficher la fonction correspondante.

Reportez-vous aux rubriques suivantes :

- ♦ « Tâches de gestion des boîtes aux lettres utilisateur » page 77
- ♦ « Tâches de gestion des boîtes aux lettres Office 365 » page 80
- ♦ « Tâches de gestion des boîtes aux lettres de ressources » page 81
- ♦ « Tâches de gestion des boîtes aux lettres partagées » page 83
- ♦ « Tâches de gestion des boîtes aux lettres liées » page 84
- ♦ « Tâches de gestion des dossiers publics » page 85

Tâches de gestion des boîtes aux lettres utilisateur

Vous pouvez gérer les boîtes aux lettres Microsoft Exchange des comptes utilisateur dans le domaine géré ou dans la sous-arborescence gérée. Chaque aspect de la gestion des boîtes aux lettres Microsoft Exchange nécessite différents pouvoirs. Vos pouvoirs déterminent les propriétés de boîtes aux lettres que vous pouvez modifier, ou si vous êtes autorisé à créer, cloner, afficher ou supprimer des boîtes aux lettres Microsoft Exchange. Vous pouvez également gérer les autorisations et les droits de boîte aux lettres associés à un compte utilisateur, ce qui vous permet de contrôler la

sécurité de vos environnements Microsoft Exchange. Si vous ne possédez pas le pouvoir requis pour modifier un onglet ou un champ de la boîte aux lettres sélectionnée, DRA désactive les onglets et les champs que vous ne pouvez pas modifier.

Outre les tâches définies ci-dessous, les comptes utilisateur peuvent avoir des options activées par l'administrateur DRA dans les propriétés d'objet pour configurer les paramètres de Skype et de Skype Online. Skype peut être configuré à partir de comptes utilisateur au niveau de la console de délégation et de configuration et de la console Web. Skype Online peut uniquement être configuré à partir de la console Web.

Création d'une boîte aux lettres

Vous pouvez créer une boîte aux lettres Microsoft Exchange pour un compte utilisateur existant. Vous pouvez également modifier les propriétés de la nouvelle boîte aux lettres.

REMARQUE : Lorsque vous créez une boîte aux lettres, Exchange crée les chaînes proxy nécessaires en fonction de vos paramètres de stratégie Exchange. Microsoft Exchange génère également les chaînes proxy par défaut. Par conséquent, lorsque vous consultez les propriétés de la boîte aux lettres qui vient d'être créée, les deux types de chaînes proxy s'affichent.

Clonage d'un compte utilisateur

Lorsque vous clonez un compte utilisateur, tous les groupes dont l'utilisateur est membre sont automatiquement ajoutés au nouveau compte utilisateur vous permettant ainsi de gagner du temps lors de la configuration du nouveau compte. Vous pouvez ajouter ou supprimer des groupes à partir du nouveau compte, vous pouvez activer la messagerie électronique et configurer toutes les autres propriétés comme vous le feriez pour n'importe quel nouveau compte.

REMARQUE : lorsque vous clonez un objet InetOrgPerson, vous créez un compte utilisateur.

Déplacement d'une boîte aux lettres

Vous pouvez déplacer une boîte aux lettres Microsoft Exchange d'un compte utilisateur vers une autre banque de boîte aux lettres ou un autre serveur Microsoft Exchange.

Modification des propriétés de boîte aux lettres

Vous pouvez modifier les propriétés des boîtes aux lettres Microsoft Exchange de la même manière que vous gérez les comptes utilisateur associés. Vos pouvoirs déterminent les propriétés de boîte aux lettres que vous pouvez modifier.

REMARQUE : vous ne pouvez pas modifier les propriétés de boîte aux lettres de comptes utilisateur gérés sur des serveurs membres.

Configuration des autorisations de sécurité de boîte aux lettres

Vous pouvez spécifier les comptes utilisateur, groupes ou ordinateurs pour lesquels vous souhaitez autoriser ou refuser l'envoi et la réception de messages électroniques à l'aide d'une boîte aux lettres Microsoft Exchange spécifique. Ces paramètres vous permettent de sécuriser plus efficacement votre environnement Exchange. Vous ne pouvez pas modifier des autorisations de sécurité héritées.

REMARQUE : lorsque vous gérez la sécurité d'une boîte aux lettres, des autorisations désactivées peuvent signaler qu'il s'agit d'autorisations héritées.

Suppression des autorisations de sécurité de boîte aux lettres

Vous pouvez supprimer des autorisations de sécurité de boîte aux lettres d'un compte utilisateur, groupe ou ordinateur associé à une boîte aux lettres Microsoft Exchange. La suppression des autorisations de sécurité de boîte aux lettres empêche un compte utilisateur, un groupe ou un compte d'ordinateur d'envoyer et de recevoir des messages électroniques par le biais de la boîte aux lettres spécifiée. Vous ne pouvez pas supprimer des autorisations de sécurité héritées.

Configuration des droits de boîte aux lettres

Vous pouvez accorder ou refuser des droits à d'autres comptes utilisateur, groupes ou ordinateurs pour une boîte aux lettres Microsoft Exchange spécifique. Ces paramètres vous permettent de sécuriser plus efficacement votre environnement Exchange. Vous ne pouvez pas modifier des droits de boîte aux lettres hérités.

REMARQUE : lorsque vous gérez des droits de boîte aux lettres, des autorisations désactivées peuvent signaler qu'il s'agit d'autorisations héritées.

Suppression de droits de boîte aux lettres

Vous pouvez supprimer des droits de boîte aux lettres de comptes utilisateur, groupes ou ordinateurs associés à une boîte aux lettres Microsoft Exchange spécifique. La suppression des droits de boîte aux lettres empêche un compte utilisateur, un groupe ou un compte d'ordinateur d'utiliser une boîte aux lettres spécifiée. Vous ne pouvez pas supprimer des droits de boîte aux lettres hérités.

Suppression d'une boîte aux lettres

Vous pouvez supprimer une boîte aux lettres associée à un compte utilisateur dans le domaine géré ou dans la sous-arborescence gérée. La suppression d'une boîte aux lettres supprime également tous les messages qu'elle contient.

Ajout ou modification d'une adresse électronique

Vous pouvez spécifier des adresses électroniques pour les boîtes aux lettres associées à des comptes utilisateur dans votre domaine géré ou dans la sous-arborescence gérée. Vous pouvez également assigner des adresses électroniques à des comptes utilisateur qui n'ont pas encore de boîtes aux lettres. Lors de la gestion des boîtes aux lettres Microsoft Exchange, vous pouvez ajouter uniquement les types d'adresse électronique définis par vos stratégies de génération proxy.

Indication d'une adresse de réponse

Vous pouvez définir des adresses de réponse pour une boîte aux lettres associée à un compte utilisateur dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez définir plusieurs adresses de réponse pour une boîte aux lettres. Toutefois, vous ne pouvez pas définir plusieurs types d'adresse électronique en tant qu'adresse de réponse. Par exemple, vous ne pouvez pas spécifier plusieurs adresses Internet comme adresse de réponse.

Suppression d'une adresse électronique

Vous pouvez supprimer une adresse électronique en supprimant l'adresse de la boîte aux lettres.

Spécification des options de livraison

Vous pouvez spécifier les boîtes aux lettres que l'utilisateur peut utiliser pour envoyer des messages, définir des options de réacheminement et spécifier le nombre maximal de destinataires.

Spécification des restrictions de livraison

En définissant des restrictions de livraison, vous pouvez limiter la taille des messages entrants et sortants et l'acceptation des messages entrants pour une boîte aux lettres spécifique.

Spécification des limites de stockage

Vous pouvez spécifier des limites de stockage, tels que les avertissements en fonction de la taille d'une boîte aux lettres. Vous pouvez également spécifier la durée de conservation des éléments supprimés.

Vérification de l'état de déplacement d'une boîte aux lettres

Vous pouvez vérifier l'état de déplacement de la boîte aux lettres et effectuer des actions sur celle-ci, telles qu'effacer son état, annuler un déplacement et reprendre un déplacement qui avait été interrompu.

Tâches de gestion des boîtes aux lettres Office 365

Cette section contient des informations relatives à l'administration des boîtes aux lettres Microsoft Office 365 dans la console de délégation et de configuration via le nœud Account and Resource Management (Gestion des comptes et des ressources), ainsi que dans la console Web. Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion sur le compte utilisateur, notamment placer des conservations pour litige et définir le transfert des messages électroniques.

IMPORTANT : DRA gère les boîtes aux lettres utilisateur Office 365, ainsi que les boîtes aux lettres partagées, de salle et de ressource migrées. Pour que DRA puisse gérer ces boîtes aux lettres, vous devez les associer à un utilisateur local ou à un utilisateur Azure géré par DRA. Les propriétés des boîtes aux lettres sont accessibles via les pages de propriétés des utilisateurs associés.

Placement d'une conservation pour litige

La définition d'une conservation pour litige d'une boîte aux lettres afin de conserver tout son contenu, y compris les éléments supprimés, les versions d'origine et les éléments modifiés. Si vous placez des boîtes aux lettres utilisateur en état de conservation pour litige, leur contenu (éventuel) est conservé. Il est également conservé dans la boîte aux lettres d'archivage de l'utilisateur. La conservation peut durer pendant une période spécifiée, ou jusqu'à ce que vous supprimiez la conservation pour litige de la boîte aux lettres.

Vous devez disposer d'une licence Exchange Online appropriée pour placer une conservation pour litige. Vous configurez la fonction via l'onglet **Conservation pour litige** dans les propriétés de l'objet Utilisateur.

Délégation d'autorisations de boîte aux lettres

Vous pouvez déléguer des autorisations de boîte aux lettres Office 365 sous l'onglet Délégation dans les propriétés de l'objet Utilisateur. Il existe trois types d'autorisations que vous pouvez déléguer : Envoyer en tant que, Envoyer de la part de et Accès complet. Ces types dépendent du type d'objet récepteur.

Affichage de l'état de la boîte aux lettres d'archivage

Vous pouvez afficher l'état de la boîte aux lettres d'archivage d'un utilisateur et les statistiques correspondantes telles que la limite de stockage et la limite d'avertissement. L'utilisateur est averti lorsque la boîte aux lettres d'archivage dépasse la limite d'avertissement d'archivage.

Affichage des statistiques d'utilisation d'une boîte aux lettres

Vous pouvez afficher la quantité utilisée du quota total de boîte aux lettres.

Configuration des restrictions de distribution des messages

En définissant des restrictions de distribution, vous pouvez limiter la taille des messages entrants et sortants et accepter ou rejeter les messages entrants pour un utilisateur spécifique.

Spécification des options de distribution

Vous pouvez configurer les options de transfert des messages et spécifier le nombre maximal de destinataires auxquels un utilisateur peut envoyer un message.

Ajout ou suppression d'une adresse électronique

Vous pouvez configurer plusieurs adresses électroniques pour une boîte aux lettres utilisateur et spécifier l'adresse électronique principale. Vous pouvez également assigner des adresses électroniques à des comptes utilisateur qui n'ont pas de boîtes aux lettres.

Masquage de l'adresse électronique

Vous pouvez masquer l'adresse électronique dans la liste d'adresses.

Ajout d'une astuce pour la messagerie

Vous pouvez ajouter du texte d'information à afficher lorsqu'un message est envoyé à l'utilisateur.

Assignation de stratégies pour une boîte aux lettres

Vous pouvez assigner une stratégie de partage, une stratégie de conservation des messages électroniques, une stratégie d'assignation de rôle ou une stratégie de carnet d'adresses pour la boîte aux lettres.

Tâches de gestion des boîtes aux lettres de ressources

La fonction de boîte aux lettres de ressources de Microsoft Exchange permet de créer une boîte aux lettres qui représente une ressource telle qu'une salle de conférence afin que vous puissiez la réserver en lui envoyant une invitation à une réunion, comme vous le feriez pour une personne. DRA comprend un ensemble de rôles, pouvoirs et stratégies qui vous permettent de gérer efficacement les boîtes aux lettres de ressources.

DRA prend en charge l'extension de l'interface pour les boîtes aux lettres de ressources, ainsi que la génération de rapports d'audit ou d'interface utilisateur. La prise en charge des scripts ADSI est également intégrée à DRA.

Création d'une boîte aux lettres de ressources

Vous pouvez créer des boîtes aux lettres de ressources dans le domaine géré ou dans la sous-arborescence gérée.

Déplacement d'une boîte aux lettres de ressources vers un autre conteneur

Vous pouvez déplacer une boîte aux lettres de ressources vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Déplacement d'une boîte aux lettres de ressources vers une autre banque de boîtes aux lettres ou un serveur Exchange

Vous pouvez déplacer une boîte aux lettres de ressources vers une autre banque de boîte aux lettres ou un serveur Microsoft Exchange.

Clonage d'une boîte aux lettres de ressources

En clonant une boîte aux lettres de ressources, vous pouvez rapidement créer d'autres boîtes aux lettres de ressources ayant des propriétés similaires. Lorsque vous clonez une boîte aux lettres de ressources, DRA complète les champs de l'assistant de clonage de la boîte aux lettres de ressources avec les valeurs de la ressource sélectionnée.

Modification du nom d'une boîte aux lettres de ressources

Vous pouvez renommer des boîtes aux lettres de ressources dans le domaine géré ou dans la sous-arborescence gérée. La modification du nom de connexion de l'utilisateur modifie également le nom de la boîte aux lettres associée au compte utilisateur.

Ajout d'une boîte aux lettres de ressources à un groupe

Vous pouvez ajouter des boîtes aux lettres de ressources à un groupe spécifique dans le domaine géré ou dans la sous-arborescence gérée.

Suppression d'une boîte aux lettres de ressources

Vous pouvez supprimer une boîte aux lettres de ressources du domaine géré ou de la sous-arborescence gérée. Si vous supprimez une boîte aux lettres de ressources, tous les messages de cette boîte et tous les objets Utilisateur désactivés associés sont également supprimés. Si vous le souhaitez, vous pouvez remplacer la suppression des objets Utilisateur désactivés lorsque vous supprimez la boîte aux lettres. Si vous supprimez un objet Utilisateur associé à une boîte aux lettres de ressources, cette boîte est également supprimée.

Restauration d'une boîte aux lettres de ressources ayant été supprimée

Vous pouvez restaurer une boîte aux lettres de ressources ayant été supprimée si la corbeille de ce domaine est activée.

Modification des propriétés d'une boîte aux lettres de ressources

Vous pouvez gérer les propriétés de boîtes aux lettres de ressources dans le domaine géré ou dans la sous-arborescence gérée. Vos pouvoirs déterminent les propriétés que vous pouvez modifier.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Tâches de gestion des boîtes aux lettres partagées

Les boîtes aux lettres partagées sont utiles aux administrateurs du service d'assistance et au personnel du support technique, étant donné que toutes les réponses peuvent être configurées pour être centralisées dans une seule boîte aux lettres accessible par plusieurs utilisateurs. La boîte aux lettres doit se trouver dans un domaine DRA géré avec la stratégie Exchange activée. De plus, vous devez disposer des pouvoirs qui vous permettent de gérer des boîtes aux lettres partagées.

Lorsque vous créez une boîte aux lettres partagée, il existe deux types d'autorisations que vous pouvez déléguer à des utilisateurs : Envoyer en tant que et Accès complet. L'option Envoyer en tant que fournit l'autorisation de lire et d'envoyer des messages électroniques. Vous pouvez déléguer des autorisations aux objets Utilisateur et Groupe. Vous pouvez également spécifier des restrictions et des options de livraison, des limites de stockage, des autorisations sur un dossier ainsi que plusieurs autres options dans les propriétés de l'objet.

REMARQUE : vous ne pouvez effectuer les tâches de gestion des boîtes aux lettres partagées que via la console Web.

Création d'une boîte aux lettres partagée

Vous pouvez créer des boîtes aux lettres partagées dans le domaine géré ou dans la sous-arborescence gérée.

Déplacement d'une boîte aux lettres partagée vers un autre conteneur

Vous pouvez déplacer une boîte aux lettres partagée vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Déplacement d'une boîte aux lettres partagée vers une autre banque de boîtes aux lettres

Vous pouvez déplacer une boîte aux lettres partagée vers une autre banque de boîtes aux lettres.

Clonage d'une boîte aux lettres partagée

En clonant une boîte aux lettres partagée, vous pouvez rapidement créer d'autres boîtes aux lettres partagées ayant des propriétés similaires.

Modification du nom d'une boîte aux lettres partagée

Vous pouvez renommer des boîtes aux lettres partagées dans le domaine géré ou dans la sous-arborescence gérée. La modification du nom de connexion de l'utilisateur modifie également le nom de la boîte aux lettres associée au compte utilisateur.

Suppression d'une boîte aux lettres partagée

Vous pouvez supprimer une boîte aux lettres partagée du domaine géré ou de la sous-arborescence gérée. Si la corbeille est désactivée pour ce domaine, la suppression d'une boîte aux lettres partagée supprime définitivement cette boîte aux lettres d'Active Directory. Si la corbeille est activée pour ce domaine, lors de la suppression d'une boîte aux lettres partagée, celle-ci est déplacée vers la corbeille.

Si vous supprimez une boîte aux lettres partagée, tous les messages de cette boîte et tous les objets Utilisateur désactivés associés sont également supprimés. Si vous supprimez un objet Utilisateur associé à une boîte aux lettres partagée, cette boîte est également supprimée.

Restauration d'une boîte aux lettres partagée ayant été supprimée

Vous pouvez restaurer une boîte aux lettres partagée ayant été supprimée si la corbeille de ce domaine est activée.

Création d'une boîte aux lettres d'archivage partagée

Vous pouvez créer des boîtes aux lettres d'archivage partagées dans le domaine géré ou dans la sous-arborescence gérée.

Suppression d'une boîte aux lettres d'archivage partagée

Vous pouvez supprimer des boîtes aux lettres d'archivage partagées du domaine géré ou de la sous-arborescence gérée.

Modification des propriétés d'une boîte aux lettres partagée

Vous pouvez modifier les propriétés de boîtes aux lettres partagées du domaine géré ou de la sous-arborescence gérée. Vos pouvoirs déterminent les propriétés que vous pouvez modifier.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Tâches de gestion des boîtes aux lettres liées

Les boîtes aux lettres liées sont utiles lors de grands remaniements de l'organisation qui se produisent en cas de fusions, d'acquisitions ou de divisions de sociétés, lorsque la migration de boîte aux lettres est courante. Cette fonction permet de lier des boîtes aux lettres à partir de différentes forêts Exchange pour éviter les interruptions des messageries des utilisateurs. Les boîtes aux lettres doivent se trouver dans des domaines DRA gérés avec la stratégie Exchange activée. De plus, vous devez disposer des pouvoirs qui vous permettent de gérer des boîtes aux lettres liées. Lorsque vous créez une boîte aux lettres liée, un onglet **Boîte aux lettres liée** est ajouté aux propriétés de l'objet Utilisateur.

La gestion des boîtes aux lettres liées est uniquement prise en charge au niveau de la console Web. Vous créez une boîte aux lettres liée à partir de la barre d'outils d'un compte utilisateur sélectionné. Cette option est uniquement activée lorsque le domaine de l'utilisateur sélectionné possède une approbation de forêt externe avec d'autres domaines gérés dans DRA. Seuls les comptes utilisateur désactivés seront répertoriés lors de la recherche d'un compte à lier à un autre domaine DRA géré.

Création d'une boîte aux lettres liée

Vous pouvez créer une boîte aux lettres liée à partir de deux comptes utilisateur sélectionnés dans différentes forêts Exchange gérées.

Suppression d'une boîte aux lettres liée

Vous pouvez supprimer une boîte aux lettres liée à partir de la barre d'outils d'un utilisateur sélectionné ayant une boîte aux lettres liée.

Modification des propriétés d'une boîte aux lettres liée

Vous pouvez modifier les propriétés d'une boîte aux lettres sous l'onglet **Boîte aux lettres liée** des propriétés de l'utilisateur sélectionné.

Création d'une boîte aux lettres d'archivage liée

Vous pouvez créer une boîte aux lettres d'archivage liée à partir d'un utilisateur sélectionné possédant une boîte aux lettres liée.

Suppression d'une boîte aux lettres d'archivage liée

Vous pouvez supprimer une boîte aux lettres d'archivage liée à partir de la barre d'outils d'un utilisateur sélectionné ayant une boîte aux lettres d'archivage liée.

Restauration d'une boîte aux lettres liée ayant été supprimée

Vous pouvez restaurer une boîte aux lettres liée ayant été supprimée si la corbeille de ce domaine est activée.

Tâches de gestion des dossiers publics

Si l'administrateur DRA a créé des forêts de dossiers publics dans l'entreprise DRA gérée et vous a octroyé des pouvoirs de gestion des dossiers publics dans DRA, vous pourrez créer des dossiers publics, modifier leurs propriétés et générer des rapports d'historique des modifications. Les dossiers publics ne peuvent être créés qu'au niveau de la console Web. Vous pouvez utiliser l'option de recherche pour effectuer des recherches dans les dossiers publics. Pour plus d'informations, reportez-vous à la section « [Recherche](#) » [page 65](#).

Les tâches de dossiers publics peuvent uniquement être exécutées à partir de l'onglet **Gestion > Dossiers publics**.

Création d'un dossier public

Vous pouvez créer des dossiers publics dans les domaines, les sous-arborescences et les boîtes aux lettres de dossiers publics définis via la console Web. Vous pouvez utiliser la boîte aux lettres par défaut du domaine sélectionné ou en choisir une.

Activation de la messagerie électronique d'un dossier public

Vous pouvez activer la messagerie électronique d'un dossier public à l'aide de l'option **Activer la messagerie** dans la barre d'outils de la liste. De cette façon, vous pouvez associer des adresses électroniques au dossier public et modifier les propriétés du dossier public.

Désactivation de la messagerie électronique d'un dossier public

Vous pouvez désactiver la messagerie électronique d'un dossier public à l'aide de l'option **Désactiver la messagerie** dans la barre d'outils de la liste.

Modification des propriétés d'un dossier public

Après avoir activé la messagerie pour un dossier public existant, vous pouvez consulter ses statistiques et modifier ses propriétés. Sous ces propriétés, vous pouvez spécifier des options de distribution et de restriction, des limites de taille, des avertissements de quota, des propriétés de messagerie, des limites de durée de stockage. Vous pouvez également inclure des modérateurs pour approuver les messages et les attributs personnalisés.

REMARQUE : lorsque plusieurs dossiers publics sont sélectionnés, vous pouvez aussi mettre à jour certaines propriétés de ces derniers, notamment les quotas de stockage.

Suppression d'un dossier public

Vous pouvez supprimer des dossiers publics s'ils ne contiennent aucun sous-dossier et si l'option de messagerie est désactivée.

7 Gestion des ressources

DRA vous permet de gérer des ressources, notamment des ordinateurs, des imprimantes et d'autres périphériques, ainsi que des processus associés à ces ressources. Par exemple, si vous devez démarrer un service spécifique sur un ordinateur géré, vous pouvez rechercher cet objet Ordinateur dans DRA, accéder à ses services via les propriétés d'objet, puis redémarrer un service spécifique sur cet ordinateur à partir de DRA sans devoir vous connecter à distance à cet ordinateur.

- ♦ « [Gestion des unités organisationnelles](#) » page 87
- ♦ « [Gestion des ordinateurs](#) » page 88
- ♦ « [Gestion des services](#) » page 90
- ♦ « [Gestion des imprimantes et des travaux d'impression](#) » page 91
- ♦ « [Gestion des partages](#) » page 95
- ♦ « [Gestion des utilisateurs connectés](#) » page 96
- ♦ « [Gestion des périphériques](#) » page 96
- ♦ « [Gestion des journaux d'événements](#) » page 97
- ♦ « [Gestion des fichiers ouverts](#) » page 99

Gestion des unités organisationnelles

Cette section vous guide tout au long de l'administration des unités organisationnelles dans la console de délégation et de configuration via le nœud Account and Resource Management (Gestion des comptes et des ressources). Si vous disposez des pouvoirs appropriés, vous pouvez réaliser diverses tâches de gestion sur les unités organisationnelles, comme déplacer ces dernières vers un autre conteneur.

REMARQUE : vous ne pouvez gérer les unités organisationnelles que via la console de délégation et de configuration.

Modification des propriétés des unités organisationnelles

Vous pouvez modifier les propriétés des unités organisationnelles. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour une unité organisationnelle située dans le domaine géré ou dans la sous-arborescence gérée.

Création d'une unité organisationnelle

Vous pouvez créer une unité organisationnelle dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier les propriétés générales, telles que la description d'une unité organisationnelle.

Clonage d'une unité organisationnelle

Vous pouvez créer une unité organisationnelle en clonant une unité organisationnelle existante de la sous-arborescence ou du domaine géré. Vous pouvez également modifier les propriétés générales de la nouvelle unité organisationnelle, telles que sa description. Notez que cloner une unité organisationnelle ne clone pas les objets qu'elle contient.

Ouverture de l'arborescence Active Directory à un emplacement d'unité organisationnelle

Vous pouvez facilement et rapidement ouvrir l'arborescence Active Directory à l'emplacement d'une unité organisationnelle spécifique dans la sous-arborescence ou le domaine géré.

Déplacement d'une unité organisationnelle vers un autre conteneur

Vous pouvez déplacer une unité organisationnelle vers un autre conteneur dans le domaine géré. Lorsque vous gérez une sous-arborescence d'un domaine, vous pouvez déplacer des unités organisationnelles au sein de la hiérarchie de cette sous-arborescence.

REMARQUE

- ♦ Si le déplacement d'une unité organisationnelle vers un autre conteneur augmente vos pouvoirs sur cette unité organisationnelle, DRA ne vous autorise pas à effectuer cette opération.
 - ♦ Vous pouvez également déplacer une unité organisationnelle en la faisant glisser vers le nouvel emplacement.
-

Suppression d'une unité organisationnelle

Vous pouvez supprimer des unités organisationnelles de la sous-arborescence ou du domaine géré. Notez toutefois que vous ne pouvez supprimer que des unités organisationnelles vides. Si une unité organisationnelle contient des objets, vous ne pouvez pas la supprimer tant que vous n'avez pas supprimé tous ces objets.

Gestion des ordinateurs

DRA vous permet de gérer les ordinateurs du domaine géré ou de la sous-arborescence gérée. Par exemple, vous pouvez ajouter ou supprimer des comptes d'ordinateur des domaines gérés, mais aussi gérer les ressources de chaque ordinateur. Lorsque vous ajoutez un ordinateur à un domaine, DRA crée un compte d'ordinateur dans ce domaine pour cet ordinateur. Vous pouvez ensuite connecter l'ordinateur à ce domaine et configurer l'ordinateur pour qu'il utilise ce compte d'ordinateur. Vous pouvez également afficher et modifier les propriétés de comptes d'ordinateur. DRA vous permet aussi d'arrêter un ordinateur et de synchroniser les contrôleurs de domaine dans un domaine géré.

REMARQUE

- ♦ Vous ne pouvez gérer les ordinateurs que via la console de délégation et de configuration.
 - ♦ vous ne pouvez pas gérer des contrôleurs de domaine masqués. Le cache du domaine n'inclut pas les contrôleurs de domaine masqués. DRA n'affiche donc pas les ordinateurs des domaines masqués dans les listes ou dans les fenêtres de propriétés.
-

Spécification d'une adhésion à un groupe pour des ordinateurs

Vous pouvez ajouter ou supprimer des ordinateurs à partir d'un groupe spécifique du domaine géré ou de la sous-arborescence gérée. Vous pouvez également afficher ou modifier les propriétés de groupes existants auxquels cet ordinateur appartient.

REMARQUE : DRA vous permet d'exporter les résultats de type **Membre de** dans un fichier CSV. Pour exporter les résultats de type **Membre de** à partir de la console Web, accédez à **Gestion > Rechercher**, puis cliquez sur **Propriétés**. Accédez à l'onglet **Membre de**, puis cliquez sur l'icône **Télécharger**. Les modifications non enregistrées ne sont pas exportées. Veillez à enregistrer les modifications récentes afin qu'elles soient disponibles dans le fichier exporté.

Gestion des propriétés d'un compte d'ordinateur

Vous pouvez gérer les propriétés d'un compte d'ordinateur. Vos pouvoirs déterminent les propriétés que vous pouvez modifier pour un ordinateur situé dans le domaine géré ou dans la sous-arborescence gérée.

Ajout d'un ordinateur à un domaine

Vous pouvez ajouter un ordinateur à un domaine géré ou à une sous-arborescence gérée en créant un compte d'ordinateur.

Suppression d'un ordinateur d'un domaine

Vous pouvez supprimer un ordinateur d'un domaine géré ou d'une sous-arborescence gérée en supprimant le compte d'ordinateur.

Déplacement d'un ordinateur

Vous pouvez déplacer un ordinateur vers un autre conteneur, par exemple une unité organisationnelle, dans le domaine géré ou dans la sous-arborescence gérée.

Arrêt ou redémarrage d'un ordinateur

Vous pouvez arrêter et redémarrer un ordinateur immédiatement ou à une date et une heure définies.

Réinitialisation du mot de passe d'un compte administrateur

Pour réinitialiser le mot de passe du compte administrateur pour un ordinateur, vous devez disposer du pouvoir Réinitialiser le mot de passe de l'administrateur local ou être associé à un rôle qui contient ce pouvoir. Vous pouvez réinitialiser le mot de passe de l'administrateur pour les serveurs membres de votre domaine géré ou de la sous-arborescence gérée. Vous ne pouvez pas réinitialiser le mot de passe de l'administrateur pour un contrôleur de domaine.

Réinitialisation du compte d'ordinateur

Vous pouvez réinitialiser un compte d'ordinateur pour les serveurs membres de votre domaine géré ou de la sous-arborescence gérée. Vous ne pouvez pas réinitialiser le compte d'ordinateur d'un contrôleur de domaine.

Suppression d'un compte d'ordinateur

Vous pouvez supprimer un compte d'ordinateur du domaine géré ou de la sous-arborescence gérée. Si vous gérez un domaine Microsoft Windows, vous pouvez supprimer des comptes d'ordinateur qui contiennent d'autres objets, comme une ressource partagée. Activez l'option **Forcer la suppression** pour supprimer les objets Ordinateur d'Active Directory. Cette opération

supprime également les objets enfant, y compris les imprimantes et les dossiers partagés. Les ordinateurs supprimés et les objets associés sont déplacés vers la corbeille DRA. Les objets sont définitivement supprimés si la corbeille est désactivée lors de la suppression.

REMARQUE : Vous ne pouvez pas supprimer de comptes d'ordinateur pour les serveurs membres du domaine géré ou de la sous-arborescence gérée.

Désactivation d'un compte d'ordinateur

Vous pouvez désactiver un compte d'ordinateur dans le domaine géré ou dans la sous-arborescence gérée. La désactivation d'un compte d'ordinateur empêche les utilisateurs de cet ordinateur de se connecter à n'importe quel domaine.

Activation d'un compte d'ordinateur

Vous pouvez activer un compte d'ordinateur dans le domaine géré ou dans la sous-arborescence gérée. L'activation d'un compte d'ordinateur permet aux utilisateurs de cet ordinateur de se connecter à n'importe quel domaine.

Gestion des ressources de l'ordinateur

Pour chaque compte d'ordinateur du domaine géré ou de la sous-arborescence gérée, vous pouvez gérer les ressources associées, telles que les services, les partages, les périphériques, les imprimantes et les travaux d'impression.

Gestion des services

Un service est un type d'application bénéficiant d'un traitement spécial de la part du système d'exploitation Windows. Les services peuvent s'exécuter même si aucun utilisateur n'est actuellement connecté à un ordinateur. Les assistants administrateur qui disposent des pouvoirs appropriés peuvent gérer les services qui s'exécutent sur les ordinateurs du domaine géré ou de la sous-arborescence gérée.

Gestion des propriétés de services

Vous pouvez gérer les propriétés de services s'exécutant sur des ordinateurs dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez gérer les services en même temps que d'autres ressources de cet ordinateur.

Démarrage d'un service

Vous pouvez démarrer un service sur n'importe quel ordinateur du domaine géré ou de la sous-arborescence gérée.

Démarrage d'un service avec des paramètres

Lorsque vous démarrez des services qui acceptent des paramètres, vous pouvez spécifier ces paramètres au démarrage. Vous pouvez démarrer les services sur des ordinateurs dans le domaine géré ou dans la sous-arborescence gérée.

REMARQUE : vous ne pouvez démarrer un service avec des paramètres que via la console de délégation et de configuration.

Spécification d'un type de démarrage de services

Vous pouvez modifier le type de démarrage d'un service nécessitant par exemple, un démarrage manuel.

Spécification d'un compte de connexion à un service

Vous pouvez changer le compte de connexion à un service et choisir un autre compte que le compte système actuel. Vous pouvez spécifier le compte système local, un compte utilisateur spécifique ou un compte de service administré de groupe (gMSA) comme compte de connexion à un service.

Redémarrage d'un service

Vous pouvez redémarrer un service qui s'exécute sur un ordinateur dans le domaine géré ou dans la sous-arborescence gérée.

Pour redémarrer un service, vous devez disposer des pouvoirs permettant d'arrêter et de démarrer un service ou être associé à un rôle qui contient ces pouvoirs, tels que le rôle Arrêter le service ou Démarrer le service.

Arrêt d'un service

Vous pouvez arrêter un service qui s'exécute sur un ordinateur dans le domaine géré ou dans la sous-arborescence gérée.

Suspension d'un service

Vous pouvez suspendre un service qui s'exécute sur un ordinateur dans le domaine géré ou dans la sous-arborescence gérée. Le type de service détermine s'il peut être suspendu ou non. Par exemple, un service ayant des services dépendants pourrait ne pas pouvoir être suspendu.

Reprise d'un service suspendu

Vous pouvez reprendre un service qui a été suspendu sur un ordinateur dans le domaine géré ou dans la sous-arborescence gérée.

Gestion des imprimantes et des travaux d'impression

Pour gérer des imprimantes, vous pouvez gérer les files d'attente d'impression qui desservent ces imprimantes. DRA vous permet de suspendre ou de reprendre, mais aussi de démarrer, de modifier, d'arrêter et d'afficher les imprimantes de la ressource et celles publiées. Il vous permet également de modifier les propriétés et les priorités des travaux d'impression. Pour ajouter ou supprimer une imprimante, utilisez les outils Windows natifs.

Un serveur d'impression est un ordinateur sur lequel une ou plusieurs imprimantes logiques sont installées. Une imprimante logique est définie sur l'ordinateur qui héberge le pilote de périphérique d'impression. Une imprimante logique inclut le pilote et la file d'attente d'impression ainsi que les ports d'une imprimante. Le serveur d'impression associe les imprimantes logiques à des périphériques d'impression.

Une imprimante connectée est définie sur les ordinateurs à partir desquels des documents sont sélectionnés pour être imprimés. Une imprimante est qualifiée de connectée lorsqu'elle est connectée à un partage d'impression sur le réseau. Par conséquent, vous pouvez gérer des imprimantes et des travaux d'impression par le biais des ordinateurs associés.

Une imprimante publiée est une imprimante publiée dans Active Directory. Une imprimante publiée peut être une imprimante réseau qui n'est pas directement connectée à un serveur, ou il peut s'agir d'une imprimante hébergée par un serveur de grappe.

REMARQUE : vous ne pouvez gérer les imprimantes et les travaux d'impression que via la console de délégation et de configuration.

Pour plus d'informations sur la gestion des imprimantes et des tâches d'impression, reportez-vous aux rubriques suivantes :

- ♦ « [Tâches de gestion des imprimantes](#) » page 92
- ♦ « [Tâches de gestion des travaux d'impression](#) » page 93
- ♦ « [Tâches de gestion de l'imprimante publiée](#) » page 93
- ♦ « [Tâches de gestion des travaux d'impression des imprimantes publiées](#) » page 94

Tâches de gestion des imprimantes

Vous pouvez gérer les imprimantes associées à des ordinateurs dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes en même temps que d'autres ressources de cet ordinateur.

Cette section vous guide tout au long de l'administration des imprimantes dans la console de délégation et de configuration via le nœud Account and Resource Management (Gestion des comptes et des ressources). Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion des imprimantes, telles qu'arrêter une imprimante.

Gestion des propriétés de l'imprimante

Vous pouvez gérer les propriétés des imprimantes dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes en même temps que d'autres ressources de cet ordinateur.

Suspension d'une imprimante

Vous pouvez suspendre une imprimante associée à un ordinateur dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes en même temps que d'autres ressources de cet ordinateur.

Reprise après la suspension d'une imprimante

Vous pouvez annuler la suspension d'une imprimante associée à un ordinateur dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes en même temps que d'autres ressources de cet ordinateur.

Tâches de gestion des travaux d'impression

Vous pouvez gérer les travaux d'impression associés à des imprimantes dans le domaine géré ou dans la sous-arborescence gérée. Étant donné que les travaux d'impression sont associés à une imprimante, vous pouvez gérer les travaux d'impression en même temps que l'imprimante.

Cette section vous guide tout au long de la gestion des travaux d'impression dans le nœud Account and Resource Management (Gestion des comptes et des ressources) de la console de délégation et de configuration. Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion des travaux d'impression, telles qu'annuler un travail d'impression.

Gestion des propriétés d'un travail d'impression

Vous pouvez modifier les propriétés d'un travail d'impression dans le cadre du workflow de gestion de votre imprimante. Étant donné que les travaux d'impression sont associés à des imprimantes, vous pouvez modifier le travail d'impression dans le cadre de la gestion de l'imprimante correspondante. Les propriétés d'un travail d'impression que vous pouvez modifier dépendent du type de pouvoirs en votre possession. Pour modifier les propriétés d'un travail d'impression, vous devez pouvoir accéder à l'imprimante et à l'ordinateur correspondants.

Suspension d'un travail d'impression

Vous pouvez suspendre un travail d'impression sur une imprimante dans un domaine géré ou dans une sous-arborescence gérée. Pour suspendre un travail d'impression, vous devez pouvoir accéder à l'imprimante et à l'ordinateur correspondants. La suspension d'un travail d'impression ne supprime pas le travail d'impression de la file d'attente.

Reprise d'un travail d'impression

Vous pouvez reprendre un travail d'impression qui a été suspendu. Pour reprendre un travail d'impression, vous devez pouvoir accéder à l'imprimante et à l'ordinateur correspondants.

Redémarrage d'un travail d'impression

Vous pouvez relancer un travail d'impression arrêté. Pour redémarrer un travail d'impression, vous devez pouvoir accéder à l'imprimante et à l'ordinateur correspondants.

Annulation d'un travail d'impression

Vous pouvez annuler un travail d'impression placé en file d'attente. Lorsque vous annulez un travail d'impression, DRA supprime définitivement le travail d'impression de la file d'attente. Pour annuler un travail d'impression, vous devez pouvoir accéder à l'imprimante et à l'ordinateur correspondants.

Tâches de gestion de l'imprimante publiée

Vous pouvez gérer les imprimantes publiées dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez ajouter ou rechercher n'importe quelle imprimante publiée dans Active Directory ou des imprimantes hébergées par un serveur de grappe.

Cette section vous guide tout au long de l'administration des imprimantes publiées dans le nœud Account and Resource Management (Gestion des comptes et des ressources). Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion des imprimantes, telles qu'arrêter une imprimante.

Gestion des propriétés de l'imprimante publiée

Vous pouvez gérer les propriétés des imprimantes publiées dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées en même temps que d'autres ressources.

Rafraîchissement des informations d'une imprimante publiée

Vous pouvez rafraîchir les informations de l'imprimante publiée dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées en même temps que d'autres ressources.

Suspension d'une imprimante publiée

Vous pouvez suspendre une imprimante publiée dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées en même temps que d'autres ressources.

Reprise après la suspension d'une imprimante publiée

Vous pouvez annuler la suspension d'une imprimante publiée dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées en même temps que d'autres ressources.

Déplacement d'une imprimante publiée

Vous pouvez déplacer une imprimante publiée disponible dans un conteneur du domaine géré vers un autre conteneur du même domaine. DRA vous permet de gérer les imprimantes publiées en même temps que d'autres ressources.

Modification du nom d'une imprimante publiée

Vous pouvez renommer une imprimante publiée partagée dans Active Directory. DRA vous permet de gérer les imprimantes publiées en même temps que d'autres ressources.

REMARQUE : lorsque vous renommez une imprimante publiée dans Active Directory, le nom du partage de l'imprimante de la ressource n'est pas modifié ou le changement de nom n'est pas propagé à l'imprimante de la ressource que vous souhaitez gérer. Par exemple, si le nom de l'imprimante de la ressource est Emerald et que vous renommez l'imprimante Ruby dans Active Directory, les autres utilisateurs verront s'afficher Ruby comme nom d'imprimante, mais le nom de l'imprimante de la ressource restera Emerald.

Tâches de gestion des travaux d'impression des imprimantes publiées

Vous pouvez gérer les travaux d'impression associés à des imprimantes publiées dans le domaine géré ou dans la sous-arborescence gérée. Étant donné que les travaux d'impression sont associés à une imprimante, vous pouvez gérer les travaux d'impression en même temps que l'imprimante publiée.

Cette section vous guide tout au long de l'administration des travaux d'impression des imprimantes publiées dans le nœud Account and Resource Management (Gestion des comptes et des ressources). Si vous disposez des pouvoirs appropriés, vous pouvez effectuer différentes tâches de gestion des travaux d'impression, telles qu'annuler un travail d'impression.

Gestion des propriétés d'un travail d'impression

Vous pouvez modifier les propriétés d'un travail d'impression dans le cadre du workflow de gestion de votre imprimante publiée. Étant donné que les travaux d'impression sont associés à des imprimantes, vous pouvez modifier le travail d'impression dans le cadre de la gestion de l'imprimante publiée correspondante. Les propriétés d'un travail d'impression que vous pouvez modifier dépendent du type de pouvoirs en votre possession. Pour modifier les propriétés d'un travail d'impression, vous devez pouvoir accéder à l'imprimante publiée correspondante.

Suspension d'un travail d'impression

Vous pouvez suspendre un travail d'impression sur une imprimante publiée dans un domaine géré ou dans une sous-arborescence gérée. Pour suspendre un travail d'impression, vous devez pouvoir accéder à l'imprimante publiée correspondante. La suspension d'un travail d'impression ne supprime pas le travail d'impression de la file d'attente.

Reprise d'un travail d'impression

Vous pouvez reprendre un travail d'impression suspendu dans le domaine géré ou dans la sous-arborescence gérée. Pour reprendre un travail d'impression, vous devez pouvoir accéder à l'imprimante publiée correspondante.

Redémarrage d'un travail d'impression

Vous pouvez redémarrer un travail d'impression arrêté dans un domaine géré ou dans une sous-arborescence gérée. Pour redémarrer un travail d'impression, vous devez pouvoir accéder à l'imprimante publiée correspondante.

Annulation d'un travail d'impression

Vous pouvez annuler un travail d'impression placé dans la file d'attente d'un domaine géré ou d'une sous-arborescence gérée. Lorsque vous annulez un travail d'impression, DRA supprime définitivement le travail d'impression de la file d'attente. Pour annuler un travail d'impression, vous devez pouvoir accéder à l'imprimante publiée correspondante.

Gestion des partages

Un partage est un moyen de mettre des ressources, telles que des fichiers ou des imprimantes, à la disposition d'autres utilisateurs sur le réseau. Chaque partage est associé à un nom de partage qui fait référence à un dossier partagé sur le serveur. DRA gère les partages uniquement sur les ordinateurs se trouvant dans les domaines gérés. Pour parvenir à gérer les partages, le compte d'accès doit disposer d'autorisations de type administrateur, par exemple être membre d'un groupe d'administrateurs locaux, sur tous les ordinateurs sur lesquels vous souhaitez gérer les ressources. Pour assigner ces autorisations, ajoutez le compte d'accès au groupe d'administrateurs du domaine natif dans le domaine de l'ordinateur.

REMARQUE : vous ne pouvez gérer les partages que via la console de délégation et de configuration.

Gestion des propriétés des partages

Vous pouvez gérer les propriétés des partages dans le domaine géré ou dans la sous-arborescence gérée. DRA vous permet de gérer les partages en même temps que d'autres ressources de cet ordinateur.

Création d'un partage

Vous pouvez créer un partage pour un ordinateur dans le domaine géré ou dans la sous-arborescence gérée. Vous pouvez également modifier les propriétés de ce partage.

Clonage d'un partage

Vous pouvez cloner un partage pour un ordinateur dans le domaine géré ou dans la sous-arborescence gérée. En clonant un partage, vous pouvez rapidement créer des partages en fonction d'autres partages qui ont des propriétés similaires. Cette flexibilité vous permet d'appliquer des paramètres de manière cohérente pour tous les partages que vous créez dans un domaine donné.

Lorsque vous clonez un partage, DRA complète les champs de l'assistant de clonage du partage avec les valeurs du partage sélectionné. Vous pouvez également modifier les propriétés du nouveau partage.

Suppression d'un partage

Vous pouvez supprimer des partages d'ordinateurs situés dans le domaine géré ou dans la sous-arborescence gérée.

Gestion des utilisateurs connectés

Une session est établie chaque fois qu'un utilisateur se connecte à une ressource particulière sur un ordinateur distant. Un utilisateur est qualifié de connecté lorsqu'il est connecté à une ressource partagée sur le réseau.

DRA gère les utilisateurs connectés uniquement sur les ordinateurs se trouvant dans les domaines gérés. Le compte d'accès doit disposer d'autorisations de type administrateur, par exemple être membre d'un groupe d'administrateurs locaux, sur tous les ordinateurs sur lesquels vous souhaitez gérer des utilisateurs connectés. Pour assigner ces autorisations, ajoutez le compte d'accès au groupe d'administrateurs du domaine natif dans le domaine de l'ordinateur.

Déconnexion d'un utilisateur

Vous pouvez déconnecter un utilisateur connecté d'un ordinateur se trouvant dans le domaine géré ou dans la sous-arborescence gérée. Vous devez pouvoir accéder à l'ordinateur pour ouvrir la session. La déconnexion d'un utilisateur connecté met fin à la session ouverte.

Rafraîchissement de la liste des utilisateurs connectés

Pour être certain d'afficher les dernières informations sur les sessions ouvertes sur un ordinateur, rafraîchissez manuellement la liste des utilisateurs connectés. Vous devez pouvoir accéder à l'ordinateur pour ouvrir la session.

Gestion des périphériques

Un périphérique est n'importe quel équipement attaché à un réseau, tel qu'un ordinateur, une imprimante, un modem ou tout autre équipement périphérique.

Même si un périphérique est installé sur votre ordinateur, Windows ne peut pas le reconnaître tant que vous n'avez pas installé et configuré le pilote approprié. Un pilote de périphérique permet à un élément matériel de communiquer avec le système d'exploitation.

DRA vous permet de configurer et de gérer les périphériques uniquement sur les ordinateurs des domaines gérés. Le compte d'accès doit disposer d'autorisations de type administrateur, par exemple être membre d'un groupe d'administrateurs locaux, sur tous les ordinateurs sur lesquels vous souhaitez gérer des périphériques. Pour assigner ces autorisations, ajoutez le compte d'accès au groupe d'administrateurs du domaine natif dans le domaine de l'ordinateur.

Gestion des propriétés d'un périphérique

Vous pouvez modifier les propriétés d'un périphérique sur un ordinateur spécifique. La modification des propriétés du périphérique vous permet de modifier son type de démarrage.

Démarrage d'un périphérique

Vous pouvez démarrer un périphérique sur un ordinateur spécifique du domaine géré ou de la sous-arborescence gérée.

Arrêt d'un périphérique

Vous pouvez arrêter un périphérique sur un ordinateur spécifique du domaine géré ou de la sous-arborescence gérée.

Gestion des journaux d'événements

Un événement est une occurrence importante sur le système ou dans l'application. Le système d'exploitation Windows enregistre les informations relatives aux événements dans des fichiers journaux d'événements. Chaque ordinateur peut stocker plusieurs journaux d'événements. L'observateur d'événements Windows natif permet d'afficher les journaux d'événements. DRA gère les journaux d'événements uniquement sur les ordinateurs se trouvant dans les domaines gérés.

Il enregistre les opérations initiées par l'utilisateur dans l'archive du journal, un espace de stockage sécurisé. DRA peut également enregistrer des opérations initiées par l'utilisateur dans le journal des événements Windows en plus d'enregistrer les informations dans l'archive du journal DRA. Pour plus d'informations, reportez-vous à la section [Présentation des dates et heures](#).

Types de journaux d'événements

Les ordinateurs qui exécutent Microsoft Windows enregistrent des informations supplémentaires dans différents journaux. Les journaux sont décrits brièvement comme suit :

Type de journal	Description
ADAM	Enregistre les événements consignés par l'espace de stockage ADAM.
Application	Enregistre les événements consignés par une application sur l'ordinateur, tel qu'un démarrage ou un échec de service. Par exemple, DRA stocke les événements dans le journal de l'application.
Service Annuaire	Enregistre les événements liés aux contrôleurs de domaine assurant la maintenance de la base de données de sécurité.
Service de réplication des fichiers	Enregistre les événements liés aux services de réplication des fichiers fournis par le système d'exploitation.

Type de journal	Description
Sécurité	Enregistre les événements qui incluent des tentatives de connexion, l'accès à un fichier ou à un répertoire et des modifications de stratégie de sécurité basées sur les options de stratégie d'audit.
Système	Enregistre les événements consignés par les composants système Windows, tels que l'échec d'un pilote ou le démarrage et l'arrêt de services.

Tâches de gestion des journaux d'événements

Lorsque vous installez DRA, par défaut, les événements d'audit ne sont pas consignés dans le journal des événements Windows. Vous pouvez activer ce type de consignation en modifiant une clé de registre.

AVERTISSEMENT : soyez prudent lorsque vous modifiez votre registre Windows. Une erreur dans votre registre peut en effet empêcher le bon fonctionnement de votre ordinateur. Si une erreur se produit, vous pouvez rendre au registre l'état qu'il avait lors du dernier démarrage réussi de votre ordinateur. Pour plus d'informations, reportez-vous à l'Aide de l'éditeur de registre Windows.

Vous pouvez spécifier la taille maximale d'un fichier journal des événements et ce qui doit se produire lorsque celui-ci est plein. La fenêtre Propriétés affiche également le nom du journal, le chemin du fichier journal et le nom du fichier. Elle indique aussi quand le journal a été créé, quand il a été modifié pour la dernière fois et la date/heure du dernier accès à ce dernier. Si vous choisissez de sauvegarder le fichier journal, DRA enregistre le journal des événements sous un nom de fichier unique à un emplacement standard sur l'ordinateur sélectionné.

DRA vous permet de gérer les journaux d'événements en même temps que d'autres ressources de cet ordinateur. Si vous disposez des pouvoirs appropriés, vous pouvez effectuer diverses tâches telles que modifier les propriétés du journal des événements.

Gestion des propriétés du journal des événements

Vous pouvez modifier les propriétés du journal des événements d'un ordinateur spécifique.

Affichage des entrées du journal des événements

Vous pouvez afficher les entrées d'un journal des événements spécifique d'un ordinateur du domaine géré ou de la sous-arborescence gérée. Dans la console de délégation et de configuration, vous pouvez afficher le fichier journal des événements dans l'Observateur d'événements Windows natif.

Effacement du journal des événements

Vous pouvez effacer les entrées d'un journal des événements spécifique d'un ordinateur du domaine géré ou de la sous-arborescence gérée. Vous pouvez également enregistrer les entrées du journal des événements avant d'effacer le journal.

Gestion des fichiers ouverts

Un fichier ouvert est une connexion à des ressources partagées, telles que des fichiers ou des canaux de communication. Un canal est un mécanisme de communication interprocessus qui permet à un processus de communiquer avec un autre processus local ou distant.

DRA gère les fichiers ouverts uniquement sur les ordinateurs dans le domaine géré ou dans la sous-arborescence gérée. Étant donné que les fichiers ouverts sont associés à un ordinateur, vous pouvez gérer les fichiers ouverts en même temps que d'autres ressources de cet ordinateur. Par exemple, vous souhaitez peut-être fermer des fichiers ouverts lorsque vous arrêtez un système ou installez un nouveau périphérique ou un service. Vous pouvez également surveiller quels sont les fichiers auxquels les utilisateurs accèdent le plus souvent, afin de vous aider à mieux évaluer la sécurité des fichiers.

REMARQUE : vous ne pouvez gérer les fichiers ouverts que via la console de délégation et de configuration.

Fermeture d'un fichier

Vous pouvez fermer des fichiers ouverts à partir de ressources du réseau. Veillez à avertir les utilisateurs lorsque vous avez l'intention de fermer des fichiers ouverts. Ils pourraient avoir besoin d'un moment pour enregistrer leurs données. Pour fermer un fichier ouvert, vous devez pouvoir accéder à l'ordinateur correspondant.

Rafraîchissement de la liste des fichiers ouverts

Pour être certain d'afficher les dernières informations sur les sessions ouvertes sur un ordinateur, rafraîchissez manuellement la liste des utilisateurs connectés. Pour rafraîchir la liste des fichiers ouverts, vous devez pouvoir accéder à l'ordinateur correspondant.

8 Gestion de la corbeille

La corbeille fournit un filet de sécurité en vous permettant de supprimer temporairement des comptes utilisateur, des groupes, des contacts et des comptes d'ordinateur. Vous pouvez restaurer l'état d'origine de ces objets avec toutes les données, telles que les identificateurs de sécurité, les listes de contrôle d'accès et les adhésions aux groupes ou supprimer définitivement ces objets. Cette flexibilité vous fournit une méthode davantage sécurisée pour gérer les comptes utilisateur, les groupes, les contacts et les comptes d'ordinateur. Vous pouvez utiliser l'option de recherche pour rechercher les objets souhaités. Pour plus d'informations, reportez-vous à la section [Recherche d'objets](#).

Restauration d'un objet placé dans la corbeille

Vous pouvez restaurer des objets supprimés vers les conteneurs dans lesquels ils se trouvaient avant que vous les supprimiez. DRA restaure l'état initial de ces objets avec toutes leurs données, telles que les identificateurs de sécurité, les listes de contrôle d'accès et les adhésions aux groupes. Un objet peut être un compte utilisateur, un groupe, un contact, un groupe dynamique, une boîte aux lettres de ressources, un groupe de distribution dynamiques ou un compte d'ordinateur.

Restauration de tous les objets

Vous pouvez restaurer tous les objets placés dans la corbeille d'un domaine géré. Vous pouvez restaurer des objets placés dans la corbeille pour un domaine spécifique ou pour tous les domaines gérés. Pour restaurer des objets d'un domaine spécifique placés dans la corbeille, elle doit être activée pour ce domaine.

Suppression d'un objet de la corbeille

Vous pouvez supprimer définitivement des objets d'un domaine géré placés de la corbeille. Après avoir supprimé un objet de la corbeille, vous ne pouvez plus le restaurer. Un objet peut être un compte utilisateur, un groupe, un contact, un groupe dynamique, une boîte aux lettres de ressources, un groupe de distribution dynamiques ou un compte d'ordinateur.

Vidage de la corbeille

Vous pouvez vider la corbeille d'un domaine géré. Le vidage de la corbeille supprime définitivement tous les objets qui s'y trouvent actuellement. Vous pouvez vider la corbeille d'un domaine spécifique ou de tous les domaines gérés. Pour vider la corbeille d'un domaine spécifique, elle doit être activée pour ce domaine. Une fois vidée, vous ne pouvez pas restaurer les objets supprimés.