NetIQ Directory and Resource Administrator

Guide de l'utilisateur

Juin 2021

Avis juridique

À propos de ce guide

Le *Guide de l'utilisateur* fournit des informations conceptuelles sur le produit NetIQ Directory and Resource Administrator (DRA). Cet ouvrage définit la terminologie et divers concepts connexes.

Public cible

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

Documentation supplémentaire

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

Coordonnées

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

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

1 Mise en route

Avant de commencer à gérer des objets Active Directory à l'aide de NetIQ Directory and Resource Administrator (DRA), vous devez comprendre les fondements de ce que DRA fera pour votre entreprise et le rôle des composants de DRA dans l'architecture du produit.

Qu'est-ce que Directory and Resource Administrator?

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

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

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

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

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

- **Intégrité opérationnelle :** empêche les changements malveillants ou incorrects qui affectent le fonctionnement et la disponibilité des systèmes et des services grâce à un contrôle d'accès granulaire accordé aux administrateurs et à la gestion de l'accès aux systèmes et aux ressources.
- **Application du processus :** garantit l'intégrité des processus clés de gestion du changement qui vous aident à améliorer la productivité, à réduire les erreurs, à gagner du temps et à accroître l'efficacité de l'administration.
- **Intégration avec Change Guardian :** améliore l'audit pour les événements générés dans Active Directory en dehors de DRA et de Workflow Automation.

Comprendre les composants de Directory and Resource Administrator

Les composants de DRA que vous utilisez couramment pour gérer les accès privilégiés comprennent les serveurs principaux et secondaires, les consoles d'administrateur, les composants de création de rapports et le moteur de processus de travail pour automatiser les processus de travail.

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

Type d'utilisateur DRA	Interfaces utilisateur	Serveur d'administration
Administrateur DRA (La personne qui gérera la configuration du produit)	Console de délégation et de configuration	Serveur primaire
Administrateur avancé	DRA Reporting PowerShell CLI Fournisseur DRA ADSI	Tout serveur DRA
Administrateur occasionnel du service d'assistance	Nœud de gestion des comptes et des ressources dans la console de délégation et de configuration Console Web	Tout serveur DRA

Serveur d'administration DRA

Le serveur d'administration DRA stocke les données de configuration (environnement, accès délégué et stratégie), exécute les tâches d'automatisation et d'opérateur et audite l'activité du système. Tout en prenant en charge plusieurs clients de niveau console et API, le serveur est conçu pour offrir une haute disponibilité pour la redondance et l'isolation géographique par un modèle d'extension MMS

(ensemble multimaître). Dans ce modèle, chaque environnement DRA requiert un serveur d'administration DRA primaire qui se synchronise avec un certain nombre de serveurs d'administration DRA secondaires supplémentaires.

Nous vous recommandons fortement de ne pas installer les serveurs d'administration sur les contrôleurs de domaine Active Directory. Pour chaque domaine géré par DRA, assurez-vous qu'il existe au moins un contrôleur de domaine sur le même site que le serveur d'administration. Par défaut, le serveur d'administration accède au contrôleur de domaine le plus proche pour toutes les opérations de lecture et d'écriture. Lors de l'exécution de tâches propres au site, telles que les réinitialisations de mot de passe, vous pouvez spécifier un contrôleur de domaine propre au site pour traiter l'opération. Il est recommandé d'utiliser un serveur d'administration secondaire dédié pour la création de rapports, le traitement par lots et les charges de travail automatisées.

Gestion des comptes et des ressources

La gestion des comptes et des ressources est un nœud de la console de délégation et de configuration permettant aux administrateurs assistants de DRA de visualiser et de gérer les objets délégués des domaines et des services connectés.

Console Web

La console Web est une interface utilisateur basée sur le Web qui fournit un accès rapide et facile aux administrateurs assistants de DRA pour visualiser et gérer les objets délégués des domaines et des services connectés.

Les administrateurs peuvent personnaliser l'apparence et l'utilisation de la console Web pour inclure une 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 en dehors de DRA.

Un administrateur DRA peut également créer et modifier des formulaires de processus de travail automatisés afin d'exécuter des tâches automatiques de routine lorsqu'elles sont déclenchées.

L'historique unifié des modifications est une autre caractéristique de la console Web qui permet l'intégration avec les serveurs de l'historique des modifications pour vérifier les modifications apportées aux objets AD en dehors de DRA. Les options du rapport sur l'historique des modifications comprennent les éléments suivants :

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

Composants de création de rapports

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

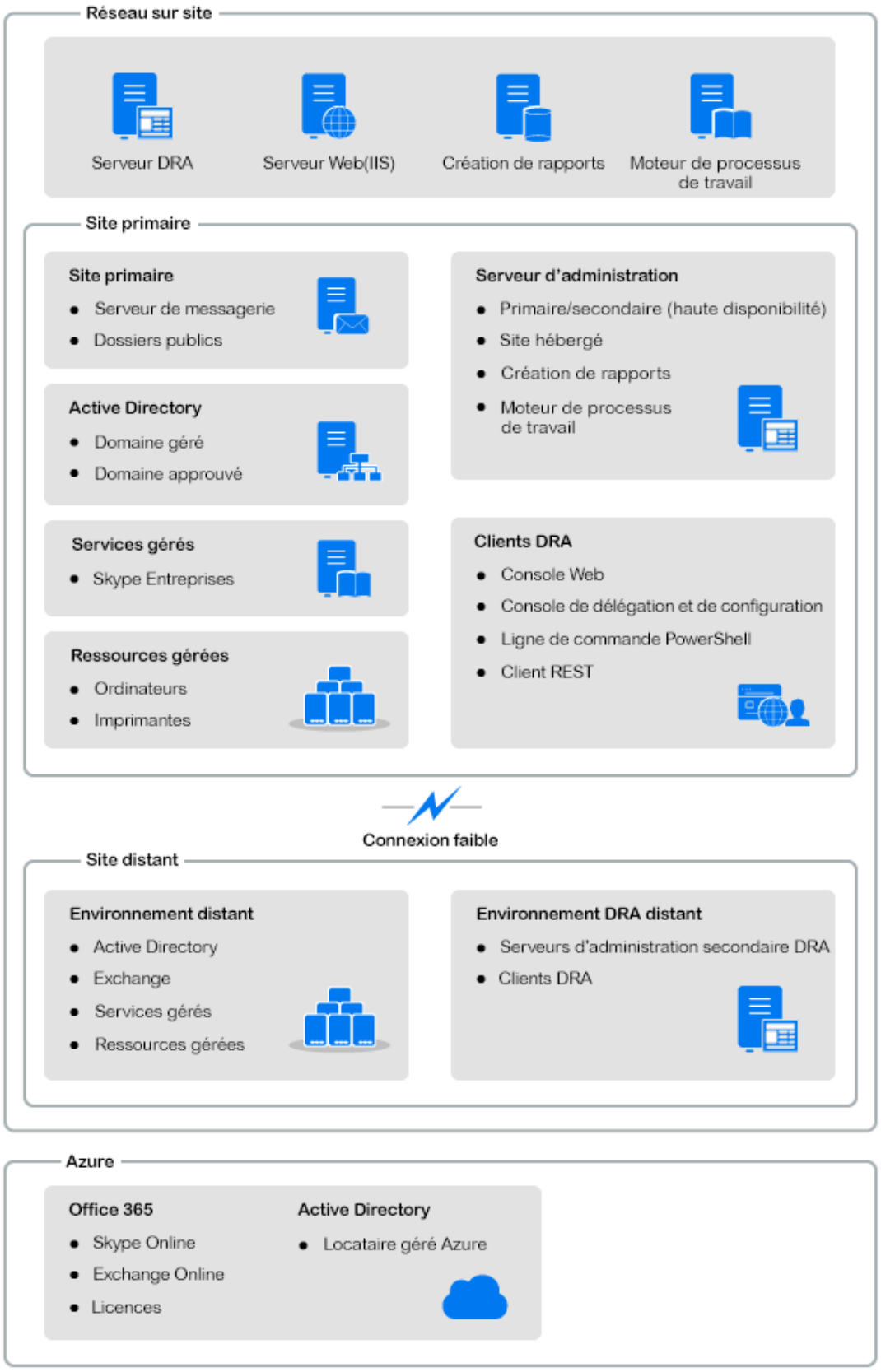
- Rapports de ressources pour les objets d'AD
- Rapports de données d'objet d'AD
- Rapports de synthèse d'AD
- Rapports de configuration de DRA
- Rapports de configuration d'Exchange
- Rapports d'Office 365 Exchange Online
- Rapports détaillés sur les tendances d'activité (par mois, domaine et pic)
-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

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

Moteur de processus de travail

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

Architecture du produit



2 Utilisation des interfaces utilisateur

Les interfaces utilisateur de DRA répondent à divers besoins d'administration. Ces interfaces comprennent :

La console Web

Elle permet d'effectuer des tâches courantes d'administration de compte et de ressources à l'aide d'une interface Web. Vous pouvez accéder à la console Web à partir de tout ordinateur exécutant Internet Explorer, Chrome ou Firefox.

Le PowerShell

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

La console de création de rapports de NetIQ

Elle permet d'afficher et de déployer des rapports de gestion afin de pouvoir auditer la sécurité de votre entreprise et de suivre les activités d'administration. Les rapports de gestion incluent les rapports d'activité, les rapports de configuration et les rapports de synthèse. Bon nombre de ces rapports peuvent être visualisés sous forme graphique.

La console Web

La console Web est une interface utilisateur basée sur le Web qui fournit un accès rapide et facile à de nombreuses tâches de compte utilisateur, de groupe, d'ordinateur, de ressource et de boîte aux lettres Microsoft Exchange. Vous pouvez personnaliser les propriétés de l'objet pour augmenter l'efficacité des tâches routinières. Vous pouvez également gérer les propriétés générales de votre propre compte utilisateur telles que l'adresse ou le numéro de téléphone cellulaire.

La console Web affiche une tâche uniquement si vous pouvez l'exécuter.

- « Démarrer la console Web » page 13
- « Configurer la console Web » page 14
- « Personnaliser la console Web » page 18
- « Gérer des objets dans la console Web » page 20
- « Générer des rapports d'historique des modifications » page 20
- « Utiliser l'automatisation de processus de travail » page 21

Démarrer la console Web

Vous pouvez lancer la console Web depuis n'importe quel ordinateur utilisant l'un des navigateurs pris en charge :

- Google Chrome

- Mozilla Firefox
- Microsoft Edge

Pour démarrer la console Web, spécifiez l'URL correspondante dans le champ d'adresse de votre navigateur Web. Par exemple, si vous avez installé le composant Web sur l'ordinateur HOUserver, tapez `https://HOUserver.entDomain.com/draclient` dans le champ d'adresse de votre navigateur Web.

REMARQUE : Pour afficher les informations les plus récentes sur le compte et sur Microsoft Exchange dans la Console Web, configurez votre navigateur Web pour qu'il vérifie les versions les plus récentes des pages mises en cache à chaque visite.

Connexion au serveur DRA

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

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

Configurer la console Web

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

REMARQUE : L'onglet **Administration** dans le générique ne s'affichera pas si vous ne disposez pas des pouvoirs administratifs suffisant.

- « Advanced Authentication » page 15
- « Image de marque de la console Web » page 15
- « Paramètres de la session client » page 17
- « Connexion au serveur » page 17

Advanced Authentication

Advanced Authentication vous permet d'aller au-delà d'un simple nom d'utilisateur et d'un mot de passe. Il vous offre un moyen plus sécurisé de protéger les informations sensibles en utilisant une authentification multifacteur. L'authentification multifacteur est une méthode de contrôle d'accès d'ordinateur qui utilise plusieurs méthodes d'authentification à partir de catégories distinctes d'informations d'identification afin de vérifier l'identité d'un utilisateur.

Une fois que l'administrateur DRA a configuré les chaînes et les événements, vous pouvez ouvrir une session sur la console Web, si vous disposez des pouvoirs nécessaires, afin d'activer Advanced Authentication. Une fois l'authentification activée, chaque utilisateur devra s'authentifier en utilisant Advanced Authentication, pour pouvoir accéder à la console Web.

Pour activer l'authentification avancée, sélectionnez **Advanced Authentication** (Authentification avancée) dans l'onglet Configuration, cliquez sur **Enable Advanced Authentication,** (Activer l'authentification avancée) et configurez le formulaire en suivant les instructions fournies pour chaque champ.

Pour de plus amples renseignements sur l'authentification avancée, consultez la rubrique « Authentification » dans le *Guide de l'administrateur de DRA*.

Image de marque de la console Web

Vous pouvez personnaliser l'écran de connexion et l'en-tête de la console Web de DRA, en procédant comme suit :

- **Générique :** il s'agit de la barre de navigation de haut niveau qui apparaît en haut de la console Web après la connexion.
  - *Image du logo ou texte de remplacement :* s'affiche à l'extrême gauche de la barre de titre. Vous pouvez afficher une image de logo ou un texte de remplacement, mais pas les deux.
  - *Couleur du générique :* superpose cette couleur à l'ensemble du générique, à l'exception de la zone de l'image du logo.
- **Écran de connexion à thème :** définit la façon dont la page de connexion apparaît lorsque vous accédez à l'URL de la console Web dans votre navigateur. The DRA theme is configured and enabled by default.
  - *Image du logo ou texte de remplacement :* s'affiche au-dessus du titre du produit et des champs d'informations d'identification. Vous pouvez afficher une image de logo ou un texte de remplacement, mais pas les deux.

- *Titre de l'application :* s'affiche entre les champs d'authentification et l'image du logo.
- *Modale de notification :* il s'agit d'une boîte de message qui recouvre et obscurcit la page de connexion jusqu'à ce que l'utilisateur clique sur **OK**. Elle est généralement utilisée pour informer l'utilisateur que l'accès à la console implique le consentement à suivre une stratégie de sécurité de l'entreprise. Une fois activé, tous les utilisateurs qui accèdent à la console Web recevront l'invite.

Configurer le générique

Pour configurer le générique :

1. Connectez-vous à la console Web et accédez à **Administration** > **Configuration** > **Marquage**.
2. Faites l'une des choses suivantes. Si vous ajoutez à la fois du texte et un fichier image, seule l'image sera affichée.
   - Actualisez l'image du logo :
     1. Ajoutez le nom du fichier image enregistré, y compris l'extension de fichier, dans le champ Image du logo de la tuile **Générique**.
     2. Enregistrez l'image du logo dans le répertoire « `Ressources` » du serveur web. Par 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 **Générique**, si nécessaire.
3. Cliquez sur **Enregistrer** au bas de la page pour terminer les changements de configuration.

Configurer l'écran de connexion

La procédure ci-dessous fournit des informations permettant de modifier les trois options configurables, à savoir le logo de l'entreprise, le titre de l'application et la modale de notification. Vous pouvez modifier une, deux ou les trois de ces options.

Pour modifier le thème par défaut de l'écran de connexion procédez comme suit :

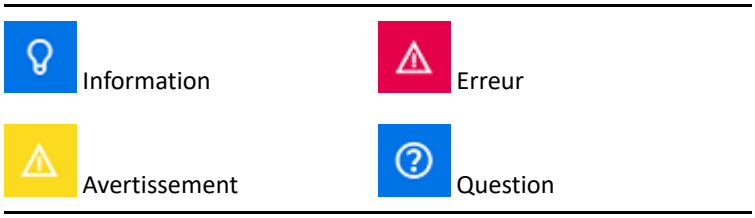
1. Enregistrez le logo de votre entreprise dans le dossier « `ressources` » du serveur Web. Par exemple :

   `C:\inetpub\wwwroot\DRAClient\assets`

   La taille optimale de l'image est de 115 x 28 pixels.
2. Connectez-vous à la console Web et accédez à **Administration** > **Configuration** > **Marquage**.
3. Remplacez le nom du fichier dans le champ Image du logo de l'entreprise de la tuile **Connexion** par le nom du fichier image enregistré, y compris l'extension de fichier.
4. Modifiez le texte du champ **Titre de l'application**, le cas échéant.
5. Cliquez sur **Show a notification modal at login** (Afficher une modale de notification à la connexion) pour activer ce paramètre, et tapez un titre pour l'invite de notification. Tapez ou collez le contenu du message que vous voulez que les utilisateurs voient dans le champ **Contenu**. Par exemple :

   You are logging into a secure network. En vous connectant à ce système, vous acceptez de vous conformer aux stratégies de sécurité de l'entreprise en matière d'accès au réseau.

6 Sélectionnez le style du message. Le style modifie le drapeau de l'image qui est associée à la boîte de message (voir ci-dessous). Si vous le souhaitez, vous pouvez cliquer sur Aperçu pour voir comment le message sera affiché.



7 Cliquez sur **Enregistrer** au bas de la page pour terminer les changements de configuration.

Paramètres de la session client

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

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

Connexion au serveur

Lorsque vous accédez à la page de connexion de la console Web dans votre navigateur, il existe des paramètres **Options** que vous pouvez configurer pour définir la manière dont vous vous connectez à DRA. Ces paramètres sont également accessibles grâce à l'option **Connexion au serveur** dans le menu du profil utilisateur de la console Web. Le port de service du serveur DRA est défini par défaut à 8775. Vous pouvez définir une nouvelle valeur par défaut pour le serveur DRA dans le profil de l'utilisateur ou dans l'écran de connexion Options lorsqu'aucune valeur par défaut n'est activée. Les paramètres de connexion de la configuration des connexions 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 des **connexions au serveur**, soit à partir du menu Options de l'écran de connexion, soit à partir du menu du profil utilisateur après la connexion :

Paramètres du serveur DRA	Description
Utiliser Découverte automatique	Trouve automatiquement un serveur DRA; aucune option de configuration n'est disponible
Connexion au serveur DRA par défaut (Affiché uniquement si la valeur par défaut est activée dans la configuration de la connexion du serveur)	Utilise le paramètre par défaut de la configuration de la connexion au serveur (lorsqu'elle est activée); aucune option de configuration n'est disponible.
Établir une connexion avec un serveur DRA précis	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** de la console Web.

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

Connexion au serveur DRA

La configuration de la connexion au serveur DRA comprend la définition d'un emplacement de serveur par défaut, la modification du port (si nécessaire) et un délai de connexion, en secondes. Vous pouvez également désactiver le réglage avec le commutateur à bascule.

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

```
ServerName.DomainName.com
```

Personnaliser la console Web

Vous pouvez personnaliser les propriétés des objets dans la console Web. Lorsqu'elles sont correctement implémentées, les personnalisations des propriétés permettent d'automatiser les tâches grâce à la gestion des objets.

Personnaliser les pages des propriétés

Si vous avez des pouvoirs d'administration de DRA, vous pouvez personnaliser les formulaires des propriétés de l'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 les types d'objets qui sont intégrés dans DRA. Vous pouvez également modifier les propriétés des types d'objets intégrés.

Les propriétés de l'objet sont clairement définies dans la liste Pages des propriétés de la console Web afin que vous puissiez facilement identifier les pages d'objet qui sont intégrées, les pages intégrées qui sont personnalisées et les pages non intégrées qui ont été créées par un administrateur.

Personnalisation d'une page des propriétés de l'objet

Vous pouvez personnaliser les formulaires des propriétés de l'objet en ajoutant ou en supprimant des pages, en modifiant des pages et des champs existants et en créant des gestionnaires personnalisés pour les attributs de propriété. Les gestionnaires personnalisés d'un champ sont exécutés chaque fois que la valeur de ce champ est modifiée. Il est possible de faire une planification de sorte que l'administrateur puisse spécifier si les gestionnaires doivent être exécutés immédiatement (à chaque pression sur une touche), lorsque le champ perd son focus, ou après un délai déterminé.

La liste d'objets dans les pages des propriétés fournit les types d'opération pour chaque type d'objet, Créer un objet et Éditer les propriétés. Ce sont les principales opérations que vos administrateurs assistants effectuent dans la console Web. Pour effectuer ces opérations, ils doivent accéder à

Management > **Search** or **Advanced Search** (Gestion > Recherche ou Recherche avancée). Ils peuvent y créer des objets à partir du menu déroulant Créer ou modifier les objets existants sélectionnés dans le tableau des résultats de la recherche grâce à l'icône Propriétés.

Pour personnaliser une page de propriété de l'objet dans la console Web procédez comme suit :

1. Connectez-vous à la console Web avec des privilèges d'administration de DRA.
2. Accédez à **Administration** > **Customization** > **Property Pages** (Administration > Personnalisation > Pages des propriétés).
3. Sélectionnez un objet et un type d'opération (Créer un objet ou Éditer un objet) dans la liste Pages des propriétés.
4. Cliquez sur l'icône **Properties** (Propriétés) .
5. Personnalisez le formulaire de propriété de l'objet en effectuant une ou plusieurs des opérations suivantes, puis appliquez vos modifications :
   - Ajouter une nouvelle page de propriétés : **+ Add Page** (+ Ajouter une page)
   - Réorganiser et supprimer les pages de propriété
   - Sélectionner une page de propriétés et personnaliser la page :
     - Réorganiser les champs de configuration sur la page :
     - Éditer des champs ou des sous-champs :
     - Ajouter un ou plusieurs champs : ou **Insert a new Field** (Insérer un nouveau champ)
     - Supprimer un ou plusieurs champs :
   - Créer des gestionnaires personnalisés pour les propriétés à l'aide de scripts, de boîtes de message ou de requêtes (LDAP, DRA ou REST)

     Pour plus d'informations sur l'utilisation des gestionnaires personnalisés, reportez-vous à la section « Ajout de gestionnaires personnalisés », dans le *Guide de l'Administrateur de DRA*.

Créer une nouvelle page de propriété de l'objet

Pour créer une nouvelle page de propriété de l'objet :

1. Connectez-vous à la console Web avec les pouvoirs d'administration de DRA et naviguez vers **Administration** > **Personnalisation** > **Pages de propriétés**, et cliquez sur **Créer**.
2. Créez le formulaire initial des propriétés de l'objet en définissant son nom, son icône, son type d'objet et la configuration de l'opération.

   Après avoir cliqué sur **OK**, les actions Créer sont ajoutées au menu déroulant Créer tandis que les actions Propriété s'affichent sous forme d'objet lorsque l'utilisateur sélectionne et modifie un objet dans la liste de recherche.
3. Personnalisez le nouveau formulaire selon vos besoins. Veuillez consulter la rubrique Personnalisation d'une page des propriétés de l'objet.

Gérer des objets dans la console Web

Pour gérer les objets dans la console Web, il suffit d'accéder à la rubrique Gestion. À partir de là, vous pouvez rechercher les 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 et prendre des mesures sur les objets Active Directory et Azure Active Directory à l'aide de DRA.

Si vous sélectionnez un objet dans la liste des résultats de la recherche, toutes les actions applicables que vous pouvez entreprendre sur cet objet sont disponibles dans la barre de tâches au-dessus de la grille. Les options disponibles sont basées sur le type d'objet sélectionné, les composants actuellement configurés pour DRA et les privilèges d'administrateur qui vous ont été attribués.

Pour modifier les propriétés d'un objet, passez la souris sur l'objet et cliquez sur l'icône **Properties** (Propriétés) qui apparaît sur la ligne de l'objet. De là, vous pouvez accéder à toutes les pages des propriétés de l'objet dans le volet de navigation sur la gauche.

IMPORTANT : Si vous souhaitez **protect an object from accidental deletion** (protéger un objet contre une suppression accidentelle), faites défiler l'écran jusqu'au bas de la page des propriétés de **General** (Général), cochez la case permettant d'activer cette fonction, puis (**Apply**) appliquez les modifications.

Pour de plus amples renseignements sur les actions que vous pouvez entreprendre sur les objets, consultez les rubriques suivantes :

- Gérer des objets Active Directory
- Gérer des objets Azure
- Gérer les boîtes aux lettres Exchange et les dossiers publics
- Gérer les ressources

Générer des rapports d'historique des modifications

Si l'historique des modifications est configuré par votre administrateur DRA et que vous disposez du pouvoir **Générer des rapports UI**, vous pouvez générer des rapports sur l'historique des modifications et exporter des rapports pour les objets gérés dans DRA. Cela inclut les modifications apportées dans le DRA et en dehors de celui-ci. Vous pouvez uniquement générer des rapports sur l'historique des modifications à partir de la console Web, qui comprend les types de rapports suivants :

- Modifications effectuées 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 de courriel de groupe et de contact créées par l'utilisateur
- Adresses de courriel de groupe et de contact supprimées par l'utilisateur
- Attributs virtuels créés ou désactivés par l'utilisateur
- Objets déplacés par l'utilisateur

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

1. Lancez la console Web.
2. Sélectionnez **Gestion > Rechercher**.
3. Définissez les critères de recherche à l'aide des options **Search by** (Rechercher par), **Search term** (Terme de recherche), et **Filters** (Filtres).
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 d'historique des modifications**.

   Dans le formulaire Rapport d'historique des modifications unifiées, vous pouvez éditer et générer vos critères de rapport à partir des options **Type**, **Target object(s)** (Objet(s) cible(s)), et **Filtres**, pour inclure la définition des serveurs où les modifications sont détectées (DRA et Change Guardian).
7. Cliquez sur **Générer** pour extraire les données d'audit et générer un rapport d'UCH.
8. Vous pouvez trier et exporter le rapport dans l'un des formats requis, tel que CSV et HTML.

Pour créer un fichier CSV du rapport affiché, vous pouvez exporter toutes les modifications générées ou seulement celles 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 **Export All** (Exporter tout) et enregistrez le rapport exporté.
- Cliquez sur **Export Current Page** (Exporter la page actuelle) et enregistrez le rapport exporté.

  Si nécessaire, vous pouvez modifier le nombre de modifications qui apparaissent sur la page, jusqu'à 200 éléments.

Utiliser l'automatisation de processus de travail

Grâce à l'automatisation du processus de travail, vous pouvez automatiser les processus informatiques en lançant des formulaires de processus de travail qui s'exécutent en même temps que les processus de travail ou lorsqu'ils sont déclenchés par un événement de processus de travail nommé créé sur le serveur d'automatisation du processus de travail.

Les formulaires de processus de travail sont enregistrés sur le serveur Web lorsqu'ils sont créés ou modifiés. Lorsque vous vous connectez à la console Web pour ce serveur, vous avez accès aux formulaires en fonction des pouvoirs délégués et de la configuration de ceux-ci. Les formulaires sont généralement disponibles pour tous les utilisateurs disposant des informations d'identification du serveur Web. Vous devez disposer des pouvoirs appropriés pour pouvoir soumettre le formulaire.

Lancer un formulaire de processus de travail : Les processus de travail sont créés dans le serveur d'automatisation du processus de travail, qui doit être intégré à DRA à l'aide de la console Web. Pour enregistrer un nouveau formulaire, l'option **Lancer un processus de travail précis**ou **Déclencher un processus de travail à l'aide d'un événement** doit être configuré dans les propriétés du formulaire. De plus amples renseignements sur ces options sont fournis ci-dessous :

- **Lancer un processus de travail précis :** Cette option répertorie tous les processus de travail disponibles qui sont en production dans le serveur de processus de travail pour DRA. Les processus de travail à remplir dans cette liste doivent être créés dans le dossier `DRA_Workflows` du serveur de Workflow Automation.

- **Déclencher le processus de travail par un événement :** Cette option permet d'exécuter des processus de travail à l'aide de déclencheurs prédéfinis. Les processus de travail avec déclencheurs sont également créés dans le serveur de Workflow Automation.

REMARQUE : Seuls les formulaires de processus de travail configurés avec Lancer un processus de travail précis auront un historique d'exécution qui peut être interrogé dans le volet de recherche principal sous **Tasks** > **Requests** (Tâches > Requêtes).

Vous trouverez de plus amples informations sur Workflow Automation dans les guides suivants que vous pouvez consulter sur le site de la documentation de DRA :

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

Gestion des comptes et des ressources

La console de gestion des comptes et des ressources permet d'accéder à la plupart des tâches d'administrateur assistant de DRA, répondant ainsi aux besoins de gestion de l'entreprise, de l'administration de base aux problèmes avancés d'assistance à la clientèle. Grâce à Gestion des comptes et des ressources, vous pouvez effectuer des tâches de gestion des comptes et des ressources et gérer les boîtes aux lettres Microsoft Exchange.

Gestion des comptes et des ressources contient les nœuds suivants :

Tous mes objets gérés

Ce nœud vous permet de gérer des objets tels que des comptes utilisateurs, des groupes, des contacts, des ressources, des groupes dynamiques, des groupes de distribution dynamiques, des boîtes aux lettres de ressources et des dossiers publics pour chaque domaine dans lequel vous avez un certain pouvoir.

Affectations de groupe temporaire

Ce nœud vous permet de gérer les appartenances à un groupe pour les utilisateurs qui n'ont besoin d'appartenir au groupe que pour une période donnée.

Requêtes avancées

Permet de construire, d'enregistrer, d'importer, d'exporter, de copier et de gérer des requêtes LDAP et d'attributs virtuels, tant personnelles que publiques.

Corbeille

Ce nœud vous permet de gérer les comptes utilisateurs, les groupes, les contacts et les ressources supprimés pour tout domaine Microsoft Windows où la Corbeille est activée.

Pour accéder au nœud Gestion des comptes et des ressources, cliquez sur **Delegation and Configuration** (Délégation et configuration) dans le dossier du programme NetIQ Administrator et développez le nœud Délégation et configuration dans la console.

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

Pour de plus amples renseignements sur l'utilisation de la gestion des comptes et des ressources, consultez les rubriques suivantes :

Établir une connexion à un serveur d'administration ou à un domaine géré

Par défaut, DRA se connecte au meilleur serveur d'administration disponible pour un domaine ou un ordinateur géré. Le meilleur serveur d'administration disponible est le serveur le plus proche, qui est généralement un serveur du site réseau. S'il n'existe pas de serveur d'administration sur le site, DRA se connecte au prochain serveur disponible du domaine ou du sous-arbre géré. Vous pouvez également spécifier le serveur d'administration ou le domaine auquel vous souhaitez vous connecter.

Lorsque vous démarrez les interfaces utilisateur pour la première fois, DRA se connecte initialement 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 peut pas se connecter au serveur d'administration de ce domaine, DRA peut afficher un message d'erreur. Assurez-vous que le serveur d'administration est disponible et réessayez.

Pour établir une connexion à un serveur d'administration :

1. Dans le menu Fichier, cliquez sur **Connexion au serveur DRA**.
2. Cliquez sur **Connexion à ce serveur DRA**.
3. Saisissez le nom du serveur d'administration en utilisant le format suivant : *nomdel'ordinateur*.
4. Cliquez sur **OK**.

Pour établir une connexion à un domaine ou un ordinateur géré :

1. Dans le menu Fichier, cliquez sur **Connexion au serveur DRA**.
2. Sélectionnez l'option appropriée, puis tapez le nom du domaine ou de l'ordinateur géré.
3. Par exemple, pour établir une connexion avec le domaine HOULAB, cliquez sur **Établir une connexion avec le serveur DRA qui gère ce domaine**, puis tapez H0ULAB.
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**.

Modifier le titre de la console

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

Pour modifier la barre de titre de la console :

1. Démarrez la console de délégation et de configuration.
2. Cliquez sur **Afficher** > **Options**.
3. Sélectionnez l'onglet Titre de la fenêtre.
4. Spécifiez les options appropriées, puis cliquez sur **OK**.

Personnaliser les colonnes de la liste

Vous pouvez sélectionner les propriétés de l'objet que DRA affiche dans les colonnes de liste. Cette fonctionnalité flexible vous permet de personnaliser des éléments de l'interface utilisateur comme les listes de résultats de recherche, afin de mieux répondre à des exigences précises de l'administration de votre entreprise. Par exemple, vous pouvez définir des colonnes pour afficher le nom de connexion de l'utilisateur ou le type de groupe, vous permettant ainsi de rechercher et de trier rapidement et efficacement les données dont vous avez besoin.

Pour personnaliser les colonnes de la liste :

1. Sélectionnez le nœud approprié. Par exemple, pour choisir les colonnes qui s'affichent lors de l'affichage des résultats de recherche sur les objets gérés, sélectionnez **Tous mes objets gérés**.
2. Dans le menu Affichage, cliquez sur **Choisir les colonnes**.
3. Dans la liste des propriétés disponibles pour ce nœud, sélectionnez les propriétés de l'objet que vous voulez afficher.
4. Pour modifier l'ordre des colonnes, sélectionnez une colonne, puis cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
5. Pour spécifier la largeur de colonne, sélectionnez une colonne, puis tapez le nombre approprié de pixels dans le champ prévu à cet effet.
6. Cliquez sur **OK**.

Gérer les objets dans Gestion des comptes et des ressources

Pour gérer les objets dans Gestion des comptes et des ressources, sélectionnez **All My Managed Objects** (Tous mes objets gérés) ou un sous-nœud dans l'arborescence. À partir de là, vous pouvez rechercher les objets par type dans les domaines, les conteneurs et les UO.

Si vous sélectionnez un objet dans la liste des résultats de recherche, toutes les actions applicables que vous pouvez entreprendre sur cet objet sont disponibles dans le menu **Tasks** (Tâches) de la barre d'outils ou dans le menu contextuel (clic droit). Les options disponibles sont basées sur le type d'objet sélectionné, les composants actuellement configurés pour DRA et les privilèges d'administrateur qui vous ont été attribués.

Pour modifier les propriétés d'un objet, sélectionnez l'objet et cliquez sur **Properties** (Propriétés) dans le menu **Tasks** (Tâches). De là, vous pouvez accéder à toutes les pages des propriétés de l'objet en cliquant sur les liens des pages dans le volet de navigation sur la gauche.

IMPORTANT : Si vous souhaitez **protéger un objet contre une suppression accidentelle**, sélectionnez l'objet et ouvrez **Properties** (Propriétés), sélectionnez **General** (Général) dans le volet de navigation, cochez la case permettant d'activer cette fonction et **appliquez** les modifications.

Pour de plus amples renseignements sur les actions que vous pouvez entreprendre sur les objets, consultez les rubriques suivantes :

- Gérer des objets Active Directory
- Gérer les boîtes aux lettres Exchange et les dossiers publics
- Gérer les ressources

Exécuter des requêtes avancées enregistrées

À l'aide de requêtes avancées, vous pouvez rechercher des utilisateurs, des contacts, des groupes, des ordinateurs, des imprimantes, des unités d'organisation et tout autre objet pris en charge par DRA. Si vous êtes autorisé à exécuter des requêtes avancées enregistrées, vous pouvez exécuter des requêtes avancées disponibles dans la liste **Requêtes enregistrées** pour tout conteneur du nœud Account and Resource Management. Pour obtenir de plus amples renseignements sur les pouvoirs qui vous sont attribués, consultez la rubrique Afficher les pouvoirs et les rôles attribués.

Pour exécuter des requêtes avancées enregistrées :

1. Développez **Account and Resource Management** > **Tous mes objets gérés**.
2. Sélectionnez le conteneur approprié. Par exemple, si vous voulez que DRA recherche les informations de 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 **Charger la requête**, puis sur **Trouver maintenant**.

Restaurer les paramètres de la console

DRA vous permet de redimensionner les fenêtres et de conserver la taille de vos fenêtres. DRA permet également de conserver de nombreux autres paramètres, notamment le dernier serveur d'administration auquel vous vous connectez, les colonnes que vous ajoutez ou supprimez des résultats de la liste et la largeur des colonnes. Si vous voulez restaurer ces paramètres aux valeurs d'origine, c'est à dire ceux avec lesquels vous avez installé DRA, vous pouvez utiliser l'option Restaurer les paramètres par défaut.

Pour restaurer les paramètres par défaut de la console :

1. Cliquez sur **Afficher** > **Options**.
2. Sélectionnez l'onglet **Paramètres enregistrés**.
3. Vérifiez les informations fournies dans la fenêtre, puis cliquez sur **Restaurer les paramètres par défaut**.

Restrictions relatives aux caractères spéciaux

Vous ne pouvez pas utiliser les caractères spéciaux suivants lorsque vous nommez des comptes utilisateurs, des groupes, des contacts, des unités d'organisation, des ordinateurs, ActiveViews, des groupes d'administrateurs assistants, des rôles, des stratégies ou des déclencheurs d'automatisation. Ces restrictions sur les noms s'appliquent au nom de l'objet ainsi qu'au nom de la règle qui définit l'objet.

Attribuer un nom aux comptes utilisateurs, aux groupes et aux ordinateurs

Lorsque vous spécifiez un nom antérieur à Windows 2000, vous ne pouvez pas utiliser les caractères spéciaux suivants :

Barre oblique inverse	\
Deux-points	:
Virgule	,
Guillemet anglais	"
Signe Égal	=
Barre oblique	/
Signe Supérieur à	>
Crochet gauche	[
Signe Inférieur à	<
Signe Plus	+
Crochet droit	]
Point virgule	;
Barre verticale	|

IMPORTANT : Pour la gestion des dossiers publics, le caractère barre oblique inverse \ n'est pas pris en charge.

Lorsque vous attribuez des noms à des comptes utilisateurs, des groupes et des ordinateurs appartenant à des domaines Microsoft Windows, vous pouvez utiliser n'importe quel caractère spécial.

Attribuer un nom aux contacts et aux unités d'organisation

Lorsque vous attribuez un nom aux contacts et aux unités d'organisation, vous pouvez utiliser n'importe quel caractère spécial.

Attribuer un nom aux ActiveViews, aux groupes d'administrateurs assistants et aux rôles

Lorsque vous attribuez un nom aux ActiveViews, aux groupes d'administrateurs assistants et aux rôles, vous ne pouvez pas utiliser la barre oblique inverse (\).

Attribuer un nom aux stratégies et aux déclencheurs d'automatisation

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

Caractères invalides dans Azure

Si des caractères invalides sont utilisés, la synchronisation entre Azure Active Directory et votre répertoire d'entreprise échouera. Reportez-vous à la sous-rubrique « *Préparation des objets et attributs du répertoire* » sur le site Web d'assistance de Microsoft Office pour en savoir plus sur ces caractères invalides.

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

1. Cliquez sur le nœud Gestion de la configuration dans la console de délégation et de configuration, et sélectionnez **Update Administration Server Options** (Mettre à jour les options du serveur d'administration).
2. Cliquez sur **Azure Sync** (Synchronisation Azure) dans le menu de l'onglet.
3. Cliquez sur **Enforce online mailbox policies for invalid characters and character length** (Appliquer les règles de boîte aux lettres en ligne pour les caractères invalides et la longueur des caractères), puis sur **OK**.

Utiliser les caractères jokers

DRA prend en charge les caractères jokers dans de nombreux champs des consoles DRA et des commandes CLI. Les caractères jokers vous permettent de définir des règles qui font correspondre plusieurs objets à une condition ou à une norme précise telle qu'une convention d'attribution de nom. Vous pouvez utiliser des caractères jokers au lieu d'expressions régulières pour réduire ou élargir l'étendue de la règle. Les caractères jokers ne sont pas sensibles à la casse. Vous pouvez également utiliser les caractères jokers point d'interrogation (?), astérisque (*) ou croisillon (#)

comme caractères normaux en insérant comme préfixe devant le caractère générique en question une barre oblique inversée (\). Par exemple, pour rechercher abc*, saisissez comme texte de recherche abc*.

DRA prend en charge les caractères jokers ci-dessous. Vous ne pouvez pas utiliser de caractères jokers dans les noms.

Élément correspondant	Caractère	Définition
N'importe quel caractère	Point d'interrogation ?	Correspond exactement à un caractère
N'importe quel chiffre	Croisillon #	Correspond à un chiffre
N'importe quel caractère, 0 ou plus de correspondance	Astérisque *	Correspond à zéro caractère ou plus

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

Exemple	Correspond	Ne correspond pas
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 caractère joker contenant des opérations logiques.

Afficher les pouvoirs et les rôles attribués

Les rôles et les pouvoirs définissent la façon dont vous gérez les objets. Un rôle est un ensemble de pouvoirs qui fournit les autorisations requises pour effectuer une tâche d'administration précise, comme la création d'un compte utilisateur ou le déplacement de répertoires partagés.

L'administrateur DRA attribue des rôles, vous ajoute à des groupes d'administrateurs assistants précis et vous associe à des ActiveViews (ensembles d'objets de domaine que vous pouvez gérer). Vous pouvez afficher ces attributions à partir de la console de gestion des comptes et des ressources. Vous n'avez pas besoin de pouvoirs auxiliaires pour afficher les rôles et les pouvoirs qui vous sont attribués.

Pour afficher les rôles et pouvoirs qui vous sont attribués :

1. Dans le menu Fichier, cliquez sur **Propriétés de DRA**.
2. Cliquez sur **Pouvoirs**.
3. Sélectionnez l'affichage approprié. Par exemple, cliquez sur **Affichage en 2D** pour afficher un tableau des membres de votre groupe d'administrateurs assistants, des pouvoirs et des rôles qui vous sont attribués et des ActiveViews associées.
4. Développez l'élément souhaité. Par exemple, dans la colonne **Pouvoir**, développez **Rôles et pouvoirs** pour afficher les rôles ou les pouvoirs individuels qui vous sont attribués.
5. Cliquez sur **OK**.

Afficher le numéro de version du produit et les correctifs installés

Vous pouvez afficher le numéro de version du produit et les correctifs installés à partir de la fenêtre Propriétés de DRA. Cette fenêtre fournit les numéros de version et les listes des correctifs installés pour le serveur d'administration et l'ordinateur client de DRA.

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

1. Dans le menu Fichier, cliquez sur **Propriétés de DRA**.
2. Cliquez sur **Général**.
3. Affichez les informations dont vous avez besoin.
4. Cliquez sur **OK**.

Afficher la licence actuelle

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

Pour afficher votre licence :

1. Dans le menu Fichier, cliquez sur **Propriétés de DRA**.
2. Cliquez sur **Licence**.
3. Vérifiez les propriétés de la licence, puis cliquez sur **OK**.

Récupérer un mot de passe BitLocker

Microsoft BitLocker stocke ses mots de passe de récupération dans Active Directory. Avec les pouvoirs nécessaires, vous pouvez utiliser la fonctionnalité DRA BitLocker Recovery pour rechercher et récupérer les mots de passe BitLocker perdus pour les utilisateurs finaux.

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

Afficher et copier un mot de passe de récupération BitLocker

Si le mot de passe BitLocker d'un ordinateur est perdu, il peut être réinitialisé en utilisant la clé de récupération du mot de passe depuis les propriétés de l'ordinateur dans Active Directory. Copiez la clé du mot de passe et fournissez-la à l'utilisateur final.

Pour afficher et copier le mot de passe de récupération :

1. Lancez la console de délégation et de configuration et accédez à **Account and Resource Management** > **All My Managed Objects** (Gestion des comptes et des ressources > Tous mes objets gérés).
2. Sélectionnez le domaine et effectuez une recherche pour obtenir la liste de tous les ordinateurs du domaine.

3 Dans la liste des ordinateurs, cliquez avec le bouton droit de la souris sur l'ordinateur approprié, puis sélectionnez **Properties** > **BitLocker Recovery Password** (Propriétés > Mot de passe de récupération BitLocker.

4 Cliquez avec le bouton droit de la souris sur le mot de passe de récupération BitLocker et copiez-le; collez ensuite le texte du mot de passe dans un fichier texte.

Trouver un mot de passe de récupération

Si le nom d'un ordinateur a été modifié, le mot de passe de récupération doit être recherché dans le domaine en utilisant les huit premiers caractères de l'ID de mot de passe.

Pour trouver un mot de passe de récupération en utilisant un identifiant de mot de passe :

1 Lancez la console de délégation et de configuration et accédez à **Account and Resource Management** > **All My Managed Objects** (Gestion des comptes et des ressources > Tous mes objets gérés).

2 Cliquez avec le bouton droit de la souris sur **Domaine géré**, puis sur **Trouver le mot de passe de récupération BitLocker**.

Pour trouver les huit premiers caractères du mot de passe de récupération, consultez la rubrique Afficher et copier un mot de passe de récupération BitLocker.

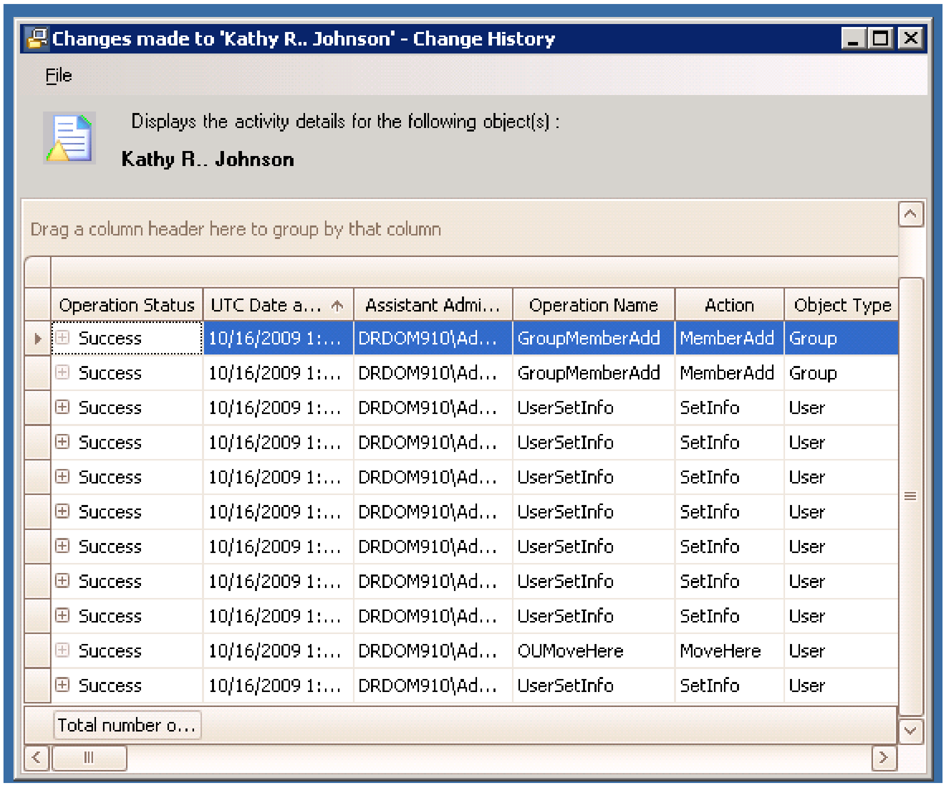
3 Dans la page **Trouver le mot de passe de récupération BitLocker**, collez les caractères copiés dans le champ de recherche, puis cliquez sur **Rechercher**.

DRA Reporting

DRA Reporting fournit des rapports intégrés et prêts à l'emploi qui vous permettent de suivre rapidement les comptes en double, les dernières connexions de compte, les détails des boîtes aux lettres Microsoft Exchange et bien plus encore. DRA Reporting fournit également des détails en temps réel sur les modifications apportées dans votre environnement, y compris les valeurs avant et après des propriétés modifiées. Vous pouvez exporter, imprimer ou afficher des rapports ou les publier dans SQL Server Reporting Services.

DRA offre deux méthodes de génération de rapports qui vous permettent de collecter et d'examiner les définitions de compte d'utilisateur, de groupe et de ressource dans votre domaine.**Rapports détaillés d'activité** et **Rapports de gestion de DRA**. Les rapports détaillés d'activité, visualisés à l'aide de la console de délégation et de configuration, fournissent des informations en temps réel sur les modifications apportées aux objets dans votre domaine. Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'une période donnée à l'aide des rapports détaillés d'activité.

La figure suivante montre un exemple de rapport détaillé d'activité :



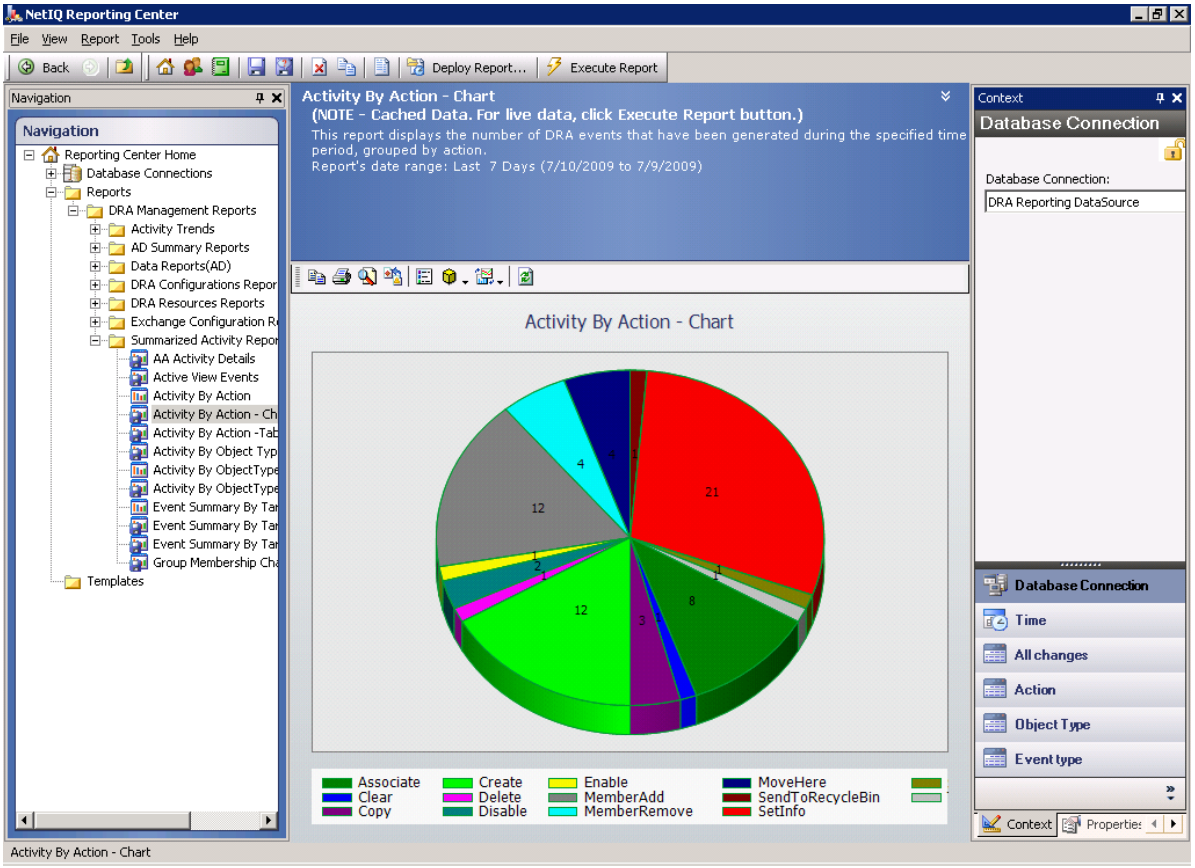
Les **rapports de gestion de DRA** facultatifs, visualisés en utilisant NetIQ Reporting Center (Reporting Center), fournissent des informations sur l'activité, la configuration et le résumé des événements dans vos domaines gérés. Certains rapports de gestion sont disponibles sous forme de représentations graphiques des données. Ces rapports intégrés peuvent également être personnalisés pour vous donner exactement les informations dont vous avez besoin.

Par exemple, vous pouvez afficher un graphique indiquant le nombre d'événements dans chaque domaine géré au cours d'une période précise à l'aide des rapports de gestion. La création de rapports vous permet d'afficher des détails sur le modèle de sécurité DRA tels que les définitions de groupes ActiveView et Administrateurs assistants.

Vous devez installer et configurer les rapports de gestion facultatifs avant de pouvoir afficher ces rapports. Pour obtenir de plus amples renseignements sur l'installation des composants de création de rapports, consultez le *Guide d'installation*. Pour obtenir de plus amples renseignements sur le module de création de rapport de DRA, consultez « DRA Reporting » page 30.

Démarrez la console de Reporting Center en accédant à NetIQ, puis au groupe de programmes de Reporting Center.

La figure suivante montre l'interface de Reporting Center avec les rapports de gestion de DRA sélectionnés.



Pour de plus amples renseignements sur les rapports de DRA, consultez les rubriques suivantes :

- « Comprendre la création de rapports dans DRA » page 32
- « Utilisation des archives de journaux par DRA » page 33
- « Comprendre les dates et les heures » page 34
- « Tâches de DRA Reporting » page 34

Comprendre la création de rapports dans DRA

DRA Reporting utilise deux méthodes de création de rapports vous permettant de visualiser les dernières modifications apportées à votre environnement ainsi que de collecter et d'examiner les définitions de compte utilisateur, de groupe et de ressource de votre domaine.

Rapports détaillés d'activité

Accessibles par la console de gestion des comptes et des ressources et 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 de DRA

Accessibles à l'aide de NetIQ Reporting Center (Reporting Center), ces rapports fournissent des informations sur l'activité, la configuration et la synthèse des événements survenus dans vos domaines gérés. Certains rapports sont disponibles sous forme de représentations graphiques des données.

Par exemple, vous pouvez afficher une liste des modifications apportées à un objet ou par un objet au cours d'une période donnée à l'aide des rapports détaillés d'activité. Vous pouvez également afficher un graphique indiquant le nombre d'événements dans chaque domaine géré au cours d'une période précise à l'aide des rapports de gestion. La création de rapports vous permet également d'afficher des détails sur le modèle de sécurité DRA tels que les définitions de groupes ActiveView et Administrateurs assistants.

DRA désactive les fonctions et les rapports que votre licence ne prend pas en charge. Vous devez également disposer des pouvoirs appropriés pour exécuter et afficher les rapports. Par conséquent, vous pouvez ne pas avoir accès à certains rapports.

Les rapports de gestion de DRA peuvent être installés et configurés en tant que fonctionnalité facultative et sont affichés dans Reporting Center. Lorsque vous activez et configurez la collecte de données, DRA collecte des informations sur les événements audités et les exporte vers une base de données SQL Server selon une planification que vous définissez. Lorsque vous vous connectez à cette base de données dans Reporting Center, vous avez accès à plus de 60 rapports intégrés :

- Rapports d'activité indiquant l'auteur et le moment de chaque événement
- Rapports de configuration indiquant l'état d'AD ou de DRA à un moment donné
- Rapports de synthèse indiquant le volume d'activité

Pour obtenir de plus amples renseignements sur la configuration de la collecte de données pour les rapports de gestion, consultez le *Guide de l'administrateur*.

Utilisation des archives de journaux par DRA

Afin de permettre la vérification et la création de rapport sur les actions de l'administrateur assistant, DRA enregistre toutes les opérations de l'utilisateur dans l'archive des journaux sur l'ordinateur du serveur d'administration. Les opérations utilisateur incluent toutes les tentatives de modification de définitions telles que la mise à jour de comptes d'utilisateurs, la suppression de groupes ou la redéfinition d'ActiveViews. DRA enregistre également des opérations internes précises telles que l'initialisation du serveur d'administration et les informations relatives au serveur. En plus de la journalisation de ces événements d'audit, DRA enregistre les valeurs avant et après de l'événement, afin que vous puissiez voir exactement ce qui a changé.

DRA utilise un dossier, **NetIQLogArchiveData**, appelé **archive de journal** pour stocker en toute sécurité les données archivées. DRA archive les journaux au fil du temps et supprime ensuite les données plus anciennes pour faire de la place aux données plus récentes par un processus appelé nettoyage.

DRA utilise les événements d'audit stockés dans les fichiers d'archive de journal pour afficher les rapports d'activité détaillés tels que les modifications apportées à un objet au cours d'une période spécifiée. Vous pouvez également configurer DRA pour exporter les informations de ces fichiers d'archivage de journaux vers une base de données SQL Server utilisée par NetIQ Reporting Center pour afficher les rapports de gestion.

DRA consigne toujours des événements d'audit dans l'archive de journal. Vous pouvez également activer ou désactiver la consignation d'événements par DRA dans les journaux d'événements Windows.

Pour obtenir de plus amples renseignements sur l'audit DRA, consultez le *Guide de l'administrateur*.

Comprendre les dates et les heures

DRA utilise les styles de **date courte** et d'**heure** spécifiés dans l'application Paramètres régionaux du Panneau de configuration pour l'affichage du rapport. Les rapports DRA indiquent la date et l'heure UTC ainsi que la date et l'heure locales pour les 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 DRA Reporting

Pour générer des rapports de gestion de DRA, installez Reporting Center et activez la collecte de données dans DRA. Pour de plus amples renseignements sur l'activation de la collecte de données, consultez le *Guide de l'administrateur*. Pour générer des rapports détaillés d'activité, cliquez avec le bouton droit de la souris sur n'importe quel objet et cliquez sur **Création de rapport(s)** pour afficher vos choix en matière de rapports sur cet objet. Les sections suivantes vous présentent les différentes tâches de création de rapports.

Afficher les rapports détaillés d'activité

Les rapports d'activité détaillés affichent des informations sur les changements dans votre environnement. Vous pouvez afficher ou imprimer un rapport; vous pouvez également enregistrer un rapport au format Excel, CSV ou TXT. Pour afficher ou imprimer des rapports, vous devez être associé au rôle d'administration de création de rapports.

Lors de l'affichage des rapports, saisissez des critères pour spécifier la période sur laquelle vous souhaitez afficher les informations. Vous pouvez également choisir d'afficher un rapport limité aux modifications apportées sur des serveurs DRA précis ou de limiter le nombre de lignes à inclure dans le rapport. Si la taille du rapport dépasse l'une des limites suivantes, DRA affiche un message indiquant que le rapport n'est pas complet :

- Taille supérieure à 500 Mo
- Temps nécessaire pour interroger tous les serveurs DRA supérieur à 5 minutes
- Nombre de lignes à afficher supérieur à 1000

Vous avez la possibilité d'afficher le rapport contenant uniquement les informations récupérées avant d'atteindre l'une de ces limites ou de modifier les critères du rapport pour afficher un rapport qui respecte 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 contenant cet objet.
   - 2b Dans le volet de recherche, spécifiez les attributs de l'objet, puis cliquez sur **Rechercher maintenant**.
3. Dans le volet de liste, cliquez avec le bouton droit de la souris sur l'objet, puis cliquez sur **Création de rapport(s)**.
4. Sélectionnez le type de rapport tel que **Modifications apportées à NomObjet** ou **Modifications apportées par NomObjet**. Les rapports disponibles varient en fonction du type d'objet sélectionné.
5. Sélectionnez les dates de début et de fin pour spécifier les modifications à afficher.
6. ***Si vous souhaitez modifier le nombre de lignes à afficher***, entrez un nombre supérieur à la valeur par défaut de 250.

   REMARQUE : Le nombre de lignes affichées s'applique à chaque serveur d'administration de votre environnement. Si vous incluez 3 serveurs d'administration dans le rapport et utilisez la valeur par défaut de 250 lignes à afficher, vous pouvez afficher jusqu'à 750 lignes dans le rapport.

   ---

7. ***Si vous voulez inclure uniquement des serveurs d'administration précis dans le rapport***, sélectionnez **Restreindre la requête à ces serveurs DRA** et saisissez le ou les noms de serveur que vous voulez inclure dans le rapport. Séparez plusieurs noms de serveur par des virgules.
8. Cliquez sur **OK**.

REMARQUE : Cela peut prendre jusqu'à 5 secondes pour que DRA affiche les dernières modifications apportées aux rapports. Par conséquent, attendez au moins 5 secondes après avoir apporté une modification avant d'essayer d'afficher un rapport contenant la modification.

Exporter les rapports détaillés d'activité

Vous pouvez exporter des rapports d'activité détaillés aux formats suivants : XLS, CSV et TXT. Le format par défaut est le format Microsoft Excel.

Pour exporter des rapports d'activité détaillés, procédez comme suit :

1. Dans la fenêtre du rapport, dans le menu Fichier, cliquez sur **Aperçu et exportation**.
2. Dans la fenêtre Aperçu, dans le menu Fichier, cliquez sur **Exporter le document** > **Fichier Excel**.
3. Sélectionnez vos options d'exportation et cliquez sur **OK**.
4. Dans la fenêtre Enregistrer sous, tapez un nom pour le fichier et cliquez sur **Enregistrer**.

Imprimer les rapports détaillés d'activité

Pour imprimer ou imprimer des rapports, vous devez être associé au rôle d'administration de création de rapports. Vous pouvez afficher ou imprimer des rapports détaillés d'activité, ainsi que les enregistrer dans différents formats.

Pour imprimer des rapports d'activité détaillés, procédez comme suit :

1. Dans la fenêtre du rapport, dans le menu Fichier, cliquez sur **Aperçu et exportation**.
2. Dans la fenêtre Aperçu, dans le menu Fichier, cliquez sur **Imprimer**.

Afficher les rapports de gestion

Vous devez installer DRA Reporting et configurer les collecteurs de données DRA pour pouvoir visualiser les rapports de gestion dans Reporting Center. Pour de plus amples renseignements sur l'installation de DRA Reporting et la configuration des collecteurs DRA, consultez le *Guide de l'administrateur*.

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

Pour afficher les rapports de gestion, procédez comme suit :

1. Connectez-vous à l'ordinateur qui exécute la console de Reporting Center.
2. Démarrez la console de **Reporting Center** en accédant à NetIQ, puis au groupe de programmes de Reporting Center.
3. Fournissez les informations requises dans la boîte de dialogue Connexion et cliquez sur **Connexion**.
4. Dans le volet de navigation, développez **Rapports** > **Rapports de gestion de DRA**.
5. Développez les catégories de rapport jusqu'à ce que vous trouviez un rapport à afficher.

6 Cliquez sur le nom du rapport dans le volet de navigation et le rapport sera chargé dans le volet de résultats situé au milieu, affichant les données mises en cache.

7 ***Si vous souhaitez que le rapport utilise les données les plus récentes,*** cliquez sur **Exécuter le rapport** dans le volet de résultats.

Vous pouvez modifier les paramètres de contexte par défaut pour afficher différents résultats de rapport. Pour obtenir de plus amples renseignements sur les paramètres de contexte dans Reporting Center, consultez le *Guide de l'administrateur*.

Personnaliser les rapports de gestion

Plus de 60 rapports de gestion sont inclus dans DRA. Reporting Center vous offre la flexibilité de personnaliser et de déployer ces rapports de plusieurs façons. Pour obtenir de plus amples renseignements sur la personnalisation et le déploiement des rapports de gestion dans Reporting Center, consultez le *Guide de l'administrateur*.

Pour personnaliser un rapport de gestion, procédez comme suit :

1 Affichez un rapport semblable à celui que vous voulez créer. Pour obtenir de plus amples renseignements, consultez Afficher les rapports de gestion.

2 Personnalisez le rapport en modifiant les propriétés du rapport et les paramètres de contexte pour afficher les informations que vous souhaitez.

3 Cliquez sur **Exécuter le rapport**.

4 Dans le menu Rapport, cliquez sur **Enregistrer le rapport sous** et spécifiez un titre ainsi qu'un emplacement pour enregistrer le nouveau rapport.

5 Cliquez sur **Enregistrer**.

Pour obtenir de plus amples renseignements sur l'utilisation des rapports de gestion dans Reporting Center, consultez le *Guide de l'administrateur*.

3 Rechercher des objets

Ce chapitre contient des informations conceptuelles et procédurales sur les fonctionnalités de recherche et de recherche LDAP.

Recherche

DRA vous permet de rechercher des objets dans les domaines Active Directory sur site, Microsoft Exchange et les locataires Azure. Vous pouvez rechercher des utilisateurs, 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 géré de groupe dans vos domaines Active Directory, et des objets tels que des boîtes aux lettres de salle, des boîtes aux lettres d'équipement, des boîtes aux lettres partagées et des groupes de distribution dynamique dans Exchange. Vous pouvez utiliser les filtres de recherche pour des recherches plus efficaces. DRA tronque automatiquement les espaces de début ou de fin de votre saisie de recherche et renvoie les résultats de la recherche.

Pour accéder à la fonction de recherche dans la console Web, accédez à **Management** > **Search** (Gestion > Recherche). Pour exécuter une recherche, sélectionnez un ou plusieurs filtres, sélectionnez une option Rechercher par, entrez un terme de recherche et cliquez sur **Rechercher**.

Par exemple, la recherche exécutée ci-dessous renvoie tous les utilisateurs du domaine ou du conteneur sélectionné dont le nom de famille est « Beck » ou dont le nom de famille se termine par ces quatre lettres.

Rechercher par	Terme de recherche saisi	Filtre sélectionné
• Nom • se termine par	beck	Utilisateur

REMARQUE : Pour obtenir un retour précis des objets recherchés lors de l'utilisation des filtres, toute modification apportée à la pagination doit être effectuée avant d'appliquer les filtres et d'exécuter la recherche. La modification du paramètre **items per page** (éléments par page) au bas de la console Web lorsque des filtres de type d'objet sont appliqués n'est pas prise en charge.

Pour accéder à la fonction de recherche dans la console de délégation et de configuration, naviguez vers Gestion des comptes et des ressources et cliquez sur **Comptes et ressources** dans le volet de visualisation.

- « Ajouter et trier des colonnes » page 41
- « Exporter les résultats de la recherche » page 42

Utiliser des caractères jokers

DRA prend en charge les caractères jokers tels que le point d'interrogation (?), l'astérisque (*) ou le croisillon (#) pour maximiser les résultats de votre recherche. Les caractères jokers ne sont pas sensibles à la casse.

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

Caractère	Élément correspondant
Point d'interrogation ?	Un caractère ou un chiffre
Croisillon #	Un chiffre
Astérisque *	Un nombre quelconque de caractères ou de chiffres

Recherche multichamps

L'option Correspondance multichamps vous permet de rechercher des correspondances avec plusieurs attributs en une seule recherche. Lorsque vous effectuez une recherche par correspondance multichamps, votre chaîne de recherche est comparée à plusieurs attributs tels que le nom, le nom affiché, le prénom et le nom de famille et si la chaîne de recherche correspond à l'un de ces attributs, l'objet est renvoyé dans les résultats de la recherche.

L'option de correspondance multichamps prend uniquement en charge les critères de recherche **"begins with"** (« Commence par »).

Par exemple, si vous avez deux utilisateurs, l'un dont le *nom affiché* est « `Martin Smith` » et l'autre dont le nom d'utilisateur principal est `martha.jones@acme.com`, et si vous effectuez une recherche en utilisant la chaîne « `Mart` », les deux utilisateurs seront renvoyés dans les résultats de la recherche.

Le tableau ci-dessous énumère les attributs qui sont 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

Type d'objet	Attributs recherchés
Groupe	displayName, mail, mailNickname, name, sAMAccountName
Compte de services gérés de groupe	displayName, name, sAMAccountName
Unité organisationnelle	name
Corbeille	name, sAMAccountName
Utilisateur	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

REMARQUE : La fonction de correspondance multiple n'est pas prise en charge dans les recherches du sélecteur d'objets dans la console de délégation et de configuration lorsque vous ajoutez des délégués ou des autorisations pour les objets d'échange énumérés ci-dessous :

- boîte aux lettres de l'utilisateur
- utilisateur à extension messagerie
- groupe à extension messagerie
- contact à extension messagerie
- groupe de distribution dynamique
- boîtes aux lettres partagées
- boîte aux lettres de ressource

Ajouter et trier des colonnes

Vous pouvez trier les objets du résultat de la recherche selon l'un des attributs suivants lorsque vous cliquez sur l'en-tête de colonne d'un attribut :

- Alias
- Nom affiché
- Courriel
- ID d'employé
- Prénom
- Nom
- Emplacement
- Nom
- Nom antérieur à Windows 2000
- Nom d'utilisateur principal

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

Exporter les résultats de la recherche

DRA permet aux administrateurs assistants d'exporter les résultats de la **recherche** dans la console Web vers un fichier CSV. Pour exporter les résultats de la **recherche** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur l'icône **Télécharger**.

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

Recherche avancée

DRA vous permet d'effectuer des requêtes LDAP et d'attributs virtuels dans vos domaines Active Directory sur site à partir de la page Recherche avancée. Vous pouvez effectuer une recherche à l'aide d'une requête existante, modifier une requête existante, créer une nouvelle requête et enregistrer de nouvelles requêtes et des requêtes modifiées pour une utilisation future en tant que requêtes publiques ou privées. Utilisez les filtres de recherche pour des recherches plus efficaces.

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

Pour accéder aux requêtes de recherche avancée dans la console de délégation et de configuration, sélectionnez le domaine, le locataire Azure ou le sous-nœud sous Gestion des comptes et des ressources, puis cliquez sur **Recherche avancée** dans la barre d'outils.

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 les utilisateurs, les groupes, les groupes de distribution dynamique, les contacts, les ordinateurs et les UO. Avec une requête d'attribut virtuel, vous pouvez filtrer les résultats renvoyés par la requête LDAP pour ne renvoyer que les résultats qui correspondent à la requête d'attribut virtuel. Les chaînes de requête d'attributs virtuels doivent commencer par `(objectCategory=<object type>)`. Pour effectuer une requête d'attribut virtuel, vous devez spécifier des chaînes de caractères pour les requêtes LDAP et les requêtes d'attribut virtuel.

Exemples de requêtes LDAP :

- Pour rechercher « all computer objects » (tous les objets ordinateurs) dans DRA :

  Requête LDAP : `(objectCategory=computer)`
- Pour rechercher des objets utilisateurs ayant la description « East\West Sales » (Ventes à l'Est et à l'Ouest) dans DRA :

  Requête LDAP : `(&(objectCategory=user)(description=East\5CWest Sales))`
- Pour rechercher « all computer objects » (tous les objets ordinateurs) dans DRA :

  Requête LDAP : `(objectCategory=computer)`

IMPORTANT : Le caractère barre oblique inverse doit être échappé dans les filtres LDAP. Remplacer par \5C.

- Pour dresser la liste « list all disabled user objects » (répertorier 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`indique LDAP_MATCHING_RULE_BIT_AND. Elle spécifie un ET au niveau du bit d'un attribut d'indicateur (un entier), tel que userAccountControl, groupType ou systemFlags, et un masque de bits (par exemple 2, 32 ou 65536). La clause est Vrai si le ET au niveau du bit de la valeur d'attribut et le masque de bit est différent de zéro, indiquant que le bit est défini.

Exemples de requêtes d'attributs virtuels :

- Pour trouver tous les utilisateurs dont le nom de l'entreprise est ABC :

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

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

- Pour trouver tous les utilisateurs ayant comme nom d'entreprise ABC dans le domaine du stockage :

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

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

- Pour trouver tous les groupes dont le nom de produit est DRA ou tous les utilisateurs dont le nom de l'entreprise est ABC :

  Requête :

  ```
  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=Use
  r)(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 trouver tous les groupes dont le nom de produit est DRA ou tous les utilisateurs dont le nom de l'entreprise est ABC dans le domaine du stockage :

  Requête :

  ```
  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=Use
  r)(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).

Gérer les requêtes avancées

DRA utilise LDAP pour prendre en charge les requêtes de recherches avancées. À l'aide des requêtes avancées, vous pouvez rechercher des utilisateurs, des contacts, des groupes, des ordinateurs, des unités organisationnelles et tout autre objet pris en charge par DRA. Si vous disposez du pouvoir d'exécuter des requêtes avancées enregistrées, vous pouvez exécuter des requêtes avancées qui sont disponibles dans les listes **My Searches** (Mes recherches) et **Public Searches** (Recherches publiques) pour tout conteneur.

Outre l'exécution d'une recherche avec une requête avancée enregistrée et la visualisation de ses détails, avec les autorisations applicables, vous pouvez également effectuer les opérations suivantes avec des requêtes avancées à partir de la page Recherche avancée :

Créer une nouvelle requête

Créez une requête avancée sur le serveur d'administration primaire ou sur le serveur d'administration 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 Mes recherches ou la liste Recherches publiques.

Modifier une requête

Sélectionnez une requête avancée existante sous Mes recherches ou Recherches publiques et utilisez l'option **Modify** (Modifier) pour modifier l'un des critères de recherche. Une fois que vous avez 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 existante sous Mes recherches ou Recherches publiques et exécutez la recherche. Après avoir exécuté la recherche, vous pouvez développer le menu déroulant **Search** (Rechercher) et sélectionner **Save As** (Enregistrer sous) pour enregistrer la requête avec un nom différent.

Personnaliser les résultats d'une requête

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

Supprimer une requête

Vous pouvez supprimer toute requête avancée qui se trouve dans la liste **My Searches** (Mes recherches). Avec les autorisations applicables, vous pouvez également supprimer les requêtes avancées dans la liste **Public Searches** (Recherches publiques). Pour supprimer une requête avancée enregistrée, sélectionnez-la dans la liste applicable et cliquez sur **Delete** (Supprimer) dans le menu déroulant Recherche.

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 propre. Pour effacer les champs d'une requête, sélectionnez **Clear** (Effacer) dans le menu déroulant Recherche.

Exporter les résultats de la recherche avancée

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

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

---

4 Gérer des objets Active Directory

Ce chapitre contient des informations conceptuelles et procédurales pour la gestion des comptes d'utilisateurs, des groupes, des groupes dynamiques, des groupes de distribution dynamiques et des contacts dans dans le nœud Gestion des comptes et des ressources de la console de délégation et de configuration et dans la console Web. Les informations relatives aux comptes utilisateurs sont plus complètes pour fournir un exemple de la façon dont vous gérez les objets en général dans les deux applications client.

Gérer les comptes utilisateurs

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

Compte utilisateur global

Un compte utilisateur qui peut être utilisé dans n'importe quel domaine qui fait confiance au domaine dans lequel le compte utilisateur a été créé. Vous pouvez accorder des autorisations précises à un compte utilisateur. Vous pouvez également faire d'un compte utilisateur un membre d'un groupe, puis lui attribuer des autorisations. Le regroupement des comptes utilisateurs permet de simplifier le processus de gestion des autorisations réseau pour de nombreux comptes utilisateurs.

Compte utilisateur local

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

Pour en savoir plus sur la gestion des comptes d'utilisateur, consultez les rubriques suivantes :

Comptes utilisateurs dans des domaines approuvés

Microsoft Windows stocke les définitions des comptes utilisateurs et des groupes dans le répertoire du domaine géré. Par conséquent, un serveur d'administration ne peut pas modifier les informations de répertoire d'un domaine approuvé, à moins que ce domaine ne soit également géré par DRA.

Par exemple, dans Gestion des comptes et des ressources, vous pouvez voir les comptes et les groupes d'utilisateurs que vous ne pouvez pas modifier. Ces comptes et ces groupes d'utilisateurs sont définis dans des domaines approuvés par l'un des domaines gérés. Cependant, vous pouvez ajouter des comptes et des groupes d'un domaine approuvé à d'autres groupes dans le domaine géré.

Tâches de gestion des comptes d'utilisateurs

Cette section vous explique comment administrer les comptes d'utilisateurs dans la console de gestion des comptes et des ressources et dans la console Web. Si vous disposez des pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion des comptes utilisateurs telles que la création et la suppression de comptes. Si vous sélectionnez plusieurs comptes utilisateurs, vous pouvez exécuter les tâches sélectionnées en une seule opération telles que supprimer, déplacer ou ajouter des utilisateurs à un groupe. Pour obtenir de plus amples renseignements sur les pouvoirs qui vous sont attribués, consultez la rubrique Afficher les pouvoirs et les rôles attribués.

Tâches du compte d'utilisateur dans 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, sélectionnez le nœud **Tous mes objets gérés** et exécutez une opération **Trouver maintenant** pour localiser et sélectionner l'objet utilisateur souhaité. Le menu Tâches indique les tâches que vous pouvez effectuer lorsque vous sélectionnez un ou plusieurs comptes utilisateurs. Plus d'options seront disponibles pour un seul utilisateur.

Dans le cas de la création d'un nouvel utilisateur, vous devez sélectionner le domaine ou l'unité organisationnelle dans lequel vous souhaitez créer l'utilisateur. Par exemple :

1. Sélectionnez le conteneur **Users** (Utilisateurs) dans un domaine sous All My Managed Objects (Tous mes objets gérés).
2. Sélectionnez **Nouveau** > **Utilisateur** dans le menu Tâches.
3. Effectuez les étapes de l'assistant de création d'utilisateur.

Gérez votre propre compte

Vous pouvez gérer votre propre compte en modifiant les propriétés générales telles que votre numéro de téléphone. Avant de gérer votre compte, assurez-vous de disposer des pouvoirs appropriés.

Copier un compte utilisateur sur un autre ActiveView

Vous pouvez copier un compte utilisateur sur un autre ActiveView. Cette action s'appelle Transférer un compte utilisateur. Pour copier un compte utilisateur vers un autre ActiveView, vous devez disposer du pouvoir Copier l'utilisateur vers un autre ActiveView à la fois dans l'ActiveViews source et cible. Le transfert d'un compte utilisateur vers un autre ActiveView ne supprime pas le compte utilisateur de l'ActiveView source.

REMARQUE : La copie d'un compte d'utilisateur vers un autre ActiveView ne peut se faire qu'à partir de la console de délégation et de configuration au moyen du nœud Gestion des comptes et des ressources.

Renommer un compte utilisateur

Vous pouvez renommer des comptes utilisateurs dans le domaine géré ou 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 de compte utilisateur dans la console Web

Vous pouvez exécuter la plupart des tâches ci-dessous à partir de l'onglet **Gestion** > **Recherche** de la console Web. Exécutez une opération de recherche pour localiser et sélectionner l'objet utilisateur nécessaire. Après avoir sélectionné un ou plusieurs objets dans la liste, la barre de tâches devient active avec des options de barre d'outils et des options de liste déroulante pour **Accounts** (Comptes) et **Exchange**. Passez la souris sur une icône de la barre d'outils ou cliquez sur un menu déroulant pour afficher leurs fonctions ou options.

Créer un compte utilisateur

Vous pouvez créer des comptes utilisateurs dans le domaine géré ou la sous-arborescence gérée. Vous pouvez également modifier les propriétés, créer une boîte aux lettres, activer le courriel et spécifier les appartenances à un groupe pour le nouveau compte.

REMARQUE

- Votre entreprise peut avoir une convention de nommage appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez attribuer au nouveau compte utilisateur.
- Par défaut, DRA place le nouveau compte utilisateur dans l'unité organisationnelle Utilisateurs du domaine géré.
- Vous ne pouvez pas créer d'objets InetOrgPerson dans DRA.

Cloner un compte utilisateur

Lorsque vous clonez un compte utilisateur, tous les groupes dont l'utilisateur est membre sont automatiquement ajoutés au nouveau compte utilisateur, ce qui vous permet de gagner du temps lors de la configuration du nouveau compte. Vous pouvez ajouter ou supprimer des groupes du nouveau compte, activer le courriel et définir toute autre configuration de propriété, comme vous le feriez pour tout nouveau compte.

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

Modifier les propriétés du compte utilisateur

Vous pouvez gérer les propriétés des comptes utilisateurs dans le domaine géré ou la sous-arborescence gérée. Les pouvoirs dont vous disposez 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 utilisateurs.

REMARQUE : Si les stratégies de répertoire de base sont activées, DRA modifie automatiquement le répertoire de base d'un compte utilisateur lorsque vous gérez ce compte. Par exemple, lorsque vous modifiez l'emplacement du répertoire de base, DRA tente de créer le répertoire de base spécifié et de déplacer le contenu du répertoire de base précédent vers le nouvel emplacement. DRA applique également les listes de contrôle d'accès affectées du répertoire précédent au nouveau répertoire.

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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.

Activer un compte utilisateur

Vous pouvez activer un compte utilisateur dans le domaine géré ou 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 précis, DRA applique également cette modification au contrôleur de domaine par défaut de ce domaine géré. Pour vérifier quel contrôleur de domaine par défaut est utilisé par DRA, consultez les propriétés du domaine.

Désactiver 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 précis, DRA applique également cette modification au contrôleur de domaine par défaut de ce domaine géré. Pour vérifier quel contrôleur de domaine par défaut est utilisé par DRA, consultez les propriétés du domaine.

Déverrouiller un compte utilisateur

Vous pouvez déverrouiller un compte utilisateur dans le domaine géré ou 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 que celui-ci est réellement 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 lors du déverrouillage d'un compte utilisateur à l'aide de la console DRA sans avoir à réinitialiser le mot de passe du compte utilisateur.

Réinitialiser un mot de passe de compte utilisateur

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

Lorsque vous réinitialisez le mot de passe d'un compte utilisateur, DRA le déverrouille automatiquement. Vous pouvez décider si DRA génère un nouveau mot de passe pour le compte utilisateur. Vous pouvez également modifier plusieurs options liées au mot de passe pour le compte. Si vous gérez un compte Microsoft Windows, vous pouvez spécifier le contrôleur de domaine auquel DRA applique ces modifications.

REMARQUE : Lorsque vous appliquez cette modification à un contrôleur de domaine précis, DRA applique également cette modification au contrôleur de domaine par défaut de ce domaine géré. Pour vérifier quel contrôleur de domaine par défaut est utilisé par DRA, consultez les propriétés du domaine.

Déplacer un compte utilisateur vers un autre conteneur

Vous pouvez déplacer un compte utilisateur dans un autre conteneur tel qu'une unité organisationnelle, dans le domaine géré ou la sous-arborescence gérée.

Supprimer un compte utilisateur

Vous pouvez supprimer un compte utilisateur dans le domaine géré ou la sous-arborescence gérée. Si la Corbeille est désactivée pour ce domaine, la suppression d'un compte utilisateur supprime définitivement le compte utilisateur dans Active Directory. Si la Corbeille est activée pour ce domaine, la suppression d'un compte utilisateur déplace le compte utilisateur vers la Corbeille.

AVERTISSEMENT : Lorsque vous créez un compte utilisateur, Microsoft Windows attribue un identifiant de sécurité (SID) à ce compte. Le SID n'est pas généré à partir du nom du compte. Microsoft Windows utilise les SID pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) de chacune des ressources. Si vous supprimez un compte utilisateur, vous ne pouvez pas restituer les capacités d'accès pour ce compte en créant un nouveau compte utilisateur portant le même nom.

Spécifier l'appartenance à un groupe pour les comptes utilisateurs

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

Transformer des comptes utilisateurs

DRA vous offre la possibilité de transformer rapidement et efficacement des comptes utilisateurs. Lorsque la personne associée à un compte utilisateur passe à de nouvelles responsabilités professionnelles, vous pouvez utiliser les fonctionnalités de transformation de DRA. Grâce aux modèles de rôle professionnel, vous pouvez rapidement ajouter, supprimer ou mettre à jour les appartenances à un groupe associées à un compte. Qu'une personne soit promue, change de service ou quitte l'entreprise, la possibilité de transformer un compte utilisateur vous permettra de gagner du temps et de l'argent et vous évitera de faire des suppositions.

Comprendre le processus de transformation

Vous pouvez utiliser les capacités de transformation de compte utilisateur pour répondre à l'un des besoins suivants :

- Supprimer des appartenances à un groupe d'un compte utilisateur

- Ajouter des appartenances à un groupe à un compte utilisateur
- Changer les propriétés de l'utilisateur
- Supprimer des appartenances à un groupe particulier tout en ajoutant d'autres à un compte utilisateur

Considérez le processus suivant avant d'essayer de transformer un compte utilisateur :

1. Décidez si vous devez ajouter, supprimer ou à la fois ajouter et supprimer des appartenances à un groupe.
2. Examinez vos modèles de retrait et d'ajout actuels pour vous assurer que vous avez les modèles de comptes utilisateurs nécessaires.
3. Si nécessaire, créez tous les modèles de comptes nécessaires.
4. Terminez l'assistant Transformer l'utilisateur.

Au fur et à mesure que DRA transforme un utilisateur, les appartenances à un groupe désignées par le modèle de retrait sont supprimées du compte utilisateur, tandis que les appartenances désignées par le modèle d'ajout sont affectées au compte utilisateur. DRA ne modifie aucune appartenance en dehors des modèles de retrait ou d'ajout. Par exemple, une personne de votre service des ventes externe est transférée de l'équipe de vente pour les États-Unis à l'équipe de vente pour l'Europe. Au sein de votre organisation, vous avez à la fois des groupes de distribution et des groupes de sécurité uniques pour ces équipes de vente et un certain nombre partagé par toutes les équipes de vente. L'équipe de vente pour les États-Unis comprend les groupes de distribution Liste de distribution des points de vente aux États-Unis et Liste de distribution pour la gestion des ventes aux États-Unis, tandis que l'équipe de vente pour l'Europe comprend les groupes de distribution Points de vente pour l'Europe et Gestion des ventes pour l'Europe. Les deux équipes font partie du groupe de sécurité Sécurité des ventes mondiales, mais disposent également de groupes de sécurité propres à chaque site.

Votre modèle de retrait, appelé modèle de vente pour les États-Unis, se verrait attribuer les appartenances aux groupes suivantes :

- Liste de distribution des points de vente aux États-Unis
- Liste de distribution pour la gestion des ventes aux États-Unis
- Sécurité des ventes mondiales
- Sécurité - États-Unis

Votre modèle additif, appelé modèle de vente pour l'Europe, se verrait attribuer les appartenances aux groupes suivantes :

- Liste de distribution des points de vente en Europe
- Liste de distribution pour la gestion des ventes en Europe
- Sécurité des ventes mondiales
- Sécurité - Europe

Au cours du processus de transformation, l'appartenance à tous les groupes désignés par le modèle Ventes aux États-Unis est d'abord supprimée pour le compte utilisateur du vendeur transféré. L'appartenance aux groupes désignés par le modèle Ventes pour l'Europe lui est ensuite ajoutée. Si cette personne était également membre du groupe de distribution Joueurs de poker, cette appartenance au groupe reste intacte.

Les pouvoirs suivants permettent à un administrateur assistant de modifier davantage 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 appartenances à un groupe en attribuant à l'un des administrateurs assistants l'un des pouvoirs suivants :

- Ajouter un utilisateur aux groupes qui se trouvent dans un modèle
- Supprimer un utilisateur aux groupes qui se trouvent dans un modèle

Vous pouvez utiliser l'une ou l'autre de ces options de limitation en fonction de vos pouvoirs pour créer une couche de sécurité au sein de votre organisation. En donnant à certaines personnes le pouvoir de ne supprimer que les groupes présents dans un modèle, vous pouvez créer des comptes utilisateurs temporaires. Ces comptes provisoires peuvent ensuite être examinés avant qu'un autre administrateur assistant utilise un compte modèle d'ajout pour accorder les nouvelles appartenances à un groupe.

Créer des modèles de transformation d'utilisateur

La transformation des comptes utilisateurs est directement liée aux rôles et à l'évolution professionnelle au sein de votre organisation. Envisagez de créer un modèle pour chaque rôle ou poste au sein de votre entreprise. DRA ne fait aucune distinction entre un modèle de compte utilisateur utilisé comme modèle de retrait ou comme modèle d'ajout. Créez un modèle de compte utilisateur unique pour chaque rôle au sein de votre organisation. Pendant la transformation, désignez le modèle comme modèle d'ajout ou de retrait. La désignation d'un modèle comme modèle de retrait n'empêche pas l'utilisation du même modèle comme modèle d'ajout dans une transformation future.

Pour créer un modèle de transformation d'utilisateur, vous devez disposer des pouvoirs permettant de créer un compte utilisateur et d'affecter ce compte utilisateur aux groupes appropriés. Vous pouvez obtenir ces pouvoirs en associant votre compte aux rôles Créer et supprimer des comptes utilisateurs et Administration de groupe dans l'ActiveViews approprié ou en attribuant les pouvoirs individuellement.

Transformer des comptes utilisateurs

La transformation d'un compte utilisateur vous permet d'ajouter, de supprimer ou à la fois d'ajouter et de supprimer les appartenances à un groupe des comptes utilisateurs. Utilisez ce processus de travail lorsque des personnes passent d’un poste à un autre au sein de votre organisation. Vous devez disposer du rôle Transformer un utilisateur ou d'un rôle contenant les pouvoirs appropriés

pour transformer les comptes utilisateurs. Cette fonction ne peut être effectuée qu'à partir de la console de délégation et de configuration au moyen du nœud 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 l'opération **Rechercher maintenant** pour localiser, puis sélectionnez l'objet utilisateur.
3. Cliquez sur **Tâches** > **Transformer**.
4. Examinez la fenêtre d'accueil, puis cliquez sur **Suivant**.
5. Dans la fenêtre Sélectionner un modèle d'utilisateur, utilisez **Parcourir** pour sélectionner l'utilisateur du modèle de retrait approprié.
6. Si vous voulez examiner les propriétés du modèle de retrait de compte utilisateur, cliquez sur **Afficher**.
7. Utilisez **Parcourir** pour sélectionner l'utilisateur du modèle d'ajout approprié.
8. Si vous voulez examiner les propriétés du modèle d'ajout de compte utilisateur, cliquez sur **Afficher**.
9. Si vous disposez des pouvoirs appropriés, vous pouvez vérifier **Modifier les autres propriétés de l'utilisateur** et sélectionner les propriétés à modifier. Cliquez sur **Suivant** pour parcourir les propriétés disponibles.
10. Cliquez sur **Suivant**.
11. Examinez la fenêtre Résumé, puis cliquez sur **Terminer**.

Gérer des groupes

En tant qu'administrateur assistant, vous pouvez utiliser DRA pour gérer les groupes et modifier leurs propriétés. Les groupes vous permettent d'accorder des autorisations précises à un ensemble défini de comptes utilisateurs. Ils vous permettent également de contrôler les données et les ressources auxquelles un compte utilisateur peut accéder dans n'importe quel domaine.

Vous pouvez gérer des groupes de tout type, peu importe l'étendue. Par exemple, vous pouvez imbriquer des groupes, permettant à un groupe d'hériter des autorisations d'un autre groupe. Vous pouvez également contrôler efficacement les appartenances aux groupes d'un domaine en ajoutant des groupes de domaines approuvés à d'autres groupes du domaine géré et en gérant des affectations de groupe temporaires.

Pour en savoir plus sur la gestion des groupes, consultez les rubriques suivantes :

- « Tâches de gestion de groupe » page 55
- « Gestion des affectations de groupe temporaires dans la console de délégation et de configuration » page 58
- « Gérer les affectations de groupe temporaires dans la console Web » page 59

Tâches de gestion de groupe

Cette section vous guide dans l'administration des groupes dans la console de délégation et de configuration au moyen du nœud Gestion des comptes et des ressources. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion de groupe telles que la modification de l'appartenance à un groupe. Si vous sélectionnez plusieurs groupes, vous pouvez exécuter les tâches sélectionnées en une seule opération telles que 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.

Ajouter des comptes aux groupes

Vous pouvez ajouter des comptes utilisateurs, 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 pour le compte, DRA ne vous permettra pas d'ajouter ce compte.

Ajouter des 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 pour le groupe source, DRA ne vous permettra pas d'ajouter ce groupe.

Modifier les propriétés du groupe

Vous pouvez modifier les propriétés des groupes locaux et globaux. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un groupe du domaine géré ou de la sous-arborescence gérée. Si vous avez installé Exchange et activé la prise en charge de Microsoft Exchange, vous pouvez modifier les propriétés de listes de distribution lors de la gestion des groupes.

Créer un groupe

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

REMARQUE

- Votre entreprise peut avoir une convention de nommage appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez attribuer au nouveau groupe.
- Par défaut, DRA place le nouveau groupe dans l'unité organisationnelle Utilisateurs du domaine géré.

Spécifier les membres du groupe

Vous pouvez ajouter ou supprimer des comptes utilisateurs, des contacts, des ordinateurs ou d'autres groupes du groupe géré. DRA vous permet de supprimer uniquement les entités de sécurité externes. Vous pouvez également afficher ou modifier les propriétés des membres de groupe existants, à l'exception des entités de sécurité externes.

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

REMARQUE

- Vous ne pouvez pas ajouter de comptes utilisateurs ou des groupes à l'un des groupes spéciaux de Windows (administrateurs, opérateurs de compte, opérateurs de sauvegarde ou opérateurs de serveur), sauf si vous êtes un administrateur Windows ou un membre du groupe spécial en question.
- DRA vous permet d'exporter les résultats de **Members** (Membres) sous forme de fichier CSV. Pour exporter les résultats de **Membres** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membres** et 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.

Spécifier l'appartenance à un groupe pour des groupes

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

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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 les autorisations de sécurité d'appartenance à un groupe

Vous pouvez définir des autorisations de sécurité Active Directory pour les appartenances à un groupe. Ces autorisations spécifient qui peut afficher (lire) et modifier (écrire) les appartenances à un groupe à l'aide de Microsoft Outlook. Ces paramètres vous permettent de sécuriser plus efficacement les listes de distribution et les groupes de sécurité de votre environnement. Vous ne pouvez pas modifier les autorisations de sécurité héritées.

REMARQUE : Lorsque vous gérez la sécurité des membres d'un groupe, les autorisations désactivées sont probablement des autorisations héritées.

Configurer la propriété du groupe

Vous pouvez définir la propriété de toute distribution ou de tout groupe de sécurité Microsoft Windows. Vous pouvez accorder l'autorisation de possession de groupe à un compte utilisateur, à un groupe ou à un contact. L'attribution de propriété à un groupe permet au compte utilisateur spécifié, au groupe ou au contact de modifier l'appartenance à ce groupe.

REMARQUE : DRA désactive la case à cocher **Le gestionnaire peut mettre à jour la liste des appartenances aux groupes** lorsque l'appartenance à un groupe est masquée sur le serveur Microsoft Exchange. Pour activer cette case à cocher, cliquez sur **Afficher les appartenances aux groupes** dans l'onglet Exchange de la fenêtre Propriétés du groupe.

Cloner un groupe

Vous pouvez cloner à la fois des groupes locaux et des groupes globaux dans des domaines gérés. Cloner des groupes crée de nouveaux groupes du même type et ayant les mêmes attributs que le groupe original. DRA tente également d'ajouter tous les membres du groupe d'origine au nouveau groupe.

En clonant un groupe, vous pouvez créer rapidement des groupes basés sur d'autres groupes ayant des propriétés similaires. Lorsque vous clonez un groupe, DRA remplit l'assistant Cloner un groupe avec les valeurs du groupe sélectionné. Vous pouvez également modifier les propriétés du nouveau groupe.

REMARQUE

- Votre entreprise peut avoir une convention de nommage appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez attribuer au nouveau groupe.
- Par défaut, DRA place le nouveau groupe dans l'unité organisationnelle Utilisateurs du domaine géré.

Supprimer un groupe

Vous pouvez supprimer des groupes locaux et globaux dans le domaine géré ou la sous-arborescence gérée. Si la Corbeille est désactivée pour ce domaine, la suppression d'un groupe supprime définitivement le groupe dans Active Directory. Si la Corbeille est activée pour ce domaine, la suppression d'un groupe déplace le groupe dans la Corbeille et désactive les propriétés du groupe.

Pour obtenir de plus amples renseignements sur la Corbeille, consultez Gérer la Corbeille.

AVERTISSEMENT : Lorsque vous créez un groupe, Microsoft Windows attribue un identifiant de sécurité (SID) à ce groupe. Le SID n'est pas généré à partir du nom du groupe. Microsoft Windows utilise les SID pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) de chacune des ressources. Si vous supprimez un groupe, vous ne pouvez pas restituer les capacités d'accès pour ce groupe en créant un nouveau groupe portant le même nom.

Déplacer un groupe dans un autre conteneur

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

Afficher les appartenances aux groupes dans les listes de distribution

Vous pouvez afficher les appartenances aux groupes dans les listes de distribution des groupes du domaine géré ou du sous-arbre géré.

Masquer les appartenances aux groupes des listes de distribution

Vous pouvez masquer les appartenances aux groupes dans les listes de distribution des groupes du domaine géré ou du sous-arbre géré.

Gestion des affectations de groupe temporaires dans la console de délégation et de configuration

Les affectations de groupe temporaire vous permettent de gérer les adhésions à un groupe pour les utilisateurs qui n'ont besoin d'appartenir au groupe que pour une période donnée. Cette section vous guide dans la gestion des affectations de groupe temporaires dans la console de délégation et de configuration sous **Account and Resource Management** (Gestion des comptes et des ressources). Avec les pouvoirs appropriés, vous pouvez effectuer des tâches telles que la création de nouvelles affectations de groupe temporaire ou la suppression des affectations de groupe temporaire ayant expiré.

Les administrateurs assistants peuvent uniquement consulter les affectations de groupe temporaires relatives aux groupes pour lesquels l'administrateur assistant a le pouvoir de modifier les adhésions de groupe (ajouter ou supprimer des membres).

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

Gérer les propriétés des affectations de groupe temporaire

Vous pouvez gérer les propriétés des affectations de groupe temporaires ou les affectations de groupe temporaires expirées enregistrées.

Si vous souhaitez replanifier une affectation de groupe temporaire, modifiez la planification dans les **propriétés** de l'affectation et enregistrez vos modifications.

Créer une affectation de groupe temporaire

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

Par défaut, lorsqu'une affectation de groupe temporaire expire, elle est supprimée au bout de sept jours, à moins que vous ne choisissiez l'option **Keep this temporary group assignment for future use** (Conserver cette affectation de groupe temporaire pour une utilisation ultérieure). Pour modifier cette période de conservation, cliquez à l'aide du bouton droit de la souris sur le nœud **Temporary Group Assignment** (Affectation de groupe temporaire) sous All My Managed Objects (Tous mes objets gérés), sélectionnez **Properties** (Propriétés) et modifiez le nombre de jours pour conserver les affectations de groupe temporaires.

Gérer les comptes d'utilisateurs dans une affectation de groupe temporaire

Vous pouvez ajouter ou supprimer des comptes d'utilisateurs des affectations de groupe temporaire sur les serveurs d'administration primaire et secondaire.

REMARQUE : Vous ne pouvez gérer les comptes d'utilisateurs que pour des affectations de groupe temporaire qui ne sont pas encore actives.

Supprimer une affectation de groupe temporaire

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

Gérer les affectations de groupe temporaires dans la console Web

Les affectations de groupe temporaire vous permettent de gérer les adhésions à un groupe pour les utilisateurs qui ont besoin d'appartenir au groupe pour une période précise. Si Azure Active Directory est configuré par l'administrateur de DRA, vous pouvez créer des affectations de groupe temporaires pour les groupes Azure, et ajouter des utilisateurs Azure et des utilisateurs synchronisés à une adhésion de groupe Azure. Dans la console Web, vous pouvez créer et gérer des affectations à partir des serveurs primaire et secondaire de DRA. Cependant, les actions que vous pouvez entreprendre sur les affectations existantes varient en fonction de l'état de l'affectation.

Les administrateurs assistants peuvent afficher les affectations de groupe temporaires uniquement pour les groupes pour lesquels ils ont le pouvoir de modifier en raison de leurs affectations ActiveView, telles que l'ajout ou la suppression de membres du groupe.

Pour gérer les affectations de groupe temporaires dans la console Web, accédez à **Tasks** > **Temporary Group Assignments** (Tâches > Affectations de groupe temporaires).

Vous pouvez effectuer les actions suivantes :

Créer une affectation de groupe temporaire

Vous pouvez créer des affectations de groupe temporaires en utilisant des groupes pour lesquels vous avez le pouvoir de modifier et de spécifier le contrôleur de domaine. Le groupe cible peut être un groupe d'un locataire géré par Azure ou un groupe d'un domaine Active Directory. Lorsque l'affectation de groupe temporaire expire, DRA la supprime automatiquement après sept jours, à moins que vous ne choisissiez l'option de conserver l'affectation de groupe temporaire pour une utilisation ultérieure.

REMARQUE : Si l'affectation de groupe temporaire configurée avec l'adhésion au groupe Azure est modifiée en dehors de DRA, l'affectation de groupe temporaire devient invalide.

Pour créer une affectation de groupe temporaire :

1. Accédez à **Tâches** > **Affectations de groupe temporaires**, et cliquez sur **Créer**.
2. Cliquez sur **Select** (Sélectionner), et trouvez le groupe en exécutant une recherche dans le conteneur applicable.
3. Si vous devez ajouter des membres au groupe, cliquez sur **Ajouter** sous **Membres** dans la page Créer une affectation de groupe temporaire, localisez et utilisez l'option **Ajouter** ➕ dans la liste de résultats pour ajouter des membres au groupe.
4. Configurez le calendrier.
5. Nommez le TGA sous General Information (Renseignements généraux), et cliquez sur **Create** (Créer).

Rechercher des affectations existantes

Lorsque vous recherchez des affectations de groupe temporaires (AGT) existantes, elles sont répertoriées dans les résultats en fonction de l'état de l'affectation, qui peut inclure les états suivants:

- **En attente :** L'AGT devrait démarrer dans un moment futur. Vous pouvez annuler, supprimer et replanifier.

- **Actif :** L'AGT a démarré et des membres concernés ont été ajoutés au groupe. Vous pouvez annuler et supprimer.
- **Actif avec erreur :** L'AGT a démarré, mais il n'a pas été possible d'ajouter tous les membres concernés au groupe. Vous pouvez annuler et supprimer.
- **Terminé :** L'AGT a expiré et tous les membres concernés ont été supprimés du groupe. Vous pouvez supprimer et replanifier.
- **Terminé avec erreur :** L'AGT a expiré, mais il n'a pas été possible de supprimer tous les membres concernés du groupe. Vous pouvez supprimer et replanifier.
- **Annulé :** L'AGT a été annulée par un utilisateur et tous les membres concernés du groupe ont été supprimés. Vous pouvez supprimer et replanifier.
- **Annulé avec erreur :** L'AGT a été annulée par un utilisateur, mais il n'a pas été possible de supprimer tous les membres concernés du groupe. Vous pouvez supprimer et replanifier.
- **Erreur :** L'AGT n'a pas réussi à ajouter ou à supprimer tous les membres. Vous pouvez supprimer et replanifier.

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

View·or· od fy·tempo ary group·assi nm nt·properties

Vous pouvez consulter ou modifier n'importe laquelle des affectations de groupe temporaires qui ont été définies lors de la création de l'affectation de groupe temporaire. Après avoir effectué une recherche d'affectations de groupe temporaires, sélectionnez une affectation pour en visualiser ou en modifier les propriétés.

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

IMPORTANT : Vous ne pouvez pas changer le groupe associé ou modifier la liste des utilisateurs tant que l'affectation de groupe temporaire est toujours active. Si vous souhaitez modifier ces éléments, vous devez d'abord annuler l'affectation.

Annuler une affectation de groupe temporaire

Vous ne pouvez annuler une affectation de groupe temporaire que lorsqu'elle se trouve dans l'un des états suivants :

- Actif
- Actif avec erreur
- En attente

Supprimer une affectation de groupe temporaire

Vous pouvez sélectionner plusieurs affectations de groupe temporaires et les supprimer. Si les affectations de groupe temporaires sélectionnées sont dans l'état Actif, Actif avec erreur ou En attente, l'option **Cancel** (Annuler) est également activée.

Gérer des groupes de distribution dynamiques

Un groupe de distribution dynamique est un objet de groupe Active Directory à extension messagerie que vous pouvez créer pour accélérer l'envoi en masse des courriels et d'autres informations.

La liste des membres d'un groupe de distribution dynamique est calculée chaque fois qu'un message est envoyé au groupe, en fonction des filtres et des conditions que vous définissez. Cela diffère d'un groupe de distribution normal, qui contient un ensemble défini de membres. Lorsqu'un courriel 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 :

- Création de rapport d'audit et d'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 des opérations de déclenchement pour les groupes de distribution dynamiques
- Prise en charge des extensions d'interface utilisateur pour les groupes de distribution dynamiques Exchange

Tâches du groupe de distribution dynamique :

Créer un groupe de distribution dynamique

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

REMARQUE

- Votre entreprise peut avoir une convention de nommage appliquée par le biais d'une stratégie qui détermine le nom que vous pouvez attribuer au nouveau groupe de distribution dynamique.
- Par défaut, DRA place le nouveau groupe de distribution dynamique dans l'unité organisationnelle Utilisateurs du domaine géré.

Pour créer un groupe de distribution dynamique dans la console de délégation et de configuration :

1. Sélectionnez le conteneur dans lequel créer un groupe à partir de Tous mes objets gérés dans le nœud de gestion des comptes et des ressources.
2. Sélectionnez **Nouveau** > **Dynamic Distribution Group** (Groupe de Distribution Dynamique) dans le menu Tâches.
3. Exécutez les étapes de l'assistant.

Pour créer un groupe de distribution dynamique dans la console Web :

1. Sélectionnez le générique **Gestion**, et sélectionnez le conteneur dans lequel créer un groupe à partir de Tous mes objets gérés dans le nœud de gestion des comptes et des ressources.
2. Sélectionnez **Groupe de Distribution Dynamique** dans le menu déroulant Créer.
3. Saisissez les informations requises dans le formulaire, puis cliquez sur **Créer**.

Cloner un groupe de distribution dynamique

Vous pouvez cloner à la fois des groupes de distribution dynamiques locaux et globaux dans des domaines gérés. Le clonage de groupes de distribution dynamiques crée de nouveaux groupes de distribution dynamiques du même type et ayant 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 basés sur d'autres groupes de distribution dynamiques ayant des propriétés similaires. Lorsque vous clonez un groupe de distribution dynamique, DRA remplit l'assistant Cloner un 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.

Déplacer un groupe de distribution dynamique dans un autre conteneur

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

Supprimer un groupe de distribution dynamique

Vous pouvez supprimer des groupes de distribution dynamiques locaux et globaux dans le domaine géré ou la sous-arborescence gérée. Si la Corbeille est désactivée pour ce domaine, la suppression d'un groupe de distribution dynamique supprime définitivement ce groupe dans Active Directory. Si la Corbeille est activée pour ce domaine, la suppression d'un groupe de distribution dynamique déplace ce groupe dans la Corbeille et désactive les propriétés du groupe de distribution dynamique.

Pour obtenir de plus amples renseignements sur la Corbeille, consultez Gérer la Corbeille.

AVERTISSEMENT : Lorsque vous créez un groupe de distribution dynamique, Microsoft Windows attribue un identifiant de sécurité (SID) à ce groupe. Le SID n'est pas généré à partir du nom du groupe de distribution dynamique. Microsoft Windows utilise les SID pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) de chacune des ressources. Si vous supprimez un groupe de distribution dynamique, vous ne pouvez pas restituer les capacités d'accès pour ce groupe en créant un nouveau groupe de distribution dynamique portant le même nom.

Modifier les propriétés du groupe de distribution dynamique

Vous pouvez modifier les propriétés des groupes de distribution dynamiques locaux et globaux. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un groupe du domaine géré ou de la sous-arborescence gérée.

Spécifier un filtre

Les membres d'une liste de diffusion dynamique sont déterminés par son filtre, que vous pouvez définir.

Spécifier les conditions

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

Gérer des groupes dynamiques

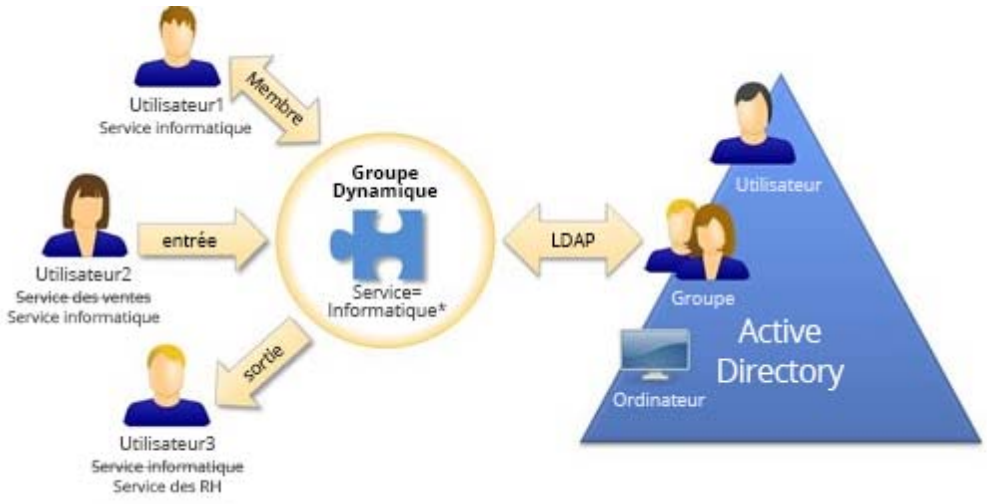
Un groupe dynamique est un groupe dont les membres changent en fonction d'un ensemble défini de critères. Dans DRA, vous pouvez créer des groupes dynamiques sans disposer d'un environnement Exchange. Les filtres d'adhésion utilisés pour gérer les groupes dynamiques dans Active Directory sont propres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

L'administrateur DRA configure le calendrier de rafraîchissement du domaine pour les groupes dynamiques dans la console de délégation et de configuration. De nouveaux membres sont ajoutés dynamiquement au groupe lorsqu'une ou plusieurs propriétés d'utilisateur correspondant aux critères du filtre de membres du groupe sont mises à jour et qu'un rafraîchissement se produit. De la même manière, un membre peut être dynamiquement retiré du groupe lorsque les propriétés correspondantes sont modifiées ou retirées à l'utilisateur.

Exemple de scénario

L'image ci-dessous décrit une utilisation typique d'un groupe dynamique Active Directory. Il y a trois groupes dynamiques dans l'image. Chaque groupe a un ensemble de critères qui détermine qui peut être ajouté au groupe et qui ne peut pas l'être. Chaque groupe contrôle l'accès à un ensemble de fichiers, de dossiers et d'applications défini.

SUGGESTION : Vous pouvez créer une *liste de membres statique* contenant les membres permanents du groupe dynamique. Vous pouvez également créer une *liste des membres exclus* qui empêche ces utilisateurs d'adhérer au groupe dynamique.



User2 (Utilisateur2) a récemment rejoint le service informatique. Une fois le groupe dynamique du service informatique mis à jour, elle sera ajoutée au groupe. Lorsque le groupe dynamique du service des ventes est mis à jour, User2 est supprimée de la liste de ses membres.

User3 (Utilisateur3), qui a quitté le service informatique pour le service des ressources humaines, sera supprimé du groupe dynamique du service informatique et ajouté au groupe dynamique du service des ressources humaines.

Préparation du scénario

Les informations ci-dessous fournissent un exemple des actions à entreprendre dans la console Web pour activer le scénario ci-dessus. Vous pouvez rendre un groupe existant dynamique ou créer un nouveau groupe dynamique. Pour des raisons de simplicité, nous n'ajouterons aucun membre statique ni exclu et nous rendrons dynamiques trois groupes existants : le groupe RH, le groupe IT et le groupe Ventes.

Mise en place du groupe dynamique :

1. For each group provided above, perform a Search operation with the Group filter enabled to locate the group.
2. Ouvrez **Propriétés** du groupe et accédez à la page **Dynamic Member Filter** (Filtre dynamique de membres).
3. Cliquez sur le curseur **Make group dynamic** (Rendre le groupe dynamique) pour activer la fonction.
4. Cliquez sur **Modifier** et tapez ou collez les critères du filtre de membre dans le champ de requête LDAP. Dans ce cas, nous recherchons des critères dans la propriété **User** > **Department** (Utilisateur > Service). Les exemples ci-dessous montrent les critères LDAP que nous utiliserons pour chaque groupe dans l'exemple scénario :
   - Groupe RH : *(&(objectClass=user)(objectCategory=person)(department=HR*))*
   - Groupe TI : *(&(objectClass=user)(objectCategory=person)(department=IT*))*
   - Groupe Ventes : *(&(objectClass=user)(objectCategory=person)(department=Sales*))*
5. Cliquez sur **Appliquer** pour enregistrer les modifications.

Actions entreprises pour changer dynamiquement l'affiliation de groupe des utilisateurs dans les propriétés de l'utilisateur sélectionné :

- User2 (Utilisateur2) à modifié la propriété **Organization** > **Department** de « Sales » à « IT ».
- User3 (Utilisateur3) à modifié la propriété **Organization** > **Department** de « IT » à « HR ».

Les changements dynamiques se produisent lors du rafraîchissement programmé du groupe dynamique ou lors d'un rafraîchissement manuel par l'administrateur DRA.

Tâches du groupe de dynamique

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

Créer un groupe dynamique

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

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

Créer un filtre

Le groupe dynamique utilise le **Dynamic Member Filter** (Filtre dynamique des membres) pour ajouter ou supprimer des utilisateurs de sa liste de membres chaque fois que le groupe est actualisé. Pour des exemples de construction de requêtes LDAP et d'attributs virtuels pour le filtre, vous pouvez vous référer aux exemples présentés dans « Advanced Search Queries » (Recherche avancée de requêtes). Bien que le filtre fonctionne comme un critère d'appartenance à un groupe et non comme une recherche, les exemples de requêtes sont toujours applicables :

- Exemples de requêtes LDAP
- Exemples de requêtes d'attributs virtuels

Gérer 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 propriété Filtre dynamique des membres sur un 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 avoir les pouvoirs pour modifier les objets que vous souhaitez ajouter.

Gérer la liste des membres exclus

Les utilisateurs placés dans la liste des membres exclus d'un groupe dynamique ne seront pas autorisés à 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 propriété Filtre dynamique des membres sur un utilisateur sélectionné.

Actualiser la liste des membres

Vous pouvez actualiser les membres d'un groupe dynamique à l'aide de l'action **Mise à jour des membres**.

Cloner un groupe dynamique

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

En clonant un groupe dynamique, vous pouvez créer rapidement des groupes dynamiques basés sur d'autres groupes dynamiques ayant des propriétés similaires. Lorsque vous clonez un groupe dynamique, DRA remplit l'assistant Cloner un groupe 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 groupe dans le volet des résultats de recherche et cliquez sur **Cloner** dans la barre d'outils.

Déplacer un groupe dynamique dans un autre conteneur

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

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

Supprimer un groupe dynamique

Vous pouvez supprimer des groupes dynamiques locaux et globaux dans le domaine géré ou la sous-arborescence gérée. Si la Corbeille est désactivée pour ce domaine, la suppression d'un groupe dynamique supprime définitivement le groupe dans Active Directory. Si la Corbeille est activée pour ce domaine, la suppression d'un groupe dynamique déplace ce groupe dans la Corbeille et désactive les propriétés du groupe dynamique. Pour obtenir de plus amples renseignements sur la Corbeille, consultez Gérer la Corbeille.

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

AVERTISSEMENT : Lorsque vous créez un groupe dynamique, Microsoft Windows attribue un identifiant de sécurité (SID) à ce groupe. Le SID n'est pas généré à partir du nom du groupe dynamique. Microsoft Windows utilise les SID pour enregistrer les privilèges dans les listes de contrôle d'accès (ACL) de chacune des ressources. Si vous supprimez un groupe dynamique, vous ne pouvez pas restituer les capacités d'accès pour ce groupe en créant un nouveau groupe dynamique portant le même nom.

Modifier les propriétés de groupe dynamique

Vous pouvez modifier les propriétés des groupes dynamiques locaux et globaux. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un groupe du domaine géré ou de la sous-arborescence gérée.

REMARQUE : DRA vous permet d'exporter les résultats de **Membres** et **Membre de** sous forme de fichier CSV. Pour exporter les résultats de **Membres** ou de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membres** ou **Membre de** et 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.

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

Ajouter des 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 dynamique parent.

Pour ajouter un groupe dynamique à un autre groupe dynamique, sélectionnez le groupe dans le volet des résultats de 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 pour le groupe dynamique source, DRA ne vous permettra pas d'ajouter ce groupe.

Configurer les autorisations de sécurité d'appartenance à un groupe

Vous pouvez définir des autorisations de sécurité Active Directory pour les appartenances au groupe. Ces autorisations spécifient qui peut afficher (lire) et modifier (écrire) les appartenances 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 de votre environnement. Vous ne pouvez pas modifier les autorisations de sécurité héritées.

Vous pouvez mettre à jour ces paramètres à partir de la page de propriété **Sécurité des membres** sur un groupe dynamique sélectionné.

REMARQUE : Lorsque vous gérez la sécurité des membres d'un groupe dynamique, les autorisations désactivées sont probablement des autorisations héritées.

Configurer la propriété de groupe dynamique

Vous pouvez accorder l'autorisation de possession de groupe dynamique à un compte utilisateur, à un groupe ou à un contact. L'attribution de propriété à un groupe dynamique permet au compte utilisateur spécifié, au groupe ou au contact de modifier l'appartenance à ce groupe.

Vous pouvez mettre à jour ces paramètres à partir de la page de propriété **Gérés par** sur un groupe dynamique sélectionné.

Afficher les appartenances aux groupes dynamiques dans les listes de distribution

Vous pouvez afficher les appartenances aux groupes dynamiques dans les listes de distribution des groupes du domaine géré ou du sous-arbre géré.

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

Masquer les appartenances aux groupes dynamiques des listes de distribution

Vous pouvez masquer les appartenances aux groupes dynamiques dans les listes de distribution des groupes du domaine géré ou du sous-arbre géré.

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

REMARQUE : L'option **Masquer l'appartenance au groupe** est désactivée pour les listes de distribution Microsoft Exchange 2007.

Gérer les contacts

DRA vous permet de gérer de nombreux objets réseau, notamment les contacts et les adresses de courriel associées. Les contacts sont disponibles uniquement en mode mixte ou dans des domaines Microsoft Windows natifs. Les contacts ne possèdent pas d'identifiant de sécurité (SID), contrairement aux comptes utilisateurs et aux groupes. Utilisez des contacts pour ajouter des membres à des listes de distribution ou à des groupes sans leur donner accès aux services réseau.

Vous pouvez ajouter des contacts aux groupes de sécurité ou de distribution dans les domaines en mode mixte et natif. Les groupes de sécurité pouvant être utilisés en tant que listes de distribution dans Microsoft Windows, vous pouvez ajouter des contacts à ces groupes. La présence d'un contact dans un groupe de sécurité global n'empêche pas la conversion de ce groupe en groupe de sécurité universel lorsque vous migrez vers un domaine Microsoft Windows en mode natif.

Vous pouvez exécuter la plupart des tâches ci-dessous à partir de l'onglet **Gestion** > **Recherche** de la console Web. Exécutez une opération de recherche pour localiser et sélectionner le contact nécessaire. Après avoir sélectionné un ou plusieurs contacts dans la liste, la barre de tâches devient active avec des options de barre d'outils et des options de liste déroulante pour **Exchange**. Passez la souris sur une icône de la barre d'outils ou cliquez sur un menu déroulant pour afficher leurs fonctions ou options.

Modifier les propriétés d'un contact

Vous pouvez modifier les propriétés d'un contact. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un contact du domaine géré ou de la sous-arborescence gérée. Si vous avez installé Exchange et activé la prise en charge d'Exchange, vous pouvez modifier les propriétés des adresses de courriel lors de la gestion des contacts.

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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.

Créer un contact

Vous pouvez créer des contacts dans le domaine géré ou la sous-arborescence gérée. Vous pouvez également modifier les propriétés, activer le courriel et spécifier des adresses de courriel ainsi que les appartenances aux groupes pour le nouveau contact.

Pour créer un nouveau contact, accédez à **Gestion** > **Recherche**, et sélectionnez **Contact** dans le menu déroulant Créer.

Cloner un contact

En clonant un contact, vous pouvez créer rapidement des contacts basés sur d'autres contacts ayant des propriétés similaires. Lorsque vous clonez un contact, DRA remplit l'assistant Cloner un contact avec les valeurs du contact sélectionné. Vous pouvez également modifier les propriétés, activer le courriel et spécifier des adresses de courriel ainsi que les appartenances aux groupes pour le nouveau contact.

Gérer les appartenances aux groupes pour les contacts

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

Déplacer un contact vers une autre unité organisationnelle

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

Supprimer un contact

Vous pouvez supprimer un contact dans le domaine géré ou la sous-arborescence gérée. Si la Corbeille est désactivée pour ce domaine, la suppression d'un contact supprime définitivement le contact dans Active Directory. Si la Corbeille est activée pour ce domaine, la suppression d'un contact déplace ce dernier vers la Corbeille.

Pour obtenir de plus amples renseignements sur la Corbeille, consultez Gérer la Corbeille.

Gérer les comptes de services gérés de groupe

Un compte de service géré de groupe (gMSA) est un compte de domaine géré que vous pouvez affecter à des services sur des ressources informatiques. Vous ne devez pas mettre à jour manuellement le mot de passe de ces comptes dans Active Directory; les mots de passe de ces comptes sont automatiquement gérés par Windows Server.

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

Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches liées aux comptes de services gérés de groupe. Exécutez une opération de recherche pour localiser et sélectionner l'objet gMSA nécessaire. Après avoir sélectionné un ou plusieurs objets dans la liste, la barre de tâches devient active 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 un autre et de modifier les propriétés de gMSA. Vous pouvez également télécharger les résultats de la recherche sous forme de fichier CSV. Cliquez sur les options pour afficher leurs fonctions.

Créer un gMSA

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

Pour créer un nouveau gMSA, accédez à **Gestion** > **Rechercher**, et sélectionnez **Compte de services gérés de groupe** dans le menu déroulant Créer.

Modifier les propriétés d'un gMSA

Vous pouvez modifier les propriétés d'un gMSA. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un gMSA du domaine géré.

Activer un gMSA

L'activation d'un gMSA vous permet d'utiliser le gMSA comme informations d'identification de connexion pour un service informatique. Vous pouvez activer ou désactiver un gMSA à partir de l'onglet Comptes.

Gérer les adhésions aux groupes pour les gMSA

Vous pouvez ajouter ou supprimer des comptes gérés de groupe d'un groupe précis du domaine géré ou de la sous-arborescence gérée.

Déplacer un gMSA dans un autre conteneur

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

Supprimer un gMSA

Vous pouvez supprimer un compte de service géré de groupe dans le domaine géré ou la sous-arborescence gérée.

5 Gérer des objets Azure

Ce chapitre contient des informations conceptuelles et procédurales pour la gestion des comptes d'utilisateurs Azure, des contacts Azure et des groupes Azure dans la console Web. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion des utilisateurs Azure, des contacts Azure et des groupes Azure, comme la création et la suppression d'objets de compte utilisateur Azure.

Vous pouvez exécuter la plupart des tâches pour les objets d'utilisateur Azure, de contacts Azure et de groupe Azure à partir de l'onglet **Gestion** > **Recherche** de la console Web en recherchant des objets dans l'un des noeuds suivants :

- Tous mes objets gérés
- Tous mes locataires gérés
- Un sous-nœud de Tous mes locataires gérés

Les sujets abordés sont les suivants :

Gérer des comptes d'utilisateurs Azure

En tant qu'administrateur assistant, vous pouvez utiliser DRA pour gérer les comptes d'utilisateurs Azure et modifier les propriétés des comptes d'utilisateurs Azure lorsque Azure Active Directory est configuré par l'administrateur DRA.

Exécutez une opération de recherche pour localiser et sélectionner l'objet utilisateur Azure nécessaire. Après avoir sélectionné un ou plusieurs objets dans la liste, la barre des tâches devient active avec des options telles que supprimer, autoriser, bloquer, réinitialiser le mot de passe et modifier les propriétés. Vous pouvez également télécharger les résultats de la recherche sous forme de fichier CSV. Cliquez sur les options pour afficher leurs fonctions.

Créer un compte d'utilisateur Azure

Vous pouvez créer des comptes d'utilisateur Azure dans Azure Active Directory. Vous pouvez également activer le courriel et spécifier les adhésions de groupe pour le nouveau compte.

Modifier les propriétés du compte d'utilisateur Azure

Vous pouvez gérer les propriétés des comptes d'utilisateurs Azure dans Azure Active Directory. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un compte d'utilisateur Azure. Si le compte d'utilisateur Azure possède une boîte aux lettres Office 365 ou si le compte d'utilisateur Azure est activé pour la messagerie, vous pouvez gérer les propriétés liées à la boîte aux lettres et à la messagerie pour le compte d'utilisateur Azure.

Vous pouvez gérer les stratégies des boîtes aux lettres, définir des restrictions et des options de distribution, fixer des limites de stockage, déléguer les autorisations des boîtes aux lettres, mettre les litiges en attente, gérer les adresses courriel, etc.

REMARQUE

- Vous pouvez mettre à jour les propriétés Mobile Phone (Téléphone cellulaire) et Office Phones (Téléphones de bureau) uniquement pour les utilisateurs Azure qui ne sont pas des administrateurs.
- DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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 à un compte d'utilisateur Azure

Vous pouvez permettre à un compte d'utilisateur Azure de se connecter à Azure Active Directory.

Bloquer la connexion à un compte d'utilisateur

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

Réinitialiser un mot de passe de compte d’utilisateur Azure

Vous pouvez réinitialiser le mot de passe d'un compte d'utilisateur Azure dans Azure Active Directory et choisir si DRA génère un nouveau mot de passe pour le compte ou non.

Supprimer un compte d'utilisateur Azure

Vous pouvez supprimer un compte d'utilisateur Azure de Azure Active Directory, mais il ne peut pas être restauré à partir de DRA.

Indiquer une adhésion à un groupe Azure pour les comptes d'utilisateurs Azure

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

Gérer les groupes Azure

En tant qu'administrateur assistant, vous pouvez utiliser DRA pour gérer les groupes Azure lorsque Azure Active Directory est configuré par l'administrateur de DRA. Les groupes Azure vous permettent d'accorder des autorisations précises à un ensemble défini de comptes d'utilisateurs. Ils vous permettent également de contrôler les données et les ressources auxquelles un compte d'utilisateur peut accéder dans n'importe quel locataire.

Exécutez une opération de recherche pour localiser et sélectionner l'objet de groupe Azure nécessaire. Après avoir sélectionné un ou plusieurs objets dans la liste, la barre de tâches devient active 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 de groupes existants et de modifier les propriétés des groupes. Cliquez sur les options pour afficher leurs fonctions.

REMARQUE : Membres pris en charge; les membres d'un groupe Azure peuvent être des utilisateurs Azure, des groupes Azure, des contacts Azure, des utilisateurs synchronisés, des contacts synchronisés et des groupes synchronisés.

Ajouter des comptes aux groupes Azure

Vous pouvez ajouter des comptes, des contacts et des groupes, à la fois sur site et sur Azure, à un groupe géré par Azure.

Cette tâche ajoute plusieurs comptes à un groupe sélectionné. Vous pouvez ajouter un seul compte à un groupe en sélectionnant le compte approprié. Si l'ajout d'un compte à un autre groupe augmente vos pouvoirs pour le compte, DRA ne vous permet pas d'ajouter le compte.

Groupes imbriqués dans Azure

Vous pouvez imbriquer des groupes en ajoutant d'autres groupes (sur site et sur 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 Azure augmente vos pouvoirs pour le groupe source, DRA ne vous permettra pas d'ajouter ce groupe.

Créer un groupe Azure

Vous pouvez créer un groupe Azure dans Azure Active Directory. Vous pouvez également modifier les propriétés, telles que l'ajout des membres du groupe Azure, du nouveau groupe.

Si un propriétaire n'est pas indiqué, DRA fournit par défaut le compte d'accès du locataire Azure en tant que propriétaire.

Modifier les propriétés du groupe Azure

Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un groupe d'Azure Active Directory. Si la stratégie Exchange est activée, vous pouvez gérer les propriétés Exchange pour les groupes Azure compatibles avec la messagerie, comme le groupe Office 365, le groupe de sécurité compatible avec la messagerie et la liste de distribution. Selon le type de groupe, vous pouvez gérer les adresses courriel du groupe, spécifier qui peut envoyer des courriels au groupe, spécifier les utilisateurs qui peuvent envoyer des courriels au nom du groupe, définir les options d'approbation des courriels, etc.

REMARQUE : DRA vous permet d'exporter les résultats de **Membres** et **Membre de** sous forme de fichier CSV. Naviguez vers l'onglet **Membres** ou **Membre de** et 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 d'utilisateur ou à un groupe. L'octroi de la propriété du groupe permet au compte d'utilisateur ou au groupe spécifié de gérer le groupe, y compris l'adhésion.

Supprimer un groupe Azure

Vous pouvez supprimer des groupes Azure d'Azure Active Directory, mais ils ne peuvent pas être restaurés à partir de DRA.

Gérer des contacts Azure

Les contacts Azure sont des objets de messagerie contenant une adresse courriel externe. En tant qu'administrateur assistant, vous pouvez utiliser DRA pour gérer les contacts Azure et modifier les propriétés de contacts Azure lorsque Azure Active Directory est configuré par l'administrateur de DRA.

Exécutez une opération de recherche pour localiser et sélectionner l'objet de contact Azure nécessaire. Après avoir sélectionné un ou plusieurs objets dans la liste, la barre de tâches devient active avec des options permettant de supprimer des objets, d'ajouter des objets à des groupes, de retirer des objets de groupes et de modifier les propriétés des contacts. Vous pouvez également télécharger les résultats de la recherche sous forme de fichier CSV. Cliquez sur les options pour afficher leurs fonctions.

Créer un contact Azure

Vous pouvez créer un contact Azure dans le locataire géré et spécifier les informations de contact et les courriels pour le nouveau contact Azure.

Modifier les propriétés du contact Azure

Vous pouvez modifier les propriétés d'un contact Azure. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un contact Azure du locataire géré. Si la stratégie Exchange est activée, vous pouvez gérer les propriétés liées au courriel, comme définir des restrictions de distribution pour les messages, spécifier qui peut envoyer des messages au nom de ce contact Azure, spécifier si le contact Azure est visible dans la liste d'adresses, etc.

Activer la modération des messages

Vous pouvez définir des options pour modérer les messages envoyés à un contact Azure. Lorsque vous activez la modération, les messages envoyés au contact Azure seront approuvés par un modérateur que vous définissez avant que les messages ne soient distribués. Vous pouvez également spécifier les utilisateurs et les groupes qui sont exemptés du processus d'approbation.

Gérer les adhésions aux groupes pour les contacts Azure

Vous pouvez ajouter ou supprimer des contacts Azure aux groupes de sécurité et aux listes de distribution compatibles avec la messagerie.

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Naviguez vers l'onglet **Membre de** et cliquez sur l'icône **Download Saved Membership** (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 ils ne peuvent pas être restaurés à partir de DRA.

6 Gérer les boîtes aux lettres Exchange et les dossiers publics

À l'aide de DRA, vous pouvez gérer les boîtes aux lettres Microsoft Exchange en tant qu'extension des propriétés du compte utilisateur. Cette intégration vous permet de simplifier vos processus de travail d'administration afin de pouvoir administrer efficacement les propriétés d'Exchange. Vous pouvez également lier des boîtes aux lettres à partir de forêts de comptes utilisateurs et de comptes Exchange et gérer des boîtes aux lettres de ressources, des boîtes aux lettres partagées et des dossiers publics.

Gestion des tâches de la boîte 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 à partir de l'onglet **Exchange Tasks** (Tâches Exchange) dans les propriétés de l'objet. Cette option est également accessible à partir du menu **Tasks** (Tâches) ou du menu contextuel de l'objet sélectionné. En règle générale, sélectionnez le nœud **Tous mes objets gérés** et exécutez une opération **Trouver maintenant** pour localiser et sélectionner l'objet souhaité.

Gérer les tâches de boîte aux lettres dans 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 souhaité. Une fois que vous avez sélectionné un ou plusieurs objets dans la liste, la barre des tâches devient active. Cliquez sur les options pour afficher leurs fonctions.

Voir les rubriques suivantes :

- « Tâches de gestion pour les boîtes aux lettres d'utilisateur » page 75
- « Tâches de gestion pour les boîtes aux lettres Office 365 » page 78
- « Tâches de gestion pour les boîtes aux lettres de ressources » page 79
- « Tâches de gestion pour les boîtes aux lettres partagées » page 81
- « Tâches de gestion pour les boîtes aux lettres liées » page 82
- « Tâches de gestion pour les dossiers publics » page 83

Tâches de gestion pour les boîtes aux lettres d'utilisateur

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

contrôler la sécurité de vos environnements Microsoft Exchange. Si vous ne disposez pas des pouvoirs nécessaires pour modifier un onglet ou un champ de la boîte aux lettres sélectionnée, DRA désactive ces onglets et ces champs.

En plus des tâches définies ci-dessous, l'administrateur DRA peut activer des options dans les propriétés de l'objet des comptes utilisateurs pour configurer les paramètres de Skype et de Skype Online. Skype peut être configuré à partir de comptes d'utilisateur dans la console de délégation et de configuration et la console Web. Skype Online ne peut être configuré qu'à partir de la console Web.

Créer 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 génère les chaînes de mandataire nécessaires en fonction de vos paramètres de stratégie Exchange. Microsoft Exchange génère également des chaînes de mandataire par défaut. Par conséquent, lorsque vous affichez les propriétés de la boîte aux lettres nouvellement créée, vous voyez les deux types de chaînes de mandataire.

Cloner un compte utilisateur

Lorsque vous clonez un compte utilisateur, tous les groupes dont l'utilisateur est membre sont automatiquement ajoutés au nouveau compte utilisateur, ce qui vous permet de gagner du temps lors de la configuration du nouveau compte. Vous pouvez ajouter ou supprimer des groupes du nouveau compte, activer le courriel et définir toute autre configuration de propriété, comme vous le feriez pour tout nouveau compte.

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

Déplacer une boîte aux lettres

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

Modifier les propriétés d'une boîte aux lettres

Vous pouvez modifier les propriétés des boîtes aux lettres Microsoft Exchange lors de la gestion des comptes utilisateurs associés. Les pouvoirs dont vous disposez déterminent les propriétés de boîte aux lettres que vous pouvez modifier.

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

Configurer les autorisations de sécurité d'une boîte aux lettres

Vous pouvez spécifier les comptes utilisateur, les groupes ou les ordinateurs auxquels vous souhaitez accorder ou refuser la possibilité d'envoyer et de recevoir des courriels à l'aide d'une boîte aux lettres Microsoft Exchange donnée. Ces paramètres vous permettent de sécuriser plus efficacement votre environnement Exchange. Vous ne pouvez pas modifier les autorisations de sécurité héritées.

REMARQUE : Lorsque vous gérez la sécurité d'une boîte aux lettres, les autorisations désactivées sont probablement des autorisations héritées.

Supprimer les autorisations de sécurité d'une boîte aux lettres

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

Configurer les droits d'une boîte aux lettres

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

REMARQUE : Lorsque vous gérez les droits d'une boîte aux lettres, les autorisations désactivées sont probablement des autorisations héritées.

Supprimer les droits d'une boîte aux lettres

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

Supprimer une boîte aux lettres

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

Ajouter ou modifier une adresse de courriel

Vous pouvez spécifier des adresses de courriel pour les boîtes aux lettres associées à des comptes utilisateurs dans votre domaine géré ou sous-arborescence gérée. Vous pouvez également attribuer des adresses de courriel à des comptes utilisateurs ne disposant pas encore de boîtes aux lettres. Lors de la gestion de boîtes aux lettres Microsoft Exchange, vous ne pouvez ajouter que les types d'adresse de courriel définis par vos stratégies de génération de mandataire.

Spécifier une adresse de réponse

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

Supprimer une adresse de courriel

Vous pouvez supprimer une adresse de courriel en la supprimant de la boîte aux lettres.

Spécifier les options de distribution

Vous pouvez spécifier les boîtes aux lettres que l'utilisateur peut utiliser pour envoyer des messages, définir des options de transfert et spécifier les limites de destinataire.

Spécifier les restrictions de distribution

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

Spécifier les limites de stockage

Vous pouvez spécifier des limites de stockage qui enverront des avertissements, en fonction de la taille d'une boîte aux lettres. Vous pouvez également spécifier des durées de conservation pour les éléments supprimés.

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

Vous pouvez vérifier l'état des déplacements de boîtes aux lettres et effectuer des actions sur ces déplacements, telles que l'effacement de l'état, l'annulation d'un déplacement et la reprise d'un déplacement qui a été interrompu.

Tâches de gestion pour les boîtes aux lettres Office 365

Cette section contient des informations pour l'administration des boîtes aux lettres Microsoft Office 365 dans la console de délégation et de configuration au moyen du nœud Gestion des comptes et des ressources et dans la console Web. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion des comptes d'utilisateurs, telles que la mise en suspens de litiges, la mise en place d'un réacheminement de courriel, etc.

IMPORTANT : DRA gère les boîtes aux lettres d'utilisateurs Office 365 ainsi que les boîtes aux lettres partagées, de salle et d'équipement migrées. Pour que DRA gère ces boîtes aux lettres, elles doivent être associées à un utilisateur sur site ou un utilisateur Azure géré par DRA. Les propriétés de la boîte aux lettres seront disponibles sur les pages de propriétés pour les utilisateurs associés.

Activer une suspension pour litige

Définissez une suspension pour litige sur une boîte aux lettres afin de conserver tout son contenu, y compris les éléments supprimés et les versions d'origine des éléments modifiés. L'activation de la suspension pour litige de la boîte aux lettres d'un utilisateur préserve également le contenu, s'il existe, dans la boîte aux lettres d'archivage de l'utilisateur. La suspension peut se poursuivre pendant une période déterminée ou jusqu'à ce que vous supprimiez la suspension pour litige de la boîte aux lettres.

Vous devez disposer d'une licence Exchange Online appropriée pour pouvoir effectuer une suspension pour litige. Pour configurer la fonction, utilisez l'onglet **Suspension pour litige** dans les propriétés de l'objet utilisateur.

Déléguer les autorisations de boîte aux lettres

Vous pouvez déléguer des autorisations de boîte aux lettres Office 365 en utilisant l'onglet Délégation de boîte aux lettres dans les propriétés de l'objet utilisateur. Il existe trois types d'autorisations que vous pouvez déléguer, l'envoi en tant que, l'envoi de la part de et l'accès complet. Les types d'autorisations qui peuvent être déléguées dépendent du type d'objet destinataire.

Afficher l'état de la boîte aux lettres des archives

Vous pouvez visualiser l'état de la boîte aux lettres d'archives d'un utilisateur et les statistiques des boîtes aux lettres d'archives telles que la limite de stockage et la limite d'avertissement. Lorsque la boîte aux lettres d'archives dépasse la limite d'avertissement des archives, l'utilisateur en est informé.

Afficher les statistiques d'utilisation des boîtes aux lettres

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

Configurer les 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.

Spécifier les options de distribution

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

Ajouter ou supprimer une adresse de courriel

Vous pouvez configurer plus d'une adresse courriel pour une boîte aux lettres utilisateur et spécifier l'adresse courriel principale. Vous pouvez également attribuer des adresses courriel à des comptes utilisateurs ne disposant pas de boîtes aux lettres.

Masquer l'adresse courriel

Vous pouvez indiquer si vous souhaitez que l'adresse courriel n'apparaisse pas dans la liste d'adresses.

Ajouter MailTip

Vous pouvez ajouter le texte informatif que vous souhaitez voir s'afficher lorsqu'un courriel est envoyé à l'utilisateur.

Attribuer des stratégies pour la boîte aux lettres

Vous pouvez affecter une stratégie de partage, une stratégie de conservation des courriels, une stratégie d'attribution de rôles ou une stratégie de carnet d'adresses à la boîte aux lettres.

Tâches de gestion pour les boîtes aux lettres de ressources

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

DRA prend en charge l'extension de l'interface utilisateur 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.

Créer une boîte aux lettres de ressources

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

Déplacer une boîte aux lettres de ressources vers un autre conteneur

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

Déplacer 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 boîtes aux lettres ou un serveur Exchange.

Cloner une boîte aux lettres de ressources

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

Renommer une boîte aux lettres de ressources

Vous pouvez renommer des boîtes aux lettres de ressources dans le domaine géré ou 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.

Ajouter une boîte aux lettres de ressources à un groupe

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

Supprimer une boîte aux lettres de ressources

Vous pouvez supprimer une boîte aux lettres de ressources dans le domaine géré ou la sous-arborescence gérée. La suppression d'une boîte aux lettres de ressources supprime également tous les messages de la boîte aux lettres et tout objet utilisateur désactivé associé à la boîte aux lettres de ressources. Si vous le souhaitez, vous pouvez annuler la suppression des objets utilisateurs désactivés lorsque vous supprimez la boîte aux lettres. Si vous supprimez un objet utilisateur associé à une boîte aux lettres de ressources, celle-ci est également supprimée.

Restaurer une boîte aux lettres de ressources

Vous pouvez restaurer une boîte aux lettres de ressources qui a été supprimée si la Corbeille de ce domaine est activée.

Modifier les propriétés d'une boîte aux lettres de ressources

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

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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 pour les boîtes aux lettres partagées

Les boîtes aux lettres partagées sont utiles aux administrateurs du service d'assistance et au personnel de l'assistance technique, car toutes les réponses peuvent être configurées pour aller dans une seule boîte aux lettres accessible à plusieurs utilisateurs. La boîte aux lettres doit être dans un domaine DRA géré pour lequel la stratégie Exchange est activée; vous devez par ailleurs disposer de pouvoirs pour gérer les boîtes aux lettres partagées.

Lorsque vous créez une boîte aux lettres partagée, vous pouvez déléguer aux utilisateurs deux types d'autorisations : Envoyer en tant que et Accès complet. Envoyer en tant que autorise la lecture et l'envoi de courriels. Vous pouvez déléguer des autorisations à la fois aux objets utilisateur et aux objets de groupe. Vous pouvez également spécifier des restrictions de distribution, des options de distribution, des limites de stockage, des autorisations de dossier et plusieurs autres options dans les propriétés de l’objet.

REMARQUE : Vous pouvez effectuer des tâches de gestion pour les boîtes aux lettres partagées uniquement par l'intermédiaire de la console Web.

Créer une boîte aux lettres partagée

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

Déplacer une boîte aux lettres partagée vers un autre conteneur

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

Déplacer 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.

Cloner une boîte aux lettres partagée

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

Renommer une boîte aux lettres partagée

Vous pouvez renommer des boîtes aux lettres partagées dans le domaine géré ou 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.

Supprimer une boîte aux lettres partagée

Vous pouvez supprimer une boîte aux lettres partagée dans le domaine géré ou la sous-arborescence gérée. Si la Corbeille est désactivée pour ce domaine, la suppression d'une boîte aux lettres partagée supprime définitivement celle-ci dans Active Directory. Si la Corbeille est activée pour ce domaine, la suppression d'une boîte aux lettres partagée déplace cette dernière vers la Corbeille.

La suppression d'une boîte aux lettres partagée supprime également tous les messages de la boîte aux lettres et tout objet utilisateur désactivé associé à la boîte aux lettres partagée. Si vous supprimez un objet utilisateur associé à une boîte aux lettres partagée, celle-ci est également supprimée.

Restaurer une boîte aux lettres partagée supprimée

Vous pouvez restaurer une boîte aux lettres partagée qui a été supprimée si la Corbeille de ce domaine est activée.

Créer une archive de boîte aux lettres partagée

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

Supprimer une archive de boîte aux lettres partagée

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

Modifier les propriétés d'une boîte aux lettres partagée

Vous pouvez modifier les propriétés des boîtes aux lettres partagées dans le domaine géré ou la sous-arborescence gérée. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier.

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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 pour les boîtes aux lettres liées

Les boîtes aux lettres liées sont utiles pour les modifications d'organisation importantes intervenant lors de fusions, d'acquisitions et de scissions d'entreprises, lorsque la migration des boîtes aux lettres est courante. Cette fonctionnalité permet de relier des boîtes aux lettres de différentes forêts Exchange afin d'éviter toute perturbation du courriel des utilisateurs. Les boîtes aux lettres doivent être dans des domaines DRA gérés pour lesquels la stratégie Exchange est activée; vous devez par ailleurs disposer de pouvoirs pour gérer les 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 dans la console Web. Vous pouvez créer une boîte aux lettres liée à partir de la barre d'outils d'un compte utilisateur sélectionné. Cette option est activée uniquement lorsque le domaine de l'utilisateur sélectionné dispose d'une approbation de forêt externe avec d'autres domaines gérés dans DRA. Seuls les comptes utilisateurs désactivés seront répertoriés lors de la recherche d'un compte avec lequel établir un lien dans un autre domaine DRA géré.

Créer une boîte aux lettres liée

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

Supprimer une boîte aux lettres liée

Vous pouvez supprimer une boîte aux lettres liée dans la barre d'outils d'un utilisateur sélectionné disposant d'une boîte aux lettres liée.

Modifier les propriétés d'une boîte aux lettres liée

Vous pouvez modifier les propriétés d'une boîte aux lettres liée à partir de l'onglet **Boîte aux lettres liée** dans les propriétés d'un utilisateur sélectionné.

Créer 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.

Supprimer une boîte aux lettres d'archivage liée

Vous pouvez supprimer une boîte aux lettres d'archivage liée dans la barre d'outils d'un utilisateur sélectionné disposant d'une boîte aux lettres d'archivage liée.

Restaurer une boîte aux lettres liée supprimée

Vous pouvez restaurer une boîte aux lettres liée qui a été supprimée si la Corbeille de ce domaine est activée.

Tâches de gestion pour les dossiers publics

Si l'administrateur DRA a créé des forêts de dossiers publics dans l'entreprise gérée DRA et vous a autorisé à gérer les dossiers publics dans DRA, alors vous pouvez créer des dossiers publics, modifier leurs propriétés et générer des rapports sur l'historique des modifications. La création et la modification de dossiers publics ne peuvent être effectuées que dans la console Web. Vous pouvez utiliser l'option de recherche pour interroger des dossiers publics. Pour obtenir de plus amples renseignements, consultez *« Recherche » page 39*.

Vous pouvez exécuter des tâches de dossiers publics à partir de l'onglet **Gestion** > **Dossiers publics**.

Créer un dossier public

Vous pouvez créer de nouveaux dossiers publics dans les domaines, les sous-arborescences et les boîtes aux lettres de dossiers publics spécifiés à l'aide de la console Web. Vous pouvez utiliser la boîte aux lettres par défaut pour le domaine sélectionné ou en choisir une autre.

Activer le courriel pour un dossier public

Vous pouvez activer le courriel pour un dossier public à l'aide de l'option **Activer le courriel** dans la barre d'outils de la liste. Cela vous permet d'associer des adresses de courriel au dossier public et de modifier les propriétés de celui-ci.

Désactiver le courriel pour un dossier public

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

Modifier les propriétés du dossier public

Après avoir activé le courriel sur un dossier public existant, vous pouvez afficher les statistiques du dossier et modifier les propriétés de ce dossier public. Dans ces propriétés, vous pouvez spécifier les options de distribution à l'utilisateur et les restrictions, les limites de taille et les avertissements de quota, les propriétés de messagerie, la durée limite de conservation, l'inclusion de modérateurs pour approuver les messages et les attributs personnalisés.

REMARQUE : Vous pouvez également mettre à jour certaines propriétés pour plusieurs dossiers publics lorsque plusieurs d'entre eux sont sélectionnés tels que les quotas de stockage.

Supprimer un dossier public

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

7 Gérer les 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 donné sur un ordinateur géré, vous pouvez rechercher cet objet ordinateur dans DRA, accéder à ses services à l'aide des propriétés de l'objet, puis redémarrer un service précis sur cet ordinateur à partir de DRA sans jamais avoir besoin de vous connecter à distance sur cet ordinateur.

Gestion des unités organisationnelles (UO)

Cette section vous guide dans l'administration des UO dans la console de délégation et de configuration au moyen du nœud Gestion des comptes et des ressources. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion des unités organisationnelles, telles que le déplacement d'une unité organisationnelle vers un autre conteneur.

REMARQUE : Vous pouvez gérer les UO uniquement à l'aide de la console de délégation et de configuration.

Modifier les propriétés d'une unité organisationnelle

Vous pouvez modifier les propriétés des unités organisationnelles. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour une unité organisationnelle du domaine géré ou de la sous-arborescence gérée.

Créer une unité organisationnelle

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

Cloner une unité organisationnelle

Vous pouvez créer une nouvelle unité organisationnelle en clonant une unité organisationnelle existante à partir du domaine géré ou de la sous-arborescence gérée. Vous pouvez également modifier des propriétés générales d'une nouvelle unité organisationnelle, telles que la description de l'unité organisationnelle. Le clonage d'une unité organisationnelle ne permet pas de cloner les objets qu'elle contient.

Ouvrir l'arborescence Active Directory à un emplacement d'unité organisationnelle

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

Déplacer une unité organisationnelle vers un autre conteneur

Vous pouvez déplacer une unité organisationnelle vers un autre conteneur du domaine géré. Lors de la gestion de la 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 l'unité organisationnelle déplacée, DRA ne vous permet pas de la déplacer.
- Vous pouvez également déplacer une unité organisationnelle en la faisant glisser vers le nouvel emplacement.

Supprimer une unité organisationnelle

Vous pouvez supprimer une unité organisationnelle dans le domaine géré ou la sous-arborescence gérée. Vous ne pouvez supprimer que des unités organisationnelles vides. Si une unité organisationnelle contient des objets, vous ne pouvez pas la supprimer. Pour supprimer une unité organisationnelle contenant des objets, supprimez d'abord tous les objets avant de supprimer l'unité organisationnelle.

Gérer des ordinateurs

DRA vous permet d'administrer les ordinateurs du domaine géré ou de la sous-arborescence gérée. Par exemple, vous pouvez ajouter ou supprimer des comptes d’ordinateur dans les domaines gérés, ainsi que 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 vous connecter à l'ordinateur de ce domaine et le configurer pour qu'il utilise ce compte d'ordinateur. Vous pouvez également afficher et modifier les propriétés des comptes d’ordinateur. DRA vous permet également d’arrêter un ordinateur et de synchroniser les contrôleurs de domaine d’un domaine géré.

REMARQUE

- Vous pouvez gérer les ordinateurs uniquement à l'aide de la console de délégation et de configuration.
- Vous ne pouvez pas gérer les contrôleurs de domaine cachés. Le cache de domaine n'inclut pas les contrôleurs de domaine masqués. Par conséquent, DRA n'affiche pas les ordinateurs du domaine caché dans les listes ou les fenêtres des propriétés.

Spécifier l'appartenance au groupe pour des ordinateurs

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

REMARQUE : DRA vous permet d'exporter les résultats de **Member Of** (Membre de) sous forme de fichier CSV. Pour exporter les résultats de **Membre de** à partir de la console Web, allez dans **Gestion** > **Recherche** et cliquez sur **Propriétés**. Naviguez vers l'onglet **Membre de** et 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.

Gérer les propriétés du compte d'ordinateur

Vous pouvez gérer les propriétés du compte d'ordinateur. Les pouvoirs dont vous disposez déterminent les propriétés que vous pouvez modifier pour un ordinateur du domaine géré ou de la sous-arborescence gérée.

Ajouter un ordinateur à un domaine

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

Supprimer 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.

Déplacer un ordinateur

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

Arrêter ou redémarrer un ordinateur

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

Réinitialiser le mot de passe du compte administrateur

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

Réinitialiser le compte d'ordinateur

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

Supprimer un compte d'ordinateur

Vous pouvez supprimer un compte d'ordinateur dans le domaine géré ou la sous-arborescence gérée. Si vous gérez un domaine Microsoft Windows, vous pouvez supprimer les comptes d'ordinateur contenant d'autres objets tels qu'une ressource partagée. Activez l'option **Force Delete** (Forcer la suppression) pour supprimer les objets ordinateur d'Active Directory. Cela permettra également de supprimer les objets enfants, y compris les imprimantes et les dossiers

partagés. Les ordinateurs supprimés et leurs objets associés sont déplacés vers la Corbeille de DRA. Si la Corbeille est désactivée lors de la suppression, les objets sont définitivement supprimés.

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

Désactiver un compte d'ordinateur

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

Activer un compte d'ordinateur

Vous pouvez activer un compte d'ordinateur dans le domaine géré ou 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.

Gérer les ressources informatiques

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.

Gérer les services

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

Gérer les propriétés d'un service

Vous pouvez gérer les propriétés des services s'exécutant sur des ordinateurs du domaine géré ou de la sous-arborescence gérée. Vous pouvez gérer des services tout en gérant d'autres ressources pour cet ordinateur.

Démarrer un service

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

Démarrer un service avec des paramètres

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

REMARQUE : Vous pouvez démarrer un service avec des paramètres uniquement au moyen de la console de délégation et de configuration.

Spécifier un type de démarrage de service

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

Spécifier un compte de connexion à un service

Vous pouvez modifier le compte de connexion à un service pour un compte autre que le compte système actuel. Vous pouvez spécifier le compte système local, un compte utilisateur spécifique ou un compte de service géré de groupe (gMSA) comme compte de connexion au service.

Redémarrer un service

Vous pouvez redémarrer un service exécuté sur un ordinateur du domaine géré ou de la sous-arborescence gérée.

Pour redémarrer un service, vous devez disposer des pouvoirs Arrêter un service et Démarrer un service ou être associé à un rôle qui contient ces pouvoirs, comme le rôle Démarrer un service et le rôle Arrêter un service.

Arrêter un service

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

Suspendre un service

Vous pouvez suspendre un service exécuté sur un ordinateur du domaine géré ou de la sous-arborescence gérée. La possibilité de suspendre un service ou non dépend du type de service. Par exemple, il est possible que vous ne puissiez pas suspendre un service comportant des services dépendants.

Reprendre un service

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

Gérer les imprimantes et les travaux d'impression

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

Un serveur d'impression est un ordinateur sur lequel une ou plusieurs imprimantes logiques sont installées. Une imprimante logique est définie sur l'ordinateur doté du pilote de périphérique d'imprimante. Une imprimante logique comprend le pilote d’impression, la file d'attente d'impression et les ports d’une imprimante. Le serveur d'impression associe les imprimantes logiques aux périphériques d'impression.

Une imprimante connectée est définie sur les ordinateurs à partir desquels les documents sont sélectionnés pour impression. Une imprimante connectée est une connexion à un partage d’impression sur le réseau. Par conséquent, vous pouvez gérer les imprimantes et les travaux d'impression à l'aide 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 une imprimante hébergée par un serveur en grappe.

REMARQUE : Vous pouvez gérer les imprimantes et les travaux d'impression uniquement au moyen de la console de délégation et de configuration.

Pour en savoir plus sur la gestion des imprimantes et des tâches d'impression, consultez les rubriques suivantes :

- « Tâches de gestion des imprimantes » page 90
- « Tâches de gestion des travaux d'impression » page 90
- « Tâches de gestion d'une imprimante publiée » page 91
- « Tâches de gestion des travaux d'impression pour les imprimantes publiées » page 92

Tâches de gestion des imprimantes

Vous pouvez gérer les imprimantes associées aux ordinateurs du domaine géré ou de la sous-arborescence gérée. DRA vous permet de gérer les imprimantes tout en gérant d'autres ressources pour cet ordinateur.

Cette section vous guide dans l'administration des imprimantes dans la console de délégation et de configuration au moyen du nœud Gestion des comptes et des ressources. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion d'imprimantes telles que l'arrêt de l'imprimante.

Gérer les propriétés de l'imprimante

Vous pouvez gérer les propriétés des imprimantes du domaine géré ou de la sous-arborescence gérée. DRA vous permet de gérer les imprimantes tout en gérant d'autres ressources pour cet ordinateur.

Suspendre une imprimante

Vous pouvez suspendre une imprimante associée à un ordinateur du domaine géré ou de la sous-arborescence gérée. DRA vous permet de gérer les imprimantes tout en gérant d'autres ressources pour cet ordinateur.

Reprendre les impressions sur une imprimante

Vous pouvez reprendre les impressions sur une imprimante associée à un ordinateur du domaine géré ou de la sous-arborescence gérée. DRA vous permet de gérer les imprimantes tout en gérant d'autres ressources pour cet ordinateur.

Tâches de gestion des travaux d'impression

Vous pouvez gérer les travaux d'impression associés aux imprimantes du domaine géré ou de la sous-arborescence gérée. Les travaux d'impression étant associés à une imprimante, vous pouvez gérer les travaux d'impression tout en gérant l'imprimante.

Cette section vous guide dans la gestion des travaux d'impression dans le nœud Gestion des comptes et des ressources de la console de délégation et de configuration. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion des travaux d'impression telles que l'annulation d'un travail d'impression.

Gérer les propriétés d'un travail d'impression

Vous pouvez modifier les propriétés d'un travail d'impression dans le cadre de votre processus de travail de gestion des imprimantes. Les travaux d'impression étant associés aux imprimantes, vous pouvez modifier le travail tout en gérant l'imprimante correspondante. Les propriétés de travail d'impression que vous pouvez modifier dépendent du type de pouvoirs dont vous disposez. Pour modifier les propriétés de travail d'impression, vous devez pouvoir accéder à l'imprimante et à l'ordinateur correspondants.

Suspendre un travail d'impression

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

Reprendre 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.

Redémarrer un travail d'impression

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

Annuler un travail d'impression

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

Tâches de gestion d'une imprimante publiée

Vous pouvez gérer des imprimantes publiées du domaine géré ou de la sous-arborescence gérée. Vous pouvez ajouter ou rechercher des imprimantes publiées dans Active Directory ou des imprimantes hébergées par un serveur de grappe.

Cette section vous explique comment administrer les imprimantes publiées dans le nœud Gestion des comptes et des ressources. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion d'imprimantes telles que l'arrêt de l'imprimante.

Gérer les propriétés d'une imprimante publiée

Vous pouvez gérer les propriétés des imprimantes publiées du domaine géré ou de la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées tout en gérant d'autres ressources.

Actualiser les informations d'une imprimante publiée

Vous pouvez actualiser les informations d'une imprimante publiée dans le domaine géré ou la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées tout en gérant d'autres ressources.

Suspendre une imprimante publiée

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

Reprendre les impressions sur une imprimante publiée

Vous pouvez reprendre les impressions sur une imprimante publiée qui a été suspendue dans le domaine géré ou la sous-arborescence gérée. DRA vous permet de gérer les imprimantes publiées tout en gérant d'autres ressources.

Déplacer 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 tout en gérant d'autres ressources.

Renommer une imprimante publiée

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

REMARQUE : Renommer une imprimante publiée dans Active Directory ne modifie pas le nom du partage d'imprimante de ressources ni ne répercute la modification de nom sur l'imprimante de ressources que vous souhaitez gérer. Par exemple, si le nom d'imprimante de la ressource est Emerald et que vous renommez celle-ci Ruby dans Active Directory, le nom de l'imprimante tel que le verra les autres utilisateurs, sera alors Ruby, mais le nom de l'imprimante de la ressource restera Emerald.

Tâches de gestion des travaux d'impression pour les imprimantes publiées

Vous pouvez gérer les travaux d'impression associés aux imprimantes publiées du domaine géré ou de la sous-arborescence gérée. Les travaux d'impression étant associés à une imprimante, vous pouvez gérer les travaux d'impression tout en gérant l'imprimante publiée.

Cette section vous explique comment administrer les imprimantes publiées dans le nœud Gestion des comptes et des ressources. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches de gestion des travaux d'impression telles que l'annulation d'un travail d'impression.

Gérer les propriétés d'un travail d'impression

Vous pouvez modifier les propriétés d'un travail d'impression dans le cadre de votre processus de travail de gestion des imprimantes publiées. Les travaux d'impression étant associés à une imprimante, vous pouvez gérer les travaux d'impression tout en gérant l'imprimante publiée correspondante. Les propriétés de travail d'impression que vous pouvez modifier dépendent du type de pouvoirs dont vous disposez. Pour modifier les propriétés de travail d'impression, vous devez pouvoir accéder à l'imprimante publiée correspondante.

Suspendre un travail d'impression

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

Reprendre un travail d'impression

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

Redémarrer un travail d'impression

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

Annuler un travail d'impression

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

Gérer les partages

Un partage est un moyen de rendre des ressources, telles que des fichiers ou des imprimantes, accessibles aux autres utilisateurs du réseau. Chaque partage possède un nom de partage qui fait référence à un dossier partagé sur le serveur. DRA gère les partages uniquement sur les ordinateurs des domaines gérés. Pour gérer efficacement les partages, le compte d'accès doit disposer des autorisations d'administrateur, par exemple en étant membre du groupe Administrateurs locaux, sur tous les ordinateurs sur lesquels vous souhaitez gérer les ressources. Pour attribuer ces autorisations, ajoutez le compte d'accès au groupe natif des administrateurs de domaine du domaine de l'ordinateur.

REMARQUE : Vous pouvez gérer des partages uniquement à l'aide de la console de délégation et de configuration.

Gérer les propriétés de partage

Vous pouvez gérer les propriétés des partages du domaine géré ou de la sous-arborescence gérée. DRA vous permet de gérer les partages tout en gérant d'autres ressources pour cet ordinateur.

Créer un partage

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

Cloner un partage

Vous pouvez cloner un partage pour un ordinateur du domaine géré ou de la sous-arborescence gérée. En clonant un partage, vous pouvez créer rapidement des partages basés sur d'autres partages ayant des propriétés similaires. Cette flexibilité vous permet d'appliquer des paramètres cohérents pour tous les partages que vous créez dans un domaine donné.

Lorsque vous clonez un partage, DRA remplit l'assistant Cloner un partage avec les valeurs du partage sélectionné. Vous pouvez également modifier les propriétés du nouveau partage.

Supprimer un partage

Vous pouvez supprimer des partages des ordinateurs du domaine géré ou de la sous-arborescence gérée.

Gérer des utilisateurs connectés

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

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

Déconnecter un utilisateur

Vous pouvez déconnecter un utilisateur connecté d'un ordinateur du domaine géré ou de la sous-arborescence gérée. Vous devez pouvoir accéder à l'ordinateur et à cette session ouverte. La déconnexion d'un utilisateur met fin à la session ouverte.

Actualiser la liste des utilisateurs connectés

Pour vous assurer que les informations affichées sont les plus récentes sur les sessions ouvertes sur un ordinateur, actualisez manuellement la liste des utilisateurs connectés. Vous devez pouvoir accéder à l'ordinateur et à cette session ouverte.

Gérer des périphériques

Un périphérique est un équipement connecté à un réseau tel qu'un ordinateur, une imprimante, un modem ou tout autre équipement périphérique.

Bien qu'un périphérique puisse être 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 matériel donné 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 des autorisations d'administrateur, par exemple en étant membre du groupe Administrateurs locaux, sur tous les ordinateurs sur lesquels vous souhaitez gérer des périphériques. Pour attribuer ces autorisations, ajoutez le compte d'accès au groupe natif des administrateurs de domaine du domaine de l'ordinateur.

Gérer les propriétés d'un périphérique

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

Démarrer un périphérique

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

Arrêter un périphérique

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

Gérer des journaux d'événements

Un événement est une occurrence importante du système ou de l'application. Le système d'exploitation Windows enregistre des informations sur les événements dans des fichiers de journal des événements. Plusieurs journaux d'événements peuvent être stockés sur chaque ordinateur. Utilisez l'observateur d'événements Windows natif pour afficher les journaux d'événements. DRA gère les journaux d'événements uniquement sur les ordinateurs des domaines gérés.

DRA enregistre les opérations lancées par l'utilisateur dans l'archive de journal, qui est un espace de stockage sécurisé. Vous avez également la possibilité de faire en sorte que DRA enregistre également les opérations lancées par l'utilisateur dans le journal des événements Windows en plus des informations enregistrées dans l'archive du journal DRA. Pour obtenir de plus amples renseignements, consultez Comprendre les dates et les heures.

Types de journal des événements

Les ordinateurs exécutant Microsoft Windows enregistrent des informations supplémentaires dans divers journaux. Les journaux sont brièvement décrits comme suit :

Type de journal	Description
ADAM	Enregistre les événements enregistrés par l'espace de stockage ADAM.
Application	Enregistre les événements enregistrés par une application sur l'ordinateur tels que le démarrage ou l'échec d'un service. Par exemple, DRA stocke les événements dans le journal des applications.
Service de répertoire	Enregistre les événements liés aux contrôleurs de domaine assurant la maintenance de la base de données de sécurité.
Service de réplication de fichiers	Enregistre les événements liés aux services de réplication de fichiers fournis par le système d'exploitation.
Sécurité	Enregistre les événements comprenant les tentatives de connexion, l'accès aux fichiers et aux répertoires et les modifications de stratégie de sécurité basées sur les options de stratégie d'audit.
Système	Enregistre les événements enregistrés par les composants du système Windows tels que l'échec du démarrage ou de l'arrêt d'un pilote ou de services.

Tâches de gestion du journal des événements

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

AVERTISSEMENT : Soyez prudent lorsque vous modifiez votre registre Windows. S'il y a une erreur dans votre registre, votre ordinateur peut devenir non fonctionnel. Si une erreur se produit, vous pouvez restaurer le registre à son état lors du dernier démarrage de votre ordinateur. Pour obtenir de plus amples renseignements, consultez l'aide de l'éditeur de registre Windows.

Vous pouvez spécifier la taille maximale d'un fichier journal des événements et ce qu'il advient d'un journal des événements lorsqu'il est plein. La fenêtre des propriétés affiche également le nom du journal, le chemin d'accès au fichier journal et le nom du fichier, la date de création du journal, de sa dernière modification et de son dernier accès. Si vous choisissez de sauvegarder le fichier journal, DRA enregistre le journal des événements avec un nom de fichier unique à un emplacement standard sur l'ordinateur sélectionné.

DRA vous permet de gérer les journaux d'événements tout en gérant d'autres ressources pour cet ordinateur. Avec les pouvoirs appropriés, vous pouvez effectuer diverses tâches telles que la modification des propriétés du journal des événements.

Gérer les propriétés du journal des événements

Vous pouvez modifier les propriétés du journal des événements pour un ordinateur donné.

Afficher les entrées du journal des événements

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

Effacer le journal des événements

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

Gérer les fichiers ouverts

Un fichier ouvert est une connexion à des ressources partagées telles que des fichiers ou des canaux. 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 du domaine et de la sous-arborescence gérés. Étant donné que les fichiers ouverts sont associés à un ordinateur, vous pouvez gérer les fichiers ouverts tout en gérant d'autres ressources pour cet ordinateur. Par exemple, vous pouvez vouloir fermer les fichiers ouverts lorsque vous arrêtez un système ou installez un nouveau périphérique ou un service. Vous pouvez également contrôler les fichiers auxquels les utilisateurs accèdent le plus souvent, ce qui vous permet de mieux évaluer la sécurité des fichiers.

REMARQUE : Vous pouvez gérer l'ouverture des fichiers uniquement à l'aide de la console de délégation et de configuration.

Fermer un fichier

Vous pouvez fermer les fichiers ouverts sur des ressources connectées au réseau. C'est une bonne idée d'informer les utilisateurs lorsque vous avez l'intention de fermer des fichiers ouverts. Ils peuvent avoir besoin de temps pour sauvegarder leurs données. Pour fermer un fichier ouvert, vous devez pouvoir accéder à l'ordinateur correspondant.

Actualiser la liste des fichiers ouverts

Pour vous assurer que les informations affichées sont les plus récentes sur les sessions ouvertes sur un ordinateur, actualisez manuellement la liste des utilisateurs connectés. Pour actualiser la liste des fichiers ouverts, vous devez pouvoir accéder à l'ordinateur correspondant.

8 Gérer la Corbeille

La Corbeille fournit un filet de sécurité en vous permettant de supprimer temporairement les comptes utilisateurs, les groupes, les contacts et les comptes d'ordinateurs. Vous pouvez ensuite restaurer ces objets à leur état d'origine avec toutes les données telles que les SID, les listes de contrôle d'accès et les appartenances à un groupe ou supprimer définitivement ces objets. Cette flexibilité offre un moyen plus sûr de gérer les comptes d'utilisateurs, les groupes, les contacts et les comptes d'ordinateur. Vous pouvez utiliser l'option de recherche pour rechercher les objets requis. Pour obtenir de plus amples renseignements, consultez *Rechercher des objets*.

Restaurer un objet de la Corbeille

Vous pouvez restaurer des objets supprimés dans les conteneurs à partir desquels vous les avez supprimés. DRA restaure ces objets à leur état d'origine avec toutes les données telles que les SID, les listes de contrôle d'accès et les appartenances à un groupe. Un objet peut être un compte utilisateur, un groupe, un contact, un groupe dynamique, une boîte aux lettres de ressources, un groupe de distribution dynamique ou un compte d'ordinateur.

Restaurer tous les objets

Vous pouvez restaurer tous les objets de la Corbeille pour un domaine géré. Vous pouvez restaurer des objets de la Corbeille pour un domaine précis ou pour tous les domaines gérés. Pour restaurer des objets de la Corbeille pour un domaine précis, la Corbeille doit être activée pour ce domaine.

Supprimer un objet de la Corbeille

Vous pouvez supprimer définitivement des objets de la Corbeille d'un domaine géré. Une fois que vous avez supprimé un objet de la Corbeille, vous ne pouvez pas restaurer l'objet. Un objet peut être un compte utilisateur, un groupe, un contact, un groupe dynamique, une boîte aux lettres de ressources, un groupe de distribution dynamique ou un compte d'ordinateur.

Vider la Corbeille

Vous pouvez vider la Corbeille d'un domaine géré. Le fait de vider la corbeille supprime définitivement tous les objets qui se trouvent dans celle-ci. Vous pouvez vider la Corbeille pour un domaine précis ou pour tous les domaines gérés. Pour vider la Corbeille pour un domaine précis, elle doit être activée pour ce domaine. Une fois la Corbeille vidée, vous ne pouvez pas restaurer les objets supprimés.