Red Hat Enterprise Linux 9

Intégration directe des systèmes RHEL avec Windows Active Directory

Joindre des hôtes RHEL à AD et accéder aux ressources dans AD

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Intégration directe des systèmes RHEL avec Windows Active Directory

Joindre des hôtes RHEL à AD et accéder aux ressources dans AD

Notice légale

Résumé

Les administrateurs peuvent joindre les hôtes Red Hat Enterprise Linux (RHEL) à un domaine Active Directory (AD) en utilisant le System Security Services Daemon (SSSD) ou le service Samba Winbind pour accéder aux ressources AD. Il est également possible d'accéder aux ressources AD sans intégration de domaine en utilisant un compte de service géré (MSA).

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

Dans le domaine de la gestion de l'identité, les remplacements terminologiques prévus sont les suivants :

- ***block list*** remplace *blacklist*
- ***allow list*** remplace *whitelist*
- ***secondary*** remplace *slave*
- Le mot *master* sera remplacé par des termes plus précis, en fonction du contexte :
  - ***IdM server*** remplace *IdM master*
  - ***CA renewal server*** remplace *CA renewal master*
  - ***CRL publisher server*** remplace *CRL master*
  - ***multi-supplier*** remplace *multi-master*

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. CONNEXION DIRECTE DES SYSTÈMES RHEL À AD À L'AIDE DE SSSD

Deux composants sont nécessaires pour connecter un système RHEL à Active Directory (AD). L'un des composants, SSSD, interagit avec la source centrale d'identité et d'authentification, et l'autre, **realmd**, détecte les domaines disponibles et configure les services système RHEL sous-jacents, en l'occurrence SSSD, pour qu'ils se connectent au domaine.

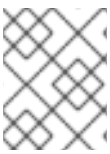
Cette section décrit l'utilisation du System Security Services Daemon (SSSD) pour connecter un système RHEL à Active Directory (AD).

- Aperçu de l'intégration directe à l'aide de SSSD
- Plateformes Windows prises en charge pour une intégration directe
- Assurer la prise en charge des types de chiffrement courants dans AD et RHEL
- Connexion directe à AD
- Comment le fournisseur AD gère les mises à jour dynamiques du DNS
- Modification des paramètres DNS dynamiques pour le fournisseur AD
- Comment le fournisseur AD gère les domaines de confiance
- Remplacer l'autodécouverte des sites Active Directory par SSSD
- commandes de domaine

1.1. APERÇU DE L'INTÉGRATION DIRECTE À L'AIDE DE SSSD

SSSD permet d'accéder à un annuaire d'utilisateurs pour l'authentification et l'autorisation par le biais d'une structure commune avec mise en cache des utilisateurs pour permettre les connexions hors ligne. SSSD est hautement configurable ; il fournit des modules d'authentification enfichables (PAM) et l'intégration du service de commutation de noms (NSS), ainsi qu'une base de données pour stocker les utilisateurs locaux ainsi que des données d'utilisateur étendues récupérées à partir d'un serveur central. SSSD est le composant recommandé pour connecter un système RHEL à l'un des types de serveurs d'identité suivants :

- Active Directory
- Gestion des identités (IdM) dans RHEL
- Tout serveur LDAP ou Kerberos générique



NOTE

L'intégration directe avec SSSD ne fonctionne par défaut qu'au sein d'une seule forêt AD.

La manière la plus pratique de configurer SSSD pour intégrer directement un système Linux à AD est d'utiliser le service **realmd**. Il permet aux appelants de configurer l'authentification du réseau et l'appartenance à un domaine de manière standard. Le service **realmd** découvre automatiquement les informations sur les domaines et les zones accessibles et ne nécessite pas de configuration avancée pour rejoindre un domaine ou une zone.

Vous pouvez utiliser SSSD pour l'intégration directe et indirecte avec AD et il vous permet de passer d'une approche d'intégration à l'autre. L'intégration directe est un moyen simple d'introduire les systèmes RHEL dans un environnement AD. Toutefois, à mesure que le nombre de systèmes RHEL augmente, vos déploiements nécessitent généralement une meilleure gestion centralisée des stratégies liées à l'identité, telles que le contrôle d'accès basé sur l'hôte, sudo ou les mappages d'utilisateurs SELinux. Au départ, vous pouvez maintenir la configuration de ces aspects des systèmes RHEL dans des fichiers de configuration locaux. Cependant, avec un nombre croissant de systèmes, la distribution et la gestion des fichiers de configuration sont plus faciles avec un système de provisionnement tel que Red Hat Satellite. Lorsque l'intégration directe n'est plus adaptée, vous devez envisager l'intégration indirecte. Pour plus d'informations sur le passage de l'intégration directe (les clients RHEL sont dans le domaine AD) à l'intégration indirecte (IdM avec confiance en AD), voir Déplacement des clients RHEL du domaine AD vers le serveur IdM.

Pour plus d'informations sur le type d'intégration qui convient à votre cas d'utilisation, voir Décider entre l'intégration indirecte et l'intégration directe.

Ressources supplémentaires

- La page de manuel **realm(8)**.
- La page de manuel **sssd-ad(5)**.
- La page de manuel **sssd(8)**.

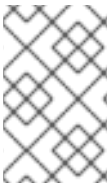
1.2. PLATEFORMES WINDOWS PRISES EN CHARGE POUR UNE INTÉGRATION DIRECTE

Vous pouvez intégrer directement votre système RHEL aux forêts Active Directory qui utilisent les niveaux fonctionnels de forêt et de domaine suivants :

- Gamme de niveaux fonctionnels de la forêt : Windows Server 2008 - Windows Server 2016
- Gamme de niveaux fonctionnels du domaine : Windows Server 2008 - Windows Server 2016

L'intégration directe a été testée sur les systèmes d'exploitation suivants :

- Windows Server 2022 (RHEL 9.1 et supérieur)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2



NOTE

Windows Server 2019 et Windows Server 2022 n'introduisent pas de nouveau niveau fonctionnel. Le niveau fonctionnel le plus élevé que Windows Server 2019 et Windows Server 2022 utilisent est Windows Server 2016.

1.3. ASSURER LA PRISE EN CHARGE DES TYPES DE CHIFFREMENT COURANTS DANS AD ET RHEL

Par défaut, SSSD prend en charge les types de chiffrement Kerberos RC4, AES-128 et AES-256.

Le cryptage RC4 a été déprécié et désactivé par défaut, car il est considéré comme moins sûr que les nouveaux types de cryptage AES-128 et AES-256. En revanche, les informations d'identification des utilisateurs d'Active Directory (AD) et les liens de confiance entre les domaines AD prennent en charge le cryptage RC4 et peuvent ne pas prendre en charge les types de cryptage AES.

En l'absence de types de chiffrement communs, la communication entre les hôtes RHEL et les domaines AD risque de ne pas fonctionner, ou certains comptes AD risquent de ne pas pouvoir s'authentifier. Pour remédier à cette situation, modifiez l'une des configurations suivantes :

Activer la prise en charge du cryptage AES dans Active Directory (option recommandée)

Pour s'assurer que les trusts entre les domaines AD dans une forêt AD prennent en charge les types de cryptage AES fort, voir l'article Microsoft suivant : AD DS : Security : Erreur Kerberos "Unsupported etype" lors de l'accès à une ressource dans un domaine de confiance

Activer la prise en charge de RC4 dans RHEL

Sur chaque hôte RHEL où l'authentification contre les contrôleurs de domaine AD a lieu :

a. Utilisez la commande **update-crypto-policies** pour activer la sous-politique cryptographique **AD-SUPPORT-LEGACY** en plus de la politique cryptographique **DEFAULT**.

```
[root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT-LEGACY
Setting system policy to DEFAULT:AD-SUPPORT-LEGACY
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

b. Redémarrer l'hôte.

Ressources supplémentaires

- Voir Utilisation de stratégies cryptographiques à l'échelle du système .

1.4. CONNEXION DIRECTE À AD

Le System Security Services Daemon (SSSD) est le composant recommandé pour connecter un système Red Hat Enterprise Linux (RHEL) à Active Directory (AD). Cette section décrit comment s'intégrer directement à AD en utilisant le mappage d'ID, qui est la valeur par défaut de SSSD, ou en utilisant des attributs POSIX.

- Découvrir et rejoindre un domaine AD à l'aide de SSSD
- Options pour l'intégration avec AD : utiliser le mappage d'ID ou les attributs POSIX
- Connexion à AD à l'aide d'attributs POSIX définis dans Active Directory
- Connexion à plusieurs domaines dans différentes forêts AD avec SSSD

1.4.1. Découvrir et rejoindre un domaine AD à l'aide de SSSD

Cette procédure décrit comment découvrir un domaine AD et connecter un système RHEL à ce domaine à l'aide de SSSD.

Conditions préalables

- Assurez-vous que les ports suivants des contrôleurs de domaine AD sont ouverts et accessibles à l'hôte RHEL.

Tableau 1.1. Ports requis pour l'intégration directe de systèmes Linux dans AD à l'aide de SSSD

Service	Port	Protocol	Notes
DNS	53	UDP et TCP	
LDAP	389	UDP et TCP	
Samba	445	UDP et TCP	Pour les objets de stratégie de groupe AD (GPO)
Kerberos	88	UDP et TCP	
Kerberos	464	UDP et TCP	Utilisé par **kadmin** pour définir et modifier un mot de passe
Catalogue global LDAP	3268	TCP	Si l'option **id_provider = ad** est utilisée
NTP	123	UDP	En option

- Assurez-vous que vous utilisez le serveur du contrôleur de domaine AD pour le DNS.
- Vérifiez que l'heure des deux systèmes est synchronisée. Cela permet à Kerberos de fonctionner correctement.

Procédure

1. Install the following packages:

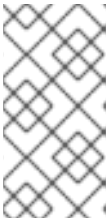
```
# dnf install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. Pour afficher les informations relatives à un domaine spécifique, exécutez **realm discover** et ajoutez le nom du domaine que vous souhaitez découvrir :

```
# realm discover ad.example.com
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
  configured: no
  server-software: active-directory
  client-software: sssd
```

```
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common
```

Le système **realmd** utilise les recherches DNS SRV pour trouver automatiquement les contrôleurs de domaine de ce domaine.



NOTE

Le système **realmd** peut découvrir les domaines Active Directory et Identity Management. Si les deux domaines existent dans votre environnement, vous pouvez limiter les résultats de la découverte à un type de serveur spécifique à l'aide de l'option **--server-software=active-directory**.

3. Configurez le système RHEL local à l'aide de la commande **realm join**. La suite **realmd** édite automatiquement tous les fichiers de configuration requis. Par exemple, pour un domaine nommé **ad.example.com**:

```
# realm join ad.example.com
```

Verification steps

- Affiche les détails d'un utilisateur AD, tel que l'utilisateur administrateur :

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:1450400500:1450400513:Administrator:/home/administrator
@ad.example.com:/bin/bash
```

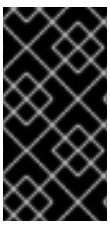
Ressources supplémentaires

- Voir la page de manuel **realm(8)**.
- Voir la page de manuel **nmcli(1)**.

1.4.2. Options pour l'intégration avec AD : utiliser le mappage d'ID ou les attributs POSIX

Les systèmes Linux et Windows utilisent des identifiants différents pour les utilisateurs et les groupes :

- Linux utilise *user IDs* (UID) et *group IDs* (GID). Voir Introduction à la gestion des comptes d'utilisateurs et de groupes sur *Configuring Basic System Settings*. Les UID et GID de Linux sont conformes à la norme POSIX.
- Windows utilise *security IDs* (SID).



IMPORTANT

Après avoir connecté un système RHEL à AD, vous pouvez vous authentifier avec votre nom d'utilisateur et votre mot de passe AD. Ne créez pas d'utilisateur Linux portant le même nom qu'un utilisateur Windows, car les noms en double pourraient provoquer un conflit et interrompre le processus d'authentification.

Pour vous authentifier sur un système RHEL en tant qu'utilisateur AD, vous devez disposer d'un UID et d'un GID. SSSD offre la possibilité de s'intégrer à AD en utilisant le mappage d'ID ou les attributs POSIX. Par défaut, le mappage d'ID est utilisé.

Générer automatiquement de nouveaux UID et GID pour les utilisateurs AD

SSSD peut utiliser le SID d'un utilisateur AD pour générer algorithmiquement des ID POSIX dans un processus appelé *ID mapping*. Le mappage d'ID crée une correspondance entre les SID dans AD et les ID sur Linux.

- Lorsque SSSD détecte un nouveau domaine AD, il lui attribue une série d'identifiants disponibles.
- Lorsqu'un utilisateur AD se connecte pour la première fois à une machine cliente SSSD, SSSD crée une entrée pour l'utilisateur dans le cache SSSD, y compris un UID basé sur le SID de l'utilisateur et la plage d'ID pour ce domaine.
- Étant donné que les identifiants d'un utilisateur AD sont générés de manière cohérente à partir du même SID, l'utilisateur possède les mêmes UID et GID lorsqu'il se connecte à n'importe quel système Red Hat Enterprise Linux.

Voir Découvrir et rejoindre un domaine AD à l'aide de SSSD .

NOTE

Lorsque tous les systèmes clients utilisent SSSD pour mapper les SID avec les ID Linux, le mappage est cohérent. Si certains clients utilisent des logiciels différents, choisissez l'une des options suivantes :

- Veillez à ce que le même algorithme de mappage soit utilisé sur tous les clients.
- Utiliser les attributs POSIX explicites définis dans AD.

Utiliser les attributs POSIX définis dans AD

AD peut créer et stocker des attributs POSIX, tels que **uidNumber**, **gidNumber**, **unixHomeDirectory** ou **loginShell**.

Lors de l'utilisation du mappage d'ID décrit ci-dessus, SSSD crée de nouveaux UID et GID, qui remplacent les valeurs définies dans AD. Pour conserver les valeurs définies dans AD, vous devez désactiver le mappage d'ID dans SSSD.

Voir Connexion à AD à l'aide d'attributs POSIX définis dans Active Directory .

1.4.3. Connexion à AD à l'aide d'attributs POSIX définis dans Active Directory

Pour de meilleures performances, publiez les attributs POSIX dans le catalogue global AD. Si les attributs POSIX ne sont pas présents dans le catalogue global, SSSD se connecte aux contrôleurs de domaine individuels directement sur le port LDAP.

Conditions préalables

- Assurez-vous que les ports suivants de l'hôte RHEL sont ouverts et accessibles aux contrôleurs de domaine AD.

Tableau 1.2. Ports requis pour l'intégration directe de systèmes Linux dans AD à l'aide de SSSD

Service	Port	Protocol	Notes
DNS	53	UDP et TCP	
LDAP	389	UDP et TCP	
Kerberos	88	UDP et TCP	
Kerberos	464	UDP et TCP	Utilisé par kadmin pour définir et modifier un mot de passe
Catalogue global LDAP	3268	TCP	Si l'option **id_provider = ad** est utilisée
NTP	123	UDP	En option

- Assurez-vous que vous utilisez le serveur du contrôleur de domaine AD pour le DNS.
- Vérifiez que l'heure des deux systèmes est synchronisée. Cela permet à Kerberos de fonctionner correctement.

Procédure

1. Install the following packages:

```
# dnf install realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. Configurez le système RHEL local avec le mappage d'ID désactivé à l'aide de la commande **realm join** avec l'option **--automatic-id-mapping=no**. La suite **realmd** édite automatiquement tous les fichiers de configuration requis. Par exemple, pour un domaine nommé **ad.example.com**:

```
# realm join --automatic-id-mapping=no ad.example.com
```

3. Si vous avez déjà rejoint un domaine, vous pouvez désactiver manuellement le mappage d'identifiants dans SSSD :

   a. Open the **/etc/sssd/sssd.conf** file.

   b. Dans la section Domaine AD, ajoutez le paramètre **ldap_id_mapping = false**.

   c. Supprimez les caches SSSD :

```
rm -f /var/lib/sss/db/*
```

   d. Restart SSSD:

```
systemctl restart sssd
```

SSSD utilise désormais les attributs POSIX d'AD, au lieu de les créer localement.

NOTE

Vous devez avoir configuré les attributs POSIX appropriés (**uidNumber**, **gidNumber**, **unixHomeDirectory**, et **loginShell**) pour les utilisateurs dans AD.

Verification steps

- Affiche les détails d'un utilisateur AD, tel que l'utilisateur administrateur :

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:10000:10000:Administrator:/home/Administrator:/bin/bash
```

Ressources supplémentaires

- Pour plus de détails sur le mappage d'ID et le paramètre **ldap_id_mapping**, voir la page de manuel **sssd-ldap(8)**.

1.4.4. Connexion à plusieurs domaines dans différentes forêts AD avec SSSD

Vous pouvez utiliser un compte de service géré (MSA) d'Active Directory (AD) pour accéder à des domaines AD situés dans des forêts différentes où il n'y a pas de confiance entre elles.

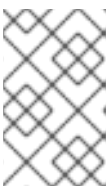
Voir Accès à AD avec un compte de service géré .

1.5. COMMENT LE FOURNISSEUR AD GÈRE LES MISES À JOUR DYNAMIQUES DU DNS

Active Directory (AD) maintient activement ses enregistrements DNS en temporisant (*aging*) et en supprimant (*scavenging*) les enregistrements inactifs.

Par défaut, le service SSSD actualise l'enregistrement DNS d'un client RHEL aux intervalles suivants :

- Chaque fois que le fournisseur d'identité est mis en ligne.
- Chaque fois que le système RHEL redémarre.
- À l'intervalle spécifié par l'option **dyndns_refresh_interval** dans le fichier de configuration **/etc/sssd/sssd.conf**. La valeur par défaut est **86400** secondes (24 heures).



NOTE

Si vous définissez l'option **dyndns_refresh_interval** sur le même intervalle que le bail DHCP, vous pouvez mettre à jour l'enregistrement DNS après le renouvellement du bail IP.

SSSD envoie des mises à jour DNS dynamiques au serveur AD en utilisant Kerberos/GSSAPI pour DNS (GSS-TSIG). Cela signifie qu'il suffit d'activer les connexions sécurisées à AD.

Ressources supplémentaires

- La page de manuel **sssd-ad(5)**.

1.6. MODIFICATION DES PARAMÈTRES DNS DYNAMIQUES POUR LE FOURNISSEUR AD

Le service System Security Services Daemon (SSSD) rafraîchit l'enregistrement DNS d'un client Red Hat Enterprise Linux (RHEL) joint à un environnement AD à des intervalles par défaut. La procédure suivante permet d'ajuster ces intervalles.

Conditions préalables

- Vous avez joint un hôte RHEL à un environnement Active Directory avec le service SSSD.
- Vous devez disposer des autorisations **root** pour modifier le fichier de configuration **/etc/sssd/sssd.conf**.

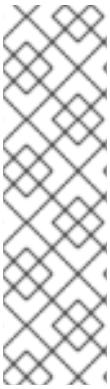
Procédure

1. Ouvrez le fichier de configuration **/etc/sssd/sssd.conf** dans un éditeur de texte.
2. Ajoutez les options suivantes à la section **[domain]** pour votre domaine AD afin de définir l'intervalle de rafraîchissement des enregistrements DNS sur 12 heures, de désactiver la mise à jour des enregistrements PTR et de définir la durée de vie de l'enregistrement DNS (TTL) sur 1 heure.

```
[domain/ad.example.com]
id_provider = ad
...
dyndns_refresh_interval = 43200
dyndns_update_ptr = false
dyndns_ttl = 3600
```

3. Enregistrez et fermez le fichier de configuration **/etc/sssd/sssd.conf**.
4. Redémarrez le service SSSD pour charger les modifications de configuration.

```
[root@client ~]# systemctl restart sssd
```



NOTE

Vous pouvez désactiver les mises à jour dynamiques du DNS en définissant l'option **dyndns_update** du fichier **sssd.conf** sur **false**:

```
[domain/ad.example.com]
id_provider = ad
...

dyndns_update = false
```

Ressources supplémentaires

- Comment le fournisseur AD gère les mises à jour dynamiques du DNS
- **sssd-ad(5)** page de manuel

1.7. COMMENT LE FOURNISSEUR AD GÈRE LES DOMAINES DE CONFIANCE

Cette section décrit la manière dont SSSD gère les domaines de confiance si vous définissez l'option **id_provider = ad** dans le fichier de configuration **/etc/sssd/sssd.conf**.

- SSSD ne prend en charge que les domaines d'une seule forêt AD. Si SSSD nécessite un accès à plusieurs domaines de plusieurs forêts, envisagez d'utiliser IPA with trusts (de préférence) ou le service **winbindd** au lieu de SSSD.
- Par défaut, SSSD découvre tous les domaines de la forêt et, si une demande d'objet dans un domaine de confiance arrive, SSSD tente de la résoudre.
  Si les domaines de confiance ne sont pas joignables ou sont géographiquement éloignés, ce qui les rend lents, vous pouvez définir le paramètre **ad_enabled_domains** dans **/etc/sssd/sssd.conf** pour limiter les domaines de confiance à partir desquels SSSD résout les objets.
- Par défaut, vous devez utiliser des noms d'utilisateur pleinement qualifiés pour résoudre les problèmes des utilisateurs des domaines de confiance.

Ressources supplémentaires

- La page de manuel **sssd.conf(5)**.

1.8. REMPLACER L'AUTODÉCOUVERTE DES SITES ACTIVE DIRECTORY PAR SSSD

Les forêts Active Directory (AD) peuvent être très étendues, avec de nombreux contrôleurs de domaine, domaines, domaines enfants et sites physiques différents. AD utilise le concept de **sites** pour identifier l'emplacement physique de ses contrôleurs de domaine. Cela permet aux clients de se connecter au contrôleur de domaine le plus proche géographiquement, ce qui augmente les performances du client.

Cette section décrit comment SSSD utilise la découverte automatique pour trouver un site AD auquel se connecter, et comment vous pouvez remplacer la découverte automatique et spécifier un site manuellement.

1.8.1. Comment SSSD gère l'autodécouverte des sites AD

Par défaut, les clients SSSD utilisent la découverte automatique pour trouver leur site AD et se connecter au contrôleur de domaine le plus proche. Le processus se compose des étapes suivantes :

1. SSSD effectue une requête SRV pour trouver les contrôleurs de domaine (DC) dans le domaine. SSSD lit le domaine de découverte à partir des options **dns_discovery_domain** ou **ad_domain** du fichier de configuration SSSD.
2. SSSD effectue des pings LDAP sans connexion (CLDAP) vers ces DC en 3 lots pour éviter de pinger trop de DC et d'éviter les dépassements de temps dus aux DC inaccessibles. Si le SSSD reçoit des informations sur le site et la forêt au cours de l'un de ces lots, il ignore les autres lots.

3. SSSD crée et enregistre une liste de serveurs spécifiques au site et de serveurs de secours.

1.8.2. Remplacer l'autodécouverte des sites AD

Pour remplacer le processus de découverte automatique, spécifiez le site AD auquel vous souhaitez que le client se connecte en ajoutant l'option **ad_site** à la section **[domain]** du fichier **/etc/sssd/sssd.conf**. Cet exemple configure le client pour qu'il se connecte au site AD **ExampleSite**.

Conditions préalables

- Vous avez joint un hôte RHEL à un environnement Active Directory à l'aide du service SSSD.
- Vous pouvez vous authentifier en tant qu'utilisateur **root** afin de pouvoir modifier le fichier de configuration **/etc/sssd/sssd.conf**.

Procédure

1. Open the **/etc/sssd/sssd.conf** file in a text editor.
2. Ajoutez l'option **ad_site** à la section **[domain]** pour votre domaine AD :

```
[domain/ad.example.com]
id_provider = ad
...
ad_site = ExampleSite
```

3. Enregistrez et fermez le fichier de configuration **/etc/sssd/sssd.conf**.
4. Redémarrez le service SSSD pour charger les modifications de configuration :

```
# systemctl restart sssd
```

1.9. COMMANDES DE DOMAINE

Le système **realmd** comporte deux grands domaines d'intervention :

- Gestion de l'inscription des systèmes dans un domaine.
- Contrôle des utilisateurs du domaine autorisés à accéder aux ressources du système local.

Dans **realmd**, utilisez l'outil de ligne de commande **realm** pour exécuter des commandes. La plupart des commandes de **realm** exigent que l'utilisateur spécifie l'action que l'utilitaire doit effectuer et l'entité, telle qu'un domaine ou un compte d'utilisateur, pour laquelle l'action doit être effectuée.

Tableau 1.3. commandes realmd

Commandement	Description
Realm Commands	
découvrir	Lancer un scan de découverte des domaines sur le réseau.

Commandement	Description
rejoindre	Ajouter le système au domaine spécifié.
quitter	Retirer le système du domaine spécifié.
liste	Liste de tous les domaines configurés pour le système ou de tous les domaines découverts et configurés.
Login Commands	
permis	Permet à des utilisateurs spécifiques ou à tous les utilisateurs d'un domaine configuré d'accéder au système local.
refuser	Restreindre l'accès au système local pour des utilisateurs spécifiques ou pour tous les utilisateurs d'un domaine configuré.

Ressources supplémentaires

- La page de manuel **realm(8)**.

CHAPITRE 2. CONNEXION DIRECTE DES SYSTÈMES RHEL À AD À L'AIDE DE SAMBA WINBIND

Deux composants sont nécessaires pour connecter un système RHEL à AD. L'un des composants, Samba Winbind, interagit avec la source d'identité et d'authentification AD, et l'autre, **realmd**, détecte les domaines disponibles et configure les services sous-jacents du système RHEL, en l'occurrence Samba Winbind, pour qu'ils se connectent au domaine AD.

Cette section décrit l'utilisation de Samba Winbind pour connecter un système RHEL à Active Directory (AD).

- Aperçu de l'intégration directe à l'aide de Samba Winbind
- Plateformes Windows prises en charge pour une intégration directe
- Assurer la prise en charge des types de chiffrement courants dans AD et RHEL
- Joindre un système RHEL à un domaine AD
- commandes de domaine

2.1. APERÇU DE L'INTÉGRATION DIRECTE À L'AIDE DE SAMBA WINBIND

Samba Winbind émule un client Windows sur un système Linux et communique avec les serveurs AD.

Vous pouvez utiliser le service **realmd** pour configurer Samba Winbind par :

- Configurer l'authentification du réseau et l'appartenance à un domaine de manière standard.
- Découvrir automatiquement des informations sur les domaines et les sphères accessibles.
- Ne nécessitant pas de configuration avancée pour rejoindre un domaine ou une zone.

Notez que :

- L'intégration directe avec Winbind dans une configuration AD multi-forêts nécessite des trusts bidirectionnels.
- Les forêts distantes doivent faire confiance à la forêt locale pour que le plug-in **idmap_ad** gère correctement les utilisateurs des forêts distantes.

Le service **winbindd** de Samba fournit une interface pour le Name Service Switch (NSS) et permet aux utilisateurs du domaine de s'authentifier auprès d'AD lorsqu'ils se connectent au système local.

L'utilisation de **winbindd** offre l'avantage de pouvoir améliorer la configuration pour partager des répertoires et des imprimantes sans installer de logiciel supplémentaire. Pour plus de détails, voir la section sur l'utilisation de Samba en tant que serveur dans le guide Déploiement de différents types de serveurs.

Ressources supplémentaires

- Voir la page de manuel **realmd**.
- Voir la page de manuel **winbindd**.

2.2. PLATEFORMES WINDOWS PRISES EN CHARGE POUR UNE INTÉGRATION DIRECTE

Vous pouvez intégrer directement votre système RHEL aux forêts Active Directory qui utilisent les niveaux fonctionnels de forêt et de domaine suivants :

- Gamme de niveaux fonctionnels de la forêt : Windows Server 2008 - Windows Server 2016
- Gamme de niveaux fonctionnels du domaine : Windows Server 2008 - Windows Server 2016

L'intégration directe a été testée sur les systèmes d'exploitation suivants :

- Windows Server 2022 (RHEL 9.1 et supérieur)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

NOTE

Windows Server 2019 et Windows Server 2022 n'introduisent pas de nouveau niveau fonctionnel. Le niveau fonctionnel le plus élevé que Windows Server 2019 et Windows Server 2022 utilisent est Windows Server 2016.

2.3. ASSURER LA PRISE EN CHARGE DES TYPES DE CHIFFREMENT COURANTS DANS AD ET RHEL

Par défaut, Samba Winbind prend en charge les types de chiffrement Kerberos RC4, AES-128 et AES-256.

Le cryptage RC4 a été déprécié et désactivé par défaut, car il est considéré comme moins sûr que les nouveaux types de cryptage AES-128 et AES-256. En revanche, les informations d'identification des utilisateurs d'Active Directory (AD) et les liens de confiance entre les domaines AD prennent en charge le cryptage RC4 et peuvent ne pas prendre en charge les types de cryptage AES.

En l'absence de types de chiffrement communs, la communication entre les hôtes RHEL et les domaines AD risque de ne pas fonctionner, ou certains comptes AD risquent de ne pas pouvoir s'authentifier. Pour remédier à cette situation, modifiez l'une des configurations suivantes :

Activer la prise en charge du cryptage AES dans Active Directory (option recommandée)

Pour s'assurer que les trusts entre les domaines AD dans une forêt AD prennent en charge les types de cryptage AES fort, voir l'article Microsoft suivant : AD DS : Security : Erreur Kerberos "Unsupported etype" lors de l'accès à une ressource dans un domaine de confiance

Activer la prise en charge de RC4 dans RHEL

Sur chaque hôte RHEL où l'authentification contre les contrôleurs de domaine AD a lieu :

a. Utilisez la commande **update-crypto-policies** pour activer la sous-politique cryptographique **AD-SUPPORT-LEGACY** en plus de la politique cryptographique **DEFAULT**.

```
[root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT-LEGACY
Setting system policy to DEFAULT:AD-SUPPORT-LEGACY
Note: System-wide crypto policies are applied on application start-up.
```

```
It is recommended to restart the system for the change of policies
to fully take place.
```

b. Redémarrer l'hôte.

Ressources supplémentaires

- Voir Utilisation de stratégies cryptographiques à l'échelle du système .

2.4. JOINDRE UN SYSTÈME RHEL À UN DOMAINE AD

Samba Winbind est une alternative au System Security Services Daemon (SSSD) pour connecter un système Red Hat Enterprise Linux (RHEL) à Active Directory (AD). Cette section décrit comment joindre un système RHEL à un domaine AD en utilisant **realmd** pour configurer Samba Winbind.

Procédure

1. Si votre AD nécessite le type de chiffrement RC4, obsolète, pour l'authentification Kerberos, activez la prise en charge de ces algorithmes de chiffrement dans RHEL :

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

2. Install the following packages:

```
# dnf install realmd oddjob-mkhomedir oddjob samba-winbind-clients \
      samba-winbind samba-common-tools samba-winbind-krb5-locator
```

3. Pour partager des répertoires ou des imprimantes sur le membre du domaine, installez le paquet **samba**:

```
# dnf install samba
```

4. Sauvegarder le fichier de configuration de **/etc/samba/smb.conf** Samba existant :

```
# mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

5. Rejoindre le domaine. Par exemple, pour rejoindre un domaine nommé **ad.example.com**:

```
# realm join --membership-software=samba --client-software=winbind ad.example.com
```

En utilisant la commande précédente, l'utilitaire **realm** s'affiche automatiquement :

- Crée un fichier **/etc/samba/smb.conf** pour un membre du domaine **ad.example.com**
- Ajoute le module **winbind** pour les recherches d'utilisateurs et de groupes au fichier **/etc/nsswitch.conf**
- Met à jour les fichiers de configuration du module d'authentification enfichable (PAM) dans le répertoire **/etc/pam.d/**
- Démarre le service **winbind** et permet au service de démarrer lorsque le système démarre

6. Il est possible de définir un autre back-end de mappage d'identifiants ou des paramètres de mappage d'identifiants personnalisés dans le fichier **/etc/samba/smb.conf**.

Pour plus de détails, voir la section Comprendre et configurer le mappage d'ID Samba

1. Modifiez le fichier **/etc/krb5.conf** et ajoutez la section suivante :

```
[plugins]
  localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
  }
```

2. Vérifiez que le service **winbind** est en cours d'exécution :

```
# systemctl status winbind
...
  Active: active (running) since Tue 2018-11-06 19:10:40 CET; 15s ago
```

IMPORTANT

Pour permettre à Samba d'interroger les informations sur les utilisateurs et les groupes du domaine, le service **winbind** doit être en cours d'exécution avant que vous ne lanciez **smb**.

3. Si vous avez installé le paquetage **samba** pour partager des répertoires et des imprimantes, activez et démarrez le service **smb**:

```
# systemctl enable --now smb
```

Verification steps

1. Afficher les détails d'un utilisateur AD, tel que le compte administrateur AD dans le domaine AD :

```
# getent passwd "AD\administrator"
AD\administrator:*:10000:10000::/home/administrator@AD:/bin/bash
```

2. Interroger les membres du groupe des utilisateurs du domaine dans le domaine AD :

```
# getent group "AD\Domain Users"
  AD\domain users:x:10000:user1,user2
```

3. Si vous le souhaitez, vérifiez que vous pouvez utiliser les utilisateurs et les groupes du domaine lorsque vous définissez les autorisations sur les fichiers et les répertoires. Par exemple, pour définir le propriétaire du fichier **/srv/samba/example.txt** comme étant **AD\administrator** et le groupe comme étant **AD\Domain Users**:

```
# chown "AD\administrator":"AD\Domain Users" /srv/samba/example.txt
```

4. Vérifiez que l'authentification Kerberos fonctionne comme prévu :

   a. Sur le membre du domaine AD, obtenez un ticket pour le principal **administrator@AD.EXAMPLE.COM**:

```
# kinit administrator@AD.EXAMPLE.COM
```

b. Affiche le ticket Kerberos mis en cache :

```
# klist
Ticket cache: KCM:0
Default principal: administrator@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
01.11.2018 10:00:00  01.11.2018 20:00:00
krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
        renew until 08.11.2018 05:00:00
```

5. Affichez les domaines disponibles :

```
# wbinfo --all-domains
BUILTIN
SAMBA-SERVER
AD
```

Ressources supplémentaires

- Si vous ne souhaitez pas utiliser les algorithmes de chiffrement RC4, qui sont obsolètes, vous pouvez activer le type de chiffrement AES dans AD. Voir
- Activation du type de cryptage AES dans Active Directory à l'aide d'un GPO
- **realm(8)** page de manuel

2.5. COMMANDES DE DOMAINE

Le système **realmd** comporte deux grands domaines d'intervention :

- Gestion de l'inscription des systèmes dans un domaine.
- Contrôle des utilisateurs du domaine autorisés à accéder aux ressources du système local.

Dans **realmd**, utilisez l'outil de ligne de commande **realm** pour exécuter des commandes. La plupart des commandes de **realm** exigent que l'utilisateur spécifie l'action que l'utilitaire doit effectuer et l'entité, telle qu'un domaine ou un compte d'utilisateur, pour laquelle l'action doit être effectuée.

Tableau 2.1. commandes realmd

Commandement	Description
Realm Commands	
découvrir	Lancer un scan de découverte des domaines sur le réseau.
rejoindre	Ajouter le système au domaine spécifié.

Commandement	Description
quitter	Retirer le système du domaine spécifié.
liste	Liste de tous les domaines configurés pour le système ou de tous les domaines découverts et configurés.
Login Commands	
permis	Permet à des utilisateurs spécifiques ou à tous les utilisateurs d'un domaine configuré d'accéder au système local.
refuser	Restreindre l'accès au système local pour des utilisateurs spécifiques ou pour tous les utilisateurs d'un domaine configuré.

Ressources supplémentaires

- La page de manuel **realm(8)**.

CHAPITRE 3. GESTION DES CONNEXIONS DIRECTES À AD

Vous pouvez utiliser le System Security Services Daemon (SSSD) ou Samba Winbind pour connecter votre système Red Hat Enterprise Linux (RHEL) à Active Directory (AD). Cette section décrit comment modifier et gérer votre connexion à AD lorsque votre système RHEL est déjà configuré en tant que client AD.

Conditions préalables

- Vous avez connecté votre système RHEL au domaine Active Directory, soit avec SSSD, soit avec Samba Winbind.

3.1. MODIFICATION DE L'INTERVALLE DE RENOUVELLEMENT DU KEYTAB DE L'HÔTE KERBEROS PAR DÉFAUT

SSSD renouvelle automatiquement le fichier keytab de l'hôte Kerberos dans un environnement AD si le paquet **adcli** est installé. Le démon vérifie quotidiennement si le mot de passe du compte machine est plus ancien que la valeur configurée et le renouvelle si nécessaire.

L'intervalle de renouvellement par défaut est de 30 jours. Pour modifier la valeur par défaut, suivez les étapes de cette procédure.

Procédure

1. Ajoutez le paramètre suivant au fournisseur AD dans votre fichier **/etc/sssd/sssd.conf**:

```
ad_maximum_machine_account_password_age = value_in_days
```

2. Restart SSSD:

```
# systemctl restart sssd
```

3. Pour désactiver le renouvellement automatique du keytab de l'hôte Kerberos, définissez **ad_maximum_machine_account_password_age = 0**.

Ressources supplémentaires

- La page de manuel **adcli(8)**.
- La page de manuel **sssd.conf(5)**.

3.2. SUPPRESSION D'UN SYSTÈME RHEL D'UN DOMAINE AD

Cette procédure décrit comment supprimer un système Red Hat Enterprise Linux (RHEL) intégré à Active Directory (AD) directement du domaine AD.

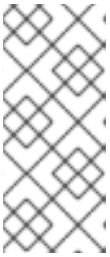
Conditions préalables

- Vous avez utilisé le System Security Services Daemon (SSSD) ou Samba Winbind pour connecter votre système RHEL à AD.

Procédure

1. Retirez un système d'un domaine d'identité à l'aide de la commande **realm leave**. La commande supprime la configuration du domaine de SSSD et du système local.

```
# realm leave ad.example.com
```



NOTE

Lorsqu'un client quitte un domaine, le compte n'est pas supprimé d'AD ; seule la configuration du client local est supprimée. Si vous souhaitez supprimer le compte AD, exécutez la commande avec l'option **--remove**. Le système vous demande votre mot de passe d'utilisateur et vous devez avoir les droits nécessaires pour supprimer un compte d'Active Directory.

2. Utilisez l'option **-U** avec la commande **realm leave** pour spécifier un utilisateur différent afin de supprimer un système d'un domaine d'identité.
Par défaut, la commande **realm leave** est exécutée en tant qu'administrateur par défaut. Pour AD, le compte administrateur s'appelle **Administrator**. Si un utilisateur différent a été utilisé pour rejoindre le domaine, il peut être nécessaire d'effectuer la suppression en tant que cet utilisateur.

```
# realm leave [ad.example.com] -U [AD.EXAMPLE.COM\user]'
```

La commande tente d'abord de se connecter sans informations d'identification, mais elle demande un mot de passe si nécessaire.

Verification steps

- Vérifiez que le domaine n'est plus configuré :

```
# realm discover [ad.example.com]
ad.example.com
   type: kerberos
   realm-name: EXAMPLE.COM
   domain-name: example.com
   configured: no
   server-software: active-directory
   client-software: sssd
   required-package: oddjob
   required-package: oddjob-mkhomedir
   required-package: sssd
   required-package: adcli
   required-package: samba-common-tools
```

Ressources supplémentaires

- Voir la page de manuel **realm(8)**.

3.3. DÉFINITION DE L'ORDRE DE RÉSOLUTION DES DOMAINES DANS SSSD POUR RÉSOUDRE LES NOMS D'UTILISATEUR AD COURTS

Par défaut, vous devez spécifier des noms d'utilisateur complets, tels que **ad_username@ad.example.com** et **group@ad.example.com**, pour résoudre les utilisateurs et les groupes Active Directory (AD) sur un hôte RHEL connecté à AD avec le service SSSD.

Cette procédure définit l'ordre de résolution des domaines dans la configuration SSSD afin que vous puissiez résoudre les utilisateurs et les groupes AD à l'aide de noms courts, tels que **ad_username**. Cet exemple de configuration recherche les utilisateurs et les groupes dans l'ordre suivant :

1. Domaine enfant Active Directory (AD) **subdomain2.ad.example.com**
2. Domaine enfant AD **subdomain1.ad.example.com**
3. Domaine racine AD **ad.example.com**

Conditions préalables

- Vous avez utilisé le service SSSD pour connecter l'hôte RHEL directement à AD.

Procédure

1. Ouvrez le fichier **/etc/sssd/sssd.conf** dans un éditeur de texte.
2. Définissez l'option **domain_resolution_order** dans la section **[sssd]** du fichier.

```
domain_resolution_order = subdomain2.ad.example.com, subdomain1.ad.example.com, ad.example.com
```

3. Enregistrez et fermez le fichier.
4. Restart the SSSD service to load the new configuration settings.

```
[root@ad-client ~]# systemctl restart sssd
```

Étapes de la vérification

- Vérifiez que vous pouvez récupérer les informations relatives à un utilisateur du premier domaine en utilisant uniquement un nom court.

```
[root@ad-client ~]# id <user_from_subdomain2>
uid=1916901142(user_from_subdomain2) gid=1916900513(domain users) groups=1916900513(domain users)
```

3.4. GESTION DES AUTORISATIONS DE CONNEXION POUR LES UTILISATEURS DU DOMAINE

Par défaut, le contrôle d'accès côté domaine est appliqué, ce qui signifie que les politiques de connexion pour les utilisateurs d'Active Directory (AD) sont définies dans le domaine AD lui-même. Ce comportement par défaut peut être remplacé par un contrôle d'accès côté client. Avec le contrôle d'accès côté client, les autorisations de connexion sont définies par les stratégies locales uniquement.

Si un domaine applique un contrôle d'accès côté client, vous pouvez utiliser le site **realmd** pour configurer des règles de base d'autorisation ou de refus d'accès pour les utilisateurs de ce domaine.

NOTE

Les règles d'accès autorisent ou refusent l'accès à tous les services du système. Des règles d'accès plus spécifiques doivent être définies sur une ressource spécifique du système ou dans le domaine.

3.4.1. Permettre l'accès aux utilisateurs au sein d'un domaine

Par défaut, les stratégies de connexion pour les utilisateurs d'Active Directory (AD) sont définies dans le domaine AD lui-même. Cette section explique comment remplacer ce comportement par défaut et configurer un hôte RHEL pour permettre l'accès des utilisateurs au sein d'un domaine AD.

IMPORTANT

Il n'est pas recommandé d'autoriser l'accès à tous par défaut tout en le refusant à des utilisateurs spécifiques à l'aide de realm permit **-x**. Red Hat recommande plutôt de maintenir une politique de non-accès par défaut pour tous les utilisateurs et de n'accorder l'accès qu'à des utilisateurs sélectionnés à l'aide de realm permit.

Conditions préalables

- Votre système RHEL est membre du domaine Active Directory.

Procédure

1. Accorder l'accès à tous les utilisateurs :

```
# realm permit --all
```

2. Accorder l'accès à des utilisateurs spécifiques :

```
$ realm permit aduser01@example.com
$ realm permit 'AD.EXAMPLE.COM\aduser01'
```

Actuellement, vous ne pouvez autoriser l'accès qu'aux utilisateurs des domaines primaires et non aux utilisateurs des domaines de confiance. Cela est dû au fait que la connexion de l'utilisateur doit contenir le nom de domaine et que SSSD ne peut actuellement pas fournir à **realmd** des informations sur les domaines enfants disponibles.

Verification steps

1. Utilisez SSH pour vous connecter au serveur en tant qu'utilisateur **aduser01@example.com**:

```
$ ssh aduser01@example.com@server_name
[aduser01@example.com@server_name ~]$
```

2. Utilisez la commande ssh une seconde fois pour accéder au même serveur, cette fois-ci en tant qu'utilisateur **aduser02@example.com**:

```
$ ssh aduser02@example.com@server_name
Authentication failed.
```

Remarquez que l'utilisateur **aduser02@example.com** se voit refuser l'accès au système. Vous n'avez

accordé l'autorisation de se connecter au système qu'à l'utilisateur **aduser01@example.com**. Tous les autres utilisateurs de ce domaine Active Directory sont rejetés en raison de la politique de connexion spécifiée.

NOTE

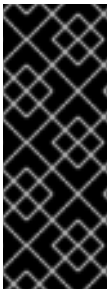
Si vous attribuez la valeur true à **use_fully_qualified_names** dans le fichier **sssd.conf**, toutes les requêtes doivent utiliser le nom de domaine complet. En revanche, si vous attribuez la valeur false à **use_fully_qualified_names**, il est possible d'utiliser le nom pleinement qualifié dans les requêtes, mais seule la version simplifiée est affichée dans le résultat.

Ressources supplémentaires

- Voir la page de manuel **realm(8)**.

3.4.2. Refuser l'accès aux utilisateurs d'un domaine

Par défaut, les stratégies de connexion des utilisateurs Active Directory (AD) sont définies dans le domaine AD lui-même. Cette section explique comment remplacer ce comportement par défaut et configurer un hôte RHEL pour qu'il refuse l'accès aux utilisateurs d'un domaine AD.



IMPORTANT

Il est plus sûr de n'autoriser l'accès qu'à des utilisateurs ou groupes spécifiques que de refuser l'accès à certains, tout en l'autorisant à tous les autres. Par conséquent, il n'est pas recommandé d'autoriser l'accès à tous par défaut tout en le refusant à des utilisateurs spécifiques avec l'option realm permit **-x**. Red Hat recommande plutôt de maintenir une politique de non-accès par défaut pour tous les utilisateurs et de n'accorder l'accès qu'à des utilisateurs sélectionnés à l'aide de realm permit.

Conditions préalables

- Votre système RHEL est membre du domaine Active Directory.

Procédure

1. Refuser l'accès à tous les utilisateurs du domaine :

```
# realm deny --all
```

   Cette commande empêche les comptes **realm** de se connecter à la machine locale. Utilisez **realm permit** pour limiter la connexion à des comptes spécifiques.

2. Vérifiez que l'adresse **login-policy** de l'utilisateur du domaine est définie sur **deny-any-login**:

```
[root@replica1 ~]# realm list
example.net
  type: kerberos
  realm-name: EXAMPLE.NET
  domain-name: example.net
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
```

```
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd
required-package: adcli
required-package: samba-common-tools
login-formats: %U@example.net
login-policy: deny-any-login
```

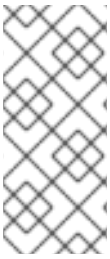
3. Refuser l'accès à des utilisateurs spécifiques en utilisant l'option **-x**:

```
$ realm permit -x 'AD.EXAMPLE.COM\aduser02'
```

Verification steps

- Utilisez SSH pour vous connecter au serveur en tant qu'utilisateur **aduser01@example.net**.

```
$ ssh aduser01@example.net@server_name
Authentication failed.
```



NOTE

Si vous attribuez la valeur true à **use_fully_qualified_names** dans le fichier **sssd.conf**, toutes les requêtes doivent utiliser le nom de domaine complet. En revanche, si vous attribuez la valeur false à **use_fully_qualified_names**, il est possible d'utiliser le nom pleinement qualifié dans les requêtes, mais seule la version simplifiée est affichée dans le résultat.

Ressources supplémentaires

- Voir la page de manuel **realm(8)**.

3.5. APPLICATION DU CONTRÔLE D'ACCÈS AUX OBJETS DE STRATÉGIE DE GROUPE DANS RHEL

Un GPO (*Group Policy Object*) est un ensemble de paramètres de contrôle d'accès stockés dans Microsoft Active Directory (AD) qui peuvent s'appliquer aux ordinateurs et aux utilisateurs dans un environnement AD. En spécifiant des GPO dans AD, les administrateurs peuvent définir des politiques de connexion honorées par les clients Windows et les hôtes Red Hat Enterprise Linux (RHEL) connectés à AD.

Les sections suivantes décrivent comment vous pouvez gérer les GPO dans votre environnement :

- Comment SSSD interprète les règles de contrôle d'accès aux GPO
- Liste des paramètres GPO pris en charge par SSSD
- Liste des options SSSD permettant de contrôler l'application des GPO
- Modifier le mode de contrôle d'accès aux GPO
- Création et configuration d'un GPO pour un hôte RHEL

3.5.1. Comment SSSD interprète les règles de contrôle d'accès aux GPO

Par défaut, SSSD récupère les objets de stratégie de groupe (GPO) des contrôleurs de domaine Active Directory (AD) et les évalue pour déterminer si un utilisateur est autorisé à se connecter à un hôte RHEL particulier joint à AD.

SSSD associe AD *Windows Logon Rights* aux noms de service PAM (Pluggable Authentication Module) afin d'appliquer ces autorisations dans un environnement GNU/Linux.

En tant qu'administrateur AD, vous pouvez limiter la portée des règles GPO à des utilisateurs, groupes ou hôtes spécifiques en les répertoriant sur le site *security filter*.

Limitations du filtrage par les hôtes

Les anciennes versions de SSSD n'évaluent pas les hôtes dans les filtres de sécurité AD GPO.

- **RHEL 8.3.0 and newer:** SSSD prend en charge les utilisateurs, les groupes et les hôtes dans les filtres de sécurité.
- **RHEL versions older than 8.3.0:** SSSD ignore les entrées d'hôtes et ne prend en charge que les utilisateurs et les groupes dans les filtres de sécurité.
  Pour s'assurer que SSSD applique le contrôle d'accès basé sur les GPO à un hôte spécifique, créez une nouvelle unité d'organisation (OU) dans le domaine AD, déplacez le système vers la nouvelle OU, puis liez les GPO à cette OU.

Limitations du filtrage par groupes

SSSD ne prend actuellement pas en charge les groupes intégrés d'Active Directory, tels que **Administrators** avec Security Identifier (SID) **S-1-5-32-544**. Red Hat recommande de ne pas utiliser les groupes intégrés AD dans les GPO AD ciblant les hôtes RHEL.

Ressources supplémentaires

- Pour obtenir une liste des options GPO de Windows et des options SSSD correspondantes, voir Liste des paramètres GPO pris en charge par SSSD .

3.5.2. Liste des paramètres GPO pris en charge par SSSD

Le tableau suivant présente les options SSSD qui correspondent aux options GPO Active Directory telles qu'elles sont spécifiées dans le site *Group Policy Management Editor* sous Windows.

Tableau 3.1. Options de contrôle d'accès aux GPO récupérées par SSSD

Option GPO	Option correspondante **sssd.conf**
Autoriser la connexion locale Refuser la connexion locale	**ad_gpo_map_interactive**
Autoriser la connexion via les services de bureau à distance Refuser la connexion via les services de bureau à distance	**ad_gpo_map_remote_interactive**
Accéder à cet ordinateur à partir du réseau Refuser l'accès à cet ordinateur à partir du réseau	**ad_gpo_map_network**

Option GPO	Option correspondante **sssd.conf**
Autoriser la connexion en tant que travail par lots Refuser la connexion en tant que travail par lots	**ad_gpo_map_batch**
Autoriser la connexion en tant que service Refuser la connexion en tant que service	**ad_gpo_map_service**

Ressources supplémentaires

- Pour plus d'informations sur ces paramètres **sssd.conf**, tels que les services PAM (Pluggable Authentication Module) qui correspondent aux options GPO, voir l'entrée de page du manuel **sssd-ad(5)**.

3.5.3. Liste des options SSSD permettant de contrôler l'application des GPO

Vous pouvez définir les options SSSD suivantes pour limiter la portée des règles GPO.

L'option ad_gpo_access_control

Vous pouvez définir l'option **ad_gpo_access_control** dans le fichier **/etc/sssd/sssd.conf** pour choisir entre trois modes différents de fonctionnement du contrôle d'accès basé sur les GPO.

Tableau 3.2. Tableau des valeurs ad_gpo_access_control

Valeur de ad_gpo_access_control	Comportement
enforcing	Les règles de contrôle d'accès basées sur les GPO sont évaluées et appliquées. **This is the default setting in RHEL 8.**
permissive	Les règles de contrôle d'accès basées sur les GPO sont évaluées mais **not** appliquées ; un message **syslog** est enregistré chaque fois que l'accès est refusé. Il s'agit du paramètre par défaut dans RHEL 7. Ce mode est idéal pour tester les ajustements de politique tout en permettant aux utilisateurs de continuer à se connecter.
disabled	Les règles de contrôle d'accès basées sur les GPO ne sont ni évaluées ni appliquées.

L'option ad_gpo_implicit_deny

L'option **ad_gpo_implicit_deny** est définie par défaut sur **False**. Dans cet état par défaut, les utilisateurs sont autorisés à accéder si les GPO applicables ne sont pas trouvés. Si vous définissez cette option sur **True**, vous devez explicitement autoriser l'accès des utilisateurs à l'aide d'une règle de GPO.

Vous pouvez utiliser cette fonctionnalité pour renforcer la sécurité, mais veillez à ne pas refuser l'accès involontairement. Red Hat recommande de tester cette fonctionnalité lorsque **ad_gpo_access_control** est défini sur **permissive**.

Les deux tableaux suivants montrent quand un utilisateur est autorisé ou refusé en fonction des droits de connexion autorisés et refusés définis du côté du serveur AD et de la valeur de **ad_gpo_implicit_deny**.

Tableau 3.3. Comportement de connexion avec ad_gpo_implicit_deny défini sur False (default)

autoriser les règles	règles de refus	résultat
manquant	manquant	tous les utilisateurs sont autorisés
manquant	présent	seuls les utilisateurs ne figurant pas dans les règles de refus sont autorisés
présent	manquant	seuls les utilisateurs figurant dans les règles d'autorisation sont autorisés
présent	présent	seuls les utilisateurs figurant dans les règles d'autorisation (allow-rules) et non dans les règles de refus (deny-rules) sont autorisés

Tableau 3.4. Comportement de connexion avec ad_gpo_implicit_deny réglé sur True

autoriser les règles	règles de refus	résultat
manquant	manquant	aucun utilisateur n'est autorisé
manquant	présent	aucun utilisateur n'est autorisé
présent	manquant	seuls les utilisateurs figurant dans les règles d'autorisation sont autorisés
présent	présent	seuls les utilisateurs figurant dans les règles d'autorisation (allow-rules) et non dans les règles de refus (deny-rules) sont autorisés

Ressources supplémentaires

- Pour la procédure de modification du mode d'application des GPO dans SSSD, voir Modification du mode de contrôle d'accès aux GPO .
- Pour plus de détails sur chacun des différents modes de fonctionnement des GPO, voir l'entrée **ad_gpo_access_control** dans la page du manuel **sssd-ad(5)**.

3.5.4. Modifier le mode de contrôle d'accès aux GPO

Cette procédure modifie la manière dont les règles de contrôle d'accès basées sur les GPO sont évaluées et appliquées sur un hôte RHEL connecté à un environnement Active Directory (AD).

Dans cet exemple, vous allez changer le mode de fonctionnement de la GPO de **enforcing** (par défaut) à **permissive** à des fins de test.

IMPORTANT

Si les erreurs suivantes s'affichent, cela signifie que les utilisateurs d'Active Directory ne peuvent pas se connecter en raison des contrôles d'accès basés sur les GPO :

- Sur **/var/log/secure**:

```
Oct 31 03:00:13 client1 sshd[124914]: pam_sss(sshd:account): Access denied for user aduser1: 6 (Permission denied)
Oct 31 03:00:13 client1 sshd[124914]: Failed password for aduser1 from 127.0.0.1 port 60509 ssh2
Oct 31 03:00:13 client1 sshd[124914]: fatal: Access denied for user aduser1 by PAM account configuration [preauth]
```

- Sur **/var/log/sssd/sssd__example.com_.log**:

```
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_perform_hbac_processing] (0x0040): GPO access check failed: [1432158236](Host Access Denied)
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_cse_done] (0x0040): HBAC processing failed: [1432158236](Host Access Denied}
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_access_done] (0x0040): GPO-based access control failed.
```

Si ce comportement n'est pas souhaité, vous pouvez temporairement attribuer la valeur **ad_gpo_access_control** à **permissive**, comme décrit dans cette procédure, pendant que vous recherchez les paramètres GPO appropriés dans AD.

Conditions préalables

- Vous avez joint un hôte RHEL à un environnement AD à l'aide de SSSD.
- La modification du fichier de configuration **/etc/sssd/sssd.conf** nécessite les autorisations de **root**.

Procédure

1. Arrêtez le service SSSD.

```
[root@server ~]# systemctl stop sssd
```

2. Open the **/etc/sssd/sssd.conf** file in a text editor.
3. Définissez **ad_gpo_access_control** à **permissive** dans la section **domain** pour le domaine AD.

```
[domain/example.com]
ad_gpo_access_control=permissive
...
```

4. Enregistrez le fichier **/etc/sssd/sssd.conf**.
5. Redémarrez le service SSSD pour charger les modifications de configuration.

```
[root@server ~]# systemctl restart sssd
```

Ressources supplémentaires

- Pour obtenir la liste des différents modes de contrôle d'accès aux GPO, voir Liste des options SSSD permettant de contrôler l'application des GPO.

3.5.5. Création et configuration d'une GPO pour un hôte RHEL dans l'interface graphique AD

Un objet de stratégie de groupe (GPO) est un ensemble de paramètres de contrôle d'accès stockés dans Microsoft Active Directory (AD) qui peuvent s'appliquer aux ordinateurs et aux utilisateurs dans un environnement AD. La procédure suivante crée un GPO dans l'interface utilisateur graphique (GUI) AD pour contrôler l'accès à la connexion d'un hôte RHEL intégré directement au domaine AD.

Conditions préalables

- Vous avez joint un hôte RHEL à un environnement AD à l'aide de SSSD.
- Vous disposez des privilèges d'administrateur AD pour effectuer des modifications dans AD à l'aide de l'interface graphique.

Procédure

1. Dans **Active Directory Users and Computers**, créez une unité d'organisation (OU) à associer au nouveau GPO :
   a. Cliquez avec le bouton droit de la souris sur le domaine.
   b. Choisissez **New**.
   c. Choisissez **Organizational Unit**.
2. Cliquez sur le nom de l'objet ordinateur qui représente l'hôte RHEL (créé lorsqu'il a rejoint Active Directory) et faites-le glisser dans la nouvelle OU. En plaçant l'hôte RHEL dans sa propre OU, la GPO cible cet hôte.
3. Dans le site **Group Policy Management Editor**, créez une nouvelle GPO pour l'OU que vous avez créée :
   a. Développer **Forest**.
   b. Développer **Domains**.
   c. Élargissez votre domaine.
   d. Cliquez avec le bouton droit de la souris sur la nouvelle OU.
   e. Choisissez **Create a GPO in this domain**.
4. Spécifiez un nom pour le nouveau GPO, par exemple **Allow SSH access** ou **Allow Console/GUI access** et cliquez sur **OK**.
5. Modifiez la nouvelle GPO :
   a. Sélectionnez l'OU dans l'éditeur **Group Policy Management**.
   b. Cliquez avec le bouton droit de la souris et choisissez **Edit**.

c. Sélectionnez **User Rights Assignment**.

d. Sélectionner **Computer Configuration**

e. Sélectionnez **Policies**.

f. Sélectionnez **Windows Settings**.

g. Sélectionnez **Security Settings**.

h. Sélectionnez **Local Policies**.

i. Sélectionnez **User Rights Assignment**.

6. Attribuer des autorisations de connexion :

   a. Double-cliquez sur **Allow log on locally** pour autoriser l'accès à la console locale/à l'interface utilisateur.

   b. Double-cliquez sur **Allow log on through Remote Desktop Services** pour accorder l'accès SSH.

7. Ajoutez le(s) utilisateur(s) que vous souhaitez voir accéder à l'une ou l'autre de ces politiques aux politiques elles-mêmes :

   a. Cliquez sur **Add User or Group**.

   b. Saisissez le nom d'utilisateur dans le champ vide.

   c. Cliquez sur **OK**.

Ressources supplémentaires

- Pour plus de détails sur les objets de stratégie de groupe, voir Objets de stratégie de groupe dans la documentation Microsoft.

3.5.6. Ressources supplémentaires

- Pour plus d'informations sur la connexion d'un hôte RHEL à un environnement Active Directory, voir Connexion directe des systèmes RHEL à AD à l'aide de SSSD .

CHAPITRE 4. ACCÈS À AD AVEC UN COMPTE DE SERVICE GÉRÉ

Les comptes de services gérés (MSA) d'Active Directory (AD) vous permettent de créer un compte dans AD qui correspond à un ordinateur spécifique. Vous pouvez utiliser un MSA pour vous connecter aux ressources AD en tant que principal utilisateur spécifique, sans joindre l'hôte RHEL au domaine AD.

Cette section aborde les sujets suivants :

- Les avantages d'un compte de service géré
- Configuration d'un compte de service géré pour un hôte RHEL
- Mise à jour du mot de passe d'un compte de service géré
- Spécifications des comptes de services gérés
- Options pour la commande adcli create-msa

4.1. LES AVANTAGES D'UN COMPTE DE SERVICE GÉRÉ

Si vous souhaitez permettre à un hôte RHEL d'accéder à un domaine Active Directory (AD) sans le rejoindre, vous pouvez utiliser un compte de service géré (MSA) pour accéder à ce domaine. Un MSA est un compte AD correspondant à un ordinateur spécifique, que vous pouvez utiliser pour vous connecter aux ressources AD en tant que principal utilisateur spécifique.

Par exemple, si le domaine AD **production.example.com** a une relation de confiance à sens unique avec le domaine AD **lab.example.com**, les conditions suivantes s'appliquent :

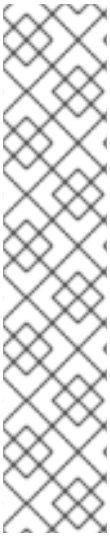
- Le domaine **lab** fait confiance aux utilisateurs et aux hôtes du domaine **production**.
- Le domaine **production** fait **not** confiance aux utilisateurs et aux hôtes du domaine **lab**.

Cela signifie qu'un hôte rattaché au domaine **lab**, tel que **client.lab.example.com**, ne peut pas accéder aux ressources du domaine **production** par l'intermédiaire de la confiance.

Si vous souhaitez créer une exception pour l'hôte **client.lab.example.com**, vous pouvez utiliser l'utilitaire **adcli** pour créer une MSA pour l'hôte **client** dans le domaine **production.example.com**. En vous authentifiant auprès du principal Kerberos de la MSA, vous pouvez effectuer des recherches LDAP sécurisées dans le domaine **production** à partir de l'hôte **client**.

4.2. CONFIGURATION D'UN COMPTE DE SERVICE GÉRÉ POUR UN HÔTE RHEL

Cette procédure crée un compte de service géré (MSA) pour un hôte du domaine Active Directory (AD) **lab.example.com** et configure SSSD pour que vous puissiez accéder au domaine AD **production.example.com** et vous y authentifier.



NOTE

Si vous devez accéder aux ressources AD à partir d'un hôte RHEL, Red Hat vous recommande de joindre l'hôte RHEL au domaine AD à l'aide de la commande **realm**. Reportez-vous à Connexion directe des systèmes RHEL à AD à l'aide de SSSD .

N'effectuez cette procédure que si l'une des conditions suivantes s'applique :

- Vous ne pouvez pas joindre l'hôte RHEL au domaine AD et vous souhaitez créer un compte pour cet hôte dans AD.
- Vous avez joint l'hôte RHEL à un domaine AD et vous devez accéder à un autre domaine AD dans lequel les informations d'identification de l'hôte du domaine que vous avez joint ne sont pas valides, comme dans le cas d'une confiance à sens unique.

Conditions préalables

- Assurez-vous que les ports suivants de l'hôte RHEL sont ouverts et accessibles aux contrôleurs de domaine AD.

Service	Port	Protocoles
DNS	53	TCP, UDP
LDAP	389	TCP, UDP
LDAPS (facultatif)	636	TCP, UDP
Kerberos	88	TCP, UDP

- Vous avez le mot de passe d'un administrateur AD qui a le droit de créer des MSA dans le domaine **production.example.com**.
- Vous disposez des droits d'administrateur requis pour exécuter la commande **adcli** et pour modifier le fichier de configuration **/etc/sssd/sssd.conf**.
- *(Optional)* Vous avez installé le paquetage **krb5-workstation**, qui comprend l'utilitaire de diagnostic **klist**.

Procédure

1. Créer un MSA pour l'hôte dans le domaine AD **production.example.com**.

```
[root@client ~]# adcli create-msa --domain=production.example.com
```

2. Affichez les informations sur la MSA à partir du fichier clé Kerberos qui a été créé. Notez le nom de la MSA :

```
[root@client ~]# klist -k /etc/krb5.keytab.production.example.com
Keytab name: FILE:/etc/krb5.keytab.production.example.com
KVNO Principal
```

```
---- ------------------------------------------------------------
  2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
  2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes128-cts-hmac-sha1-96)
```

3. Ouvrez le fichier **/etc/sssd/sssd.conf** et choisissez la configuration de domaine SSSD appropriée à ajouter :

   - Si le MSA correspond à un **AD domain from a different forest**, créez une nouvelle section de domaine nommée **[domain/<name_of_domain>]**, et entrez les informations sur le MSA et le keytab. Les options les plus importantes sont **ldap_sasl_authid**, **ldap_krb5_keytab**, et **krb5_keytab**:

     ```
     [domain/production.example.com]
     ldap_sasl_authid = CLIENT!S3A$@PRODUCTION.EXAMPLE.COM
     ldap_krb5_keytab = /etc/krb5.keytab.production.example.com
     krb5_keytab = /etc/krb5.keytab.production.example.com
     ad_domain = production.example.com
     krb5_realm = PRODUCTION.EXAMPLE.COM
     access_provider = ad
     ...
     ```

   - Si le MSA correspond à un **AD domain from the local forest**, créez une nouvelle section de sous-domaine au format **[domain/root.example.com/sub-domain.example.com]**, et entrez des informations sur le MSA et le keytab. Les options les plus importantes sont **ldap_sasl_authid**, **ldap_krb5_keytab**, et **krb5_keytab**:

     ```
     [domain/ad.example.com/production.example.com]
     ldap_sasl_authid = CLIENT!S3A$@PRODUCTION.EXAMPLE.COM
     ldap_krb5_keytab = /etc/krb5.keytab.production.example.com
     krb5_keytab = /etc/krb5.keytab.production.example.com
     ad_domain = production.example.com
     krb5_realm = PRODUCTION.EXAMPLE.COM
     access_provider = ad
     ...
     ```

Verification steps

- Vérifiez que vous pouvez récupérer un ticket Kerberos (TGT) en tant que MSA :

  ```
  [root@client ~]# kinit -k -t /etc/krb5.keytab.production.example.com 'CLIENT!S3A$'
  [root@client ~]# klist
  Ticket cache: KCM:0:54655
  Default principal: CLIENT!S3A$@PRODUCTION.EXAMPLE.COM

  Valid starting       Expires              Service principal
  11/22/2021 15:48:03  11/23/2021 15:48:03
  krbtgt/PRODUCTION.EXAMPLE.COM@PRODUCTION.EXAMPLE.COM
  ```

- Dans AD, vérifiez que vous avez un MSA pour l'hôte dans l'unité d'organisation (OU) des comptes de services gérés.

Ressources supplémentaires

- Connexion directe des systèmes RHEL à AD à l'aide de SSSD

4.3. MISE À JOUR DU MOT DE PASSE D'UN COMPTE DE SERVICE GÉRÉ

Les comptes de services gérés (MSA) ont un mot de passe complexe qui est maintenu automatiquement par Active Directory (AD). Par défaut, le System Services Security Daemon (SSSD) met automatiquement à jour le mot de passe MSA dans le keytab Kerberos s'il date de plus de 30 jours, ce qui le maintient à jour par rapport au mot de passe dans AD. Cette procédure explique comment mettre à jour manuellement le mot de passe de votre MSA.

Conditions préalables

- Vous avez précédemment créé une MSA pour un hôte dans le domaine AD production.example.com.
- *(Optional)* Vous avez installé le paquetage **krb5-workstation**, qui comprend l'utilitaire de diagnostic **klist**.

Procédure

1. *(Optional)* Affiche le numéro de version de la clé (KVNO) de la MSA dans la base de données Kerberos. Le KVNO actuel est 2.

```
[root@client ~]# klist -k /etc/krb5.keytab.production.example.com
Keytab name: FILE:/etc/krb5.keytab.production.example.com
KVNO Principal
---- --------------------------------------------------------------------
   2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   2 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes128-cts-hmac-sha1-96)
```

2. Mettre à jour le mot de passe de la MSA dans le domaine AD **production.example.com**.

```
[root@client ~]# adcli update --domain=production.example.com --host-
keytab=/etc/krb5.keytab.production.example.com --computer-password-lifetime=0
```

Verification steps

- Vérifiez que vous avez incrémenté le KVNO dans le keytab Kerberos :

```
[root@client ~]# klist -k /etc/krb5.keytab.production.example.com
Keytab name: FILE:/etc/krb5.keytab.production.example.com
KVNO Principal
---- --------------------------------------------------------------------
   3 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   3 CLIENT!S3A$@PRODUCTION.EXAMPLE.COM (aes128-cts-hmac-sha1-96)
```

4.4. SPÉCIFICATIONS DES COMPTES DE SERVICES GÉRÉS

Les comptes de services gérés (MSA) créés par l'utilitaire **adcli** ont les caractéristiques suivantes :

- Ils ne peuvent pas avoir de nom de principal de service (SPN) supplémentaire.

- Par défaut, le principal Kerberos pour la MSA est stocké dans un keytab Kerberos nommé ***<default_keytab_location>.<Active_Directory_domain>***comme ***/etc/krb5.keytab.production.example.com***.

- Les noms de MSA sont limités à 20 caractères ou moins. Les 4 derniers caractères sont un suffixe de 3 caractères aléatoires issus de plages de chiffres et de majuscules et minuscules ASCII ajoutés au nom court de l'hôte que vous avez fourni, en utilisant un caractère **!** comme séparateur. Par exemple, un hôte portant le nom court **myhost** reçoit une MSA avec les spécifications suivantes :

Spécifications	Valeur
Attribut du nom commun (CN)	**myhost!A2c**
Nom NetBIOS	**myhost!A2c$**
sAMAccountName	**myhost!A2c$**
Principal Kerberos dans le domaine AD **production.example.com**	**myhost!A2c$@PRODUCTION.EXAMPLE.COM**

4.5. OPTIONS POUR LA COMMANDE ADCLI CREATE-MSA

Outre les options globales que vous pouvez transmettre à l'utilitaire **adcli**, vous pouvez spécifier les options suivantes pour contrôler spécifiquement la manière dont il gère les comptes de service gérés (MSA).

-N, --computer-name

Le nom court et non pointé de la MSA qui sera créée dans le domaine Active Directory (AD). Si vous ne spécifiez pas de nom, la première partie de **--host-fqdn** ou sa valeur par défaut est utilisée avec un suffixe aléatoire.

-O, --domain-ou=OU=*<path_to_OU>*

Le nom distinctif complet de l'unité d'organisation (OU) dans laquelle créer la MSA. Si vous ne spécifiez pas cette valeur, la MSA est créée dans l'emplacement par défaut **OU=CN=Managed Service Accounts,DC=EXAMPLE,DC=COM**.

-H, --host-fqdn=host

Remplacer le nom de domaine DNS complet de la machine locale. Si vous ne spécifiez pas cette option, le nom d'hôte de la machine locale est utilisé.

-K, --host-keytab=*<path_to_keytab>*

Chemin d'accès au fichier keytab de l'hôte pour stocker les informations d'identification MSA. Si vous ne spécifiez pas cette valeur, l'emplacement par défaut **/etc/krb5.keytab** est utilisé avec le nom de domaine Active Directory en minuscules ajouté comme suffixe, par exemple **/etc/krb5.keytab.domain.example.com**.

--use-ldaps

Créer l'ASM sur un canal LDAP sécurisé (LDAPS).

--verbose

Imprimez des informations détaillées lors de la création de la MSA.

--show-details

Imprimez les informations relatives à la MSA après l'avoir créée.

--show-password

Imprimez le mot de passe MSA après avoir créé le MSA.