Red Hat Enterprise Linux 9

Migration vers la gestion des identités sur RHEL 9

Mise à niveau d'un environnement IdM RHEL 8 vers RHEL 9 et migration de solutions LDAP externes vers IdM

Last Updated: 2024-02-20

Red Hat Enterprise Linux 9 Migration vers la gestion des identités sur RHEL 9

Mise à niveau d'un environnement IdM RHEL 8 vers RHEL 9 et migration de solutions LDAP externes vers IdM

Notice légale

Résumé

Red Hat ne prend en charge la gestion d'identité (IdM) que sur Red Hat Enterprise Linux (RHEL). Si vous utilisez IdM sur RHEL 8 ou un répertoire LDAP, vous pouvez migrer ces solutions vers IdM sur RHEL 9.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF 3

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT 4

PARTIE I. MIGRATION DE L'IDM DE RHEL 8 VERS RHEL 9 5

CHAPITRE 1. MIGRATION DE VOTRE ENVIRONNEMENT IDM DES SERVEURS RHEL 8 VERS LES SERVEURS RHEL 9 6
1.1. CONDITIONS PRÉALABLES À LA MIGRATION DE L'IDM DE RHEL 8 À 9 7
1.2. INSTALLATION DE LA RÉPLIQUE RHEL 9 9
1.3. ATTRIBUTION DU RÔLE DE SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION AU SERVEUR IDM RHEL 9 11
1.4. ARRÊT DE LA GÉNÉRATION DE CRL SUR UN SERVEUR D'AUTORITÉ DE CERTIFICATION IDM RHEL 8 12
1.5. DÉMARRAGE DE LA GÉNÉRATION DE CRL SUR LE NOUVEAU SERVEUR CA IDM RHEL 9 13
1.6. ARRÊT ET MISE HORS SERVICE DU SERVEUR RHEL 8 14

CHAPITRE 2. MISE À NIVEAU D'UN CLIENT IDM DE RHEL 8 À RHEL 9 15

PARTIE II. MIGRATION VERS L'IDM À PARTIR DE SOURCES EXTERNES 16

CHAPITRE 3. MIGRATION VERS IDM SUR RHEL 9 À PARTIR DE FREEIPA SUR DES DISTRIBUTIONS LINUX NON RHEL 17

CHAPITRE 4. MIGRATION D'UN ANNUAIRE LDAP VERS IDM 19
4.1. CONSIDÉRATIONS RELATIVES À LA MIGRATION DE LDAP VERS IDM 19
4.2. PLANIFICATION DE LA CONFIGURATION DU CLIENT LORS DE LA MIGRATION DE LDAP VERS IDM 20
4.3. PLANIFICATION DE LA MIGRATION DES MOTS DE PASSE LORS DE LA MIGRATION DE LDAP VERS IDM 22
4.4. AUTRES CONSIDÉRATIONS ET EXIGENCES EN MATIÈRE DE MIGRATION 25
4.5. PERSONNALISATION DE LA MIGRATION DE LDAP VERS IDM 28
4.6. MIGRATION D'UN SERVEUR LDAP VERS IDM 31
4.7. MIGRATION DE LDAP VERS IDM SUR SSL 35

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* est remplacé par un langage 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**.

PARTIE I. MIGRATION DE L'IDM DE RHEL 8 VERS RHEL 9

CHAPITRE 1. MIGRATION DE VOTRE ENVIRONNEMENT IDM DES SERVEURS RHEL 8 VERS LES SERVEURS RHEL 9

Pour mettre à niveau un environnement IdM RHEL 8 vers RHEL 9, vous devez d'abord ajouter de nouvelles répliques IdM RHEL 9 à votre environnement IdM RHEL 8, puis retirer les serveurs RHEL 8.

AVERTISSEMENT

- La mise à niveau des serveurs IdM RHEL 8 vers RHEL 9 n'est pas prise en charge.
- Pour plus d'informations sur l'ajout d'une réplique IdM RHEL 9 en mode FIPS à un déploiement IdM RHEL 8 en mode FIPS, voir la section Gestion des identités à l'adresse *Considerations in adopting RHEL 9* .
- Après la mise à niveau de votre réplique IdM vers RHEL 9.2, le centre de distribution Kerberos (KDC) IdM peut ne pas délivrer de tickets d'attribution de tickets (TGT) aux utilisateurs qui n'ont pas d'identifiants de sécurité (SID) attribués à leurs comptes. Par conséquent, les utilisateurs ne peuvent pas se connecter à leurs comptes.
  Pour contourner le problème, générez des SID en exécutant **# ipa config-mod --enable-sid --add-sids** en tant qu'administrateur IdM sur une autre réplique IdM dans la topologie. Ensuite, si les utilisateurs ne peuvent toujours pas se connecter, examinez le journal des erreurs du serveur d'annuaire. Il se peut que vous deviez ajuster les plages d'ID pour inclure les identités POSIX des utilisateurs.
- La migration directe vers RHEL 9 à partir de RHEL 7 ou de versions antérieures n'est pas prise en charge. Pour mettre à jour correctement vos données IdM, vous devez effectuer des migrations incrémentielles.
  Par exemple, pour migrer un environnement IdM RHEL 7 vers RHEL 9 :
  a. Migrer des serveurs RHEL 7 vers les serveurs RHEL 8. Voir Migrer vers la gestion des identités sur RHEL 8.
  b. Migrer des serveurs RHEL 8 vers les serveurs RHEL 9, comme décrit dans cette section.

Cette section décrit comment **migrate** toutes les données et configurations de gestion d'identité (IdM) d'un serveur Red Hat Enterprise Linux (RHEL) 8 vers un serveur RHEL 9.

La procédure de migration comprend

1. Configurer un serveur IdM RHEL 9 et l'ajouter en tant que réplique à votre environnement IdM RHEL 8 actuel. Pour plus de détails, voir Installation du réplica RHEL 9 .
2. Faire du serveur RHEL 9 le serveur de renouvellement de l'autorité de certification (CA). Pour plus de détails, voir Attribution du rôle de serveur de renouvellement de l'autorité de certification au serveur IdM RHEL 9.

3. Arrêt de la génération de la liste de révocation des certificats (CRL) sur le serveur RHEL 8 et redirection des demandes de CRL vers la réplique RHEL 9. Pour plus d'informations, voir Arrêt de la génération de CRL sur un serveur d'autorité de certification IdM RHEL 8.

4. Démarrer la génération de la CRL sur le serveur RHEL 9. Pour plus de détails, voir Démarrer la génération de CRL sur le nouveau serveur CA IdM RHEL 9.

5. Arrêt et mise hors service du serveur de renouvellement de l'autorité de certification RHEL 8 d'origine. Pour plus d'informations, voir Arrêt et mise hors service du serveur RHEL 8 .

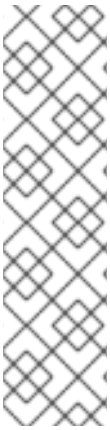
Dans les procédures suivantes :

- **rhel9.example.com** est le système RHEL 9 qui deviendra le nouveau serveur de renouvellement de l'autorité de certification.

- **rhel8.example.com** est le serveur de renouvellement de l'autorité de certification RHEL 8 d'origine. Pour identifier le serveur Red Hat Enterprise Linux 8 qui est le serveur de renouvellement de l'autorité de certification, exécutez la commande suivante sur n'importe quel serveur IdM :

```
[root@rhel8 ~]# ipa config-show | grep "CA renewal"
IPA CA renewal master: rhel8.example.com
```

  Si votre déploiement IdM n'utilise pas d'autorité de certification IdM, tout serveur IdM fonctionnant sous RHEL 8 peut être **rhel8.example.com**.



NOTE

Effectuez les étapes des sections suivantes **only** si votre déploiement IdM utilise une autorité de certification (CA) intégrée :

- Attribution du rôle de serveur de renouvellement de l'autorité de certification au serveur IdM RHEL 9
- Arrêt de la génération de CRL sur un serveur d'autorité de certification IdM RHEL 8
- Démarrage de la génération de CRL sur le nouveau serveur CA IdM RHEL 9

1.1. CONDITIONS PRÉALABLES À LA MIGRATION DE L'IDM DE RHEL 8 À 9

Sur **rhel8.example.com**:

1. Mettre à jour le système vers la dernière version de RHEL 8.

IMPORTANT

Si vous migrez vers RHEL 9.0, ne mettez pas à jour vers une version plus récente que RHEL 8.6. La migration à partir de RHEL 8.7 n'est prise en charge que pour RHEL 9.1.

2. Mettez à jour les **ipa-*** les paquets vers leur dernière version :

```
[root@rhel8 ~]# dnf update ipa-*
```

AVERTISSEMENT

Lors de la mise à niveau de plusieurs serveurs de gestion des identités (IdM), attendez au moins 10 minutes entre chaque mise à niveau.

Lorsque deux serveurs ou plus sont mis à niveau simultanément ou avec de courts intervalles entre les mises à niveau, il n'y a pas assez de temps pour répliquer les changements de données après la mise à niveau dans toute la topologie, ce qui peut entraîner des événements de réplication conflictuels.

Sur **rhel9.example.com**:

1. La dernière version de Red Hat Enterprise Linux est installée sur le système. Pour plus d'informations, voir Effectuer une installation standard de RHEL 9 .
2. Assurez-vous que le système est un client IdM inscrit dans le domaine pour lequel le serveur **rhel8.example.com** IdM fait autorité. Pour plus d'informations, voir Installation d'un client IdM : Scénario de base.
3. Assurez-vous que le système répond aux exigences requises pour l'installation du serveur IdM. Voir Préparation du système pour l'installation du serveur IdM .
4. Assurez-vous de connaître le serveur de temps avec lequel **rhel8.example.com** est synchronisé :

```
[root@rhel8 ~]# ntpstat
synchronised to NTP server (ntp.example.com) at stratum 3
   time correct to within 42 ms
   polling server every 1024 s
```

5. Assurez-vous que le système est autorisé à installer un réplica IdM. Voir Autoriser l'installation d'un réplica sur un client IdM.
6. Mettez à jour les **ipa-*** les paquets vers leur dernière version :

```
[root@rhel8 ~]# dnf update ipa-*
```

Ressources supplémentaires

- Pour déterminer les rôles de serveur que vous souhaitez installer sur le nouveau serveur primaire IdM, **rhel9.example.com**, consultez les liens suivants :
  - Pour plus d'informations sur le rôle du serveur CA dans IdM, voir Planification des services CA.
  - Pour plus de détails sur le rôle du serveur DNS dans IdM, voir Planification des services DNS et des noms d'hôtes.

  - Pour plus de détails sur l'intégration basée sur la confiance inter-forêts entre un IdM et Active Directory (AD), voir Intégration indirecte.

- Pour pouvoir installer des rôles de serveur spécifiques pour IdM dans RHEL 9, vous devez télécharger des paquets à partir de dépôts IdM spécifiques : Installation des paquets requis pour un serveur IdM.

- Pour mettre à niveau un système de RHEL 8 à RHEL 9, voir Mise à niveau de RHEL 8 à RHEL 9 .

1.2. INSTALLATION DE LA RÉPLIQUE RHEL 9

1. Listez les rôles de serveur présents dans votre environnement RHEL 8 :

```
[root@rhel8 ~]# ipa server-role-find --status enabled --server rhel8.example.com
----------------------
3 server roles matched
----------------------
  Server name: rhel8.example.com
  Role name: CA server
  Role status: enabled

  Server name: rhel8.example.com
  Role name: DNS server
  Role status: enabled
[... output truncated ...]
```

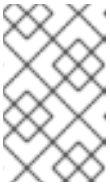
2. (Facultatif) Si vous souhaitez utiliser pour **rhel9.example.com** les mêmes transitaires par serveur que ceux utilisés par **rhel8.example.com**, affichez les transitaires par serveur pour **rhel8.example.com**:

```
[root@rhel8 ~]# ipa dnsserver-show rhel8.example.com
----------------------------
1 DNS server matched
----------------------------
  Server name: rhel8.example.com
  SOA mname: rhel8.example.com.
  Forwarders: 192.0.2.20
  Forward policy: only
------------------------------------------------
Number of entries returned 1
------------------------------------------------
```

3. Installez le logiciel du serveur IdM sur **rhel9.example.com** pour le configurer comme une réplique du serveur IdM RHEL 8, y compris tous les rôles de serveur présents sur **rhel8.example.com**. Pour installer les rôles de l'exemple ci-dessus, utilisez ces options avec la commande **ipa-replica-install**:

   - **--setup-ca** pour configurer le composant du système de certification

   - **--setup-dns** et **--forwarder** pour configurer un serveur DNS intégré et définir un forwarder par serveur pour prendre en charge les requêtes DNS qui sortent du domaine IdM



NOTE

En outre, si votre déploiement IdM est en relation de confiance avec Active Directory (AD), ajoutez l'option **--setup-adtrust** à la commande **ipa-replica-install** pour configurer la capacité de confiance AD sur **rhel9.example.com**.

- **--ntp-server** pour spécifier un serveur NTP ou **--ntp-pool** pour spécifier un pool de serveurs NTP
  Pour configurer un serveur IdM avec l'adresse IP 192.0.2.1 qui utilise un forwarder par serveur avec l'adresse IP 192.0.2.20 et qui se synchronise avec le serveur NTP **ntp.example.com**:

```
[root@rhel9 ~]# ipa-replica-install --setup-ca --ip-address 192.0.2.1 --setup-dns --forwarder 192.0.2.20 --ntp-server ntp.example.com
```

  Il n'est pas nécessaire de spécifier le serveur IdM RHEL 8 lui-même car si le DNS fonctionne correctement, **rhel9.example.com** le trouvera en utilisant l'autodécouverte du DNS.

4. (Facultatif) Ajoutez un enregistrement de service **_ntp._udp** (SRV) pour votre serveur de temps externe **NTP** au DNS du serveur IdM nouvellement installé, **rhel9.example.com**. La présence de l'enregistrement SRV pour le serveur de temps dans le DNS IdM garantit que les futures installations de répliques et de clients RHEL 9 sont automatiquement configurées pour se synchroniser avec le serveur de temps utilisé par **rhel9.example.com**. En effet, **ipa-client-install** recherche l'entrée DNS **_ntp._udp** à moins que les options **--ntp-server** ou **--ntp-pool** ne soient fournies dans l'interface de ligne de commande (CLI) de l'installation.

Vérification

1. Vérifiez que les services IdM sont en cours d'exécution sur **rhel9.example.com**:

```
[root@rhel9 ~]# ipactl status
Directory Service: RUNNING
[... output truncated ...]
ipa: INFO: The ipactl command was successful
```

2. Vérifiez que les rôles de serveur pour **rhel9.example.com** sont les mêmes que pour **rhel8.example.com**:

```
[root@rhel9 ~]# kinit admin
[root@rhel9 ~]# ipa server-role-find --status enabled --server rhel9.example.com
----------------------
2 server roles matched
----------------------
  Server name: rhel9.example.com
  Role name: CA server
  Role status: enabled

  Server name: rhel9.example.com
  Role name: DNS server
  Role status: enabled
```

3. (Facultatif) Affichez les détails de l'accord de réplication entre **rhel8.example.com** et **rhel9.example.com**:

```
[root@rhel9 ~]# ipa-csreplica-manage list --verbose rhel9.example.com
Directory Manager password:

rhel8.example.com
last init status: None
last init ended: 1970-01-01 00:00:00+00:00
last update status: Error (0) Replica acquired successfully: Incremental update succeeded
last update ended: 2019-02-13 13:55:13+00:00
```

4. (Facultatif) Si votre déploiement IdM est en relation de confiance avec AD, vérifiez qu'il fonctionne :

   a. Vérifier la configuration de Kerberos

   b. Tentative de résolution d'un utilisateur AD sur **rhel9.example.com**:

   ```
   [root@rhel9 ~]# id aduser@ad.domain
   ```

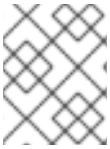
5. Vérifiez que **rhel9.example.com** est synchronisé avec le serveur **NTP**:

```
[root@rhel8 ~]# chronyc tracking
Reference ID    : CB00710F (ntp.example.com)
Stratum         : 3
Ref time (UTC)  : Wed Feb 16 09:49:17 2022
[... output truncated ...]
```

Ressources supplémentaires

- Priorités de la configuration DNS
- Exigences en matière de services horaires pour l'IdM

1.3. ATTRIBUTION DU RÔLE DE SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION AU SERVEUR IDM RHEL 9



NOTE

Ne suivez les étapes de cette section que si votre déploiement IdM utilise une autorité de certification (AC) intégrée.

Sur **rhel9.example.com**, configurez **rhel9.example.com** en tant que nouveau serveur de renouvellement de l'autorité de certification :

1. Configurez **rhel9.example.com** pour gérer le renouvellement des certificats du sous-système CA :

```
[root@rhel9 ~]# ipa config-mod --ca-renewal-master-server rhel9.example.com
 ...
 IPA masters: rhel8.example.com, rhel9.example.com
 IPA CA servers: rhel8.example.com, rhel9.example.com
 IPA CA renewal master: rhel9.example.com
```

   La sortie confirme que la mise à jour a été effectuée avec succès.

2. Sur **rhel9.example.com**, activez la tâche de mise à jour des certificats :
   a. Ouvrez le fichier de configuration **/etc/pki/pki-tomcat/ca/CS.cfg** pour le modifier.
   b. Supprimez l'entrée **ca.certStatusUpdateInterval** ou définissez l'intervalle souhaité en secondes. La valeur par défaut est **600**.
   c. Enregistrez et fermez le fichier de configuration **/etc/pki/pki-tomcat/ca/CS.cfg**.
   d. Redémarrer les services IdM :

```
[user@rhel9 ~]$ ipactl restart
```

3. Sur **rhel8.example.com**, désactivez la tâche de mise à jour des certificats :
   a. Ouvrez le fichier de configuration **/etc/pki/pki-tomcat/ca/CS.cfg** pour le modifier.
   b. Remplacez **ca.certStatusUpdateInterval** par **0**, ou ajoutez l'entrée suivante si elle n'existe pas :

```
ca.certStatusUpdateInterval=0
```

   c. Enregistrez et fermez le fichier de configuration **/etc/pki/pki-tomcat/ca/CS.cfg**.
   d. Redémarrer les services IdM :

```
[user@rhel8 ~]$ ipactl restart
```

1.4. ARRÊT DE LA GÉNÉRATION DE CRL SUR UN SERVEUR D'AUTORITÉ DE CERTIFICATION IDM RHEL 8

NOTE

Ne suivez les étapes de cette section que si votre déploiement IdM utilise une autorité de certification (AC) intégrée.

Cette section décrit comment arrêter la génération de la liste de révocation de certificats (CRL) sur le serveur de l'autorité de certification **rhel8.example.com** à l'aide de la commande **ipa-crlgen-manage**.

Conditions préalables

- Vous devez être connecté en tant que root.

Procédure

1. (Facultatif) Vérifiez que **rhel8.example.com** génère la CRL :

```
[root@rhel8 ~]# ipa-crlgen-manage status
CRL generation: enabled
Last CRL update: 2021-10-31 12:00:00
Last CRL Number: 6
The ipa-crlgen-manage command was successful
```

2. Arrêter la génération de la CRL sur le serveur **rhel8.example.com**:

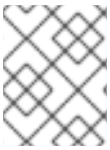
```
[root@rhel8 ~]# ipa-crlgen-manage disable
Stopping pki-tomcatd
Editing /var/lib/pki/pki-tomcat/conf/ca/CS.cfg
Starting pki-tomcatd
Editing /etc/httpd/conf.d/ipa-pki-proxy.conf
Restarting httpd
CRL generation disabled on the local host. Please make sure to configure CRL generation on another master with ipa-crlgen-manage enable.
The ipa-crlgen-manage command was successful
```

3. Optionnellement, vérifiez si le serveur **rhel8.example.com** a cessé de générer la CRL :

```
[root@rhel7 ~]# ipa-crlgen-manage status
```

Le serveur **rhel8.example.com** a cessé de générer la CRL. L'étape suivante consiste à activer la génération de la CRL sur **rhel9.example.com**.

1.5. DÉMARRAGE DE LA GÉNÉRATION DE CRL SUR LE NOUVEAU SERVEUR CA IDM RHEL 9



NOTE

Ne suivez les étapes de cette section que si votre déploiement IdM utilise une autorité de certification (AC) intégrée.

Conditions préalables

- Vous devez être connecté en tant que root sur la machine **rhel9.example.com**.

Procédure

1. Pour commencer à générer la CRL sur **rhel9.example.com**, utilisez la commande **ipa-crlgen-manage enable**:

```
[root@rhel9 ~]# ipa-crlgen-manage enable
Stopping pki-tomcatd
Editing /var/lib/pki/pki-tomcat/conf/ca/CS.cfg
Starting pki-tomcatd
Editing /etc/httpd/conf.d/ipa-pki-proxy.conf
Restarting httpd
Forcing CRL update
CRL generation enabled on the local host. Please make sure to have only a single CRL generation master.
The ipa-crlgen-manage command was successful
```

Verification steps

- Pour vérifier si la génération de CRL est activée, utilisez la commande **ipa-crlgen-manage status**:

```
[root@rhel8 ~]# ipa-crlgen-manage status
CRL generation: enabled
Last CRL update: 2021-10-31 12:10:00
Last CRL Number: 7
The ipa-crlgen-manage command was successful
```

1.6. ARRÊT ET MISE HORS SERVICE DU SERVEUR RHEL 8

1. Assurez-vous que toutes les données, y compris les dernières modifications, ont été correctement transférées de **rhel8.example.com** à **rhel9.example.com**. Par exemple :

   a. Ajouter un nouvel utilisateur sur **rhel8.example.com**:

   ```
   [root@rhel8 ~]# ipa user-add random_user
   First name: random
   Last name: user
   ```

   b. Vérifiez que l'utilisateur a été répliqué sur **rhel9.example.com**:

   ```
   [root@rhel9 ~]# ipa user-find random_user
   --------------
   1 user matched
   --------------
     User login: random_user
     First name: random
     Last name: user
   ```

2. Arrêtez tous les services IdM sur **rhel8.example.com** pour forcer la découverte du domaine sur le nouveau serveur **rhel9.example.com**.

   ```
   [root@rhel7 ~]# ipactl stop
   Stopping CA Service
   Stopping pki-ca:                                   [  OK  ]
   Stopping HTTP Service
   Stopping httpd:                                    [  OK  ]
   Stopping MEMCACHE Service
   Stopping ipa_memcached:                            [  OK  ]
   Stopping DNS Service
   Stopping named:                                    [  OK  ]
   Stopping KPASSWD Service
   Stopping Kerberos 5 Admin Server:                  [  OK  ]
   Stopping KDC Service
   Stopping Kerberos 5 KDC:                           [  OK  ]
   Stopping Directory Service
   Shutting down dirsrv:
     EXAMPLE-COM...                                   [  OK  ]
     PKI-IPA...                                       [  OK  ]
   ```

   Ensuite, l'utilitaire **ipa** contactera le nouveau serveur par le biais d'un appel de procédure à distance (RPC).

3. Supprimez le serveur RHEL 8 de la topologie en exécutant les commandes de suppression sur le serveur RHEL 9. Pour plus de détails, voir Désinstallation d'un serveur IdM .

CHAPITRE 2. MISE À NIVEAU D'UN CLIENT IDM DE RHEL 8 À RHEL 9

Contrairement aux serveurs IdM, la mise à niveau d'un client IdM de RHEL 8 à RHEL 9 est possible. L'utilitaire de mise à niveau en place de Leapp effectue tous les changements de configuration nécessaires.

PARTIE II. MIGRATION VERS L'IDM À PARTIR DE SOURCES EXTERNES

CHAPITRE 3. MIGRATION VERS IDM SUR RHEL 9 À PARTIR DE FREEIPA SUR DES DISTRIBUTIONS LINUX NON RHEL

Pour migrer un déploiement FreeIPA sur une distribution Linux non RHEL vers un déploiement Identity Management (IdM) sur des serveurs RHEL 9, vous devez d'abord ajouter une nouvelle réplique d'autorité de certification (CA) IdM RHEL 9 à votre environnement FreeIPA existant, lui transférer les rôles liés aux certificats, puis mettre hors service les serveurs FreeIPA non RHEL.

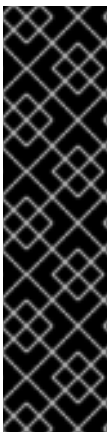
AVERTISSEMENT

La conversion sur place d'un serveur FreeIPA non RHEL en un serveur IdM RHEL 9 à l'aide de l'outil Convert2RHEL n'est pas prise en charge.

IMPORTANT

L'utilisation de l'algorithme **SHA-1** étant désactivée dans la stratégie cryptographique du système **DEFAULT** dans RHEL 9, plusieurs problèmes connus peuvent survenir si un système RHEL 9 est utilisé dans le même déploiement IdM qu'un système non RHEL-9. Pour plus de détails, voir :

- Notes de mise à jour pour Red Hat Enterprise Linux 9.0
- Notes de mise à jour pour Red Hat Enterprise Linux 9.1
- Notes de mise à jour pour Red Hat Enterprise Linux 9.2



IMPORTANT

Après la mise à niveau de votre réplique IdM vers RHEL 9.2, le centre de distribution Kerberos (KDC) IdM peut ne pas délivrer de tickets d'attribution de tickets (TGT) aux utilisateurs qui n'ont pas d'identifiants de sécurité (SID) attribués à leurs comptes. Par conséquent, les utilisateurs ne peuvent pas se connecter à leurs comptes.

Pour contourner le problème, générez des SID en exécutant **# ipa config-mod --enable-sid --add-sids** en tant qu'administrateur IdM sur une autre réplique IdM dans la topologie. Ensuite, si les utilisateurs ne peuvent toujours pas se connecter, examinez le journal des erreurs du serveur d'annuaire. Il se peut que vous deviez ajuster les plages d'ID pour inclure les identités POSIX des utilisateurs.

Conditions préalables

Sur le système RHEL 9 :

1. La dernière version de Red Hat Enterprise Linux est installée sur le système. Pour plus d'informations, voir Effectuer une installation standard de RHEL 9 .
2. S'assurer que le système est un client IdM inscrit dans le domaine pour lequel le serveur FreeIPA fait autorité. Pour plus d'informations, voir Installation d'un client IdM : Scénario de base .

3. Assurez-vous que le système répond aux exigences requises pour l'installation du serveur IdM. Voir Préparation du système pour l'installation du serveur IdM .

4. Assurez-vous que le système est autorisé à installer un réplica IdM. Voir Autoriser l'installation d'un réplica sur un client IdM.

Sur le serveur FreeIPA non RHEL :

1. Assurez-vous de connaître le serveur de temps avec lequel le système est synchronisé :

```
[root@freeipaserver ~]# ntpstat
synchronised to NTP server (ntp.example.com) at stratum 3
  time correct to within 42 ms
  polling server every 1024 s
```

2. Mettez à jour les **ipa-*** les paquets vers leur dernière version :

```
[root@freeipaserver ~]# dnf update ipa-*
```

Procédure

1. Pour effectuer la migration, suivez la même procédure que pour la migration de votre environnement IdM des serveurs RHEL 8 vers les serveurs RHEL 9, avec votre réplique d'autorité de certification FreeIPA non RHEL agissant en tant que serveur RHEL 8 :

   a. Configurez un serveur RHEL 9 et ajoutez-le comme réplique IdM à votre environnement FreeIPA actuel sur la distribution Linux non RHEL. Pour plus de détails, voir Installation de la réplique RHEL 9.

   b. Faire de la réplique RHEL 9 le serveur de renouvellement de l'autorité de certification (CA). Pour plus de détails, voir Attribution du rôle de serveur de renouvellement de l'autorité de certification au serveur IdM RHEL 9.

   c. Arrêtez la génération de la liste de révocation des certificats (CRL) sur le serveur non RHEL et redirigez les demandes de CRL vers la réplique RHEL 9. Pour plus d'informations, voir Arrêt de la génération de CRL sur un serveur d'autorité de certification IdM RHEL 8 .

   d. Lancez la génération de la CRL sur le serveur RHEL 9. Pour plus de détails, voir Lancer la génération de CRL sur le nouveau serveur CA IdM RHEL 9.

   e. Arrêtez et mettez hors service le serveur de renouvellement de l'autorité de certification FreeIPA non RHEL d'origine. Pour plus de détails, voir Arrêter et décommissionner le serveur RHEL 8.

Ressources supplémentaires

- Migration de votre environnement IdM des serveurs RHEL 8 vers les serveurs RHEL 9

CHAPITRE 4. MIGRATION D'UN ANNUAIRE LDAP VERS IDM

Si vous avez précédemment déployé un serveur LDAP pour les recherches d'identité et d'authentification, vous pouvez migrer le service de recherche vers Identity Management (IdM). IdM propose un outil de migration pour vous aider dans les tâches suivantes :

- Transfert des comptes d'utilisateurs, y compris les mots de passe et l'appartenance à des groupes, sans perte de données.
- Éviter les mises à jour coûteuses de la configuration sur les clients.

Le processus de migration décrit ici suppose un scénario de déploiement simple avec un espace de noms dans LDAP et un dans IdM. Pour des environnements plus complexes, tels que ceux avec des espaces de noms multiples ou des schémas personnalisés, contactez les services d'assistance de Red Hat.

4.1. CONSIDÉRATIONS RELATIVES À LA MIGRATION DE LDAP VERS IDM

Le processus de passage d'un serveur LDAP à la gestion de l'identité (IdM) se déroule selon les étapes suivantes :

- Migration du site *clients*. Planifiez cette étape avec soin. Déterminez les services utilisés par chaque client dans votre infrastructure actuelle. Il peut s'agir par exemple de Kerberos ou de Systems Security Services Daemon (SSSD). Déterminez ensuite lesquels de ces services vous pouvez utiliser dans le déploiement final de l'IdM. Pour plus d'informations, voir Planification de la configuration du client lors de la migration de LDAP vers IdM.
- Migration du site *data*.
- Migration du site *passwords*. Planifiez cette étape avec soin. Outre les mots de passe, IdM exige des hachages Kerberos pour chaque compte d'utilisateur. Certaines considérations et certains chemins de migration pour les mots de passe sont abordés dans Planification de la migration des mots de passe lors de la migration de LDAP vers IdM.

Vous pouvez d'abord migrer la partie serveur et ensuite les clients ou d'abord les clients et ensuite le serveur. Pour plus d'informations sur les deux types de migration, voir Séquence de migration de LDAP vers IdM.

IMPORTANT

Il est fortement recommandé de mettre en place un environnement LDAP de test et de tester le processus de migration avant de tenter de migrer l'environnement LDAP réel. Lors du test de l'environnement, procédez comme suit

1. Créez un utilisateur test dans IdM et comparez le résultat des utilisateurs migrés à celui de l'utilisateur test. Assurez-vous que les utilisateurs migrés contiennent l'ensemble minimal d'attributs et de classes d'objets présents sur l'utilisateur test.
2. Comparez les résultats des utilisateurs migrés, tels qu'ils apparaissent sur IdM, aux utilisateurs sources, tels qu'ils apparaissent sur le serveur LDAP d'origine. Assurez-vous que les attributs importés ne sont pas copiés deux fois et qu'ils ont les bonnes valeurs.

4.2. PLANIFICATION DE LA CONFIGURATION DU CLIENT LORS DE LA MIGRATION DE LDAP VERS IDM

La gestion des identités (IdM) peut prendre en charge un certain nombre de configurations client différentes, avec divers degrés de fonctionnalité, de flexibilité et de sécurité. Décidez de la configuration qui convient le mieux à chaque client en fonction de son système d'exploitation et de vos priorités en matière de maintenance informatique. Tenez également compte du domaine fonctionnel du client : une machine de développement nécessite généralement une configuration différente de celle des serveurs de production ou des ordinateurs portables des utilisateurs.

IMPORTANT

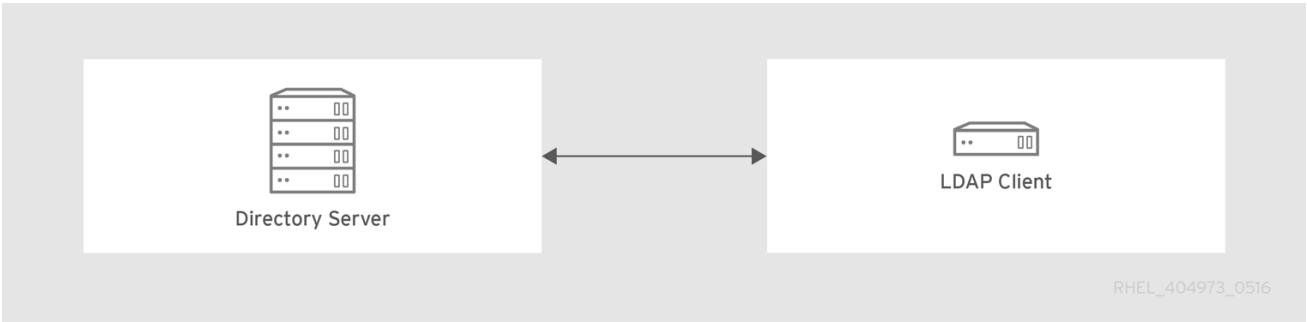
Dans la plupart des environnements, les clients se connectent au domaine IdM de différentes manières. Les administrateurs doivent décider du scénario qui convient le mieux à chaque client.

4.2.1. Configuration initiale du client avant la migration

Avant de décider des spécificités de la configuration du client dans la gestion des identités (IdM), il faut d'abord établir les spécificités de la configuration actuelle, avant la migration.

L'état initial de presque tous les déploiements LDAP à migrer est l'existence d'un service LDAP fournissant des services d'identité et d'authentification.

Figure 4.1. Configuration de base de l'annuaire LDAP et du client



Les clients Linux et Unix utilisent les bibliothèques PAM_LDAP et NSS_LDAP pour se connecter directement aux services LDAP. Ces bibliothèques permettent aux clients d'extraire des informations sur les utilisateurs de l'annuaire LDAP comme si les données étaient stockées dans **/etc/passwd** ou **/etc/shadow**. Dans la réalité, l'infrastructure peut être plus complexe si un client utilise LDAP pour les recherches d'identité et Kerberos pour l'authentification ou d'autres configurations.

Il existe des différences structurelles entre un annuaire LDAP et un serveur de gestion des identités (IdM), notamment en ce qui concerne la prise en charge des schémas et la structure de l'arborescence de l'annuaire. Pour plus d'informations sur ces différences, voir la section **Contrasting IdM with a Standard LDAP Directory** de la page Planification de la configuration du client lors de la migration de LDAP vers IdM. Ces différences peuvent avoir un impact sur les données, en particulier sur l'arborescence de l'annuaire, qui affecte les noms d'entrée. Cependant, les différences ont peu d'impact sur la configuration du client et sur la migration des clients vers IdM.

4.2.2. Configuration recommandée pour les clients RHEL

NOTE

La configuration client décrite dans cette section n'est prise en charge que pour les versions RHEL 6.1 et ultérieures et RHEL 5.7 ultérieures, qui prennent en charge les dernières versions de SSSD et le paquetage **ipa-client**. Les versions plus anciennes de RHEL peuvent être configurées comme décrit dans Configuration alternative prise en charge.

Le System Security Services Daemon (SSSD) de Red Hat Enterprise Linux (RHEL) utilise des bibliothèques PAM et NSS spéciales, **pam_sss** et **nss_sss**. Grâce à ces bibliothèques, SSSD peut s'intégrer très étroitement à la gestion des identités (IdM) et bénéficier de toutes ses fonctions d'authentification et d'identité. SSSD dispose d'un certain nombre de fonctions utiles, telles que la mise en cache des informations d'identité afin que les utilisateurs puissent se connecter même si la connexion au serveur central est perdue.

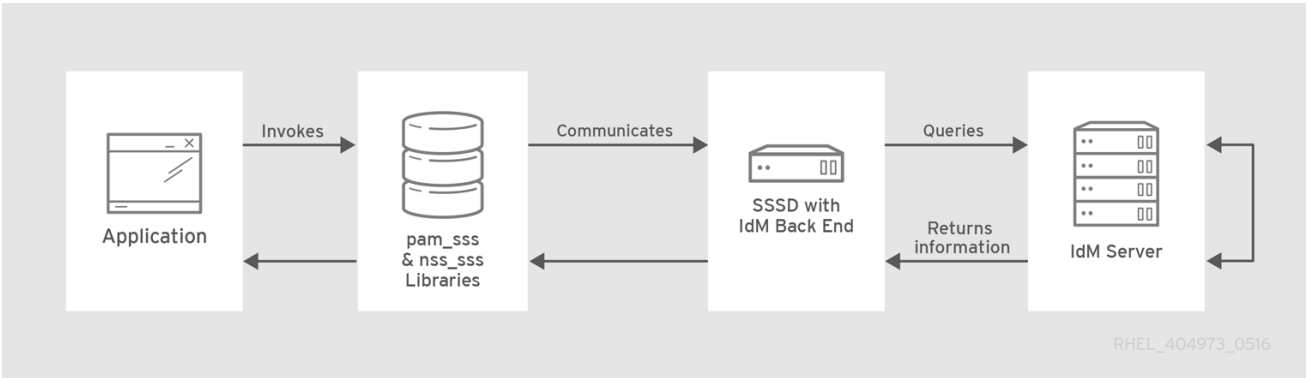
Contrairement aux services d'annuaire LDAP génériques qui utilisent les bibliothèques **pam_ldap** et **nss_ldap**, SSSD établit des relations entre les informations d'identité et d'authentification en définissant *domains*. Dans SSSD, un domaine définit les fonctions dorsales suivantes :

- Authentification
- Recherche d'identité
- Accès
- Modification du mot de passe

Le domaine SSSD est ensuite configuré pour utiliser un site *provider* afin de fournir les informations nécessaires à l'une ou à l'ensemble de ces fonctions. La configuration du domaine nécessite toujours un fournisseur *identity*. Les trois autres fournisseurs sont facultatifs ; si un fournisseur d'authentification, d'accès ou de mot de passe n'est pas défini, c'est le fournisseur d'identité qui est utilisé pour cette fonction.

SSSD peut utiliser IdM pour toutes ses fonctions d'arrière-plan. Il s'agit de la configuration idéale, car elle offre toute la gamme des fonctionnalités de l'IdM, contrairement aux fournisseurs d'identité LDAP génériques ou à l'authentification Kerberos. Par exemple, au cours des opérations quotidiennes, le SSSD applique les règles de contrôle d'accès basées sur l'hôte et les fonctions de sécurité de l'IdM.

Figure 4.2. Clients et SSSD avec un back-end IdM



Le script **ipa-client-install** configure automatiquement SSSD pour qu'il utilise IdM pour tous ses services back-end, de sorte que les clients RHEL sont configurés par défaut avec la configuration recommandée.

Informations complémentaires

- Comprendre le SSSD et ses avantages

4.2.3. Configuration alternative supportée

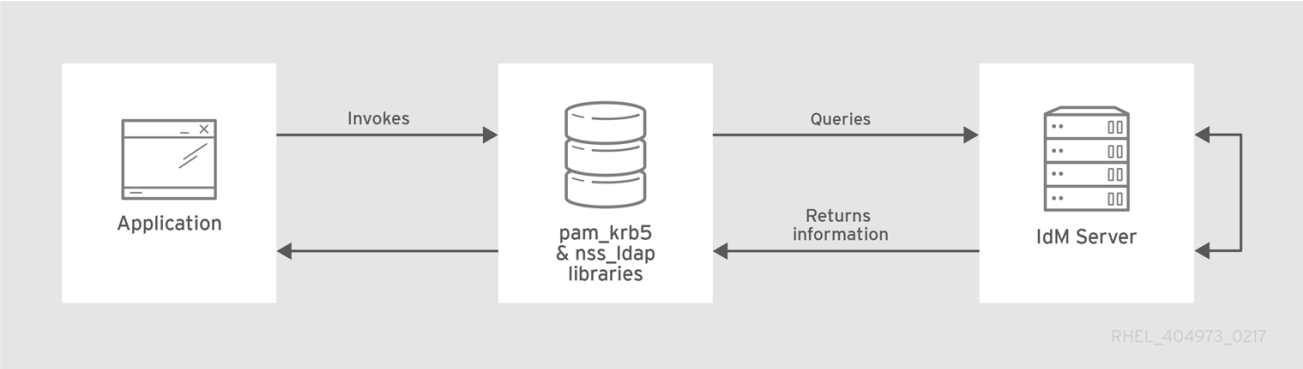
Les systèmes Unix et Linux tels que Mac, Solaris, HP-UX, AIX et Scientific Linux prennent en charge tous les services gérés par la gestion des identités (IdM), mais n'utilisent pas SSSD. De même, les anciennes versions de Red Hat Enterprise Linux (RHEL), en particulier 6.1 et 5.6, prennent en charge SSSD mais ont une version plus ancienne qui ne prend pas en charge IdM en tant que fournisseur d'identité.

S'il n'est pas possible d'utiliser une version moderne de SSSD sur un système, les clients peuvent être configurés de la manière suivante :

- Le client se connecte au serveur IdM comme s'il s'agissait d'un serveur d'annuaire LDAP pour les recherches d'identité, en utilisant **nss_ldap**.
- Le client se connecte au serveur IdM comme s'il s'agissait d'un KDC Kerberos ordinaire, en utilisant **pam_krb5**.

Pour plus d'informations sur la configuration d'un site *RHEL client with an older version of SSSD* afin qu'il utilise le serveur IdM comme fournisseur d'identité et domaine d'authentification Kerberos, voir la section Configuration des fournisseurs d'identité et d'authentification pour SSSD du manuel RHEL 7 *System-Level Authentication Guide*.

Figure 4.3. Clients et IdM avec LDAP et Kerberos



La meilleure pratique consiste généralement à utiliser la configuration la plus sûre possible pour un client. Cela signifie SSSD ou LDAP pour les identités et Kerberos pour l'authentification. Cependant, dans certaines situations de maintenance et structures informatiques, il peut être nécessaire de recourir au scénario le plus simple possible : configurer LDAP pour fournir à la fois l'identité et l'authentification en utilisant les bibliothèques **nss_ldap** et **pam_ldap** sur les clients.

4.3. PLANIFICATION DE LA MIGRATION DES MOTS DE PASSE LORS DE LA MIGRATION DE LDAP VERS IDM

Une question cruciale à laquelle il faut répondre avant de migrer les utilisateurs de LDAP vers Identity Management (IdM) est de savoir s'il faut migrer les mots de passe des utilisateurs ou non. Les options suivantes sont disponibles :

Migration des utilisateurs sans mot de passe

Peut être réalisée plus rapidement mais nécessite plus de travail manuel de la part des administrateurs et des utilisateurs. Dans certaines situations, c'est la seule option possible : par exemple, si l'environnement LDAP d'origine stockait les mots de passe des utilisateurs en clair ou si les mots de passe ne répondent pas aux exigences de la politique de mot de passe définie dans l'IdM.

Lors de la migration de comptes d'utilisateurs sans mot de passe, vous réinitialisez tous les mots de passe des utilisateurs. Les utilisateurs migrés se voient attribuer un mot de passe temporaire qu'ils modifient lors de leur première connexion. Pour plus d'informations sur la réinitialisation des mots de passe, voir Modification et réinitialisation des mots de passe des utilisateurs dans la documentation de HREL 7 IdM.

Migration des utilisateurs avec leurs mots de passe

Cette solution permet une transition plus aisée, mais nécessite également une gestion parallèle de l'annuaire LDAP et de l'IdM au cours du processus de migration et de transition. La raison en est que, par défaut, IdM utilise Kerberos pour l'authentification et exige que chaque utilisateur ait un hachage Kerberos stocké dans le serveur d'annuaire IdM en plus du mot de passe standard de l'utilisateur. Pour générer le hachage, le mot de passe de l'utilisateur doit être accessible au serveur IdM en texte clair. Lorsque vous créez un nouveau mot de passe utilisateur, le mot de passe est disponible en clair avant d'être haché et stocké dans IdM. Toutefois, lorsque l'utilisateur est migré à partir d'un répertoire LDAP, le mot de passe de l'utilisateur associé est déjà haché, de sorte que la clé Kerberos correspondante ne peut pas être générée.

IMPORTANT

Par défaut, les utilisateurs ne peuvent pas s'authentifier auprès du domaine IdM ou accéder aux ressources IdM tant qu'ils n'ont pas de hash Kerberos - même si les comptes d'utilisateurs existent déjà. Il existe une solution de contournement : l'utilisation de l'authentification LDAP dans IdM au lieu de l'authentification Kerberos. Avec cette solution, les hashs Kerberos ne sont pas nécessaires pour les utilisateurs. Toutefois, cette solution limite les capacités de l'IdM et n'est pas recommandée.

Les sections suivantes expliquent comment migrer les utilisateurs et leurs mots de passe :

- Méthodes de migration des mots de passe lors de la migration de LDAP vers IdM
  - Utilisation d'une page web
  - Utilisation de SSSD
- Planifier la migration des mots de passe LDAP en clair
- Planification de la migration des mots de passe LDAP qui ne répondent pas aux exigences de l'IdM

4.3.1. Méthodes de migration des mots de passe lors de la migration de LDAP vers IdM

Pour migrer des comptes d'utilisateurs de LDAP vers Identity Management (IdM) sans obliger les utilisateurs à changer leurs mots de passe, vous pouvez utiliser les méthodes suivantes :

Method 1: Using the migration web page

Demander aux utilisateurs d'entrer leurs identifiants LDAP une seule fois dans une page spéciale de l'interface utilisateur Web IdM, ***https://ipaserver.example.com/ipa/migration***. Un script exécuté en arrière-plan capture alors le mot de passe en clair et met correctement à jour le compte utilisateur avec le mot de passe et un hachage Kerberos approprié.

Method 2 (recommended): Using SSSD

Atténuez l'impact de la migration sur les utilisateurs en utilisant le démon des services de sécurité du système (SSSD) pour générer les clés utilisateur requises. C'est le meilleur scénario pour les déploiements avec un grand nombre d'utilisateurs ou lorsque les utilisateurs ne doivent pas être gênés par les changements de mot de passe.

Flux de travail

1. Un utilisateur tente de se connecter à une machine avec SSSD.
2. SSSD tente d'effectuer une authentification Kerberos contre le serveur IdM.
3. Bien que l'utilisateur existe dans le système, l'authentification échoue avec l'erreur *key type is not supported* parce que les hachages Kerberos n'existent pas encore.
4. SSSD effectue une liaison LDAP en texte clair par le biais d'une connexion sécurisée.
5. L'IdM intercepte cette demande de liaison. Si l'utilisateur a un principal Kerberos mais pas de hachages Kerberos, le fournisseur d'identité IdM génère les hachages et les stocke dans l'entrée de l'utilisateur.
6. Si l'authentification est réussie, SSSD se déconnecte de l'IdM et réessaie l'authentification Kerberos. Cette fois, la demande aboutit car le hachage existe dans l'entrée.

Avec la méthode 2, l'ensemble du processus est invisible pour les utilisateurs. Ils se connectent à un service client sans remarquer que leur mot de passe a été transféré de LDAP à IdM.

4.3.2. Planifier la migration des mots de passe LDAP en clair

Bien que dans la plupart des déploiements, les mots de passe LDAP soient stockés de manière cryptée, certains utilisateurs ou certains environnements peuvent utiliser des mots de passe en clair pour les entrées utilisateur.

Lorsque les utilisateurs sont transférés du serveur LDAP au serveur IdM, leurs mots de passe en clair ne sont pas transférés car IdM n'autorise pas les mots de passe en clair. Au lieu de cela, un principal Kerberos est créé pour chaque utilisateur, le keytab est défini sur true et le mot de passe est défini comme expiré. Cela signifie que l'IdM demande à l'utilisateur de réinitialiser le mot de passe lors de la prochaine connexion. Pour plus d'informations, voir Planifier la migration des mots de passe LDAP qui ne répondent pas aux exigences de l'IdM.

4.3.3. Planification de la migration des mots de passe LDAP qui ne répondent pas aux exigences de l'IdM

Si les mots de passe des utilisateurs dans le répertoire d'origine ne sont pas conformes aux politiques de mot de passe définies dans la gestion des identités (IdM), les mots de passe deviennent invalides après la migration.

La réinitialisation du mot de passe est effectuée automatiquement la première fois qu'un utilisateur tente d'obtenir un ticket Kerberos (TGT) dans le domaine IdM en entrant **kinit**. L'utilisateur est obligé de changer son mot de passe :

```
[migrated_idm_user@idmclient ~]$ kinit
Password for migrated_idm_user@IDM.EXAMPLE.COM:
Password expired.  You must change it now.
Enter new password:
Enter it again:
```

4.4. AUTRES CONSIDÉRATIONS ET EXIGENCES EN MATIÈRE DE MIGRATION

Lorsque vous planifiez une migration d'un serveur LDAP vers la gestion des identités (IdM), assurez-vous que votre environnement LDAP est en mesure de fonctionner avec le script de migration IdM.

4.4.1. Serveurs LDAP pris en charge pour la migration

Le processus de migration d'un serveur LDAP vers IdM utilise un script spécial, **ipa migrate-ds**, pour effectuer la migration. Ce script a des exigences spécifiques concernant la structure de l'annuaire LDAP et les entrées LDAP. La migration n'est possible que pour les services d'annuaire conformes à LDAPv3, qui comprennent plusieurs annuaires courants :

- Sun ONE Directory Server
- Serveur d'annuaire Apache
- OpenLDAP

La migration d'un serveur LDAP vers IdM a été testée avec Red Hat Directory Server et OpenLDAP.

NOTE

La migration à l'aide du script de migration est *not* prise en charge pour Microsoft Active Directory car il ne s'agit pas d'un répertoire conforme à LDAPv3. Pour obtenir de l'aide sur la migration à partir d'Active Directory, contactez les services professionnels de Red Hat.

4.4.2. Exigences de l'environnement LDAP pour la migration

Il existe de nombreux scénarios de configuration possibles pour les serveurs LDAP et pour la gestion des identités (IdM), ce qui influe sur la fluidité du processus de migration. Les exemples de procédures de migration présentés dans ce chapitre reposent sur les hypothèses suivantes concernant l'environnement :

- Un seul domaine d'annuaire LDAP est en cours de migration vers un domaine IdM. Il n'y a pas de consolidation.
- Le mot de passe d'un utilisateur est stocké sous forme de hachage dans l'annuaire LDAP. Pour obtenir une liste des hachages pris en charge, consultez la section Password Storage Schemes dans le titre *Configuration, Command, and File Reference* disponible dans la section Red Hat Directory Server 10 de la documentation de Red Hat Directory Server .
- L'instance d'annuaire LDAP est à la fois le magasin d'identité et la méthode d'authentification. Les machines clientes sont configurées pour utiliser la bibliothèque **pam_ldap** ou **nss_ldap** afin de se connecter au serveur LDAP.
- Les entrées utilisent uniquement le schéma LDAP standard. Les entrées qui contiennent des classes d'objets ou des attributs personnalisés ne sont pas migrées vers IdM.
- La commande **migrate-ds** ne migre que les comptes suivants :
  - Ceux qui contiennent un attribut **gidNumber**. L'attribut est requis par la classe d'objets **posixAccount**.

- Ceux qui contiennent un attribut **sn**. L'attribut est requis par la classe d'objets **person**.

4.4.3. Exigences du système IdM pour la migration

Dans le cas d'un annuaire de taille modérée (environ 10 000 utilisateurs et 10 groupes), il est nécessaire de disposer d'un système IdM cible suffisamment puissant pour permettre la migration. Les exigences minimales pour une migration sont les suivantes

- 4 cœurs
- 4GB de RAM
- 30 Go d'espace disque
- Une taille de tampon SASL de 2MB, qui est la valeur par défaut pour un serveur IdM
  En cas d'erreurs de migration, augmentez la taille de la mémoire tampon :

```
[root@ipaserver ~]# ldapmodify -x -D 'cn=directory manager' -w password -h
ipaserver.example.com -p 389

dn: cn=config
changetype: modify
replace: nsslapd-sasl-max-buffer-size
nsslapd-sasl-max-buffer-size: 4194304

modifying entry "cn=config"
```

  Définir la valeur de **nsslapd-sasl-max-buffer-size** en octets.

Ressources supplémentaires

- Recommandations concernant le matériel du serveur IdM

4.4.4. Considérations sur les règles sudo

Si vous utilisez **sudo** avec LDAP, vous devez migrer manuellement les règles **sudo** stockées dans LDAP vers Identity Management (IdM). Red Hat vous recommande de recréer les groupes de réseau dans IdM en tant que groupes d'hôtes. IdM présente automatiquement les groupes d'hôtes comme des groupes de réseaux traditionnels pour les configurations **sudo** qui n'utilisent pas le fournisseur SSSD **sudo**.

4.4.5. Outils de migration de LDAP vers IdM

Identity Management (IdM) utilise une commande spécifique, **ipa migrate-ds**, pour exécuter le processus de migration afin que les données de l'annuaire LDAP soient correctement formatées et importées dans le serveur IdM. Lors de l'utilisation de **ipa migrate-ds**, l'utilisateur du système distant, spécifié par l'option **--bind-dn**, doit avoir un accès en lecture à l'attribut **userPassword**, sinon les mots de passe ne seront pas migrés.

Le serveur IdM doit être configuré pour fonctionner en mode migration, puis le script de migration peut être utilisé. Pour plus de détails, voir Migration d'un serveur LDAP vers IdM .

4.4.6. Amélioration des performances de la migration de LDAP vers IdM

Une migration LDAP est essentiellement une opération d'importation spécialisée pour l'instance 389

Directory Server (DS) au sein du serveur IdM. L'optimisation de l'instance 389 DS pour améliorer les performances de l'opération d'importation peut contribuer à améliorer les performances globales de la migration.

Deux paramètres influent directement sur les performances des importations :

- L'attribut **nsslapd-cachememsize**, qui définit la taille autorisée pour le cache d'entrée. Il s'agit d'une mémoire tampon qui est automatiquement fixée à 80 % de la taille totale de la mémoire cache. Pour les opérations d'importation importantes, vous pouvez augmenter ce paramètre et éventuellement la taille de la mémoire cache elle-même. Cette augmentation améliorera l'efficacité du service d'annuaire dans la gestion d'un grand nombre d'entrées ou d'entrées avec de grands attributs.
  Pour plus d'informations sur la modification de l'attribut à l'aide de la commande **dsconf**, voir Ajustement de la taille du cache d'entrée .

- L'option de configuration system **ulimit** définit le nombre maximal de processus autorisés pour un utilisateur du système. Le traitement d'une base de données volumineuse peut dépasser cette limite. Dans ce cas, augmentez la valeur :

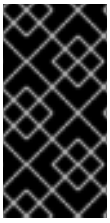
  ```
  [root@server ~]# ulimit -u 4096
  ```

Ressources supplémentaires

- Ajustement des performances du serveur d'annuaire IdM

4.4.7. Séquence de migration de LDAP vers IdM

La migration vers IdM comporte quatre étapes principales, dont l'ordre varie selon que l'on souhaite d'abord migrer le site *server* ou le site *clients*.



IMPORTANT

Les migrations "client d'abord" et "serveur d'abord" fournissent toutes deux une procédure de migration générale, mais elles peuvent ne pas fonctionner dans tous les environnements. Mettez en place un environnement LDAP de test et testez le processus de migration avant d'essayer de migrer l'environnement LDAP réel.

La migration du client d'abord

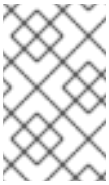
SSSD est utilisé pour modifier la configuration du client lorsqu'un serveur de gestion d'identité (IdM) est configuré :

1. Déployer SSSD.
2. Reconfigurer les clients pour qu'ils se connectent au serveur LDAP actuel et qu'ils basculent ensuite vers IdM.
3. Installer le serveur IdM.
4. Migrer les données des utilisateurs à l'aide du script IdM **ipa migrate-ds**. Ce script exporte les données de l'annuaire LDAP, les formate pour le schéma IdM, puis les importe dans IdM.
5. Mettre le serveur LDAP hors ligne et permettre aux clients de basculer vers IdM de manière transparente.

Migration vers le serveur d'abord

La migration de LDAP vers IdM vient en premier :

1. Installer le serveur IdM.
2. Migrer les données des utilisateurs à l'aide du script IdM **ipa migrate-ds**. Ce script exporte les données de l'annuaire LDAP, les formate pour le schéma IdM, puis les importe dans IdM.
3. *Optional.* Déployer SSSD.
4. Reconfigurer les clients pour qu'ils se connectent à IdM. Il n'est pas possible de remplacer simplement le serveur LDAP. L'arborescence de l'IdM - et donc les DN d'entrée des utilisateurs - est différente de l'arborescence précédente.
   Bien qu'il soit nécessaire de reconfigurer les clients, il n'est pas nécessaire de le faire immédiatement. Les clients mis à jour peuvent pointer vers le serveur IdM tandis que d'autres clients pointent vers l'ancien répertoire LDAP, ce qui permet une phase de test et de transition raisonnable après la migration des données.



NOTE

Ne pas faire fonctionner en parallèle un service d'annuaire LDAP et le serveur IdM pendant très longtemps. En effet, les données des utilisateurs risquent de devenir incohérentes entre les deux services.

4.5. PERSONNALISATION DE LA MIGRATION DE LDAP VERS IDM

Vous pouvez migrer vos services d'authentification et d'autorisation d'un serveur LDAP vers Identity Management (IdM) à l'aide de la commande **ipa migrate-ds**. Sans options supplémentaires, la commande prend l'URL LDAP de l'annuaire à migrer et exporte les données sur la base des paramètres par défaut courants.

Vous pouvez personnaliser le processus de migration et la manière dont les données sont identifiées et exportées en utilisant différentes options de la commande **ipa migrate-ds**. Personnalisez la migration si l'arborescence de votre annuaire LDAP a une structure unique ou si vous savez que vous devez exclure certaines entrées ou certains attributs dans les entrées.

4.5.1. Exemples de personnalisation du DN de liaison et du DN de base lors de la migration de LDAP vers IdM

Utilisez la commande **ipa migrate-ds** pour migrer de LDAP vers Identity Management (IdM). Sans options supplémentaires, la commande prend l'URL LDAP de l'annuaire à migrer et exporte les données sur la base des paramètres par défaut courants. Cette section décrit des exemples de modification des paramètres par défaut.

```
# ipa migrate-ds ldap://ldap.example.com:389
```

Personnalisation du DN de liaison

Par défaut, le DN "**cn=Directory Manager**" est utilisé pour se lier à l'annuaire LDAP distant. Utilisez l'option **--bind-dn** pour spécifier un DN de liaison personnalisé :

```
# ipa migrate-ds ldap://ldap.example.com:389 --bind-dn=cn=Manager,dc=example,dc=com
```

Personnaliser le contexte de dénomination

Si le contexte de nommage du serveur LDAP diffère de celui utilisé dans IdM, les DN de base des objets sont transformés. Par exemple : **uid=*user*,ou=people,dc=ldap,dc=example,dc=com** est migré en **uid=*user*,ou=people,dc=idm,dc=example,dc=com**. L'option **--base-dn** permet de modifier la cible des sous-arbres des conteneurs et de définir ainsi le DN de base utilisé sur le serveur LDAP distant pour la migration :

```
# ipa migrate-ds --base-dn="ou=people,dc=example,dc=com" ldap://ldap.example.com:389
```

Ressources supplémentaires

- **ipa migrate-ds --help**

4.5.2. La migration de sous-arbres spécifiques

La structure de répertoire par défaut place les entrées relatives aux personnes dans la sous-arborescence **ou=People** et les entrées relatives aux groupes dans la sous-arborescence **ou=Groups**. Ces sous-arbres sont des entrées de conteneur pour ces différents types de données d'annuaire. Si vous n'utilisez aucune option avec la commande **migrate-ds**, l'utilitaire suppose que l'annuaire LDAP donné utilise la structure **ou=People** et **ou=Groups**.

De nombreux déploiements peuvent avoir une structure de répertoire entièrement différente ou vous pouvez ne vouloir exporter que certaines parties de l'arborescence d'origine. En tant qu'administrateur, vous pouvez utiliser les options suivantes pour spécifier le RDN d'un sous-arbre d'utilisateur ou de groupe différent sur le serveur LDAP source :

- **--user-container**
- **--group-container**

NOTE

Dans les deux cas, la sous-arborescence doit être un nom distinctif relatif (RDN) et doit être relative au DN de base. Par exemple, vous pouvez migrer l'arborescence **>ou=Employees,dc=example,dc=com** en utilisant **--user-container=ou=Employees**.

Par exemple :

```
[ipaserver ~]# ipa migrate-ds --user-container=ou=employees \
--group-container="ou=employee groups" ldap://ldap.example.com:389
```

Il est possible d'ajouter l'option **--scope** à la commande **ipa migrate-ds** pour définir le champ d'application :

- **onelevel**: Valeur par défaut. Seules les entrées du conteneur spécifié sont migrées.
- **subtree**: Les entrées du conteneur spécifié et de tous les sous-conteneurs sont migrées.
- **base**: Seul l'objet spécifié est migré.

4.5.3. L'inclusion et l'exclusion d'inscriptions

Par défaut, le script **ipa migrate-ds** importe chaque entrée d'utilisateur avec la classe d'objet **person** et chaque entrée de groupe avec la classe d'objet **groupOfUniqueNames** ou **groupOfNames**.

Dans certains chemins de migration, il peut être nécessaire de n'exporter que certains types d'utilisateurs et de groupes ou, au contraire, d'exclure certains utilisateurs et groupes. Vous pouvez sélectionner les *types* d'utilisateurs et de groupes à inclure en définissant les classes d'objets à rechercher lors de la recherche d'entrées d'utilisateurs ou de groupes.

Cette option est particulièrement utile lorsque vous utilisez des classes d'objets personnalisées pour différents types de *user*. Par exemple, la commande suivante ne migre que les utilisateurs ayant la classe d'objets personnalisée **fullTimeEmployee**:

```
[root@ipaserver ~]# ipa migrate-ds --user-objectclass=fullTimeEmployee
ldap://ldap.example.com:389
```

En raison des différents types de groupes, cette fonction est également très utile pour ne migrer que certains types de *groups*, tels que les groupes d'utilisateurs, tout en excluant d'autres types de groupes, tels que les groupes de certificats. Par exemple :

```
[root@ipaserver ~]# ipa migrate-ds --group-objectclass=groupOfNames --group-
objectclass=groupOfUniqueNames ldap://ldap.example.com:389
```

La spécification d'entrées d'utilisateurs et de groupes à migrer en fonction de la classe d'objets exclut implicitement tous les autres utilisateurs et groupes de la migration.

Il peut également être utile de migrer toutes les entrées d'utilisateurs et de groupes, à l'exception d'une petite poignée d'entrées. Vous pouvez exclure des comptes d'utilisateurs ou de groupes spécifiques tout en migrant tous les autres comptes de ce type. Par exemple, ceci n'exclut qu'un groupe de loisirs et deux utilisateurs :

```
[root@ipaserver ~]# ipa migrate-ds --exclude-groups="Golfers Group" --exclude-
users=idmuser101 --exclude-users=idmuser102 ldap://ldap.example.com:389
```

Les déclarations d'exclusion sont appliquées aux utilisateurs correspondant au modèle dans l'attribut **uid** et aux groupes correspondant au modèle dans l'attribut **cn**.

Vous pouvez migrer une classe d'objets générale mais exclure des entrées spécifiques de cette classe. Par exemple, ceci inclut spécifiquement les utilisateurs de la classe d'objets **fullTimeEmployee**, mais exclut trois gestionnaires :

```
[root@ipaserver ~]# ipa migrate-ds --user-objectclass=fullTimeEmployee --exclude-
users=jsmith --exclude-users=bjensen --exclude-users=mreynolds
ldap://ldap.example.com:389
```

4.5.4. L'exclusion des attributs d'entrée

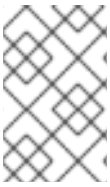
Par défaut, tous les attributs et toutes les classes d'objets d'une entrée d'utilisateur ou de groupe sont migrés. Dans certains scénarios, cela peut ne pas être réaliste, soit en raison de contraintes de bande passante et de réseau, soit parce que les données d'attribut ne sont plus pertinentes. Par exemple, si les utilisateurs se voient attribuer de nouveaux certificats d'utilisateur lorsqu'ils rejoignent le domaine de la gestion des identités (IdM), la migration de l'attribut **userCertificate** serait inutile.

Vous pouvez ignorer des classes d'objets et des attributs spécifiques en utilisant les options suivantes avec la commande **migrate-ds**:

- **--user-ignore-objectclass**
- **--user-ignore-attribute**
- **--group-ignore-objectclass**
- **--group-ignore-attribute**

Par exemple, pour exclure l'attribut **userCertificate** et la classe d'objets **strongAuthenticationUser** pour les utilisateurs et la classe d'objets **groupOfCertificates** pour les groupes :

```
[root@ipaserver ~]# ipa migrate-ds --user-ignore-attribute=userCertificate --user-ignore-objectclass=strongAuthenticationUser --group-ignore-objectclass=groupOfCertificates ldap://ldap.example.com:389
```



NOTE

Veillez à ne pas ignorer les attributs obligatoires. De même, lorsque vous excluez des classes d'objets, veillez à exclure tous les attributs que seule cette classe d'objets prend en charge.

Ressources supplémentaires

- Exigences de l'environnement LDAP pour la migration

4.5.5. Le schéma à utiliser lors de la migration de LDAP vers IdM et la fonction de comparaison des schémas

Identity Management (IdM) utilise le schéma RFC2307bis pour définir les identités des utilisateurs, des hôtes, des groupes d'hôtes et d'autres réseaux. Toutefois, si le serveur LDAP utilisé comme source pour la migration utilise plutôt le schéma RFC2307, spécifiez l'option **--schema** avec la commande **ipa migrate-ds**:

```
[root@ipaserver ~]# ipa migrate-ds --schema=RFC2307 ldap://ldap.example.com:389
```

Par ailleurs, IdM dispose d'un site intégré **schema compat feature**qui lui permet de reformater les données pour les systèmes qui ne prennent pas en charge la norme RFC2307bis. Le plugin compat est activé par défaut, ce qui signifie que le serveur d'annuaire calcule une vue alternative des utilisateurs et des groupes et fournit cette vue dans l'entrée du conteneur **cn=users,cn=compat,dc=example,dc=com**. Pour ce faire, il calcule à l'avance le contenu de ses entrées au démarrage et les actualise si nécessaire.

Il est recommandé de désactiver cette fonction pendant la migration afin de réduire la surcharge du système.

4.6. MIGRATION D'UN SERVEUR LDAP VERS IDM

Vous pouvez migrer vos services d'authentification et d'autorisation d'un serveur LDAP vers Identity Management (IdM) à l'aide de la commande **ipa migrate-ds**.

AVERTISSEMENT

Il s'agit d'une procédure de migration générale qui peut ne pas fonctionner dans tous les environnements.

Il est fortement recommandé de mettre en place un environnement LDAP de test et de tester le processus de migration avant de tenter de migrer l'environnement LDAP réel. Lors du test de l'environnement, procédez comme suit

1. Créez un utilisateur test dans IdM et comparez le résultat des utilisateurs migrés à celui de l'utilisateur test.
2. Comparez les résultats des utilisateurs migrés, tels qu'ils apparaissent sur IdM, aux utilisateurs sources, tels qu'ils apparaissent sur le serveur LDAP d'origine.

Pour plus d'informations, voir la section **Verification** ci-dessous.

Conditions préalables

- Vous disposez de droits d'administrateur sur le répertoire LDAP.
- Si IdM est déjà installé, vous disposez des privilèges d'administrateur pour IdM.
- Vous êtes connecté en tant que **root** sur le système RHEL sur lequel vous exécutez la procédure ci-dessous.
- Vous avez lu et compris les chapitres suivants :
  - Considérations relatives à la migration de LDAP vers IdM .
  - Planification de la configuration du client lors de la migration de LDAP vers IdM .
  - Planification de la migration des mots de passe lors de la migration de LDAP vers IdM .
  - Autres considérations et exigences en matière de migration .
  - Personnalisation de la migration de LDAP vers IdM .

Procédure

1. Si IdM n'est pas encore installé : installez le serveur IdM, y compris tout schéma de répertoire LDAP personnalisé, sur une machine différente de celle sur laquelle le répertoire LDAP existant est installé. Pour plus de détails, voir Installation de la gestion des identités .

NOTE

Les schémas d'utilisateurs ou de groupes personnalisés sont peu pris en charge par IdM. Ils peuvent poser des problèmes lors de la migration en raison de l'incompatibilité des définitions d'objets.

2. Pour des raisons de performance, désactivez le plug-in compat :

```
# ipa-compat-manage disable
```

Pour plus d'informations sur la fonction de comparaison des schémas et sur les avantages qu'il y a à la désactiver pour la migration, voir Le schéma à utiliser lors de la migration de LDAP vers IdM et la fonction de comparaison des schémas.

3. Redémarrer l'instance d'IdM Directory Server :

```
# systemctl restart dirsrv.target
```

4. Configurer le serveur IdM pour permettre la migration :

```
# ipa config-mod --enable-migration=TRUE
```

En attribuant à **--enable-migration** la valeur TRUE, vous effectuez les opérations suivantes :

- Autoriser les mots de passe pré-hachés lors d'une opération d'ajout LDAP.
- Configurez SSSD pour qu'il essaie la séquence de migration des mots de passe si l'authentification Kerberos initiale échoue. Pour plus d'informations, voir la section Flux de travail dans Utilisation de SSSD lors de la migration des mots de passe de LDAP vers IdM .

5. Exécutez le script de migration IdM, **ipa migrate-ds**, avec les options correspondant à votre cas d'utilisation. Pour plus d'informations, voir Personnaliser la migration de LDAP vers IdM .

```
# ipa migrate-ds --your-options ldap://ldap.example.com:389
```

NOTE

Si vous n'avez pas désactivé le plug-in compat dans l'une des étapes précédentes, ajoutez l'option **--with-compat** à **ipa migrate-ds**:

```
# ipa migrate-ds --your-options --with-compat
ldap://ldap.example.com:389
```

6. Réactiver le plug-in compat :

```
# ipa-compat-manage enable
```

7. Redémarrer le serveur d'annuaire IdM :

```
# systemctl restart dirsrv.target
```

8. Lorsque les mots de passe de tous les utilisateurs ont été migrés, désactivez le mode de migration :

```
# ipa config-mod --enable-migration=FALSE
```

9. [Facultatif] Lorsque tous les utilisateurs ont été migrés, reconfigurez les clients non-SSSD pour qu'ils utilisent l'authentification Kerberos, c'est-à-dire **pam_krb5**, au lieu de l'authentification LDAP, c'est-à-dire **pam_ldap**. Pour plus d'informations, voir Configuration d'un client Kerberos dans RHEL 7 *System-level Authentication Guide*.

10. Demandez aux utilisateurs de générer leurs mots de passe Kerberos hachés. Choisissez l'une des méthodes décrites dans la section Planification de la migration des mots de passe lors de la migration de LDAP vers IdM.

    - Si vous optez pour la méthode SSSD :

        - Déplacez les clients qui ont installé SSSD de l'annuaire LDAP vers l'annuaire IdM et inscrivez-les en tant que clients avec IdM. Cette opération permet de télécharger les clés et les certificats nécessaires.
          Sur les clients Red Hat Enterprise Linux, vous pouvez le faire en utilisant la commande **ipa-client-install**. Par exemple :

          ```
          # ipa-client-install --enable-dns-update
          ```

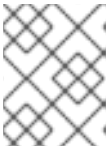
    - Si vous optez pour la méthode de la page web de migration IdM :

        - Demander aux utilisateurs de se connecter à l'IdM en utilisant la page web de migration :

          ```
          https://ipaserver.example.com/ipa/migration
          ```

11. Pour surveiller le processus de migration des utilisateurs, interrogez l'annuaire LDAP existant pour voir quels comptes d'utilisateurs ont un mot de passe mais n'ont pas encore de clé principale Kerberos.

    ```
    $ ldapsearch -LL -x -D 'cn=Directory Manager' -w secret -b
    'cn=users,cn=accounts,dc=example,dc=com' '(&(!(krbprincipalkey=))(userpassword=))'
    uid
    ```

    NOTE

    Inclure les guillemets simples autour du filtre afin qu'il ne soit pas interprété par l'interpréteur de commandes.

12. Lorsque la migration de tous les clients et utilisateurs est terminée, désactivez l'annuaire LDAP.

Vérification

1. Créez un utilisateur test dans IdM en utilisant la commande **ipa user-add**. Comparez les résultats des utilisateurs migrés à ceux de l'utilisateur test. Assurez-vous que les utilisateurs migrés contiennent l'ensemble minimal d'attributs et de classes d'objets présents sur l'utilisateur test. Par exemple :

    ```
    $ ipa user-show --all testing_user
    dn: uid=testing_user,cn=users,cn=accounts,dc=idm,dc=example,dc=com
    User login: testing_user
    First name: testing
    Last name: user
    Full name: testing user
    Display name: testing user
    Initials: tu
    Home directory: /home/testing_user
    GECOS: testing user
    Login shell: /bin/sh
    ```

```
Principal name: testing_user@IDM.EXAMPLE.COM
Principal alias: testing_user@IDM.EXAMPLE.COM
Email address: testing_user@idm.example.com
UID: 1689700012
GID: 1689700012
Account disabled: False
Preserved user: False
Password: False
Member of groups: ipausers
Kerberos keys available: False
ipauniqueid: 843b1ac8-6e38-11ec-8dfe-5254005aad3e
mepmanagedentry: cn=testing_user,cn=groups,cn=accounts,dc=idm,dc=example,dc=com
objectclass: top, person, organizationalperson, inetorgperson, inetuser, posixaccount,
krbprincipalaux, krbticketpolicyaux, ipaobject,
        ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry
```

2. Comparez les résultats des utilisateurs migrés, tels qu'ils apparaissent sur IdM, aux utilisateurs sources, tels qu'ils apparaissent sur le serveur LDAP d'origine. Assurez-vous que les attributs importés ne sont pas copiés deux fois et qu'ils ont les bonnes valeurs.

Ressources supplémentaires

- Migration de LDAP vers IdM sur SSL

4.7. MIGRATION DE LDAP VERS IDM SUR SSL

Vous pouvez migrer vos services d'authentification et d'autorisation d'un serveur LDAP vers Identity Management (IdM) à l'aide de la commande **ipa migrate-ds**. Cette section décrit comment crypter les données transmises lors de la migration.

AVERTISSEMENT

Il s'agit d'une procédure de migration générale qui peut ne pas fonctionner dans tous les environnements.

Il est fortement recommandé de mettre en place un environnement LDAP de test et de tester le processus de migration avant de tenter de migrer l'environnement LDAP réel. Lors du test de l'environnement, procédez comme suit

1. Créez un utilisateur test dans IdM et comparez le résultat des utilisateurs migrés à celui de l'utilisateur test.
2. Comparez les résultats des utilisateurs migrés, tels qu'ils apparaissent sur IdM, aux utilisateurs sources, tels qu'ils apparaissent sur le serveur LDAP d'origine.

Pour plus d'informations, voir la section **Verification** ci-dessous.

Conditions préalables

- Vous disposez de droits d'administrateur sur le répertoire LDAP.
- Si IdM est déjà installé, vous disposez des privilèges d'administrateur pour IdM.
- Vous êtes connecté en tant que **root** sur le système RHEL sur lequel vous exécutez la procédure ci-dessous.
- Vous avez lu et compris les chapitres suivants :
  - Considérations relatives à la migration de LDAP vers IdM .
  - Planification de la configuration du client lors de la migration de LDAP vers IdM .
  - Planification de la migration des mots de passe lors de la migration de LDAP vers IdM .
  - Autres considérations et exigences en matière de migration .
  - Personnalisation de la migration de LDAP vers IdM .

Procédure

1. Stocker le certificat de l'autorité de certification qui a émis le certificat du serveur LDAP distant dans un fichier sur le futur serveur IdM. Par exemple : **/tmp/remote.crt**.
2. Suivez les étapes décrites dans la section Migration d'un serveur LDAP vers IdM . Cependant, pour une connexion LDAP cryptée pendant la migration, utilisez le protocole **ldaps** dans l'URL et passez l'option **--ca-cert-file** à la commande **ipa migrate-ds**. Par exemple :

```
# ipa migrate-ds --ca-cert-file=/tmp/remote.crt --your-other-options
ldaps://ldap.example.com:636
```

Vérification

1. Créez un utilisateur test dans IdM en utilisant la commande **ipa user-add**. Comparez les résultats des utilisateurs migrés à ceux de l'utilisateur test. Assurez-vous que les utilisateurs migrés contiennent l'ensemble minimal d'attributs et de classes d'objets présents sur l'utilisateur test. Par exemple :

```
$ ipa user-show --all testing_user
dn: uid=testing_user,cn=users,cn=accounts,dc=idm,dc=example,dc=com
User login: testing_user
First name: testing
Last name: user
Full name: testing user
Display name: testing user
Initials: tu
Home directory: /home/testing_user
GECOS: testing user
Login shell: /bin/sh
Principal name: testing_user@IDM.EXAMPLE.COM
Principal alias: testing_user@IDM.EXAMPLE.COM
Email address: testing_user@idm.example.com
UID: 1689700012
GID: 1689700012
Account disabled: False
Preserved user: False
```

```
Password: False
Member of groups: ipausers
Kerberos keys available: False
ipauniqueid: 843b1ac8-6e38-11ec-8dfe-5254005aad3e
mepmanagedentry: cn=testing_user,cn=groups,cn=accounts,dc=idm,dc=example,dc=com
objectclass: top, person, organizationalperson, inetorgperson, inetuser, posixaccount,
krbprincipalaux, krbticketpolicyaux, ipaobject,
        ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry
```

2. Comparez les résultats des utilisateurs migrés, tels qu'ils apparaissent sur IdM, aux utilisateurs sources, tels qu'ils apparaissent sur le serveur LDAP d'origine. Assurez-vous que les attributs importés ne sont pas copiés deux fois et qu'ils ont les bonnes valeurs.