Red Hat Enterprise Linux 9

Reprise après sinistre grâce à la gestion des identités

Récupération de l'IdM après une perte de serveur ou de données

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Reprise après sinistre grâce à la gestion des identités

Récupération de l'IdM après une perte de serveur ou de données

Notice légale

Résumé

Les scénarios de perte de serveurs et de données, par exemple en raison d'une défaillance matérielle, constituent les risques les plus élevés dans les environnements informatiques. Dans le cas d'un tel événement dans un environnement Red Hat Identity Management (IdM), le processus de récupération dépend du type de problème, de la topologie IdM et des mesures qui ont été prises pour atténuer de telles situations. Par exemple, vous pouvez récupérer un ou plusieurs serveurs dans une topologie de réplication IdM, et vous pouvez récupérer des données en utilisant des sauvegardes et des instantanés IdM. Pendant ou après la récupération, il peut être nécessaire d'ajuster les paramètres du client, tels que les serveurs DNS et la configuration Kerberos.

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.

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. SCÉNARIOS DE CATASTROPHE DANS L'IDM

Il existe deux grandes catégories de scénarios de catastrophe : *server loss* et *data loss*.

Tableau 1.1. Perte de serveur ou perte de données

Type de catastrophe	Exemple de causes	Comment réagir
Server loss: Le déploiement de l'IdM perd un ou plusieurs serveurs.	• Dysfonctionnement du matériel	• Récupération d'un serveur unique avec réplication
Data loss: Les données IdM sont modifiées de manière inattendue sur un serveur et le changement est propagé à d'autres serveurs.	• Un utilisateur supprime accidentellement des données • Un bogue logiciel modifie les données	• Récupération des données perdues grâce aux instantanés de VM • Récupérer les données perdues grâce aux sauvegardes IdM • Gérer la perte de données

CHAPITRE 2. RÉCUPÉRATION D'UN SERVEUR UNIQUE AVEC RÉPLICATION

Si un seul serveur est gravement perturbé ou perdu, le fait de disposer de plusieurs répliques permet de créer une réplique de remplacement et de rétablir rapidement le niveau de redondance antérieur.

Si votre topologie IdM contient une autorité de certification (AC) intégrée, les étapes de retrait et de remplacement d'une réplique endommagée diffèrent selon qu'il s'agit du serveur de renouvellement de l'AC ou d'autres répliques.

2.1. RÉCUPÉRATION APRÈS LA PERTE DU SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION

Si le serveur de renouvellement de l'autorité de certification (CA) est perdu, vous devez d'abord promouvoir une autre réplique de CA pour remplir le rôle de serveur de renouvellement de CA, puis déployer une réplique de CA de remplacement.

Conditions préalables

- Votre déploiement utilise l'autorité de certification interne de l'IdM.
- Les services CA sont installés sur une autre réplique de l'environnement.

AVERTISSEMENT

Un déploiement IdM est irrécupérable si :

1. Le serveur de renouvellement de l'AC a été perdu.
2. Aucun autre serveur ne dispose d'une autorité de certification.
3. Aucune sauvegarde d'un réplica avec le rôle CA n'existe.
   Il est essentiel d'effectuer des sauvegardes à partir d'un réplica ayant le rôle d'autorité de certification afin de protéger les données des certificats. Pour plus d'informations sur la création et la restauration de sauvegardes, voir Préparation à la perte de données avec les sauvegardes IdM .

Procédure

1. À partir d'une autre réplique de votre environnement, faites en sorte qu'une autre réplique de l'autorité de certification de l'environnement agisse en tant que nouveau serveur de renouvellement de l'autorité de certification. Voir Modification et réinitialisation du serveur de renouvellement de l'autorité de certification IdM.
2. À partir d'un autre réplica de votre environnement, supprimez les accords de réplication vers le serveur de renouvellement de l'autorité de certification perdu. Voir Suppression d'un serveur de la topologie à l'aide de l'interface de ligne de commande.

3. Installez un nouveau réplica CA pour remplacer le réplica CA perdu. Voir Installation d'un réplica IdM avec une autorité de certification.

4. Mettre à jour le DNS pour refléter les changements dans la topologie du réplica. Si IdM DNS est utilisé, les enregistrements de service DNS sont mis à jour automatiquement.

5. Vérifiez que les clients IdM peuvent atteindre les serveurs IdM. Voir Ajustement des clients IdM pendant la récupération.

Verification steps

1. Testez le serveur Kerberos sur la nouvelle réplique en récupérant avec succès un Ticket-Granting-Ticket Kerberos en tant qu'utilisateur IdM.

```
[root@server ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. Testez la configuration du serveur d'annuaire et du SSSD en récupérant les informations relatives aux utilisateurs.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. Testez la configuration de l'autorité de certification à l'aide de la commande **ipa cert-show**.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

Ressources supplémentaires

- Utilisation du serveur de renouvellement de l'autorité de certification IdM

2.2. RÉCUPÉRATION APRÈS LA PERTE D'UNE RÉPLIQUE RÉGULIÈRE

Pour remplacer un réplica qui n'est pas le serveur de renouvellement de l'autorité de certification (CA), supprimez le réplica perdu de la topologie et installez un nouveau réplica à sa place.

Conditions préalables

- Le serveur de renouvellement de l'AC fonctionne correctement. Si le serveur de renouvellement de l'autorité de certification a été perdu, voir Récupération après la perte du serveur de renouvellement de l'autorité de certification.

Procédure

1. Supprimez les accords de réplication pour le serveur perdu. Voir Désinstallation d'un serveur IdM.
2. Déployez un nouveau réplica avec les services souhaités (CA, KRA, DNS). Voir Installation d'une réplique IdM.
3. Mettre à jour le DNS pour refléter les changements dans la topologie du réplica. Si IdM DNS est utilisé, les enregistrements de service DNS sont mis à jour automatiquement.
4. Vérifiez que les clients IdM peuvent atteindre les serveurs IdM. Voir Ajustement des clients IdM pendant la récupération.

Verification steps

1. Testez le serveur Kerberos sur la nouvelle réplique en récupérant avec succès un Ticket-Granting-Ticket Kerberos en tant qu'utilisateur IdM.

```
[root@newreplica ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@newreplica ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. Testez le serveur d'annuaire et la configuration SSSD sur la nouvelle réplique en récupérant les informations sur les utilisateurs.

```
[root@newreplica ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
```

```
GID: 1965200000
Account disabled: False
Password: True
Member of groups: admins, trust admins
Kerberos keys available: True
```

CHAPITRE 3. RÉCUPÉRATION DE PLUSIEURS SERVEURS PAR RÉPLICATION

Si plusieurs serveurs sont perdus en même temps, déterminez si l'environnement peut être reconstruit en examinant lequel des cinq scénarios suivants s'applique à votre situation.

3.1. RÉCUPÉRATION APRÈS LA PERTE DE PLUSIEURS SERVEURS DANS LE CADRE D'UN DÉPLOIEMENT SANS AUTORITÉ DE CERTIFICATION

Les serveurs dans un déploiement sans AC sont tous considérés comme égaux, vous pouvez donc reconstruire l'environnement en supprimant et en remplaçant les répliques perdues dans n'importe quel ordre.

Conditions préalables

- Votre déploiement utilise une autorité de certification (AC) externe.

Procédure

- Voir Récupération après la perte d'une réplique régulière .

3.2. RÉCUPÉRATION APRÈS LA PERTE DE PLUSIEURS SERVEURS LORSQUE LE SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION EST INDEMNE

Si le serveur de renouvellement de l'AC est intact, vous pouvez remplacer les autres serveurs dans n'importe quel ordre.

Conditions préalables

- Votre déploiement utilise l'autorité de certification interne de l'IdM.

Procédure

- Voir Récupération après la perte d'une réplique régulière .

3.3. RÉCUPÉRATION APRÈS LA PERTE DU SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION ET D'AUTRES SERVEURS

Si vous perdez le serveur de renouvellement de l'autorité de certification et d'autres serveurs, faites passer un autre serveur de l'autorité de certification au rôle de serveur de renouvellement de l'autorité de certification avant de remplacer les autres répliques.

Conditions préalables

- Votre déploiement utilise l'autorité de certification interne de l'IdM.
- Au moins une réplique de l'AC est indemne.

Procédure

1. Promouvoir un autre réplica de CA pour remplir le rôle de serveur de renouvellement de CA. Voir Récupération après la perte du serveur de renouvellement de l'autorité de certification.
2. Remplacez toutes les autres répliques perdues. Voir Récupération après la perte d'un réplica normal.

3.4. RÉCUPÉRATION APRÈS LA PERTE DE TOUTES LES RÉPLIQUES DE L'AUTORITÉ DE CERTIFICATION

Sans aucune réplique d'autorité de certification, l'environnement IdM a perdu la capacité de déployer des répliques supplémentaires et de se reconstruire.

Conditions préalables

- Votre déploiement utilise l'autorité de certification interne de l'IdM.

Procédure

- Cette situation est une perte totale.

Ressources supplémentaires

- Pour se préparer à une perte totale de l'infrastructure, voir Préparation à la perte de données avec les snapshots de VM.

3.5. RÉCUPÉRATION D'UNE PERTE TOTALE D'INFRASTRUCTURE

Si tous les serveurs sont perdus en même temps et qu'il n'y a pas d'instantanés de la machine virtuelle (VM) ou de sauvegardes de données à partir desquelles restaurer, cette situation est irrécupérable.

Procédure

- Cette situation est une perte totale.

Ressources supplémentaires

- Préparation à la perte de données avec les snapshots de VM .

CHAPITRE 4. RÉCUPÉRATION DES DONNÉES PERDUES GRÂCE AUX INSTANTANÉS DE VM

En cas de perte de données, vous pouvez restaurer un instantané de machine virtuelle (VM) d'une réplique d'autorité de certification (CA) pour réparer les données perdues ou déployer un nouvel environnement à partir de cet instantané.

4.1. RÉCUPÉRATION À PARTIR D'UN INSTANTANÉ DE VM UNIQUEMENT

Si un sinistre affecte tous les serveurs IdM et qu'il ne reste qu'un instantané d'une machine virtuelle (VM) répliquée de l'autorité de certification IdM, vous pouvez recréer votre déploiement en supprimant toutes les références aux serveurs perdus et en installant de nouvelles répliques.

Conditions préalables

- Vous avez préparé un instantané de VM d'une réplique de VM CA. Voir Préparation à la perte de données avec les snapshots VM.

Procédure

1. Démarrez l'instantané souhaité de la réplique de la VM CA.
2. Supprimez les accords de réplication pour toutes les répliques perdues.

```
[root@server ~]# ipa server-del lost-server1.example.com
[root@server ~]# ipa server-del lost-server2.example.com
...
```

3. Installez un deuxième réplica de CA. Voir Installation d'un réplica IdM avec une autorité de certification.
4. Le réplica CA de la VM est maintenant le serveur de renouvellement CA. Red Hat recommande de promouvoir une autre réplique CA dans l'environnement pour qu'elle agisse en tant que serveur de renouvellement CA. Voir Modification et réinitialisation du serveur de renouvellement CA IdM.
5. Recréer la topologie de réplique souhaitée en déployant des répliques supplémentaires avec les services souhaités (CA, DNS). Voir Installation d'un réplica IdM
6. Mettre à jour le DNS pour refléter la nouvelle topologie des répliques. Si IdM DNS est utilisé, les enregistrements de service DNS sont mis à jour automatiquement.
7. Vérifiez que les clients IdM peuvent atteindre les serveurs IdM. Voir Ajustement des clients IdM pendant la récupération.

Verification steps

1. Testez le serveur Kerberos sur chaque réplique en récupérant avec succès un ticket Kerberos en tant qu'utilisateur IdM.

```
[root@server ~]# kinit admin
Password for admin@EXAMPLE.COM:
```

```
[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. Testez le serveur d'annuaire et la configuration SSSD sur chaque réplique en récupérant les informations sur les utilisateurs.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. Testez le serveur CA sur chaque réplique CA à l'aide de la commande **ipa cert-show**.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

Ressources supplémentaires

- Planification de la topologie de la réplique .

4.2. RÉCUPÉRATION D'UN INSTANTANÉ DE VM DANS UN ENVIRONNEMENT PARTIELLEMENT FONCTIONNEL

Si un sinistre affecte certains serveurs IdM alors que d'autres fonctionnent encore correctement, il se peut que vous souhaitiez restaurer le déploiement à l'état capturé dans un instantané de machine virtuelle (VM). Par exemple, si toutes les répliques d'autorité de certification (CA) sont perdues alors que d'autres répliques sont encore en production, vous devrez ramener une réplique de CA dans l'environnement.

Dans ce scénario, supprimez les références aux répliques perdues, restaurez la réplique CA à partir de l'instantané, vérifiez la réplication et déployez de nouvelles répliques.

Conditions préalables

- Vous avez préparé un instantané de VM d'une réplique de VM CA. Voir Préparation à la perte de données avec les snapshots VM.

Procédure

1. Supprimez tous les accords de réplication vers les serveurs perdus. Voir Désinstallation d'un serveur IdM.
2. Démarrez l'instantané souhaité de la réplique de la VM CA.
3. Supprimez tout accord de réplication entre le serveur restauré et les serveurs perdus.

```
[root@restored-CA-replica ~]# ipa server-del lost-server1.example.com
[root@restored-CA-replica ~]# ipa server-del lost-server2.example.com
...
```

4. Si le serveur restauré n'a pas d'accords de réplication avec l'un des serveurs encore en production, connectez le serveur restauré à l'un des autres serveurs pour mettre à jour le serveur restauré.

```
[root@restored-CA-replica ~]# ipa topologysegment-add
Suffix name: domain
Left node: restored-CA-replica.example.com
Right node: server3.example.com
Segment name [restored-CA-replica.com-to-server3.example.com]: new_segment
---------------------------
Added segment "new_segment"
---------------------------
  Segment name: new_segment
  Left node: restored-CA-replica.example.com
  Right node: server3.example.com
  Connectivity: both
```

5. Examinez les journaux d'erreurs du serveur d'annuaire à l'adresse **/var/log/dirsrv/slapd-YOUR-INSTANCE/errors** pour voir si la réplique de l'autorité de certification de l'instantané se synchronise correctement avec les autres serveurs IdM.
6. Si la réplication sur le serveur restauré échoue parce que sa base de données est trop obsolète, réinitialisez le serveur restauré.

```
[root@restored-CA-replica ~]# ipa-replica-manage re-initialize --from
server2.example.com
```

7. Si la base de données sur le serveur restauré est correctement synchronisée, continuez en déployant des répliques supplémentaires avec les services souhaités (CA, DNS) conformément à la section Installation d'une réplique IdM.

Verification steps

1. Testez le serveur Kerberos sur chaque réplique en récupérant avec succès un ticket Kerberos en tant qu'utilisateur IdM.

```
[root@server ~]# kinit admin
```

```
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. Testez le serveur d'annuaire et la configuration SSSD sur chaque réplique en récupérant les informations sur les utilisateurs.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. Testez le serveur CA sur chaque réplique CA à l'aide de la commande **ipa cert-show**.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

Ressources supplémentaires

- Récupération d'un snapshot de VM pour établir un nouvel environnement IdM .

4.3. RÉCUPÉRATION D'UN SNAPSHOT DE VM POUR ÉTABLIR UN NOUVEL ENVIRONNEMENT IDM

Si le réplica de l'autorité de certification (CA) à partir d'un snapshot de machine virtuelle (VM) restauré ne peut pas se répliquer avec d'autres serveurs, créez un nouvel environnement IdM à partir du snapshot de VM.

Pour établir un nouvel environnement IdM, isolez le serveur VM, créez des répliques supplémentaires à partir de celui-ci et basculez les clients IdM dans le nouvel environnement.

Conditions préalables

- Vous avez préparé un instantané de VM d'une réplique de VM CA. Voir Préparation à la perte de données avec les snapshots VM.

Procédure

1. Démarrez l'instantané souhaité de la réplique de la VM CA.
2. Isoler le serveur restauré du reste du déploiement actuel en supprimant tous ses segments de topologie de réplication.
   a. Tout d'abord, affichez tous les segments de topologie de réplication **domain**.

```
[root@restored-CA-replica ~]# ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: restored-CA-replica.example.com
  Right node: server2.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 8
----------------------------
```

   b. Ensuite, supprimez tous les segments de la topologie **domain** impliquant le serveur restauré.

```
[root@restored-CA-replica ~]# ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
-----------------------------
Deleted segment "new_segment"
-----------------------------
```

   c. Enfin, effectuez les mêmes opérations avec tous les segments de la topologie **ca**.

```
[root@restored-CA-replica ~]# ipa topologysegment-find
Suffix name: ca
------------------
1 segments matched
------------------
  Segment name: ca_segment
  Left node: restored-CA-replica.example.com
  Right node: server4.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

```
[root@restored-CA-replica ~]# ipa topologysegment-del
Suffix name: ca
Segment name: ca_segment
----------------------------
Deleted segment "ca_segment"
----------------------------
```

3. Installez un nombre suffisant de répliques IdM à partir du serveur restauré pour gérer la charge de déploiement. Il y a maintenant deux déploiements IdM déconnectés fonctionnant en parallèle.

4. Commuter les clients IdM pour utiliser le nouveau déploiement en codant en dur les références aux nouvelles répliques IdM. Voir Ajustement des clients IdM pendant la récupération .

5. Arrêter et désinstaller les serveurs IdM du déploiement précédent. Voir Désinstallation d'un serveur IdM.

Verification steps

1. Testez le serveur Kerberos sur chaque nouvelle réplique en récupérant avec succès un ticket Kerberos en tant qu'utilisateur IdM.

```
[root@server ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. Testez le serveur d'annuaire et la configuration SSSD sur chaque nouvelle réplique en récupérant les informations relatives aux utilisateurs.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. Testez le serveur CA sur chaque nouvelle réplique CA à l'aide de la commande **ipa cert-show**.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
```

```
Issuer: CN=Certificate Authority,O=EXAMPLE.COM
Not Before: Thu Oct 31 19:43:29 2019 UTC
Not After: Mon Oct 31 19:43:29 2039 UTC
Serial number: 1
Serial number (hex): 0x1
Revoked: False
```

CHAPITRE 5. RÉCUPÉRER LES DONNÉES PERDUES GRÂCE AUX SAUVEGARDES IDM

Vous pouvez utiliser l'utilitaire **ipa-restore** pour restaurer un serveur IdM à un état antérieur capturé dans une sauvegarde IdM.

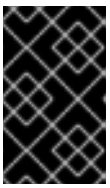
5.1. QUAND RESTAURER À PARTIR D'UNE SAUVEGARDE IDM

Vous pouvez répondre à plusieurs scénarios de désastre en restaurant à partir d'une sauvegarde IdM :

- **Undesirable changes were made to the LDAP content** Des entrées ont été modifiées ou supprimées, la réplication a effectué ces changements tout au long du déploiement et vous souhaitez revenir sur ces modifications. La restauration d'une sauvegarde de données uniquement permet de rétablir l'état antérieur des entrées LDAP sans affecter la configuration IdM elle-même.

- **Total Infrastructure Loss, or loss of all CA instances** Si un sinistre endommage toutes les répliques d'autorité de certification, le déploiement a perdu la capacité de se reconstruire en déployant des serveurs supplémentaires. Dans ce cas, il faut restaurer une sauvegarde d'une réplique d'autorité de certification et construire de nouvelles répliques à partir de celle-ci.

- **An upgrade on an isolated server failed** Le système d'exploitation reste fonctionnel, mais les données IdM sont corrompues, c'est pourquoi vous souhaitez restaurer le système IdM dans un état de bon fonctionnement connu. Red Hat recommande de travailler avec le support technique pour diagnostiquer et résoudre le problème. Si ces efforts échouent, restaurez à partir d'une sauvegarde complète du serveur.



IMPORTANT

La solution préférée en cas de défaillance matérielle ou de mise à niveau consiste à reconstruire le serveur perdu à partir d'un réplica. Pour plus d'informations, voir Récupération d'un serveur unique avec réplication .

5.2. CONSIDÉRATIONS À PRENDRE EN COMPTE LORS DE LA RESTAURATION À PARTIR D'UNE SAUVEGARDE IDM

Si vous disposez d'une sauvegarde créée avec l'utilitaire **ipa-backup**, vous pouvez restaurer votre serveur IdM ou le contenu LDAP dans l'état où ils se trouvaient lorsque la sauvegarde a été effectuée.

Voici les principales considérations à prendre en compte lors de la restauration d'une sauvegarde IdM :

- Vous ne pouvez restaurer une sauvegarde que sur un serveur dont la configuration correspond à celle du serveur sur lequel la sauvegarde a été créée à l'origine. Le serveur **must** a :
  - Le même nom d'hôte
  - La même adresse IP
  - La même version du logiciel IdM
- Si un serveur IdM parmi d'autres est restauré, le serveur restauré devient la seule source d'information pour IdM. Tous les autres serveurs **must** sont réinitialisés à partir du serveur restauré.

- Étant donné que toutes les données créées après la dernière sauvegarde seront perdues, n'utilisez pas la solution de sauvegarde et de restauration pour la maintenance normale du système.
- Si un serveur est perdu, Red Hat recommande de reconstruire le serveur en le réinstallant en tant que réplique, au lieu de le restaurer à partir d'une sauvegarde. La création d'une nouvelle réplique préserve les données de l'environnement de travail actuel. Pour plus d'informations, voir Préparation à la perte d'un serveur avec la réplication .
- Les fonctions de sauvegarde et de restauration ne peuvent être gérées qu'à partir de la ligne de commande et ne sont pas disponibles dans l'interface web de l'IdM.
- Vous ne pouvez pas restaurer des fichiers de sauvegarde situés dans les répertoires **/tmp** ou **/var/tmp**. Le serveur d'annuaire IdM utilise un répertoire **PrivateTmp** et ne peut pas accéder aux répertoires **/tmp** ou **/var/tmp** généralement disponibles pour le système d'exploitation.

ASTUCE

La restauration à partir d'une sauvegarde nécessite les mêmes versions de logiciels (RPM) sur l'hôte cible que celles qui ont été installées lorsque la sauvegarde a été effectuée. Pour cette raison, Red Hat recommande de restaurer à partir d'un instantané de machine virtuelle plutôt qu'à partir d'une sauvegarde. Pour plus d'informations, voir Récupérer des données perdues avec des snapshots de VM .

5.3. RESTAURATION D'UN SERVEUR IDM À PARTIR D'UNE SAUVEGARDE

La procédure suivante décrit la restauration d'un serveur IdM ou de ses données LDAP à partir d'une sauvegarde IdM.

Figure 5.1. Topologie de réplication utilisée dans cet exemple

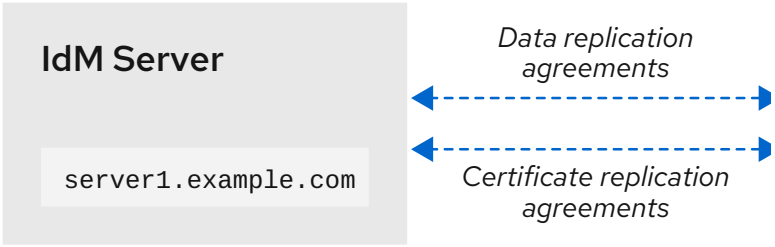


Tableau 5.1. Conventions de dénomination des serveurs utilisées dans cet exemple

Nom d'hôte du serveur	Fonction
server1.example.com	Le serveur qui doit être restauré à partir de la sauvegarde.
caReplica2.example.com	Une réplique de l'autorité de certification (CA) connectée à l'hôte **server1.example.com**.

Nom d'hôte du serveur	Fonction
replica3.example.com	Une réplique connectée à l'hôte **caReplica2.example.com**.

Conditions préalables

- Vous avez généré une sauvegarde complète du serveur ou des données uniquement du serveur IdM à l'aide de l'utilitaire **ipa-backup**. Voir Création d'une sauvegarde.
- Vos fichiers de sauvegarde ne se trouvent pas dans les répertoires **/tmp** ou **/var/tmp**.
- Avant d'effectuer une restauration complète du serveur à partir d'une sauvegarde complète du serveur, désinstallez IdM du serveur et réinstallez IdM en utilisant la même configuration de serveur qu'auparavant.

Procédure

1. Utilisez l'utilitaire **ipa-restore** pour restaurer un serveur complet ou une sauvegarde de données uniquement.
   - Si le répertoire de sauvegarde se trouve dans l'emplacement par défaut **/var/lib/ipa/backup/**, saisissez uniquement le nom du répertoire :

     ```
     [root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
     ```

   - Si le répertoire de sauvegarde ne se trouve pas à l'emplacement par défaut, saisissez son chemin d'accès complet :

     ```
     [root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
     ```

     NOTE

     L'utilitaire **ipa-restore** détecte automatiquement le type de sauvegarde que le répertoire contient et effectue le même type de restauration par défaut. Pour effectuer une restauration de données uniquement à partir d'une sauvegarde complète du serveur, ajoutez l'option **--data** à la commande **ipa-restore**:

     ```
     [root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
     ```

2. Saisissez le mot de passe du gestionnaire de répertoire.

   ```
   Mot de passe du gestionnaire d'annuaire (maître existant) :
   ```

3. Entrez **yes** pour confirmer l'écrasement des données actuelles par la sauvegarde.

   ```
   Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
   server1.example.com
   ```

```
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. L'utilitaire **ipa-restore** désactive la réplication sur tous les serveurs disponibles :

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

L'utilitaire arrête ensuite les services IdM, restaure la sauvegarde et redémarre les services :

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

5. Réinitialiser toutes les répliques connectées au serveur restauré :

   a. Listez tous les segments de topologie de réplication pour le suffixe **domain**, en prenant note des segments de topologie impliquant le serveur restauré.

```
[root@server1 ~]# ipa topologysegment-find domain
------------------
2 segments matched
------------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both

  Segment name: caReplica2.example.com-to-replica3.example.com
  Left node: caReplica2.example.com
  Right node: replica3.example.com
  Connectivity: both
----------------------------
Number of entries returned 2
----------------------------
```

b. Réinitialisez le suffixe **domain** pour tous les segments de la topologie avec le serveur restauré.
Dans cet exemple, il s'agit de réinitialiser **caReplica2** avec des données provenant de **server1**.

```
[root@caReplica2 ~]# ipa-replica-manage re-initialize --from=server1.example.com
Update in progress, 2 seconds elapsed
Update succeeded
```

c. En ce qui concerne les données relatives à l'autorité de certification, dressez la liste de tous les segments de la topologie de réplication pour le suffixe **ca**.

```
[root@server1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

d. Réinitialisez toutes les répliques de CA connectées au serveur restauré.
Dans cet exemple, nous effectuons une réinitialisation de **csreplica** à partir de **caReplica2** avec des données provenant de **server1**.

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=server1.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

6. Continuez à vous déplacer vers l'extérieur dans la topologie de réplication, en réinitialisant les répliques successives, jusqu'à ce que tous les serveurs aient été mis à jour avec les données du serveur restauré **server1.example.com**.
Dans cet exemple, il suffit de réinitialiser le suffixe **domain** sur **replica3** avec les données de **caReplica2**:

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

7. Vider le cache de SSSD sur chaque serveur pour éviter les problèmes d'authentification dus à des données non valides :

a. Arrêtez le service SSSD :

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

b. Supprimer tout le contenu mis en cache du SSSD :

```
[root@server ~]# sss_cache -E
```

c. Démarrez le service SSSD :

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

d. Redémarrer le serveur.

Ressources supplémentaires

- La page de manuel **ipa-restore (1)** couvre également en détail la manière de gérer les scénarios de réplication complexes lors de la restauration.

5.4. RESTAURATION À PARTIR D'UNE SAUVEGARDE CRYPTÉE

Cette procédure permet de restaurer un serveur IdM à partir d'une sauvegarde IdM cryptée. L'utilitaire **ipa-restore** détecte automatiquement si une sauvegarde IdM est cryptée et la restaure à l'aide du trousseau de clés racine GPG2.

Conditions préalables

- Une sauvegarde IdM chiffrée par GPG. Voir Création de sauvegardes IdM cryptées .
- Le mot de passe du gestionnaire de répertoire LDAP
- La phrase de passe utilisée lors de la création de la clé GPG

Procédure

1. Si vous avez utilisé un emplacement de trousseau personnalisé lors de la création des clés GPG2, assurez-vous que la variable d'environnement **$GNUPGHOME** est définie sur ce répertoire. Voir Création d'une clé GPG2 .

```
[root@server ~]# echo $GNUPGHOME
/root/backup
```

2. Indiquez à l'utilitaire **ipa-restore** l'emplacement du répertoire de sauvegarde.

```
[root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
```

a. Saisissez le mot de passe du gestionnaire de répertoire.

```
Mot de passe du gestionnaire d'annuaire (maître existant) :
```

b. Saisissez la phrase de passe que vous avez utilisée lors de la création de la clé GPG.

```
┌──────────────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:                │
│ "GPG User (first key) <root@example.com>"                                    │
│ 2048-bit RSA key, ID BF28FFA302EF4557,                                       │
```

```
created 2020-01-13.

Passphrase: <passphrase>

      <OK>                <Cancel>
```

3. Réinitialisez toutes les répliques connectées au serveur restauré. Voir Restauration d'un serveur IdM à partir d'une sauvegarde.

CHAPITRE 6. RESTAURATION DES SERVEURS IDM À L'AIDE DE PLAYBOOKS ANSIBLE

En utilisant le rôle Ansible **ipabackup**, vous pouvez automatiser la restauration d'un serveur IdM à partir d'une sauvegarde et le transfert de fichiers de sauvegarde entre les serveurs et votre contrôleur Ansible.

Cette section couvre les sujets suivants :

- Préparation du nœud de contrôle Ansible pour la gestion de l'IdM
- Utiliser Ansible pour restaurer un serveur IdM à partir d'une sauvegarde stockée sur le serveur
- Utiliser Ansible pour restaurer un serveur IdM à partir d'une sauvegarde stockée sur votre contrôleur Ansible
- Utiliser Ansible pour copier une sauvegarde d'un serveur IdM sur votre contrôleur Ansible
- Utilisation d'Ansible pour copier une sauvegarde d'un serveur IdM depuis votre contrôleur Ansible vers le serveur IdM
- Utiliser Ansible pour supprimer une sauvegarde d'un serveur IdM

6.1. PRÉPARATION DU NŒUD DE CONTRÔLE ANSIBLE POUR LA GESTION DE L'IDM

En tant qu'administrateur système gérant la gestion des identités (IdM), lorsque vous travaillez avec Red Hat Ansible Engine, il est recommandé de procéder comme suit :

- Créez un sous-répertoire dédié aux playbooks Ansible dans votre répertoire personnel, par exemple **~/MyPlaybooks**.
- Copiez et adaptez les exemples de playbooks Ansible des répertoires et sous-répertoires **/usr/share/doc/ansible-freeipa/*** et **/usr/share/doc/rhel-system-roles/*** dans votre répertoire **~/MyPlaybooks**.
- Incluez votre fichier d'inventaire dans votre répertoire **~/MyPlaybooks**.

En suivant cette pratique, vous pouvez trouver tous vos playbooks en un seul endroit et vous pouvez exécuter vos playbooks sans invoquer les privilèges root.

NOTE

Vous n'avez besoin que des privilèges **root** sur les nœuds gérés pour exécuter les rôles **ipaserver**, **ipareplica**, **ipaclient**, **ipabackup**, **ipasmartcard_server** et **ipasmartcard_client ansible-freeipa** . Ces rôles nécessitent un accès privilégié aux répertoires et au gestionnaire de paquets logiciels **dnf**.

Cette section décrit comment créer le répertoire **~/MyPlaybooks** et le configurer de manière à ce que vous puissiez l'utiliser pour stocker et exécuter des playbooks Ansible.

Conditions préalables

- Vous avez installé un serveur IdM sur vos nœuds gérés, ***server.idm.example.com*** et ***replica.idm.example.com***.
- Vous avez configuré le DNS et le réseau pour pouvoir vous connecter aux nœuds gérés, ***server.idm.example.com*** et ***replica.idm.example.com***directement à partir du nœud de contrôle.
- Vous connaissez le mot de passe de l'IdM **admin**.

Procédure

1. Créez un répertoire pour votre configuration Ansible et vos playbooks dans votre répertoire personnel :

```
$ mkdir ~/MyPlaybooks/
```

2. Allez dans le répertoire **~/MyPlaybooks/**:

```
$ cd ~/MyPlaybooks
```

3. Créez le fichier **~/MyPlaybooks/ansible.cfg** avec le contenu suivant :

```
[defaults]
inventory = /home/your_username/MyPlaybooks/inventory

[privilege_escalation]
become=True
```

4. Créez le fichier **~/MyPlaybooks/inventory** avec le contenu suivant :

```
[ipaserver]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com

[ipacluster:children]
ipaserver
ipareplicas

[ipacluster:vars]
ipaadmin_password=SomeADMINpassword

[ipaclients]
ipaclient1.example.com
ipaclient2.example.com

[ipaclients:vars]
ipaadmin_password=SomeADMINpassword
```

Cette configuration définit deux groupes d'hôtes, **eu** et **us**, pour les hôtes de ces sites. En outre, cette configuration définit le groupe d'hôtes **ipaserver**, qui contient tous les hôtes des groupes **eu** et **us**.

5. [Facultatif] Créez une clé publique et une clé privée SSH. Pour simplifier l'accès dans votre environnement de test, ne définissez pas de mot de passe pour la clé privée :

```
$ ssh-keygen
```

6. Copiez la clé publique SSH dans le compte IdM **admin** sur chaque nœud géré :

```
$ ssh-copy-id admin@server.idm.example.com
$ ssh-copy-id admin@replica.idm.example.com
```

Vous devez saisir le mot de passe IdM **admin** lorsque vous entrez dans ces commandes.

Ressources supplémentaires

- Installation d'un serveur de gestion des identités à l'aide d'un playbook Ansible .
- Comment constituer votre inventaire .

6.2. UTILISER ANSIBLE POUR RESTAURER UN SERVEUR IDM À PARTIR D'UNE SAUVEGARDE STOCKÉE SUR LE SERVEUR

La procédure suivante décrit comment utiliser un playbook Ansible pour restaurer un serveur IdM à partir d'une sauvegarde stockée sur cet hôte.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.
- Vous connaissez le mot de passe du gestionnaire de répertoire LDAP.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

```
$ cd ~/MyPlaybooks/
```

2. Faites une copie du fichier **restore-server.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/restore-server.yml restore-my-server.yml
```

3. Ouvrez le fichier **restore-my-server.yml** Ansible playbook pour l'éditer.

4. Adaptez le fichier en définissant les variables suivantes :

   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.

   b. Attribuez à la variable **ipabackup_name** le nom du site **ipabackup** à restaurer.

   c. Définissez la variable **ipabackup_password** avec le mot de passe du gestionnaire d'annuaire LDAP.

```
---
- name: Playbook to restore an IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>

  roles:
  - role: ipabackup
    state: restored
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
restore-my-server.yml
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

6.3. UTILISER ANSIBLE POUR RESTAURER UN SERVEUR IDM À PARTIR D'UNE SAUVEGARDE STOCKÉE SUR VOTRE CONTRÔLEUR ANSIBLE

La procédure suivante décrit comment utiliser un playbook Ansible pour restaurer un serveur IdM à partir d'une sauvegarde stockée sur votre contrôleur Ansible.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :

- Vous utilisez la version 2.8 ou ultérieure d'Ansible.
- Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
- L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
- L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
- Vous utilisez la version 2.8 ou ultérieure d'Ansible.
- Vous avez installé le paquetage **ansible-freeipa**.
- Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
- Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

- Vous connaissez le mot de passe du gestionnaire de répertoire LDAP.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

```
$ cd ~/MyPlaybooks/
```

2. Faites une copie du fichier **restore-server-from-controller.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/restore-server-from-controller.yml restore-my-server-from-my-controller.yml
```

3. Ouvrez le fichier **restore-my-server-from-my-controller.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   b. Attribuez à la variable **ipabackup_name** le nom du site **ipabackup** à restaurer.
   c. Définissez la variable **ipabackup_password** avec le mot de passe du gestionnaire d'annuaire LDAP.

```
---
- name: Playbook to restore IPA server from controller
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>
    ipabackup_from_controller: yes
```

```
roles:
- role: ipabackup
  state: restored
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
restore-my-server-from-my-controller.yml
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

6.4. UTILISER ANSIBLE POUR COPIER UNE SAUVEGARDE D'UN SERVEUR IDM SUR VOTRE CONTRÔLEUR ANSIBLE

La procédure suivante décrit comment utiliser un playbook Ansible pour copier une sauvegarde d'un serveur IdM depuis le serveur IdM vers votre contrôleur Ansible.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Pour stocker les sauvegardes, créez un sous-répertoire dans votre répertoire personnel sur le contrôleur Ansible.

```
$ mkdir ~/ipabackups
```

2. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

```
$ cd ~/MyPlaybooks/
```

3. Faites une copie du fichier **copy-backup-from-server.yml** situé dans le répertoire /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-server.yml copy-backup-from-my-server-to-my-controller.yml
```

4. Ouvrez le fichier **copy-my-backup-from-my-server-to-my-controller.yml** pour le modifier.

5. Adaptez le fichier en définissant les variables suivantes :

   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.

   b. Définissez la variable **ipabackup_name** avec le nom de **ipabackup** sur votre serveur IdM à copier dans votre contrôleur Ansible.

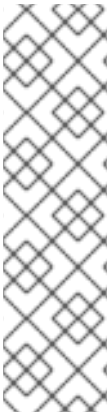
   c. Par défaut, les sauvegardes sont stockées dans le répertoire de travail actuel du contrôleur Ansible. Pour spécifier le répertoire que vous avez créé à l'étape 1, ajoutez la variable **ipabackup_controller_path** et définissez-la sur le répertoire /**home**/**user**/**ipabackups**.

```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_to_controller: yes
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

6. Enregistrer le fichier.

7. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-server-to-my-controller.yml
```



NOTE

Pour copier les sauvegardes de **all** IdM sur votre contrôleur, définissez la variable **ipabackup_name** dans Ansible playbook à **all**:

```
vars:
  ipabackup_name: all
  ipabackup_to_controller: yes
```

Pour un exemple, voir le playbook Ansible **copy-all-backups-from-server.yml** dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**.

Verification steps

- Vérifiez que votre sauvegarde se trouve dans le répertoire **/home/user/ipabackups** sur votre contrôleur Ansible :

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

6.5. UTILISATION D'ANSIBLE POUR COPIER UNE SAUVEGARDE D'UN SERVEUR IDM DEPUIS VOTRE CONTRÔLEUR ANSIBLE VERS LE SERVEUR IDM

La procédure suivante décrit comment utiliser un playbook Ansible pour copier une sauvegarde d'un serveur IdM depuis votre contrôleur Ansible vers le serveur IdM.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.

- Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Naviguez jusqu'au répertoire ~/**MyPlaybooks**/:

```
$ cd ~/MyPlaybooks/
```

2. Faites une copie du fichier **copy-backup-from-controller.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-controller.yml copy-backup-from-my-controller-to-my-server.yml
```

3. Ouvrez le fichier **copy-my-backup-from-my-controller-to-my-server.yml** pour le modifier.

4. Adaptez le fichier en définissant les variables suivantes :

   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.

   b. Définissez la variable **ipabackup_name** avec le nom de **ipabackup** sur votre contrôleur Ansible à copier sur le serveur IdM.

```
---
- name: Playbook to copy a backup from controller to the IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_from_controller: yes

  roles:
  - role: ipabackup
    state: copied
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-controller-to-my-server.yml
```

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

6.6. UTILISER ANSIBLE POUR SUPPRIMER UNE SAUVEGARDE D'UN SERVEUR IDM

La procédure suivante décrit comment utiliser un playbook Ansible pour supprimer une sauvegarde d'un serveur IdM.

Conditions préalables

- Vous avez configuré votre nœud de contrôle Ansible pour qu'il réponde aux exigences suivantes :
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa** sur le contrôleur Ansible.
  - L'exemple suppose que dans le répertoire ***~/MyPlaybooks/*** vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM.
  - L'exemple suppose que le coffre-fort **secret.yml** Ansible stocke votre **ipaadmin_password**.
  - Vous utilisez la version 2.8 ou ultérieure d'Ansible.
  - Vous avez installé le paquetage **ansible-freeipa**.
  - Vous avez créé un fichier d'inventaire Ansible avec le nom de domaine complet (FQDN) du serveur IdM sur lequel vous configurez ces options.
  - Votre fichier d'inventaire Ansible est situé dans le répertoire ~/**MyPlaybooks**/.

Procédure

1. Naviguez jusqu'au répertoire ~/MyPlaybooks/ :

```
$ cd ~/MyPlaybooks/
```

2. Faites une copie du fichier **remove-backup-from-server.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/remove-backup-from-server.yml remove-backup-from-my-server.yml
```

3. Ouvrez le fichier **remove-backup-from-my-server.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   b. Attribuez à la variable **ipabackup_name** le nom du site **ipabackup** à supprimer de votre serveur IdM.

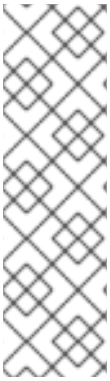
```
---
- name: Playbook to remove backup from IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
```

```
roles:
- role: ipabackup
  state: absent
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible, en spécifiant le fichier d'inventaire et le fichier du playbook :

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
remove-backup-from-my-server.yml
```



NOTE

Pour supprimer les sauvegardes **all** IdM du serveur IdM, définissez la variable **ipabackup_name** dans le carnet de commande Ansible à **all**:

```
vars:
  ipabackup_name: all
```

Pour un exemple, voir le playbook Ansible **remove-all-backups-from-server.yml** dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**.

Ressources supplémentaires

- Le fichier **README.md** dans le répertoire **/usr/share/doc/ansible-freeipa/roles/ipabackup**.
- Le répertoire **/usr/share/doc/ansible-freeipa/playbooks/**.

CHAPITRE 7. GÉRER LA PERTE DE DONNÉES

La réponse appropriée à une perte de données dépend du nombre de répliques affectées et du type de données perdues.

7.1. RÉAGIR À UNE PERTE DE DONNÉES ISOLÉE

Lorsqu'une perte de données se produit, minimisez la réplication de la perte de données en isolant immédiatement les serveurs affectés. Créez ensuite des répliques de remplacement à partir du reste de l'environnement non affecté.

Conditions préalables

- Une topologie de réplication IdM robuste avec plusieurs répliques. Voir Préparation à la perte d'un serveur avec réplication.

Procédure

1. Pour limiter la réplication de la perte de données, déconnectez toutes les répliques concernées du reste de la topologie en supprimant leurs segments de topologie de réplication.

   a. Affichez tous les segments de topologie de réplication **domain** dans le déploiement.

   ```
   [root@server ~]# ipa topologysegment-find
   Suffix name: domain
   ------------------
   8 segments matched
   ------------------
     Segment name: segment1
     Left node: server.example.com
     Right node: server2.example.com
     Connectivity: both

   ...

   ----------------------------
   Number of entries returned 8
   ----------------------------
   ```

   b. Supprimez tous les segments de la topologie **domain** impliquant les serveurs concernés.

   ```
   [root@server ~]# ipa topologysegment-del
   Suffix name: domain
   Segment name: segment1
   ----------------------------
   Deleted segment "segment1"
   ----------------------------
   ```

   c. Effectuez les mêmes actions avec tous les segments de la topologie **ca** impliquant des serveurs affectés.

   ```
   [root@server ~]# ipa topologysegment-find
   Suffix name: ca
   ------------------
   ```

```
1 segments matched
------------------
  Segment name: ca_segment
  Left node: server.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------

[root@server ~]# ipa topologysegment-del
Suffix name: ca
Segment name: ca_segment
-----------------------------
Deleted segment "ca_segment"
-----------------------------
```

2. Les serveurs affectés par la perte de données doivent être abandonnés. Pour créer des répliques de remplacement, voir Récupération de plusieurs serveurs à l'aide de la réplication .

7.2. RÉPONSE À UNE PERTE DE DONNÉES LIMITÉE SUR L'ENSEMBLE DES SERVEURS

Une perte de données peut affecter toutes les répliques de l'environnement, par exemple si la réplication effectue une suppression accidentelle sur tous les serveurs. Si la perte de données est connue et limitée, réajoutez manuellement les données perdues.

Conditions préalables

- Un instantané de machine virtuelle (VM) ou une sauvegarde IdM d'un serveur IdM contenant les données perdues.

Procédure

1. Si vous avez besoin de revoir les données perdues, restaurez l'instantané ou la sauvegarde de la VM sur un serveur isolé sur un réseau distinct.

2. Ajoutez les informations manquantes à la base de données en utilisant les commandes **ipa** ou **ldapadd**.

Ressources supplémentaires

- Récupération des données perdues grâce aux instantanés de VM .
- Sauvegarde et restauration de l'IdM .

7.3. RÉPONSE À UNE PERTE DE DONNÉES NON DÉFINIE SUR L'ENSEMBLE DES SERVEURS

Si la perte de données est importante ou indéfinie, déployez un nouvel environnement à partir d'un instantané de machine virtuelle (VM) d'un serveur.

Conditions préalables

- Un instantané de machine virtuelle (VM) contient les données perdues.

Procédure

1. Restaurer une réplique d'autorité de certification (AC) IdM à partir d'un instantané de VM dans un état connu et déployer un nouvel environnement IdM à partir de cette réplique. Voir Récupération à partir d'un instantané de VM uniquement .

2. Ajoutez toutes les données créées après la prise de l'instantané à l'aide des commandes **ipa** ou **ldapadd**.

Ressources supplémentaires

- Récupération des données perdues grâce aux instantanés de VM .

CHAPITRE 8. AJUSTEMENT DES CLIENTS IDM PENDANT LA RÉCUPÉRATION

Pendant la restauration des serveurs IdM, il se peut que vous deviez ajuster les clients IdM pour refléter les changements dans la topologie du réplica.

Procédure

1. **Adjusting DNS configuration**:

   a. Si **/etc/hosts** contient des références à des serveurs IdM, assurez-vous que les correspondances IP-nom d'hôte codées en dur sont valides.

   b. Si les clients IdM utilisent IdM DNS pour la résolution de noms, assurez-vous que les entrées **nameserver** dans **/etc/resolv.conf** pointent vers des répliques IdM opérationnelles fournissant des services DNS.

2. **Adjusting Kerberos configuration**:

   a. Par défaut, les clients IdM consultent les enregistrements du service DNS pour les serveurs Kerberos et s'adaptent aux changements dans la topologie de la réplique :

   ```
   [root@client ~]# grep dns_lookup_kdc /etc/krb5.conf
     dns_lookup_kdc = true
   ```

   b. Si les clients IdM ont été codés en dur pour utiliser des serveurs IdM spécifiques dans **/etc/krb5.conf**:

   ```
   [root@client ~]# grep dns_lookup_kdc /etc/krb5.conf
     dns_lookup_kdc = false
   ```

   assurez-vous que les entrées **kdc**, **master_kdc** et **admin_server** dans **/etc/krb5.conf** pointent vers des serveurs IdM qui fonctionnent correctement :

   ```
   [realms]
    EXAMPLE.COM = {
     kdc = functional-server.example.com:88
     master_kdc = functional-server.example.com:88
     admin_server = functional-server.example.com:749
     default_domain = example.com
     pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
     pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem
   }
   ```

3. **Adjusting SSSD configuration**:

   a. Par défaut, les clients IdM consultent les enregistrements du service DNS pour les serveurs LDAP et s'adaptent aux changements dans la topologie des répliques :

   ```
   [root@client ~]# grep ipa_server /etc/sssd/sssd.conf
   ipa_server = _srv_, functional-server.example.com
   ```

b. Si les clients IdM ont été codés en dur pour utiliser des serveurs IdM spécifiques dans **/etc/sssd/sssd.conf**, assurez-vous que les points d'entrée de **ipa_server** pointent vers des serveurs IdM qui fonctionnent correctement :

```
[root@client ~]# grep ipa_server /etc/sssd/sssd.conf
ipa_server = functional-server.example.com
```

4. **Clearing SSSD's cached information**

- Le cache SSSD peut contenir des informations obsolètes concernant les serveurs perdus. Si les utilisateurs rencontrent des problèmes d'authentification incohérents, purgez le cache SSSD :

```
[root@client ~]# sss_cache -E
```

Verification steps

1. Vérifiez la configuration Kerberos en récupérant un Ticket-Granting-Ticket Kerberos en tant qu'utilisateur IdM.

```
[root@client ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@client ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 18:44:58  11/25/2019 18:44:55  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. Vérifiez la configuration SSSD en récupérant les informations sur l'utilisateur IdM.

```
[root@client ~]# id admin
uid=1965200000(admin) gid=1965200000(admins) groups=1965200000(admins)
```