Red Hat Enterprise Linux 9

Gestion de la réplication dans la gestion des identités

Préparation et vérification des environnements de réplication

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Gestion de la réplication dans la gestion des identités

Préparation et vérification des environnements de réplication

Notice légale

Résumé

Dans un environnement Red Hat Identity Management (IdM), la réplication permet le basculement et l'équilibrage de charge. Vous pouvez configurer, vérifier et arrêter la réplication entre les serveurs à l'aide de la ligne de commande, de l'interface Web et des Playbooks Ansible.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

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

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

- ***block list*** remplace *blacklist*
- ***allow list*** remplace *whitelist*
- ***secondary*** remplace *slave*
- Le mot *master* 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**.

CHAPITRE 1. GESTION DE LA TOPOLOGIE DE RÉPLICATION

Ce chapitre décrit comment gérer la réplication entre les serveurs d'un domaine de gestion des identités (IdM).

Ressources supplémentaires

- Planification de la topologie du réplica

1.1. EXPLICATION DES ACCORDS DE RÉPLICATION, DES SUFFIXES DE TOPOLOGIE ET DES SEGMENTS DE TOPOLOGIE

Lorsque vous créez une réplique, Identity Management (IdM) crée un accord de réplication entre le serveur initial et la réplique. Les données répliquées sont ensuite stockées dans des suffixes de topologie et lorsque deux répliques ont un accord de réplication entre leurs suffixes, ces derniers forment un segment de topologie. Ces concepts sont expliqués plus en détail dans les sections suivantes :

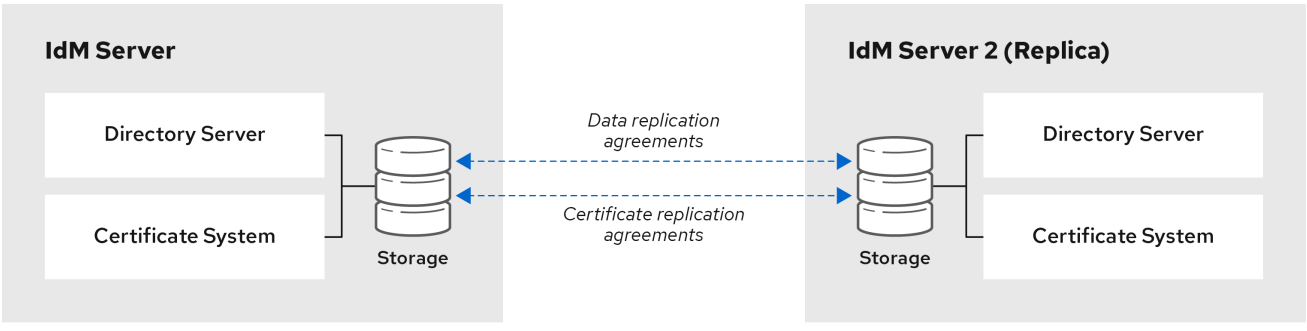
- Accords de réplication
- Suffixes de topologie
- Segments de topologie

1.1.1. Accords de réplication entre les répliques de l'IdM

Lorsqu'un administrateur crée une réplique basée sur un serveur existant, Identity Management (IdM) crée un *replication agreement* entre le serveur initial et la réplique. L'accord de réplication garantit que les données et la configuration sont répliquées en permanence entre les deux serveurs.

IdM utilise *multiple read/write replica replication* . Dans cette configuration, toutes les répliques liées par un accord de réplication reçoivent et fournissent des mises à jour et sont donc considérées comme des fournisseurs et des consommateurs. Les accords de réplication sont toujours bilatéraux.

Figure 1.1. Accords sur les serveurs et les répliques



64_RHEL_0120

IdM utilise deux types d'accords de réplication :

Accords de réplication de domaine

Ces accords reproduisent les informations relatives à l'identité.

Accords de réplication de certificats

Ces accords reproduisent les informations du certificat.

Les deux canaux de réplication sont indépendants. Deux serveurs peuvent avoir un ou les deux types d'accords de réplication configurés entre eux. Par exemple, lorsque le serveur A et le serveur B n'ont configuré qu'un accord de réplication de domaine, seules les informations relatives à l'identité sont répliquées entre eux, et non les informations relatives au certificat.

1.1.2. Suffixes de topologie

Topology suffixes stocker les données répliquées. IdM prend en charge deux types de suffixes de topologie : **domain** et **ca**. Chaque suffixe représente un serveur distinct, une topologie de réplication distincte.

Lorsqu'un accord de réplication est configuré, il joint deux suffixes de topologie du même type sur deux serveurs différents.

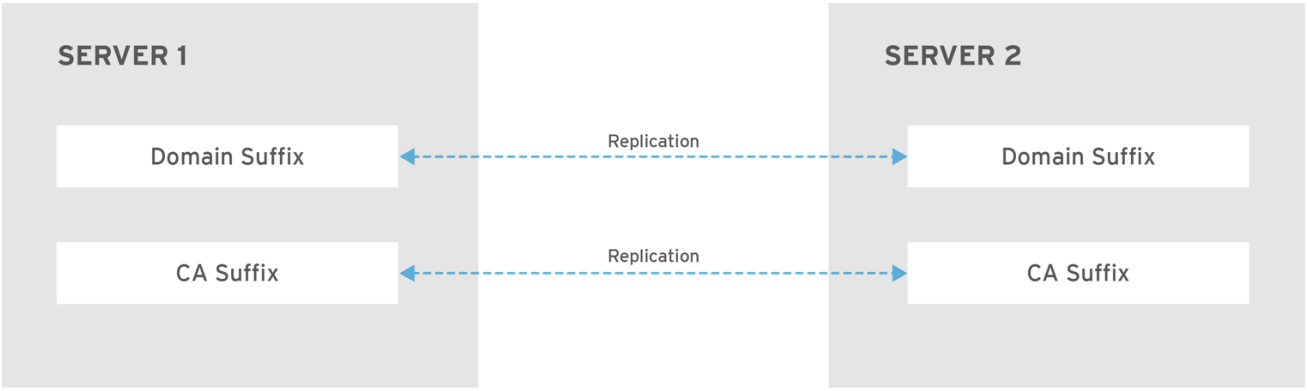
Le suffixe domain: dc=*example*,dc=*com*

Le suffixe **domain** contient toutes les données relatives au domaine.
Lorsque deux répliques ont un accord de réplication entre leurs suffixes **domain**, elles partagent les données de l'annuaire, telles que les utilisateurs, les groupes et les stratégies.

Le suffixe ca: o=ipaca

Le suffixe **ca** contient des données relatives au composant du système de certification. Il n'est présent que sur les serveurs sur lesquels une autorité de certification (CA) est installée.
Lorsque deux répliques ont un accord de réplication entre leurs suffixes **ca**, elles partagent les données du certificat.

Figure 1.2. Suffixes de topologie



Un accord initial de réplication de la topologie est établi entre deux serveurs par le script **ipa-replica-install** lors de l'installation d'une nouvelle réplique.

Exemple 1.1. Visualisation des suffixes de topologie

La commande **ipa topologysuffix-find** affiche une liste des suffixes de la topologie :

```
$ ipa topologysuffix-find
----------------------------
2 topology suffixes matched
----------------------------
  Suffix name: ca
  Managed LDAP suffix DN: o=ipaca
```

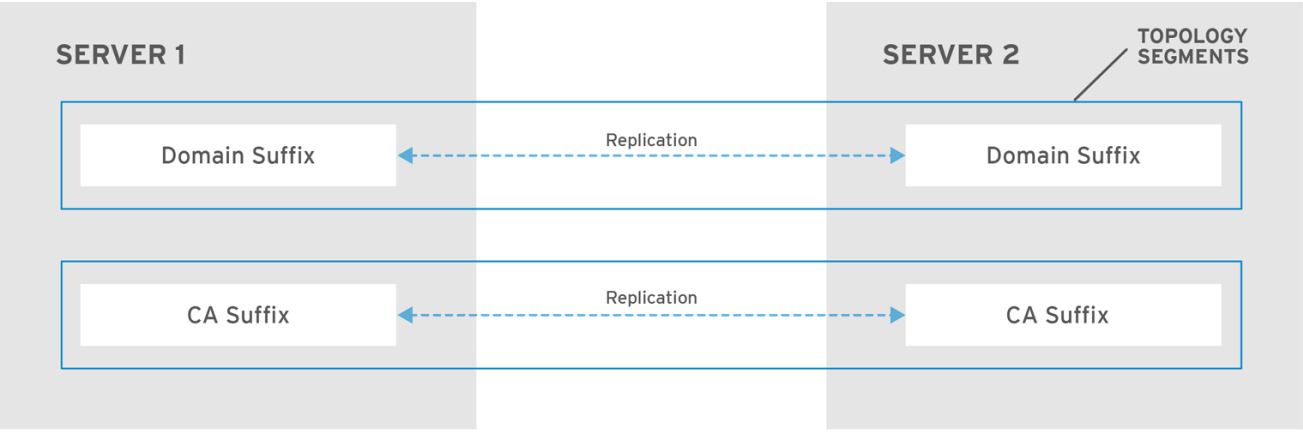
```
  Suffix name: domain
  Managed LDAP suffix DN: dc=example,dc=com
----------------------------
Number of entries returned 2
----------------------------
```

1.1.3. Segments de topologie

Lorsque deux répliques ont un accord de réplication entre leurs suffixes, les suffixes forment un *topology segment*. Chaque segment topologique est constitué d'un *left node* et d'un *right node*. Les nœuds représentent les serveurs liés par l'accord de réplication.

Les segments de topologie dans IdM sont toujours bidirectionnels. Chaque segment représente deux accords de réplication : du serveur A au serveur B, et du serveur B au serveur A. Les données sont donc répliquées dans les deux sens.

Figure 1.3. Segments de topologie



Exemple 1.2. Visualisation des segments de topologie

La commande **ipa topologysegment-find** montre les segments de topologie actuels configurés pour les suffixes de domaine ou de CA. Par exemple, pour le suffixe de domaine :

```
$ ipa topologysegment-find
Suffix name: domain
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

Dans cet exemple, les données relatives au domaine ne sont répliquées qu'entre deux serveurs : **server1.example.com** et **server2.example.com**.

Pour afficher les détails d'un segment particulier uniquement, utilisez la commande **ipa topologysegment-show**:

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: server1.example.com-to-server2.example.com
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

1.2. UTILISATION DU GRAPHE TOPOLOGIQUE POUR GÉRER LA TOPOLOGIE DE RÉPLICATION

Le graphique de la topologie dans l'interface Web montre les relations entre les serveurs du domaine. L'interface Web permet de manipuler et de transformer la représentation de la topologie.

Accès au graphe topologique

Pour accéder au graphique de la topologie :

1. Sélectionner **Serveur IPA → Topologie → Graphique de la topologie**
2. Si vous apportez des modifications à la topologie qui ne sont pas immédiatement reflétées dans le graphique, cliquez sur **Actualiser**.

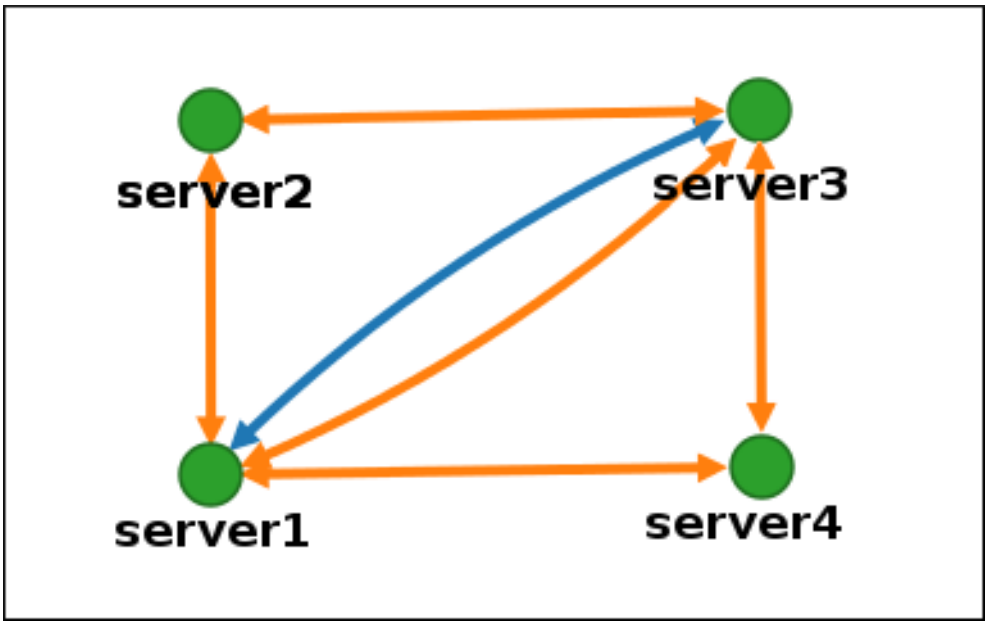
Interprétation du graphe topologique

Les serveurs liés par un accord de réplication de domaine sont reliés par une flèche orange. Les serveurs liés par un accord de réplication de CA sont reliés par une flèche bleue.

Exemple de graphique topologique : topologie recommandée

L'exemple de topologie recommandée ci-dessous montre l'une des topologies recommandées possibles pour quatre serveurs : chaque serveur est connecté à au moins deux autres serveurs, et plus d'un serveur est un serveur CA.

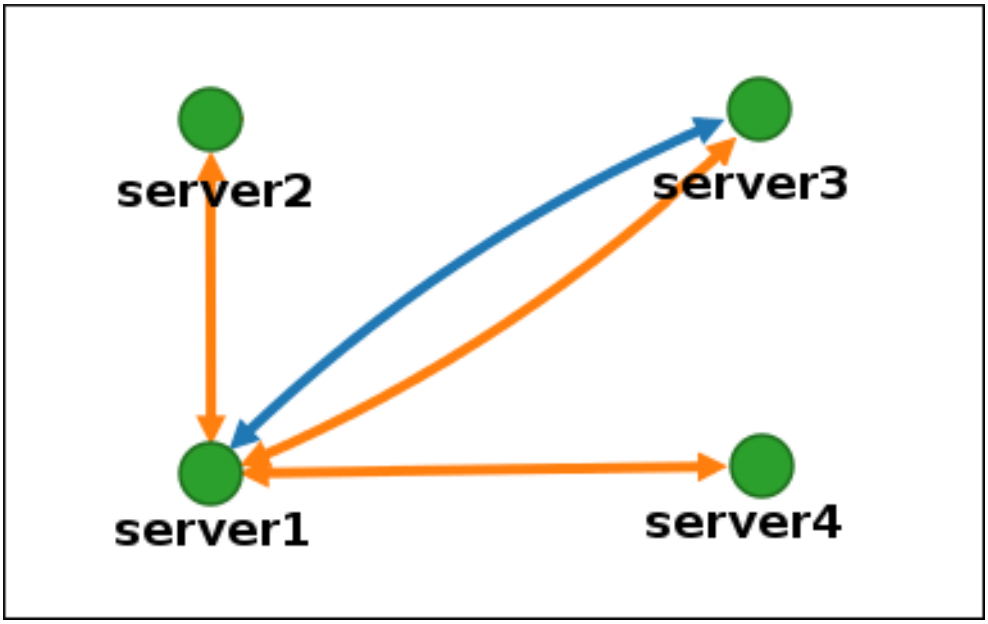
Figure 1.4. Exemple de topologie recommandée



Exemple de graphe topologique : topologie déconseillée

Dans l'exemple de topologie déconseillée ci-dessous, **server1** est un point de défaillance unique. Tous les autres serveurs ont des accords de réplication avec ce serveur, mais pas avec les autres serveurs. Par conséquent, si **server1** tombe en panne, tous les autres serveurs seront isolés. Évitez de créer des topologies de ce type.

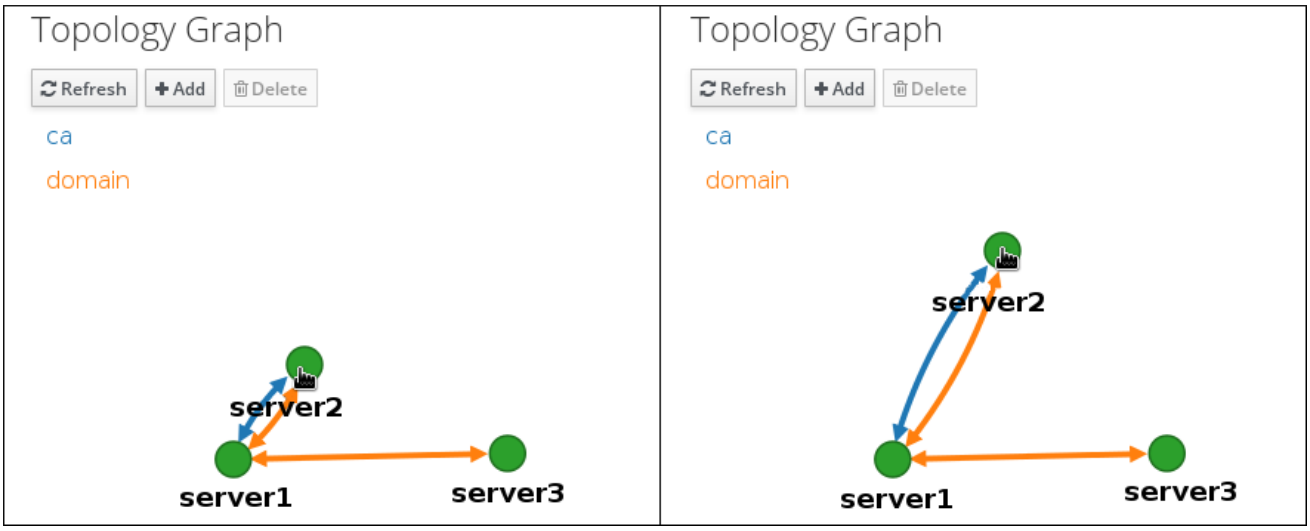
Figure 1.5. Exemple de topologie déconseillée : Point de défaillance unique



Personnaliser la vue topologique

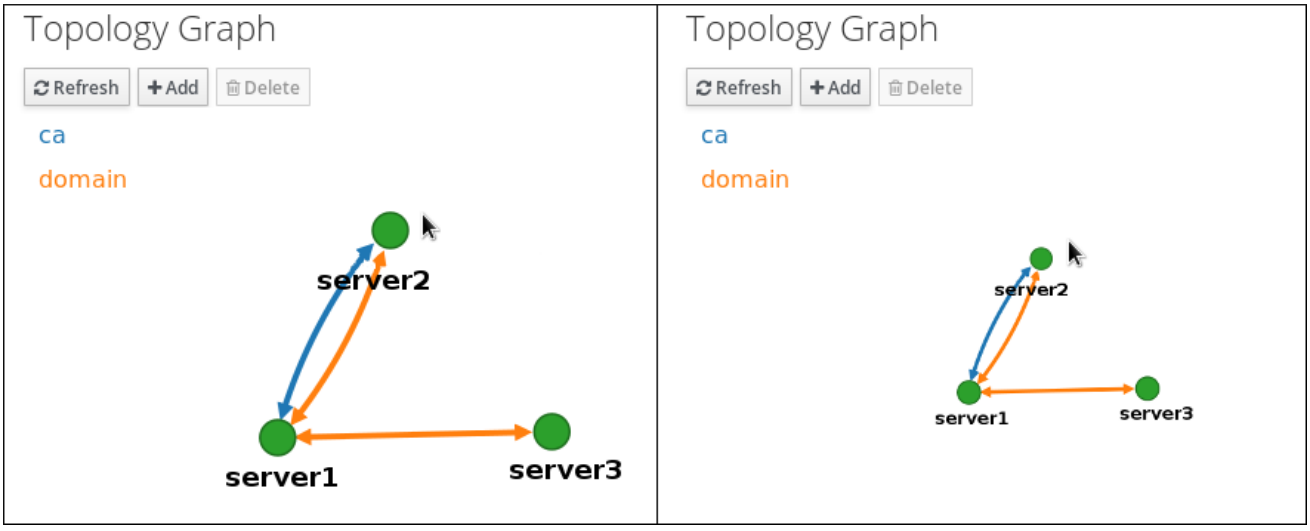
Vous pouvez déplacer des nœuds topologiques individuels en faisant glisser la souris :

Figure 1.6. Déplacement des nœuds du graphe topologique



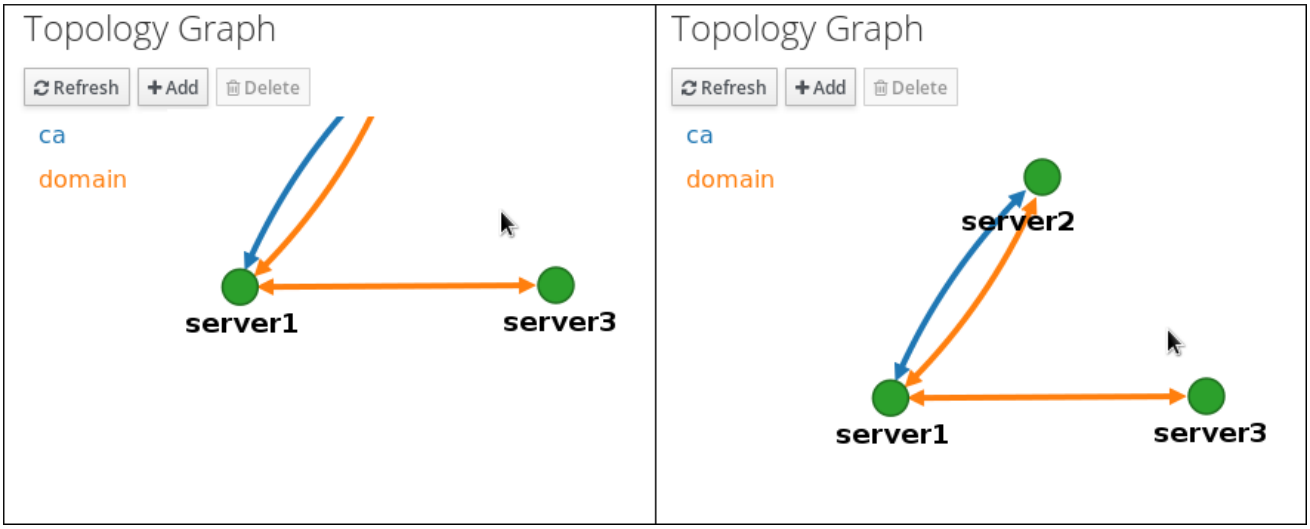
Vous pouvez agrandir ou réduire le graphique topologique à l'aide de la molette de la souris :

Figure 1.7. Zoom sur le graphe topologique



Vous pouvez déplacer le canevas du graphique topologique en maintenant le bouton gauche de la souris enfoncé :

Figure 1.8. Déplacement du canevas du graphe topologique



1.3. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE L'INTERFACE WEB

L'interface Web de la gestion des identités (IdM) vous permet de choisir deux serveurs et de créer un nouvel accord de réplication entre eux.

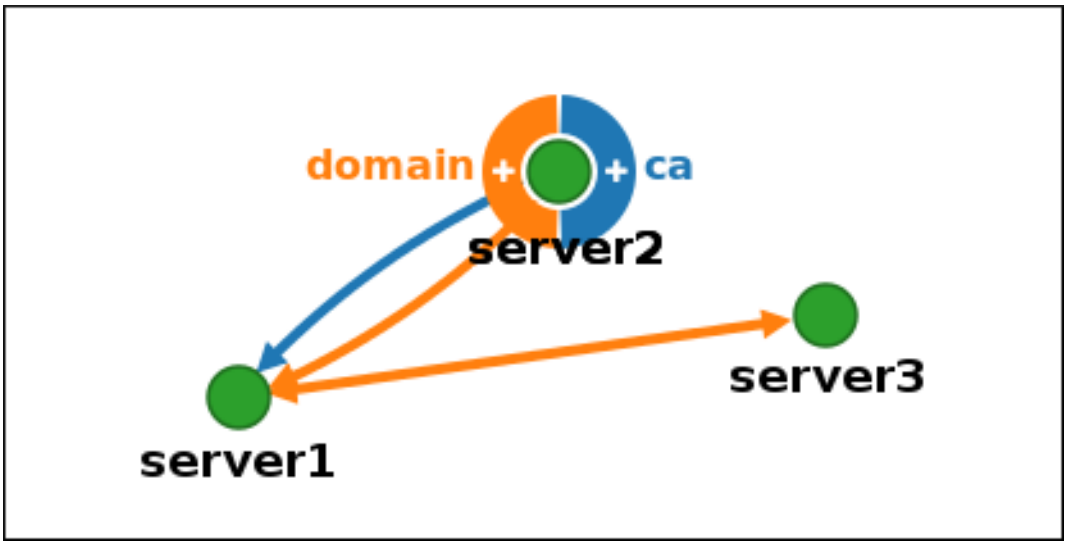
Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Dans le graphique topologique, passez votre souris sur l'un des nœuds de serveur.

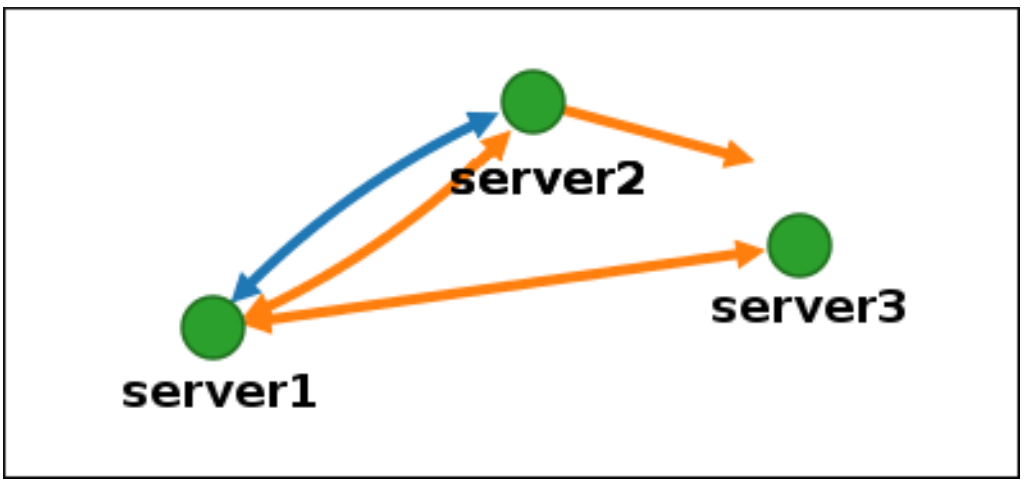
   Figure 1.9. Options de domaine ou d'autorité de certification

2. Cliquez sur la partie **domain** ou **ca** du cercle en fonction du type de segment topologique que vous souhaitez créer.

3. Une nouvelle flèche représentant le nouvel accord de réplication apparaît sous le pointeur de votre souris. Déplacez votre souris vers l'autre nœud de serveur et cliquez dessus.

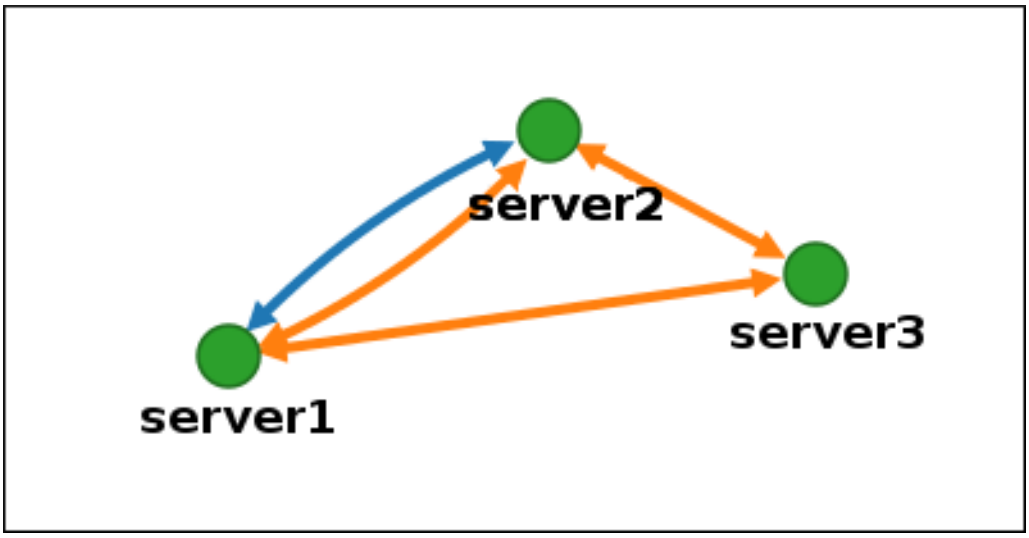
   Figure 1.10. Création d'un nouveau segment

4. Dans la fenêtre **Add topology segment**, cliquez sur **Ajouter** pour confirmer les propriétés du nouveau segment.

Le nouveau segment topologique entre les deux serveurs les associe à un accord de réplication. Le graphique de la topologie montre maintenant la topologie de réplication mise à jour :

Figure 1.11. Création d'un nouveau segment



1.4. ARRÊT DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE L'INTERFACE WEB

L'interface web de la gestion des identités (IdM) permet de supprimer un accord de réplication des serveurs.

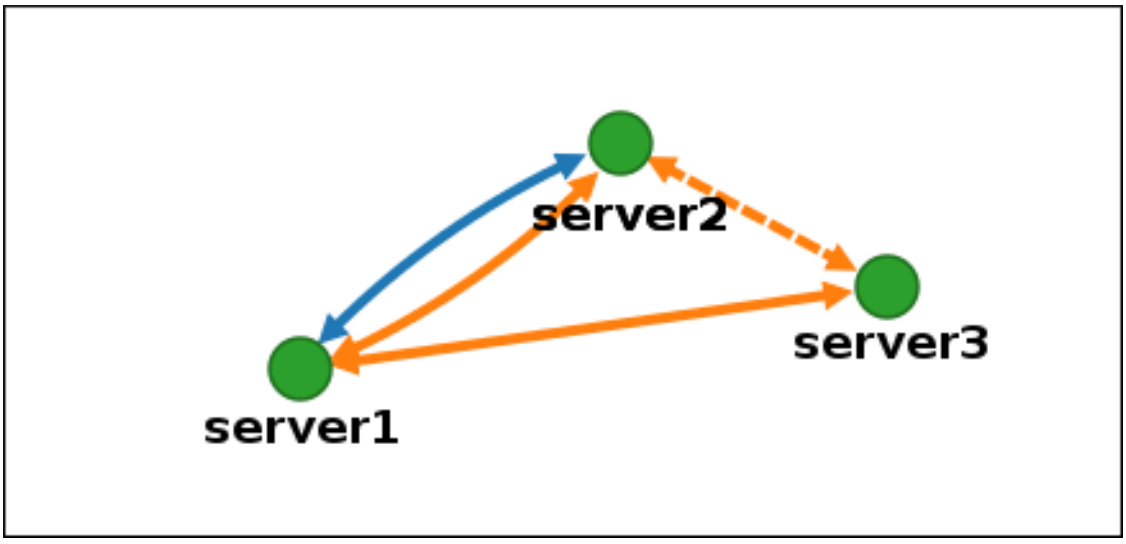
Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Cliquez sur une flèche représentant l'accord de réplication que vous souhaitez supprimer. La flèche est mise en évidence.

   Figure 1.12. Segment de topologie mis en évidence

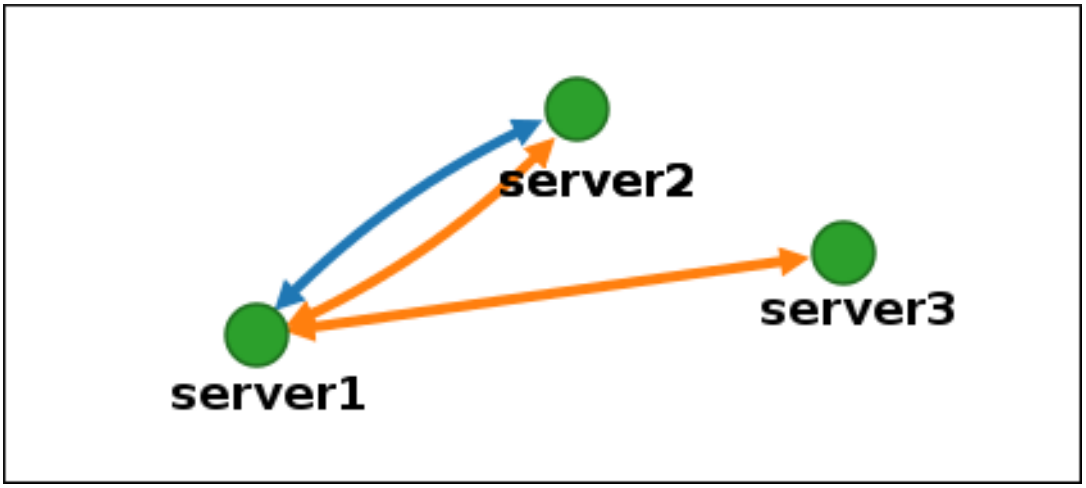
   

2. Click **Delete**.

3. Dans la fenêtre **Confirmation**, cliquez sur **OK**.

IdM supprime le segment de topologie entre les deux serveurs, ce qui supprime leur accord de réplication. Le graphique de la topologie montre maintenant la topologie de réplication mise à jour :

Figure 1.13. Segment de topologie supprimé



1.5. CONFIGURATION DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DU CLI

Vous pouvez configurer les accords de réplication entre deux serveurs à l'aide de la commande **ipa topologysegment-add**.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Utilisez la commande **ipa topologysegment-add** pour créer un segment de topologie pour les deux serveurs. Lorsque vous y êtes invité, fournissez :
   - le suffixe topologique requis : **domain** ou **ca**
   - le nœud gauche et le nœud droit, représentant les deux serveurs
   - éventuellement, un nom personnalisé pour le segment
     Par exemple :

```
$ ipa topologysegment-add
Suffix name: domain
Left node: server1.example.com
Right node: server2.example.com
Segment name [server1.example.com-to-server2.example.com]: new_segment
---------------------------
Added segment "new_segment"
---------------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

L'ajout du nouveau segment joint les serveurs dans un accord de réplication.

2. *Optional.* Utilisez la commande **ipa topologysegment-show** pour vérifier que le nouveau segment est configuré.

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: new_segment
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

1.6. ARRÊT DE LA RÉPLICATION ENTRE DEUX SERVEURS À L'AIDE DE LA CLI

Vous pouvez mettre fin aux accords de réplication à partir de la ligne de commande en utilisant la commande **ipa topology_segment-del**.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

Procédure

1. Pour arrêter la réplication, vous devez supprimer le segment de réplication correspondant entre les serveurs. Pour ce faire, vous devez connaître le nom du segment.
   Si vous ne connaissez pas le nom, utilisez la commande **ipa topologysegment-find** pour afficher tous les segments et localisez le segment requis dans la sortie. Lorsque vous y êtes invité, indiquez le suffixe de topologie requis : **domain** ou **ca**. Par exemple :

```
$ ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both

...

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

2. Utilisez la commande **ipa topologysegment-del** pour supprimer le segment topologique reliant les deux serveurs.

```
$ ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
```

```
----------------------------
Deleted segment "new_segment"
----------------------------
```

La suppression du segment supprime l'accord de réplication.

3. *Optional.* Utilisez la commande **ipa topologysegment-find** pour vérifier que le segment n'est plus répertorié.

```
$ ipa topologysegment-find
Suffix name: domain
------------------
7 segments matched
------------------
  Segment name: server2.example.com-to-server3.example.com
  Left node: server2.example.com
  Right node: server3.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 7
----------------------------
```

1.7. SUPPRESSION D'UN SERVEUR DE LA TOPOLOGIE À L'AIDE DE L'INTERFACE WEB

Vous pouvez utiliser l'interface web de la gestion des identités (IdM) pour supprimer un serveur de la topologie.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.
- Le serveur que vous souhaitez supprimer est **not** le seul serveur qui relie les autres serveurs au reste de la topologie ; cela aurait pour effet d'isoler les autres serveurs, ce qui n'est pas autorisé.
- Le serveur que vous souhaitez supprimer est **not** votre dernier serveur CA ou DNS.

AVERTISSEMENT

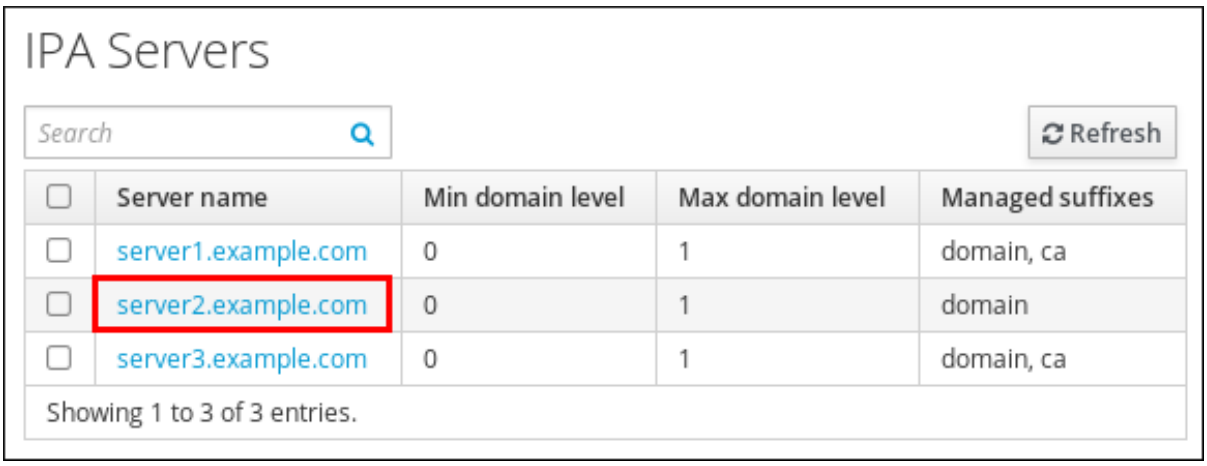
La suppression d'un serveur est une action irréversible. Si vous supprimez un serveur, la seule façon de le réintroduire dans la topologie est d'installer une nouvelle réplique sur la machine.

Procédure

Pour supprimer un serveur de la topologie sans désinstaller les composants du serveur de la machine :

1. Sélectionner **Serveur IPA → Topologie → Serveurs IPA**.
2. Cliquez sur le nom du serveur que vous souhaitez supprimer.

Figure 1.14. Sélection d'un serveur



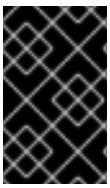
3. Cliquez sur **Supprimer le serveur**.

1.8. SUPPRESSION D'UN SERVEUR DE LA TOPOLOGIE À L'AIDE DE LA CLI

Vous pouvez utiliser l'interface de ligne de commande pour supprimer un serveur de la topologie.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.
- Le serveur que vous souhaitez supprimer est **not** le seul serveur qui relie les autres serveurs au reste de la topologie ; cela aurait pour effet d'isoler les autres serveurs, ce qui n'est pas autorisé
- Le serveur que vous souhaitez supprimer est **not** votre dernier serveur CA ou DNS.



IMPORTANT

La suppression d'un serveur est une action irréversible. Si vous supprimez un serveur, la seule façon de le réintroduire dans la topologie est d'installer une nouvelle réplique sur la machine.

Procédure

Pour supprimer **server1.example.com**:

1. Sur un autre serveur, exécutez la commande **ipa server-del** pour supprimer **server1.example.com**. La commande supprime tous les segments topologiques pointant vers le serveur :

```
[user@server2 ~]$ ipa server-del
Server name: server1.example.com
Removing server1.example.com from replication topology, please wait...
-----------------------------------------------------------
Deleted IPA server "server1.example.com"
-----------------------------------------------------------
```

2. *Optional*le programme de désinstallation du serveur se trouve à l'adresse suivante : **server1.example.com**, exécutez la commande **ipa server-install --uninstall** pour désinstaller les composants du serveur de l'ordinateur.

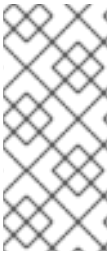
```
[root@server1 ~]# ipa server-install --uninstall
```

1.9. VISUALISATION DES RÔLES DE SERVEUR SUR UN SERVEUR IDM À L'AIDE DE L'INTERFACE WEB

En fonction des services installés sur un serveur IdM, celui-ci peut effectuer diverses opérations *server roles*. Par exemple :

- Serveur CA
- Serveur DNS
- Serveur de l'autorité de recouvrement des clés (KRA).

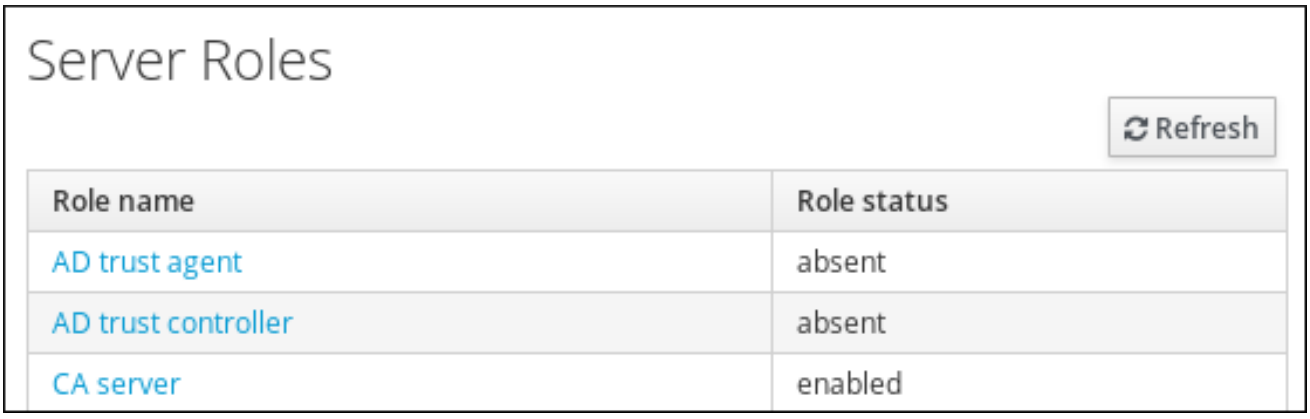
Pour une liste complète des rôles de serveur pris en charge, voir **Serveur IPA → Topologie → Rôles du serveur**.



NOTE

- L'état du rôle **absent** signifie qu'aucun serveur de la topologie ne joue le rôle en question.
- Le statut du rôle **enabled** signifie qu'un ou plusieurs serveurs de la topologie jouent le rôle en question.

Figure 1.15. Rôles des serveurs dans l'interface web



1.10. VISUALISATION DES RÔLES DE SERVEUR SUR UN SERVEUR IDM À L'AIDE DE LA CLI

En fonction des services installés sur un serveur IdM, celui-ci peut effectuer diverses opérations *server roles*. Par exemple :

- Serveur CA
- Serveur DNS

- Serveur de l'autorité de recouvrement des clés (KRA).

Les commandes suivantes permettent de voir quels serveurs jouent quel rôle dans la topologie.

- La commande **ipa config-show** affiche tous les serveurs d'autorité de certification et le serveur de renouvellement d'autorité de certification actuel :

```
$ ipa config-show
  ...
  IPA masters: server1.example.com, server2.example.com, server3.example.com
  IPA CA servers: server1.example.com, server2.example.com
  IPA CA renewal master: server1.example.com
```

- La commande **ipa server-show** permet d'afficher la liste des rôles activés sur un serveur particulier. Par exemple, pour obtenir la liste des rôles activés sur *server.example.com*:

```
$ ipa server-show
Server name: server.example.com
  ...
  Enabled server roles: CA server, DNS server, KRA server
```

- Le site **ipa server-find --servrole** recherche tous les serveurs pour lesquels un rôle de serveur particulier est activé. Par exemple, pour rechercher tous les serveurs CA :

```
$ ipa server-find --servrole "CA server"
---------------------
2 IPA servers matched
---------------------
  Server name: server1.example.com
  ...

  Server name: server2.example.com
  ...
----------------------------
Number of entries returned 2
----------------------------
```

1.11. PROMOUVOIR UN RÉPLICA EN TANT QUE SERVEUR DE RENOUVELLEMENT DE L'AUTORITÉ DE CERTIFICATION ET SERVEUR D'ÉDITION DE CRL

Si votre déploiement IdM utilise une autorité de certification (CA) intégrée, l'un des serveurs CA IdM agit en tant que serveur de renouvellement CA, un serveur qui gère le renouvellement des certificats du sous-système CA. L'un des serveurs de l'autorité de certification IdM fait également office de serveur d'édition CRL IdM, un serveur qui génère des listes de révocation de certificats. Par défaut, les rôles de serveur de renouvellement de CA et de serveur d'édition de CRL sont installés sur le premier serveur sur lequel l'administrateur système a installé le rôle CA à l'aide de la commande **ipa-server-install** ou **ipa-ca-install**.

Conditions préalables

- Vous disposez des informations d'identification de l'administrateur IdM.

1.12. RÉTROGRADER OU PROMOUVOIR DES RÉPLIQUES CACHÉES

Procédure

Après l'installation d'un réplica, vous pouvez configurer si le réplica est caché ou visible.

Pour plus de détails sur les répliques cachées, voir Le mode réplique cachée.

Si le réplica est un serveur de renouvellement de l'AC, déplacez le service vers un autre réplica avant de rendre ce réplica masqué.

For details, see

Procédure

- Pour masquer la réplique, entrez :

```
# ipa server-state replica.idm.example.com --state=hidden
```

Vous pouvez également rendre le réplica visible à l'aide de la commande suivante :

```
# ipa server-state replica.idm.example.com --state=enabled
```

CHAPITRE 2. PRÉPARATION DE L'ENVIRONNEMENT POUR LA GESTION DE L'IDM À L'AIDE DES PLAYBOOKS ANSIBLE

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**.

Grâce à cette pratique, vous pouvez retrouver tous vos playbooks en un seul endroit et vous pouvez exécuter vos playbooks sans invoquer les privilèges de l'administrateur.

NOTE

Vous n'avez besoin que des privilèges **root** sur les nœuds gérés pour exécuter les rôles **ipaserver**, **ipareplica**, **ipaclient** et **ipabackup 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 :

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

[us]
replica.idm.example.com

[ipaserver:children]
eu
us
```

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
```

Ces commandes nécessitent la saisie du mot de passe IdM **admin**.

Ressources supplémentaires

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

CHAPITRE 3. UTILISER ANSIBLE POUR GÉRER LA TOPOLOGIE DE RÉPLICATION DANS IDM

Vous pouvez maintenir plusieurs serveurs de gestion des identités (IdM) et les laisser se répliquer les uns les autres à des fins de redondance afin d'atténuer ou d'empêcher la perte de serveurs. Par exemple, si un serveur tombe en panne, les autres serveurs continuent à fournir des services au domaine. Vous pouvez également récupérer le serveur perdu en créant une nouvelle réplique basée sur l'un des serveurs restants.

Les données stockées sur un serveur IdM sont répliquées sur la base d'accords de réplication : lorsque deux serveurs ont un accord de réplication configuré, ils partagent leurs données. Les données répliquées sont stockées dans la topologie **suffixes**. Lorsque deux répliques ont un accord de réplication entre leurs suffixes, ces derniers forment une topologie **segment**.

Ce chapitre décrit comment utiliser **Red Hat Ansible Engine** pour gérer les accords de réplication IdM, les segments de topologie et les suffixes de topologie. Ce chapitre contient les sections suivantes :

- Utiliser Ansible pour s'assurer qu'un accord de réplication existe dans IdM
- Utiliser Ansible pour s'assurer que des accords de réplication existent entre plusieurs répliques IdM
- Utiliser Ansible pour vérifier l'existence d'un accord de réplication entre deux répliques
- Utiliser Ansible pour vérifier qu'un suffixe de topologie existe dans IdM
- Utiliser Ansible pour réinitialiser une réplique IdM
- Utiliser Ansible pour s'assurer qu'un accord de réplication est absent dans IdM

3.1. UTILISER ANSIBLE POUR S'ASSURER QU'UN ACCORD DE RÉPLICATION EXISTE DANS IDM

Les données stockées sur un serveur de gestion des identités (IdM) sont répliquées sur la base d'accords de réplication : lorsque deux serveurs ont un accord de réplication configuré, ils partagent leurs données. Les accords de réplication sont toujours bilatéraux : les données sont répliquées de la première réplique vers l'autre et de l'autre réplique vers la première.

Cette section décrit comment utiliser un playbook Ansible pour s'assurer qu'un accord de réplication de type **domain** existe entre **server.idm.example.com** et **replica.idm.example.com**.

Conditions préalables

- Assurez-vous de bien comprendre les recommandations relatives à la conception de votre topologie IdM (voir Connexion des répliques dans une topologie).
- Vous connaissez le mot de passe de l'IdM **admin**.
- 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**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

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

2. Copiez le fichier **add-topologysegment.yml** Ansible playbook situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology/**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/add-topologysegment.yml
add-topologysegment-copy.yml
```

3. Ouvrez le fichier **add-topologysegment-copy.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes dans la section **ipatopologysegment** task :
   - Fixer la variable **ipaadmin_password** au mot de passe de l'IdM **admin**.
   - Définissez la variable **suffix** à **domain** ou **ca**, en fonction du type de segment que vous souhaitez ajouter.
   - Définissez la variable **left** avec le nom du serveur IdM que vous voulez être le nœud gauche de l'accord de réplication.
   - Définissez la variable **right** avec le nom du serveur IdM que vous voulez être le nœud droit de l'accord de réplication.
   - Assurez-vous que la variable **state** est définie sur **present**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
- name: Add topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      left: server.idm.example.com
      right: replica.idm.example.com
      state: present
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-topologysegment-copy.yml
```

Ressources supplémentaires

- Voir Explication des accords de réplication, des suffixes de topologie et des segments de topologie.
- Voir le fichier **README-topology.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology**.

3.2. UTILISER ANSIBLE POUR S'ASSURER QUE DES ACCORDS DE RÉPLICATION EXISTENT ENTRE PLUSIEURS RÉPLIQUES IDM

Les données stockées sur un serveur de gestion des identités (IdM) sont répliquées sur la base d'accords de réplication : lorsque deux serveurs ont un accord de réplication configuré, ils partagent leurs données. Les accords de réplication sont toujours bilatéraux : les données sont répliquées de la première réplique vers l'autre et de l'autre réplique vers la première.

Cette section décrit comment garantir l'existence d'accords de réplication entre plusieurs paires de répliques dans IdM.

Conditions préalables

- Assurez-vous de bien comprendre les recommandations relatives à la conception de votre topologie IdM, énumérées dans la section Connexion des répliques dans une topologie
- Vous connaissez le mot de passe de l'IdM **admin**.
- 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**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

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

2. Copiez le fichier **add-topologysegments.yml** Ansible playbook situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology/**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/add-topologysegments.yml
add-topologysegments-copy.yml
```

3. Ouvrez le fichier **add-topologysegments-copy.yml** pour le modifier.

4. Adaptez le fichier en définissant les variables suivantes dans la section **vars**:

   - Fixer la variable **ipaadmin_password** au mot de passe de l'IdM **admin**.
   - Pour chaque segment topologique, ajoutez une ligne dans la section **ipatopology_segments** et définissez les variables suivantes :
     - Définissez la variable **suffix** à **domain** ou **ca**, en fonction du type de segment que vous souhaitez ajouter.
     - Définissez la variable **left** avec le nom du serveur IdM que vous voulez être le nœud gauche de l'accord de réplication.
     - Définissez la variable **right** avec le nom du serveur IdM que vous voulez être le nœud droit de l'accord de réplication.

5. Dans la section **tasks** du fichier **add-topologysegments-copy.yml**, assurez-vous que la variable **state** est fixée à **present**.
   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Add topology segments
  hosts: ipaserver
  gather_facts: false

  vars:
    ipaadmin_password: "{{ ipaadmin_password }}"
    ipatopology_segments:
    - {suffix: domain, left: replica1.idm.example.com , right: replica2.idm.example.com }
    - {suffix: domain, left: replica2.idm.example.com , right: replica3.idm.example.com }
    - {suffix: domain, left: replica3.idm.example.com , right: replica4.idm.example.com }
    - {suffix: domain+ca, left: replica4.idm.example.com , right: replica1.idm.example.com }

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Add topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: "{{ item.suffix }}"
      name: "{{ item.name | default(omit) }}"
      left: "{{ item.left }}"
      right: "{{ item.right }}"
      state: present
      #state: absent
      #state: checked
      #state: reinitialized
    loop: "{{ ipatopology_segments | default([]) }}"
```

6. Enregistrer le fichier.

7. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-topologysegments-copy.yml
```

Ressources supplémentaires

- Voir Explication des accords de réplication, des suffixes de topologie et des segments de topologie.
- Voir le fichier **README-topology.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology**.

3.3. UTILISER ANSIBLE POUR VÉRIFIER L'EXISTENCE D'UN ACCORD DE RÉPLICATION ENTRE DEUX RÉPLIQUES

Les données stockées sur un serveur de gestion des identités (IdM) sont répliquées sur la base d'accords de réplication : lorsque deux serveurs ont un accord de réplication configuré, ils partagent leurs données. Les accords de réplication sont toujours bilatéraux : les données sont répliquées de la première réplique vers l'autre et de l'autre réplique vers la première.

Cette section décrit comment vérifier que des accords de réplication existent entre plusieurs paires de répliques dans IdM.

Conditions préalables

- Assurez-vous de bien comprendre les recommandations relatives à la conception de votre topologie de gestion des identités (IdM), énumérées à la section Connexion des répliques dans une topologie.
- Vous connaissez le mot de passe de l'IdM **admin**.
- 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**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

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

2. Copiez le fichier **check-topologysegments.yml** Ansible playbook situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology/**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/check-topologysegments.yml
check-topologysegments-copy.yml
```

3. Ouvrez le fichier **check-topologysegments-copy.yml** pour le modifier.

4. Adaptez le fichier en définissant les variables suivantes dans la section **vars**:

   - Fixer la variable **ipaadmin_password** au mot de passe de l'IdM **admin**.

   - Pour chaque segment topologique, ajoutez une ligne dans la section **ipatopology_segments** et définissez les variables suivantes :

     - Définissez la variable **suffix** à **domain** ou **ca**, en fonction du type de segment que vous ajoutez.

     - Définissez la variable **left** avec le nom du serveur IdM que vous voulez être le nœud gauche de l'accord de réplication.

     - Définissez la variable **right** avec le nom du serveur IdM que vous voulez être le nœud droit de l'accord de réplication.

5. Dans la section **tasks** du fichier **check-topologysegments-copy.yml**, assurez-vous que la variable **state** est fixée à **present**.
   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Add topology segments
  hosts: ipaserver
  gather_facts: false

  vars:
    ipaadmin_password: "{{ ipaadmin_password }}"
    ipatopology_segments:
    - {suffix: domain, left: replica1.idm.example.com, right: replica2.idm.example.com }
    - {suffix: domain, left: replica2.idm.example.com , right: replica3.idm.example.com }
    - {suffix: domain, left: replica3.idm.example.com , right: replica4.idm.example.com }
    - {suffix: domain+ca, left: replica4.idm.example.com , right:
replica1.idm.example.com }

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Check topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: "{{ item.suffix }}"
      name: "{{ item.name | default(omit) }}"
      left: "{{ item.left }}"
      right: "{{ item.right }}"
      state: checked
    loop: "{{ ipatopology_segments | default([]) }}"
```

6. Enregistrer le fichier.

7. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory check-topologysegments-copy.yml
```

Ressources supplémentaires

- Pour plus d'informations sur le concept d'accords, de suffixes et de segments de topologie, voir Explication des accords de réplication, des suffixes de topologie et des segments de topologie .
- Voir le fichier **README-topology.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology**.

3.4. UTILISER ANSIBLE POUR VÉRIFIER QU'UN SUFFIXE DE TOPOLOGIE EXISTE DANS IDM

Dans le contexte des accords de réplication de la gestion des identités (IdM), les suffixes de topologie stockent les données qui sont répliquées. L'IdM prend en charge deux types de suffixes de topologie : **domain** et **ca**. Chaque suffixe représente un back-end distinct, une topologie de réplication distincte. Lorsqu'un accord de réplication est configuré, il relie deux suffixes de topologie du même type sur deux serveurs différents.

Le suffixe **domain** contient toutes les données relatives au domaine, telles que les utilisateurs, les groupes et les stratégies. Le suffixe **ca** contient les données relatives au système de certification. Il n'est présent que sur les serveurs sur lesquels une autorité de certification (CA) est installée.

Cette section décrit comment utiliser un playbook Ansible pour s'assurer qu'un suffixe de topologie existe dans IdM. L'exemple décrit comment s'assurer que le suffixe **domain** existe dans IdM.

Conditions préalables

- Vous connaissez le mot de passe de l'IdM **admin**.
- 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**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

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

2. Copiez le fichier **verify-topologysuffix.yml** Ansible playbook situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology/**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/ verify-topologysuffix.yml
verify-topologysuffix-copy.yml
```

3. Ouvrez le fichier **verify-topologysuffix-copy.yml** Ansible playbook pour l'éditer.

4. Adaptez le fichier en définissant les variables suivantes dans la section **ipatopologysuffix**:

   - Fixer la variable **ipaadmin_password** au mot de passe de l'IdM **admin**.
   - Définissez la variable **suffix** à **domain**. Si vous vérifiez la présence du suffixe **ca**, définissez la variable à **ca**.
   - Assurez-vous que la variable **state** est définie sur **verified**. Aucune autre option n'est possible.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to handle topologysuffix
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Verify topology suffix
    ipatopologysuffix:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      state: verified
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory verify-
topologysuffix-copy.yml
```

Ressources supplémentaires

- Voir Explication des accords de réplication, des suffixes de topologie et des segments de topologie.
- Voir le fichier **README-topology.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology**.

3.5. UTILISER ANSIBLE POUR RÉINITIALISER UNE RÉPLIQUE IDM

Si un réplica a été déconnecté pendant une longue période ou si sa base de données a été corrompue, vous pouvez le réinitialiser. La réinitialisation actualise le réplica avec un ensemble de données mises à jour. La réinitialisation peut, par exemple, être utilisée si une restauration autoritaire à partir d'une sauvegarde est nécessaire.

NOTE

Contrairement aux mises à jour de réplication, au cours desquelles les répliques ne s'envoient que les entrées modifiées, la réinitialisation rafraîchit l'ensemble de la base de données.

L'hôte local sur lequel vous exécutez la commande est le réplica réinitialisé. Pour spécifier le réplica à partir duquel les données sont obtenues, utilisez l'option **direction**.

Cette section décrit comment utiliser un playbook Ansible pour réinitialiser les données **domain** sur **replica.idm.example.com** à partir de **server.idm.example.com**.

Conditions préalables

- Vous connaissez le mot de passe de l'IdM **admin**.
- 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**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

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

2. Copiez le fichier **reinitialize-topologysegment.yml** Ansible playbook situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology/**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/reinitialize-topologysegment.yml reinitialize-topologysegment-copy.yml
```

3. Ouvrez le fichier **reinitialize-topologysegment-copy.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes dans la section **ipatopologysegment**:
   - Fixer la variable **ipaadmin_password** au mot de passe de l'IdM **admin**.
   - Fixez la variable **suffix** à **domain**. Si vous réinitialisez les données **ca**, fixez la variable à **ca**.
   - Définissez la variable **left** sur le nœud gauche de l'accord de réplication.

- Définissez la variable **right** sur le nœud de droite de l'accord de réplication.
- Définissez la variable **direction** en fonction de la direction des données réinitialisées. La direction **left-to-right** signifie que les données circulent du nœud gauche vers le nœud droit.
- Assurez-vous que la variable **state** est définie sur **reinitialized**.
  Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Reinitialize topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      left: server.idm.example.com
      right: replica.idm.example.com
      direction: left-to-right
      state: reinitialized
```

5. Enregistrer le fichier.
6. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory reinitialize-topologysegment-copy.yml
```

Ressources supplémentaires

- Voir Explication des accords de réplication, des suffixes de topologie et des segments de topologie.
- Voir le fichier **README-topology.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology**.

3.6. UTILISER ANSIBLE POUR S'ASSURER QU'UN ACCORD DE RÉPLICATION EST ABSENT DANS IDM

Les données stockées sur un serveur de gestion des identités (IdM) sont répliquées sur la base d'accords de réplication : lorsque deux serveurs ont un accord de réplication configuré, ils partagent leurs données. Les accords de réplication sont toujours bilatéraux : les données sont répliquées de la première réplique vers l'autre et de l'autre réplique vers la première.

Cette section décrit comment s'assurer qu'un accord de réplication entre deux répliques n'existe pas dans IdM. L'exemple décrit comment s'assurer qu'un accord de réplication de type **domain** n'existe pas entre les serveurs IdM **replica01.idm.example.com** et **replica02.idm.example.com**.

Conditions préalables

Conditions préalables

- Assurez-vous de bien comprendre les recommandations relatives à la conception de votre topologie IdM, énumérées dans la section Connexion des répliques dans une topologie
- Vous connaissez le mot de passe de l'IdM **admin**.
- 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**.

Procédure

1. Naviguez jusqu'à votre répertoire ***~/MyPlaybooks/*** répertoire :

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

2. Copiez le fichier **delete-topologysegment.yml** Ansible playbook situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology/**:

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/delete-topologysegment.yml
delete-topologysegment-copy.yml
```

3. Ouvrez le fichier **delete-topologysegment-copy.yml** pour le modifier.
4. Adaptez le fichier en définissant les variables suivantes dans la section **ipatopologysegment** task :
   - Fixer la variable **ipaadmin_password** au mot de passe de l'IdM **admin**.
   - Attribuez la valeur **domain** à la variable **suffix**. Si vous voulez vous assurer que les données de **ca** ne sont pas répliquées entre les nœuds de gauche et de droite, définissez la variable à **ca**.
   - Définissez la variable **left** avec le nom du serveur IdM qui est le nœud gauche de l'accord de réplication.
   - Définissez la variable **right** avec le nom du serveur IdM qui est le nœud droit de l'accord de réplication.
   - Assurez-vous que la variable **state** est définie sur **absent**.

   Il s'agit du fichier playbook Ansible modifié pour l'exemple actuel :

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver
```

```
  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
- name: Delete topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      left: replica01.idm.example.com
      right: replica02.idm.example.com:
      state: absent
```

5. Enregistrer le fichier.

6. Exécutez le playbook Ansible. Spécifiez le fichier du livre de jeu, le fichier contenant le mot de passe protégeant le fichier **secret.yml** et le fichier d'inventaire :

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory delete-topologysegment-copy.yml
```

Ressources supplémentaires

- Voir Explication des accords de réplication, des suffixes de topologie et des segments de topologie.
- Voir le fichier **README-topology.md** dans le répertoire **/usr/share/doc/ansible-freeipa/**.
- Voir les exemples de playbooks dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks/topology**.

3.7. RESSOURCES SUPPLÉMENTAIRES

- Voir Planification de la topologie du réplica .
- Voir Installation d'un réplica IdM .

CHAPITRE 4. RÉTROGRADER OU PROMOUVOIR DES RÉPLIQUES CACHÉES

Après l'installation d'un réplica, vous pouvez configurer si le réplica est caché ou visible.

Pour plus de détails sur les répliques cachées, voir Le mode réplique cachée.

Si le réplica est un serveur de renouvellement de l'AC, déplacez le service vers un autre réplica avant de rendre ce réplica masqué.

For details, see

Procédure

- Pour masquer la réplique, entrez :

```
# ipa server-state replica.idm.example.com --state=hidden
```

Vous pouvez également rendre le réplica visible à l'aide de la commande suivante :

```
# ipa server-state replica.idm.example.com --state=enabled
```

CHAPITRE 5. VÉRIFICATION DE LA RÉPLICATION DE L'IDM À L'AIDE DE HEALTHCHECK

Cette section décrit comment tester la réplication de la gestion des identités (IdM) à l'aide de l'outil Healthcheck.

Pour plus de détails, voir Healthcheck in IdM.

5.1. TESTS DE CONTRÔLE DE LA SANTÉ DE LA RÉPLICATION

L'outil Healthcheck teste la configuration de la topologie de la gestion des identités (IdM) et recherche les conflits de réplication.

Pour obtenir la liste de tous les tests, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

```
# ipa-healthcheck --list-sources
```

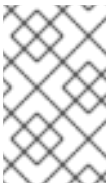
Les tests de topologie sont placés sous les sources **ipahealthcheck.ipa.topology** et **ipahealthcheck.ds.replication**:

IPATopologyDomainCheck (vérification de l'opologie du domaine)

Ce test permet de vérifier

- si la topologie n'est pas déconnectée et s'il existe des chemins de réplication entre tous les serveurs.
- si les serveurs n'ont pas plus que le nombre recommandé d'accords de réplication.
  Si le test échoue, il renvoie des erreurs, telles que des erreurs de connexion ou un trop grand nombre d'accords de réplication.

  Si le test réussit, il renvoie les domaines configurés.



NOTE

Le test exécute la commande **ipa topologysuffix-verify** pour les suffixes domain et ca (en supposant que l'autorité de certification soit configurée sur ce serveur).

ReplicationConflictCheck

Le test recherche dans LDAP les entrées correspondant à **(&(!(objectclass=nstombstone))(nsds5ReplConflict=*))**.

NOTE

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de vérifier s'il y a des problèmes.

5.2. VÉRIFICATION DE LA RÉPLICATION À L'AIDE DE HEALTHCHECK

Cette section décrit un test manuel autonome de la topologie et de la configuration de la réplication d'Identity Management (IdM) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests, ce qui vous permet d'abréger les résultats :

- Test de conflit de réplication : **--source=ipahealthcheck.ds.replication**
- Test de topologie correct : **--source=ipahealthcheck.ipa.topology**

Conditions préalables

- Vous devez effectuer les tests Healthcheck en tant qu'utilisateur **root**.

Procédure

- Pour exécuter les vérifications de conflit de réplication et de topologie Healthcheck, entrez :

```
# ipa-healthcheck --source=ipahealthcheck.ds.replication --
source=ipahealthcheck.ipa.topology
```

Quatre résultats différents sont possibles :

- SUCCESS - le test s'est déroulé avec succès.

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "SUCCESS",
  "kw": {
    "suffix": "domain"
  }
}
```

- AVERTISSEMENT - le test a réussi mais il pourrait y avoir un problème.
- ERROR - le test a échoué.

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "ERROR",
  "uuid": d6ce3332-92da-423d-9818-e79f49ed321f
  "when": 20191007115449Z
  "duration": 0.005943
  "kw": {
    "msg": "topologysuffix-verify domain failed, server2 is not connected
(server2_139664377356472 in MainThread)"
  }
}
```

- CRITIQUE - le test a échoué et affecte la fonctionnalité du serveur IdM.

Ressources supplémentaires

- Voir **man ipa-healthcheck**.