Red Hat Enterprise Linux 9

Se préparer à la reprise après sinistre grâce à la gestion des identités

Atténuer les effets des scénarios de perte de serveurs et de données dans les environnements IdM

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Se préparer à la reprise après sinistre grâce à la gestion des identités

Atténuer les effets des scénarios de perte de serveurs et de données dans les environnements IdM

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 une topologie Red Hat Identity Management (IdM), vous pouvez configurer la réplication avec d'autres serveurs, utiliser des snapshots de machines virtuelles (VM) et des sauvegardes IdM pour atténuer les effets de ces situations.

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. OUTILS DE REPRISE APRÈS SINISTRE DANS L'IDM

Une bonne stratégie de reprise après sinistre combine les outils suivants afin de se remettre d'un sinistre le plus rapidement possible avec une perte de données minimale :

Réplication

La réplication permet de copier le contenu de la base de données entre les serveurs IdM. Si un serveur IdM tombe en panne, vous pouvez remplacer le serveur perdu en créant une nouvelle réplique basée sur l'un des serveurs restants.

Instantanés de machines virtuelles (VM)

Un instantané est une vue du système d'exploitation et des applications d'une VM sur un ou tous les disques disponibles à un moment donné. Après avoir pris un instantané de la VM, vous pouvez l'utiliser pour ramener une VM et ses données IdM à un état antérieur.

Sauvegardes de l'IdM

L'utilitaire **ipa-backup** vous permet de sauvegarder les fichiers de configuration et les données d'un serveur IdM. Vous pouvez ensuite utiliser une sauvegarde pour restaurer un serveur IdM dans un état antérieur.

CHAPITRE 2. SCÉNARIOS DE CATASTROPHE DANS L'IDM

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

Tableau 2.1. Perte de serveur ou perte de données

Type de catastrophe	Exemple de causes	Comment se préparer
Server loss: Le déploiement de l'IdM perd un ou plusieurs serveurs.	• Dysfonctionnement du matériel	• Se préparer à la perte d'un serveur grâce à la 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	• Se préparer à la perte de données avec les snapshots de VM • Se préparer à la perte de données avec les sauvegardes IdM

CHAPITRE 3. SE PRÉPARER À LA PERTE D'UN SERVEUR GRÂCE À LA RÉPLICATION

Suivez les lignes directrices suivantes pour établir une topologie de réplication qui vous permettra de réagir à la perte d'un serveur.

Cette section couvre les sujets suivants :

- Connexion des répliques dans une topologie
- Exemples de topologie de réplique
- Protection des données de l'AC IdM

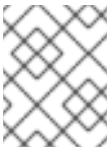
3.1. LIGNES DIRECTRICES POUR LA CONNEXION DES RÉPLIQUES IDM DANS UNE TOPOLOGIE

Connecter chaque réplique à au moins deux autres répliques

La configuration d'accords de réplication supplémentaires garantit que les informations sont répliquées non seulement entre le réplica initial et le premier serveur que vous avez installé, mais aussi entre les autres réplicas.

Connecter une réplique à un maximum de quatre autres répliques (ce n'est pas une exigence absolue)

Un grand nombre d'accords de réplication par serveur n'apporte pas d'avantages significatifs. Une réplique réceptrice ne peut être mise à jour que par une seule autre réplique à la fois et, pendant ce temps, les autres accords de réplication sont inactifs. Plus de quatre accords de réplication par réplique signifient généralement un gaspillage de ressources.



NOTE

Cette recommandation s'applique aux accords de réplication de certificats et de domaines.

Il existe deux exceptions à la limite de quatre accords de réplication par réplique :

- Vous voulez des chemins de basculement si certaines répliques ne sont pas en ligne ou ne répondent pas.
- Dans les déploiements plus importants, vous souhaitez disposer de liens directs supplémentaires entre des nœuds spécifiques.

La configuration d'un nombre élevé d'accords de réplication peut avoir un impact négatif sur les performances globales : lorsque plusieurs accords de réplication dans la topologie envoient des mises à jour, certaines répliques peuvent subir une forte contention sur le fichier de la base de données changelog entre les mises à jour entrantes et les mises à jour sortantes.

Si vous décidez d'utiliser davantage d'accords de réplication par réplique, assurez-vous que vous ne rencontrez pas de problèmes de réplication et de latence. Notez toutefois que les grandes distances et le nombre élevé de nœuds intermédiaires peuvent également entraîner des problèmes de latence.

Connecter les répliques d'un centre de données entre elles

Cela permet d'assurer la réplication du domaine au sein du centre de données.

Connecter chaque centre de données à au moins deux autres centres de données

Cela garantit la réplication du domaine entre les centres de données.

Connecter les centres de données en utilisant au moins une paire d'accords de réplication

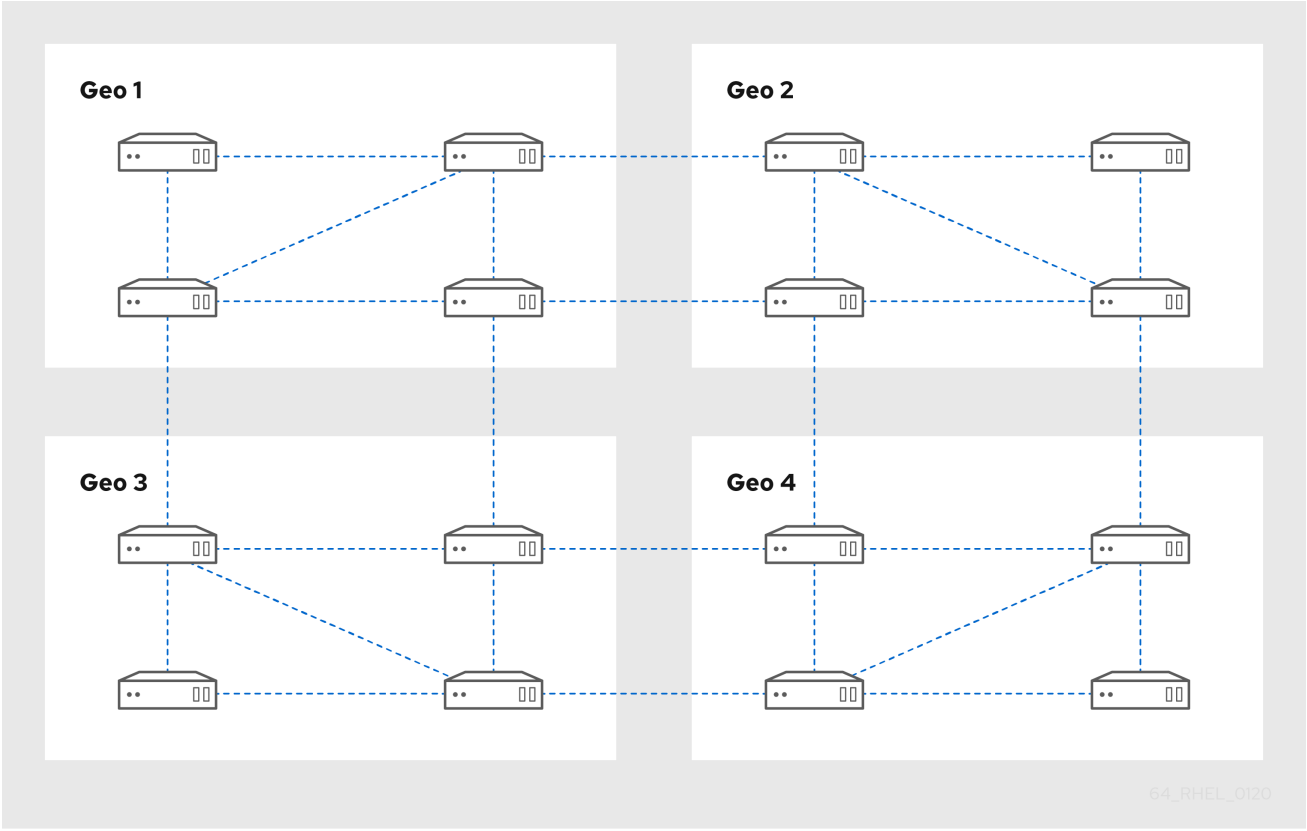
Si les centres de données A et B ont un accord de réplication de A1 à B1, le fait d'avoir un accord de réplication de A2 à B2 garantit que si l'un des serveurs est en panne, la réplication peut se poursuivre entre les deux centres de données.

3.2. EXEMPLES DE TOPOLOGIE DE RÉPLIQUE

Les figures ci-dessous montrent des exemples de topologies de gestion d'identité (IdM) basées sur les lignes directrices pour la création d'une topologie fiable.

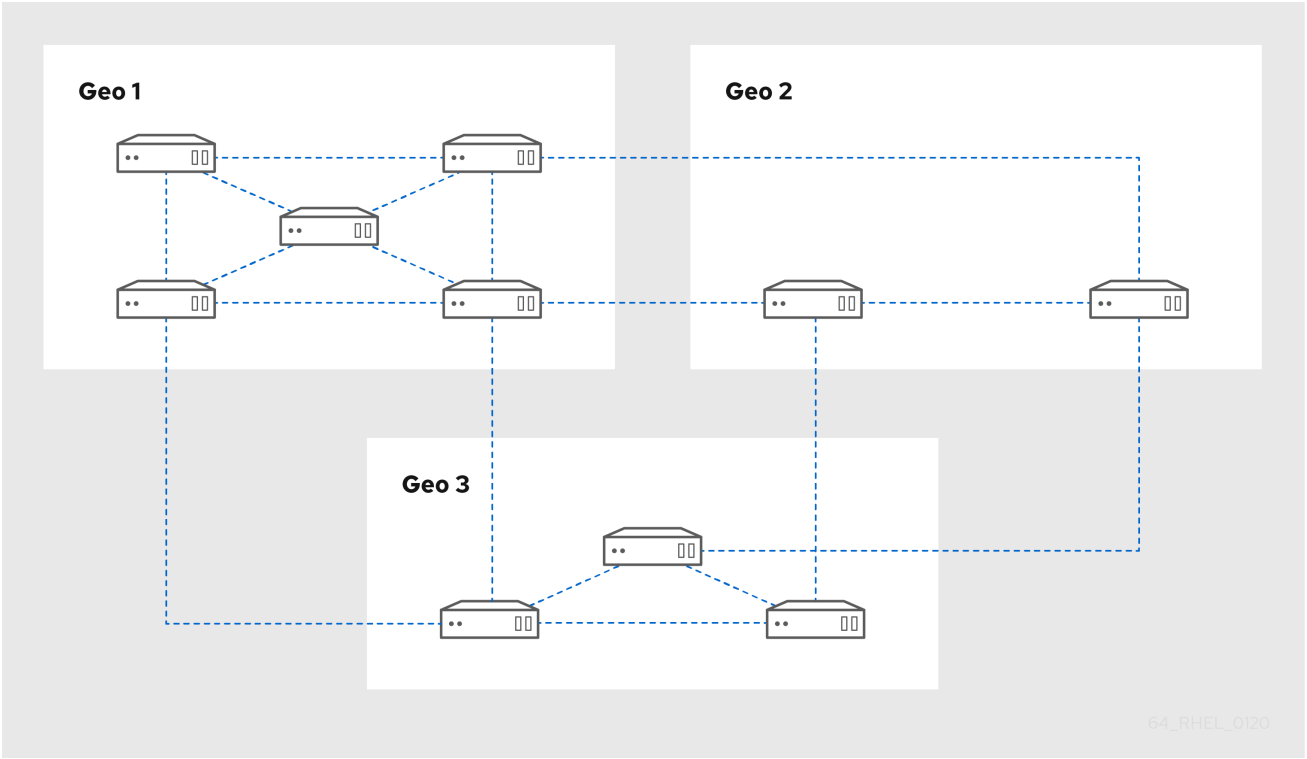
Topologie de réplication L'exemple 1 montre quatre centres de données, chacun avec quatre serveurs. Les serveurs sont reliés par des accords de réplication.

Figure 3.1. Exemple de topologie répliquée 1



Topologie de réplication L'exemple 2 montre trois centres de données, chacun avec un nombre différent de serveurs. Les serveurs sont reliés par des accords de réplication.

Figure 3.2. Exemple de topologie répliquée 2



3.3. PROTECTION DES DONNÉES DE L'AC IDM

Si votre déploiement contient l'autorité de certification (AC) IdM intégrée, installez plusieurs répliques de l'AC afin de pouvoir en créer d'autres en cas de perte de l'une d'entre elles.

Procédure

1. Configurez trois répliques ou plus pour fournir des services de CA.

   a. Pour installer une nouvelle réplique avec les services CA, exécutez **ipa-replica-install** avec l'option **--setup-ca**.

   ```
   [root@server ~]# ipa-replica-install --setup-ca
   ```

   b. Pour installer les services CA sur une réplique préexistante, exécutez **ipa-ca-install**.

   ```
   [root@replica ~]# ipa-ca-install
   ```

2. Créez des accords de réplication CA entre vos répliques CA.

```
[root@careplica1 ~]# ipa topologysegment-add
Suffix name: ca
Left node: ca-replica1.example.com
Right node: ca-replica2.example.com
Segment name [ca-replica1.example.com-to-ca-replica2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
```

```
Left node: ca-replica1.example.com
Right node: ca-replica2.example.com
Connectivity: both
```

AVERTISSEMENT

Si un seul serveur fournit des services CA et qu'il est endommagé, l'environnement entier sera perdu. Si vous utilisez l'AC IdM, Red Hat **strongly recommends** a trois répliques ou plus avec des services d'AC installés, avec des accords de réplication d'AC entre eux.

Ressources supplémentaires

- Planifier les services de l'AC.
- Installation d'une réplique IdM.
- Planification de la topologie de la réplique .

CHAPITRE 4. SE PRÉPARER À LA PERTE DE DONNÉES AVEC LES SNAPSHOTS DE VM

Les instantanés de machines virtuelles (VM) font partie intégrante d'une stratégie de récupération des données, car ils préservent l'état complet d'un serveur IdM :

- Logiciel et paramètres du système d'exploitation
- Logiciel et paramètres IdM
- Données des clients de l'IdM

La préparation d'un instantané de VM d'une réplique d'autorité de certification IdM permet de reconstruire un déploiement IdM complet après un sinistre.

AVERTISSEMENT

Si votre environnement utilise l'autorité de certification intégrée, un instantané d'une réplique *without a CA* ne sera pas suffisant pour reconstruire un déploiement, car les données des certificats ne seront pas préservées.

De même, si votre environnement utilise l'autorité de récupération des clés IdM (KRA), veillez à créer des instantanés d'une réplique KRA, sinon vous risquez de perdre la clé de stockage.

Red Hat recommande de créer des instantanés d'une VM sur laquelle sont installés tous les rôles de serveur IdM utilisés dans votre déploiement : CA, KRA, DNS.

Conditions préalables

- Un hyperviseur capable d'héberger des machines virtuelles RHEL.

Procédure

1. Configurez au moins un site **CA replica** dans le déploiement pour qu'il s'exécute à l'intérieur d'une VM.
   a. Si IdM DNS ou KRA sont utilisés dans votre environnement, envisagez d'installer les services DNS et KRA sur cette réplique également.
   b. En option, configurez cette réplique de VM en tant que réplique cachée.
2. Arrêtez périodiquement cette VM, prenez-en un instantané complet et remettez-la en ligne pour qu'elle continue à recevoir les mises à jour de réplication. Si la VM est un réplica caché, les clients IdM ne seront pas interrompus pendant cette procédure.

Ressources supplémentaires

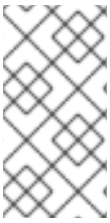
- Quels sont les hyperviseurs certifiés pour exécuter Red Hat Enterprise Linux ?
- Le mode réplique caché.

CHAPITRE 5. SE PRÉPARER À LA PERTE DE DONNÉES AVEC LES SAUVEGARDES IDM

IdM fournit l'utilitaire **ipa-backup** pour sauvegarder les données IdM et l'utilitaire **ipa-restore** pour restaurer les serveurs et les données à partir de ces sauvegardes.

Cette section couvre les sujets suivants :

- Types de sauvegarde IdM
- Conventions d'appellation pour les fichiers de sauvegarde IdM
- Éléments à prendre en compte lors de la création d'une sauvegarde
- Création d'une sauvegarde IdM
- Création d'une sauvegarde de l'IdM chiffrée par GPG2
- Création d'une clé GPG2



NOTE

Red Hat recommande d'exécuter des sauvegardes aussi souvent que nécessaire sur un site *hidden replica* avec tous les rôles de serveur installés, en particulier le rôle d'autorité de certification (CA) si l'environnement utilise l'autorité de certification IdM intégrée. Voir Installation d'une réplique cachée d'IdM.

5.1. TYPES DE SAUVEGARDE IDM

L'utilitaire **ipa-backup** vous permet de créer deux types de sauvegardes :

Sauvegarde complète du serveur

- **Contains** tous les fichiers de configuration du serveur liés à l'IdM et les données LDAP dans les fichiers LDAP Data Interchange Format (LDIF)
- Les services IdM doivent être accessibles à l'adresse **offline**.
- **Suitable for** reconstruire un déploiement IdM à partir de zéro.

Sauvegarde des données uniquement

- **Contains** Données LDAP dans les fichiers LDIF et le journal des modifications de la réplication
- Les services IdM peuvent être **online or offline**.
- **Suitable for** rétablir les données de l'IdM dans un état antérieur

5.2. CONVENTIONS D'APPELLATION POUR LES FICHIERS DE SAUVEGARDE IDM

Par défaut, IdM stocke les sauvegardes sous forme d'archives **.tar** dans des sous-répertoires du répertoire **/var/lib/ipa/backup/**.

Les archives et les sous-répertoires suivent les conventions de dénomination suivantes :

Sauvegarde complète du serveur

Une archive nommée **ipa-full.tar** dans un répertoire nommé **ipa-full-*<YEAR-MM-DD-HH-MM-SS>***avec l'heure spécifiée en heure GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
total 3056
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

Sauvegarde des données uniquement

Une archive nommée **ipa-data.tar** dans un répertoire nommé **ipa-data-*<YEAR-MM-DD-HH-MM-SS>***avec l'heure spécifiée en heure GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```

NOTE

La désinstallation d'un serveur IdM ne supprime pas automatiquement les fichiers de sauvegarde.

5.3. ÉLÉMENTS À PRENDRE EN COMPTE LORS DE LA CRÉATION D'UNE SAUVEGARDE

Cette section décrit les comportements importants et les limites de la commande **ipa-backup**.

- Par défaut, l'utilitaire **ipa-backup** fonctionne en mode déconnecté, ce qui arrête tous les services IdM. L'utilitaire redémarre automatiquement les services IdM une fois la sauvegarde terminée.
- Une sauvegarde complète du serveur doit être exécutée sur **always** avec les services IdM hors ligne, mais une sauvegarde des données uniquement peut être effectuée avec les services en ligne.
- Par défaut, l'utilitaire **ipa-backup** crée des sauvegardes sur le système de fichiers contenant le répertoire **/var/lib/ipa/backup/**. Red Hat recommande de créer régulièrement des sauvegardes sur un système de fichiers distinct du système de fichiers de production utilisé par IdM et d'archiver les sauvegardes sur un support fixe, tel qu'une bande ou un stockage optique.
- Pensez à effectuer des sauvegardes sur des répliques cachées. Les services IdM peuvent être arrêtés sur des répliques cachées sans affecter les clients IdM.
- L'utilitaire **ipa-backup** vérifie si tous les services utilisés dans votre cluster IdM, tels qu'une autorité de certification (CA), un système de noms de domaine (DNS) et un agent de récupération des clés (KRA), sont installés sur le serveur sur lequel vous exécutez la sauvegarde.

Si tous ces services ne sont pas installés sur le serveur, l'utilitaire **ipa-backup** sort avec un avertissement, car les sauvegardes effectuées sur cet hôte ne seraient pas suffisantes pour une restauration complète du cluster.
Par exemple, si votre déploiement IdM utilise une autorité de certification (CA) intégrée, une sauvegarde exécutée sur une réplique non-CA ne capturera pas les données de la CA. Red Hat recommande de vérifier que la réplique sur laquelle vous effectuez une sauvegarde **ipa-backup** dispose de tous les services IdM utilisés dans le cluster.

Vous pouvez contourner la vérification du rôle du serveur IdM à l'aide de la commande **ipa-backup --disable-role-check**, mais la sauvegarde résultante ne contiendra pas toutes les données nécessaires à la restauration complète d'IdM.

5.4. CRÉATION D'UNE SAUVEGARDE IDM

Cette section décrit comment créer une sauvegarde complète du serveur et des données uniquement en mode hors ligne et en ligne à l'aide de la commande **ipa-backup**.

Conditions préalables

- Vous devez disposer des privilèges **root** pour exécuter l'utilitaire **ipa-backup**.

Procédure

- Pour créer une sauvegarde complète du serveur en mode hors ligne, utilisez l'utilitaire **ipa-backup** sans options supplémentaires.

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- Pour créer une sauvegarde hors ligne des données uniquement, spécifiez l'option **--data**.

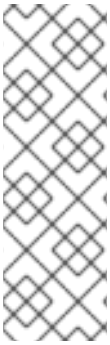
```
[root@server ~]# ipa-backup --data
```

- Pour créer une sauvegarde complète du serveur qui inclut les fichiers journaux IdM, utilisez l'option **--logs**.

```
[root@server ~]# ipa-backup --logs
```

- Pour créer une sauvegarde de données uniquement lorsque les services IdM sont en cours d'exécution, spécifiez les options **--data** et **--online**.

```
[root@server ~]# ipa-backup --data --online
```



NOTE

Si la sauvegarde échoue en raison d'un manque d'espace dans le répertoire **/tmp**, utilisez la variable d'environnement **TMPDIR** pour modifier la destination des fichiers temporaires créés par le processus de sauvegarde :

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

Pour plus de détails, voir La commande ipa-backup ne se termine pas .

Étapes de la vérification

- Le répertoire de sauvegarde contient une archive avec la sauvegarde.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

5.5. CRÉATION D'UNE SAUVEGARDE DE L'IDM CHIFFRÉE PAR GPG2

Vous pouvez créer des sauvegardes cryptées en utilisant le cryptage GNU Privacy Guard (GPG). La procédure suivante crée une sauvegarde IdM et la crypte à l'aide d'une clé GPG2.

Conditions préalables

- Vous avez créé une clé GPG2. Voir Création d'une clé GPG2 .

Procédure

- Créez une sauvegarde chiffrée par GPG en spécifiant l'option **--gpg**.

```
[root@server ~]# ipa-backup --gpg
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

Étapes de la vérification

- Assurez-vous que le répertoire de sauvegarde contient une archive cryptée avec une extension de fichier **.gpg**.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

Ressources supplémentaires

- Création d'une sauvegarde.

5.6. CRÉATION D'UNE CLÉ GPG2

La procédure suivante décrit comment générer une clé GPG2 à utiliser avec les utilitaires de cryptage.

Conditions préalables

- Vous avez besoin des privilèges de **root**.

Procédure

1. Installer et configurer l'utilitaire **pinentry**.

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. Créez un fichier **key-input** utilisé pour générer une paire de clés GPG avec les détails de votre choix. Par exemple :

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. *(Optional)* Par défaut, GPG2 stocke son trousseau de clés dans le fichier **~/.gnupg**. Pour utiliser un emplacement de trousseau personnalisé, définissez la variable d'environnement **GNUPGHOME** dans un répertoire accessible uniquement par root.

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. Générer une nouvelle clé GPG2 basée sur le contenu du fichier **key-input**.

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. Saisissez une phrase de passe pour protéger la clé GPG2. Cette phrase d'authentification permet d'accéder à la clé privée pour le décryptage.

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
```

```
│                                                                │
│ <OK>                    <Cancel>                               │
└────────────────────────────────────────────────────────────────┘
```

6. Confirmez la phrase d'authentification correcte en la saisissant à nouveau.

```
┌────────────────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                                │
│                                                                │
│ Passphrase: <passphrase>                                       │
│                                                                │
│ <OK>                    <Cancel>                               │
└────────────────────────────────────────────────────────────────┘
```

7. Vérifiez que la nouvelle clé GPG2 a été créée avec succès.

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

Étapes de la vérification

- Liste des clés GPG sur le serveur.

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

Ressources supplémentaires

- GNU Privacy Guard

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

En utilisant le rôle Ansible **ipabackup**, vous pouvez automatiser la sauvegarde d'un serveur IdM et le transfert des 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 créer une sauvegarde d'un serveur IdM
- Utiliser Ansible pour créer une sauvegarde d'un serveur IdM 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 CRÉER UNE SAUVEGARDE D'UN SERVEUR IDM

La procédure suivante décrit comment utiliser le rôle ipabackup dans un playbook Ansible pour créer une sauvegarde d'un serveur IdM et la stocker sur 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 **backup-server.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

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

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

4. Adaptez le fichier en fixant la variable **hosts** à un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**:

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

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

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
backup-my-server.yml
```

Verification steps

1. Connectez-vous au serveur IdM que vous avez sauvegardé.

2. Vérifiez que la sauvegarde se trouve dans le répertoire **/var/lib/ipa/backup**.

```
[root@server ~]# ls /var/lib/ipa/backup/
ipa-full-2021-04-30-13-12-00
```

Ressources supplémentaires

- Pour plus d'exemples de playbooks Ansible qui utilisent le rôle **ipabackup**, voir :
  - 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 CRÉER UNE SAUVEGARDE D'UN SERVEUR IDM SUR VOTRE CONTRÔLEUR ANSIBLE

La procédure suivante décrit comment utiliser le rôle **ipabackup** dans un playbook Ansible pour créer une sauvegarde d'un serveur IdM et la transférer automatiquement sur votre contrôleur Ansible. Le nom de votre fichier de sauvegarde commence par le nom d'hôte du 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. 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 **backup-server-to-controller.yml** situé dans le répertoire **/usr/share/doc/ansible-freeipa/playbooks**:

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

4. Ouvrez le fichier **backup-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. *(Optional)* Pour conserver une copie de la sauvegarde sur le serveur IdM, décommentez la ligne suivante :

```
# ipabackup_keep_on_server: yes
```

6. Par défaut, les sauvegardes sont stockées dans le répertoire de travail actuel du contrôleur Ansible. Pour spécifier le répertoire de sauvegarde 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 backup IPA server to controller
  hosts: ipaserver
```

```
  become: true
  vars:
    ipabackup_to_controller: yes
    # ipabackup_keep_on_server: yes
    ipabackup_controller_path: /home/user/ipabackups

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

7. Enregistrer le fichier.
8. 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
backup-my-server-to-my-controller.yml
```

Verification steps

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

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

Ressources supplémentaires

- Pour plus d'exemples de playbooks Ansible qui utilisent le rôle **ipabackup**, voir :
  - 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
```

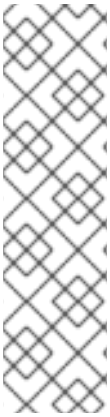
4. Ouvrez le fichier **copy-my-backup-from-my-server-to-my-controller.yml** pour le modifier.
5. Adaptez le fichier en définissant les variables suivantes :
   a. Définissez la variable **hosts** sur un groupe d'hôtes de votre fichier d'inventaire. Dans cet exemple, il s'agit du groupe d'hôtes **ipaserver**.
   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.

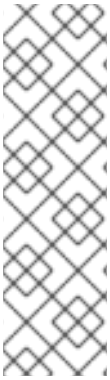
```
---
```

```
- 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/**.