# Red Hat Enterprise Linux 9

## Identity Management を使用した障害復旧への準備

IdM 環境におけるサーバーおよびデータ損失シナリオの影響を軽減する

Last Updated: 2024-08-06

# Red Hat Enterprise Linux 9 Identity Management を使用した障害復旧への準備

IdM 環境におけるサーバーおよびデータ損失シナリオの影響を軽減する

## 法律上の通知



## 概要

ハードウェア障害などによるサーバーとデータの損失シナリオは、IT 環境において最も高いリスクです。Red Hat Identity Management (IdM) トポロジーで、他のサーバーとのレプリケーションを設定し、仮想マシン (VM) スナップショットと IdM バックアップを使用することで、このような状況の影響を軽減できます。

# 目次

# RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

**Jira からのフィードバック送信 (アカウントが必要)**

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. ダイアログの下部にある **Create** をクリックします。

# 第1章 IDM における障害復旧ツール

適切な障害復旧計画は、次のツールを組み合わせて、可能な限り早く障害から復旧し、データ損失を最小限に抑えます。

**レプリケーション**

レプリケーションは、IdM サーバー間でデータベースのコンテンツをコピーします。IdM サーバーに障害が発生した場合は、障害が発生していないサーバーの 1 台から新しいレプリカを作成し、失われたサーバーを回復することもできます。

**仮想マシン (VM) のスナップショット**

スナップショットは、特定の時点で利用可能なすべてのディスクにある仮想マシンのオペレーティングシステムおよびアプリケーションのビューです。仮想マシンのスナップショットを取得したら、それを使用して仮想マシンとその IdM データを以前の状態に戻すことができます。

**IdM のバックアップ**

**ipa-backup** ユーティリティーを使用すると、IdM サーバーの設定ファイルとそのデータのバックアップを作成できます。後でバックアップを使用して、IdM サーバーを以前の状態に復元できます。

# 第2章 IDM の障害シナリオ

障害シナリオには、主に **サーバー損失** と **データ損失** の 2 種類があります。

**表2.1 サーバー損失とデータ損失の比較**

| 障害タイプ | 考えられる原因 | 準備方法 |
| --- | --- | --- |
| **サーバー損失** - IdM デプロイメントからサーバーが 1 台以上なくなる。 | • ハードウェアの誤作動 | • レプリケーションによるサーバーの損失への準備 |
| **データ損失** - サーバーで IdM データが突然修正され、変更が他のサーバーに伝播している。 | • ユーザーの過失によるデータの削除<br>• ソフトウェアバグによるデータの変更 | • 仮想マシンのスナップショットによるデータ損失への準備<br>• IdM バックアップによるデータ損失への準備 |

# 第3章 レプリケーションによるサーバーの損失への準備

次のガイドラインに従って、サーバー損失に対応できるレプリケーショントポロジーを確立します。

このセクションでは次のトピックについて説明します。

- トポロジー内でレプリカの接続
- レプリカトポロジーの例
- IdM CA データの保護

## 3.1. トポロジーで IDM レプリカを接続するためのガイドライン

**1台のレプリカを少なくとも 2 つのレプリカに接続**

追加のレプリカ合意を設定すると、初期レプリカと最初にインストールしたサーバーとの間だけでなく、他のレプリカ間でも情報が複製されます。

**レプリカを、その他のレプリカ (最大 4 つ) に接続 (必須要件ではありません)**

サーバーごとに多数のレプリカ合意を設定しても、大きな利点はありません。受信側のレプリカは、一度に 1 つの他のレプリカによってのみ更新できます。その間、その他のレプリカ合意はアイドル状態になります。通常、レプリカごとに 4 つ以上のレプリカ合意があると、リソースが無駄になります。

**注記**

この推奨事項は、証明書のレプリケーションとドメインのレプリケーションの両方に適用されます。

レプリカごとに 4 つのレプリカ合意という制限は、次の 2 つの場合には、例外として適用されません。

- 特定のレプリカがオンラインでない場合や応答していない場合にフェイルオーバーパスが必要な場合
- 大規模デプロイメントで、特定のノード間に追加の直接リンクが必要な場合

レプリカ合意を多数設定すると、全体のパフォーマンスに悪影響が及ぶ可能性があります。トポロジー内の複数のレプリカ合意が更新を送信すると、特定のレプリカの changelog データベースファイル上で、受信する更新と送信する更新の間の競合が増大することがあります。

レプリカごとにさらに多くのレプリケーションアグリーメントを使用する場合は、レプリケーションの問題やレイテンシーが発生しないようにしてください。距離が長く、中間ノードの数が多いと、レイテンシーの問題が発生する場合があることに注意してください。

**データセンター内のレプリカを互いに接続**

これにより、データセンター内のドメインレプリケーションが確実になります。

**各データセンターを少なくとも 2 つの他のデータセンターに接続**

これにより、データセンター間のドメインレプリケーションが確実になります。

**少なくとも一対のレプリカ合意を使用してデータセンターを接続**

データセンター A および B に、A1 への B1 までのレプリカ合意がある場合は、A2 から B2 へのレプリカ合意があれば、いずれかのサーバーがダウンしても、2 つのデータセンター間でレプリケーションを続行できます。

## 3.2. レプリカトポロジーの例

次のいずれかの例を使用して、信頼性の高いレプリカトポロジーを作成できます。

**図3.1 4 つのデータセンターで構成されるレプリカトポロジー。各データセンターに、レプリカ合意で接続された 4 台のサーバーがある**

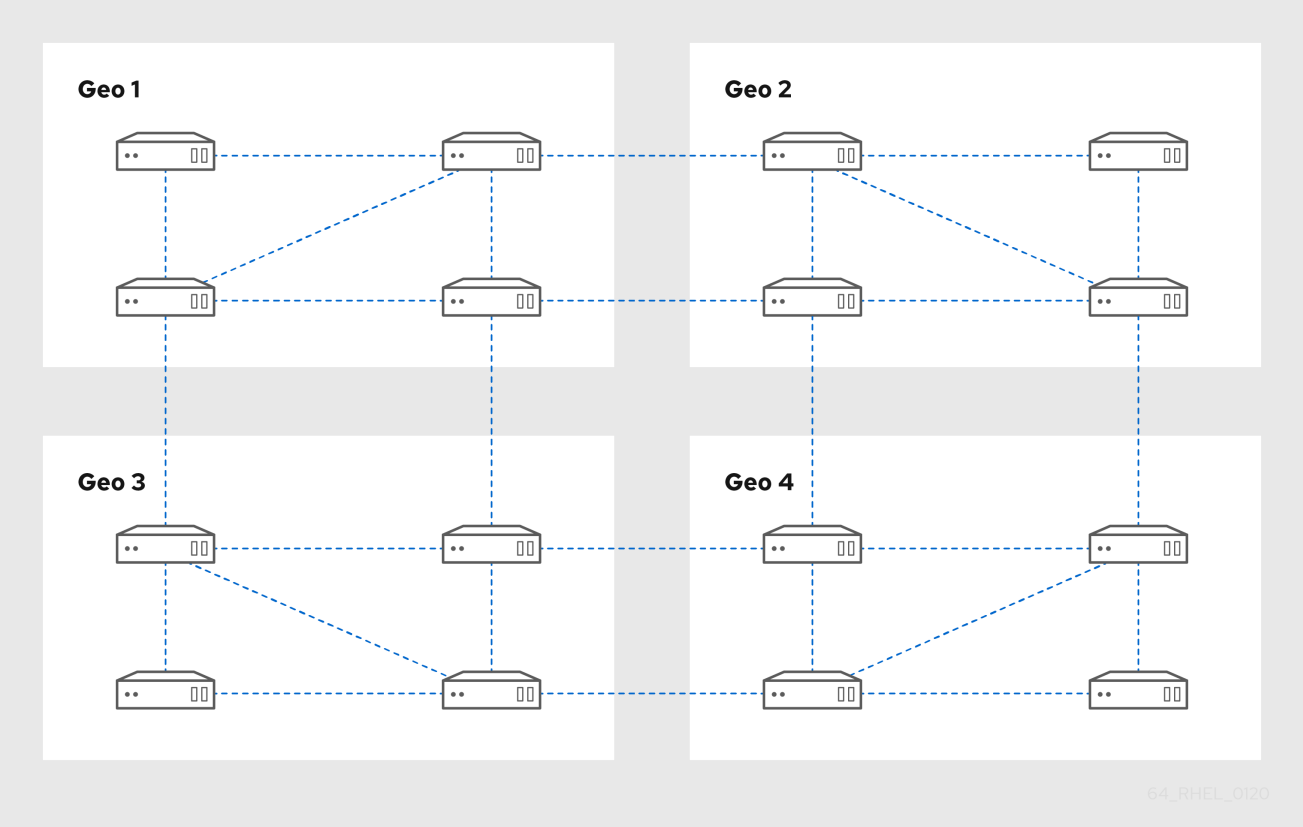
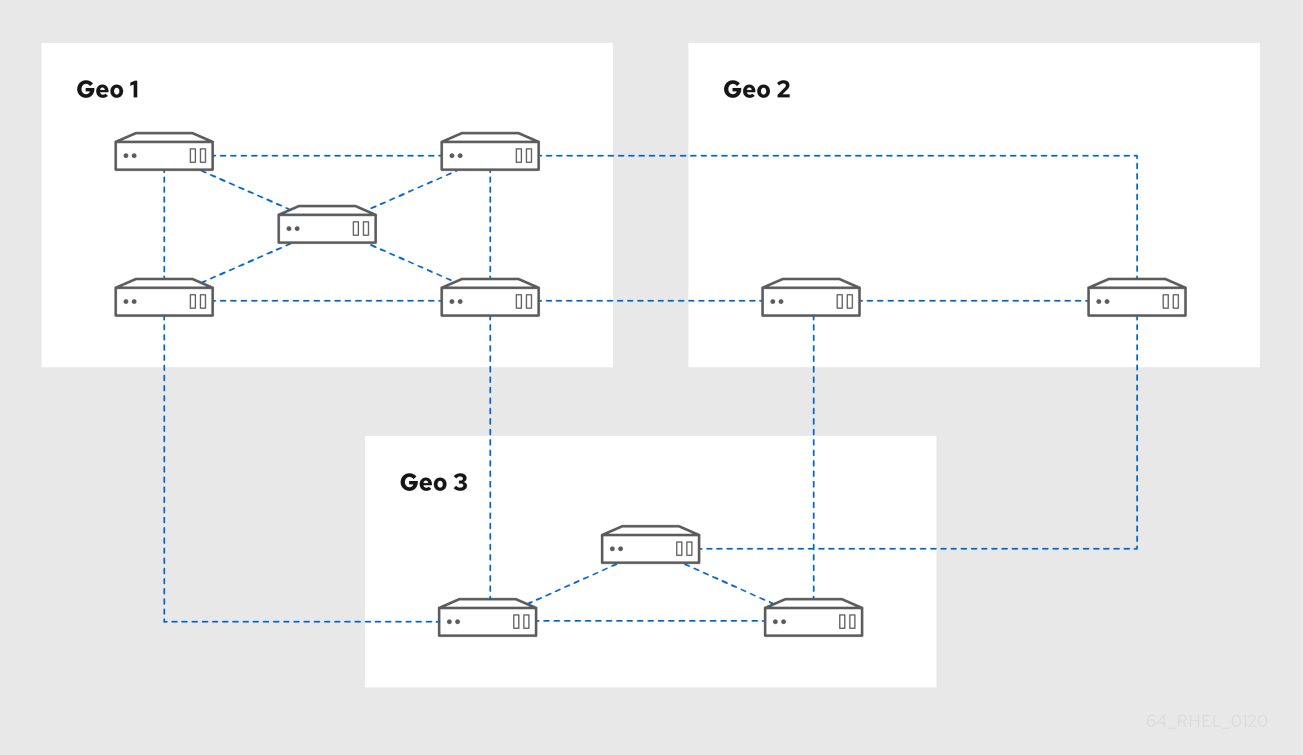


**図3.2 3 つのデータセンターで構成されるレプリカトポロジー。各データセンターに異なる数のサーバーがあり、それらがすべてレプリカ合意を通じて相互接続されている**




## 3.3. IDM CA データの保護

デプロイメントに統合 IdM 認証局 (CA) が含まれている場合は、CA レプリカをいくつかインストールして、CA レプリカが失われた場合に追加の CA レプリカを作成できるようにします。

**手順**

1. CA サービスを提供するように 3 つ以上のレプリカを設定します。
   a. CA サービスを備えた新しいレプリカをインストールするには、**--setup-ca** オプションを指定して **ipa-replica-install** を実行します。

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

   b. 既存のレプリカに CA サービスをインストールするには、**ipa-ca-install** を実行します。

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

2. CA レプリカ間で CA レプリカ合意を作成します。

```
[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
```

**警告**

CA サービスを提供するサーバーが 1 つしかない場合、それが壊れると、環境全体が失われます。IdM CA を使用する場合、CA サービスがインストールされたレプリカを 3 つ以上用意し、それらの間で CA レプリカ合意を設定ことを **強く推奨** します。

**関連情報**

- CA サービスの計画
- IdM レプリカのインストール
- レプリカトポロジーの計画

# 第4章 仮想マシンのスナップショットによるデータ損失への準備

仮想マシン (VM) スナップショットは、IdM サーバーの完全な状態を保存するものであるため、データ復旧計画に不可欠な要素です。

- オペレーティングシステムのソフトウェアおよび設定
- IdM ソフトウェアおよび設定
- IdM のカスタマーデータ

IdM 認証局 (CA) レプリカの仮想マシンスナップショットを準備しておくことで、障害後に IdM デプロイメント全体を再構築できます。

**警告**

統合 CA を使用する環境では、証明書データは保持されないため、**CA のない** レプリカのスナップショットは、デプロイメントを再構築するには不十分です。

同様に、環境が IdM Key Recovery Authority (KRA) を使用する場合は、KRA レプリカのスナップショットを作成するようにしてください。そうでないと、ストレージキーが失われる可能性があります。

Red Hat は、デプロイメントで使用されている IdM サーバーロール (CA、KRA、DNS) がすべてインストールされている仮想マシンのスナップショットを作成することを推奨します。

**前提条件**

- RHEL 仮想マシンをホストできるハイパーバイザー。

**手順**

1. デプロイメントの **CA レプリカ** を、仮想マシン内で実行するように設定します。
   a. IdM DNS または KRA が環境で使用されている場合は、このレプリカにも DNS サービスおよび KRA サービスをインストールすることを検討してください。
   b. 必要に応じて、仮想マシンレプリカを 非表示のレプリカ として設定します。
2. この仮想マシンを定期的にシャットダウンして、完全なスナップショットを取得し、オンラインに戻して、レプリケーションの更新の受信を続けます。仮想マシンが非表示のレプリカの場合は、この手順中に IdM クライアントが中断することはありません。

**関連情報**

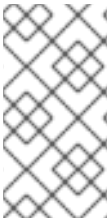
- Red Hat Enterprise Linux の実行が認定されているハイパーバイザーはどれですか?
- 非表示のレプリカモード

# 第5章 IDM バックアップによるデータ損失への準備

IdM は、IdM データをバックアップする **ipa-backup** ユーティリティーと、そのバックアップからサーバーおよびデータを復元する **ipa-restore** ユーティリティーを提供します。

このセクションでは次のトピックについて説明します。

- IdM バックアップの種類
- IdM バックアップファイルの命名規則
- バックアップの作成時の考慮事項
- IdM バックアップの作成
- GPG2 で暗号化した IdM バックアップの作成
- GPG2 キーの作成



**注記**

Red Hat は、すべてのサーバーロール (特に、環境が統合 IdM CA を使用する場合は認証局 (CA) ロール) がインストールされた **非表示のレプリカ** でバックアップを必要な頻度で実行することを推奨します。IdM 非表示レプリカのインストール を参照してください。

## 5.1. IDM バックアップの種類

**ipa-backup** ユーティリティーを使用すると、2 種類のバックアップを作成できます。

**サーバーのフルバックアップ**

- IdM に関連するすべてのサーバー設定ファイルと、LDAP データ交換形式 (LDIF) ファイルにある LDAP データがすべて **含まれます**。
- IdM サービスは **オフライン** である必要があります。
- IdM デプロイメントをゼロから再構築する場合に **適しています**。

**データのみのバックアップ**

- LDIF ファイルの LDAP データとレプリケーション変更ログが **含まれます**。
- IdM サービスは、**オンラインまたはオフライン** にできます。
- IdM データを以前の状態に復元する場合に **適しています**。

## 5.2. IDM バックアップファイルの命名規則

デフォルトでは、IdM はバックアップを **.tar** アーカイブとして **/var/lib/ipa/backup/** ディレクトリーのサブディレクトリーに保存します。

アーカイブおよびサブディレクトリーは、以下の命名規則に従います。

**サーバーのフルバックアップ**

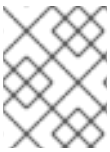
**ipa-full-<YEAR-MM-DD-HH-MM-SS>** という名前のディレクトリーにある **ipa-full.tar** という名称のアーカイブ。時間は GMT 時間で指定されます。

```
[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
```

**データのみのバックアップ**

**ipa-data-<YEAR-MM-DD-HH-MM-SS>** という名前のディレクトリーにある **ipa-data.tar** という名称のアーカイブ。時間は GMT 時間で指定されます。

```
[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
```



**注記**

IdM サーバーをアンインストールしても、バックアップファイルは自動的に削除されません。

## 5.3. バックアップの作成時の考慮事項

**ipa-backup** コマンドの重要な動作と制限事項は次のとおりです。

- デフォルトでは、**ipa-backup** ユーティリティーはオフラインモードで実行されるため、IdM サービスがすべて停止します。このユーティリティーは、バックアップ完了後に IdM サービスを自動的に再起動します。
- サーバーのフルバックアップは、**常に** IdM サービスがオフラインの状態で実行する必要がありますが、データのみのバックアップは、サービスがオンラインの状態でも実行できます。
- デフォルトでは、**ipa-backup** ユーティリティーは、**/var/lib/ipa/backup/** ディレクトリーを含むファイルシステムにバックアップを作成します。Red Hat は、IdM が使用する実稼働ファイルシステムとは別のファイルシステムでバックアップを定期的に作成し、バックアップを固定メディア (例: テープまたは光学ストレージ) にアーカイブすることを推奨します。
- 非表示のレプリカ でのバックアップの実行を検討してください。IdM サービスは、非表示のレプリカでは、IdM クライアントに影響を及ぼさずにシャットダウンできます。
- **ipa-backup** ユーティリティーは、認証局 (CA)、ドメインネームシステム (DNS)、およびキー回復エージェント (KRA) など、IdM クラスターで使用されるすべてのサービスが、バックアップを実行中のサーバーにインストールされているかどうかを確認します。サーバーにこれらのサービスがすべてインストールされていない場合、そのホスト上で取得したバックアップではクラスターを完全に復元するには不十分なため、**ipa-backup** ユーティリティーは警告を表示して終了します。
  たとえば、IdM デプロイメントで統合認証局 (CA) を使用している場合、CA のないレプリカでバックアップを実行しても、CA データは取得されません。Red Hat は、**ipa-backup** を実行するレプリカに、クラスターで使用される IdM サービスがすべてインストールされていることを確認することを推奨します。

**ipa-backup --disable-role-check** コマンドを使用すると、IdM サーバーのロールチェックを省略できます。ただし、生成されるバックアップに、IdM を完全に復元するのに必要な全データが保存されなくなります。

## 5.4. IDM バックアップの作成

**ipa-backup** コマンドを使用して、オフラインモードとオンラインモードで、完全なサーバーバックアップとデータのみのバックアップを作成します。

**前提条件**

- **ipa-backup** ユーティリティーを実行するには、**root** 権限が必要です。

**手順**

- オフラインモードでサーバーのフルバックアップを作成するには、追加オプションを指定せずに **ipa-backup** ユーティリティーを使用します。

```
[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
```

- オフラインでデータのみのバックアップを作成するには、**--data** オプションを指定します。

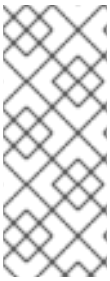
```
[root@server ~]# ipa-backup --data
```

- IdM ログファイルを含むサーバーのフルバックアップを作成するには、**--logs** オプションを使用します。

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

- IdM サービスの実行中にデータのみのバックアップを作成するには、**--data** オプションおよび **--online** オプションの両方を指定します。

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



**注記**

**/tmp** ディレクトリーに十分なスペースがないためにバックアップが失敗する場合は、**TMPDIR** 環境変数を使用して、バックアッププロセスで作成された一時ファイルの保存先を変更します。

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

**検証**

- バックアップディレクトリーにバックアップを含むアーカイブが含まれていることを確認します。

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

**関連情報**

- ipa-backup コマンドの終了に失敗する

## 5.5. GPG2 で暗号化した IDM バックアップの作成

GPG (GNU Privacy Guard) 暗号化を使用して、暗号化バックアップを作成できます。以下の手順では、IdM バックアップを作成し、GPG2 キーを使用して暗号化します。

**前提条件**

- GPG2 キーを作成している。GPG2 キーの作成 を参照してください。

**手順**

- **--gpg** オプションを指定して、GPG で暗号化したバックアップを作成します。

```
[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
```

**検証**

- バックアップディレクトリーに、ファイル拡張子が **.gpg** の暗号化されたアーカイブが含まれていることを確認します。

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

**関連情報**

- IdM バックアップの作成

## 5.6. GPG2 キーの作成

以下の手順では、暗号化ユーティリティーで使用する GPG2 キーを生成する方法を説明します。

**前提条件**

- **root** 権限がある。

**手順**

1. **pinentry** ユーティリティーをインストールして設定します。

```
[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. 希望する内容で、GPG キーペアの生成に使用する **key-input** ファイルを作成します。以下に例を示します。

```
[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. **(オプション)** デフォルトでは、GPG2 はキーリングを **~/.gnupg** ファイルに保存します。カスタムのキーリングの場所を使用するには、**GNUPGHOME** 環境変数を、root のみがアクセスできるディレクトリーに設定します。

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

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

4. **key-input** ファイルの内容に基づいて、新しい GPG2 キーを生成します。

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

5. GPG2 キーを保護するパスフレーズを入力します。このパスフレーズは、秘密鍵へのアクセスと復号に使用します。

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

6. パスフレーズを再度入力して、正しいパスフレーズを確認します。

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
```

```
|                                                 |
| Passphrase: <passphrase>                        |
|                                                 |
|  <OK>                    <Cancel>               |
└─────────────────────────────────────────────────┘
```

7. 新しい GPG2 キーが正常に作成されたことを確認します。

```
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
```

**検証**

- サーバーの GPG キーのリストを表示します。

```
[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>
```

**関連情報**

- GNU Privacy Guard

# 第6章 ANSIBLE PLAYBOOK を使用した IDM サーバーのバックアップ

**ipabackup** Ansible ロールを使用すると、IdM サーバーのバックアップを自動化し、サーバーと Ansible コントローラー間でバックアップファイルを転送できます。

このセクションでは次のトピックについて説明します。

- IdM 管理用の Ansible コントロールノードの準備
- Ansible を使用した IdM サーバーのバックアップの作成
- Ansible を使用した Ansible コントローラーへの IdM サーバーのバックアップの作成
- Ansible を使用した IdM サーバーのバックアップの Ansible コントローラーへのコピー
- Ansible を使用した IdM サーバーのバックアップの Ansible コントローラーから IdM サーバーへのコピー
- Ansible を使用した IdM サーバーからのバックアップの削除

## 6.1. IDM 管理用の ANSIBLE コントロールノードの準備

Identity Management (IdM) を管理するシステム管理者は、Red Hat Ansible Engine を使用する際に以下を行うことが推奨されます。

- ホームディレクトリーに Ansible Playbook 専用のサブディレクトリー (例: **~/MyPlaybooks**) を作成します。
- **/usr/share/doc/ansible-freeipa/*** と **/usr/share/doc/rhel-system-roles/*** ディレクトリーおよびサブディレクトリーから **~/MyPlaybooks** ディレクトリーにサンプル Ansible Playbook をコピーして調整します。
- **~/MyPlaybooks** ディレクトリーにインベントリーファイルを追加します。

この方法に従うことで、すべての Playbook を 1 カ所で見つけることができます。また、root 権限を呼び出さなくても Playbook を実行できます。

**注記**

**ipaserver**、**ipareplica**、**ipaclient**、**ipabackup**、**ipasmartcard_server**、および **ipasmartcard_client ansible-freeipa** のロールを実行するために必要なのは、管理対象ノードでの **root** 権限のみです。これらのロールには、ディレクトリーおよび **dnf** ソフトウェアパッケージマネージャーへの特権アクセスが必要です。

**~/MyPlaybooks** ディレクトリーを作成し、それを使用して Ansible Playbook を保存および実行できるように設定するには、次の手順に従います。

**前提条件**

- 管理対象ノードに IdM サーバー (**server.idm.example.com** および **replica.idm.example.com**) をインストールしている。

- DNS およびネットワークを設定し、コントロールノードから直接管理対象ノード (**server.idm.example.com** および **replica.idm.example.com**) にログインすることができる。
- IdM **admin** のパスワードを把握している。

**手順**

1. Ansible 設定および Playbook のディレクトリーをホームディレクトリーに作成します。

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

2. **~/MyPlaybooks/** ディレクトリーに移動します。

```
$ cd ~/MyPlaybooks
```

3. **~/MyPlaybooks/ansible.cfg** ファイルを以下の内容で作成します。

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

[privilege_escalation]
become=True
```

4. **~/MyPlaybooks/inventory** ファイルを以下の内容で作成します。

```
[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
```

この設定は、これらの場所にあるホストの 2 つのホストグループ (**eu** と **us**) を定義します。さらに、この設定は、**eu** および **us** グループのすべてのホストを含む **ipaserver** ホストグループを定義します。

5. [オプション] SSH 公開鍵および秘密鍵を作成します。テスト環境でのアクセスを簡素化するには、秘密鍵にパスワードを設定しないでください。

```
$ ssh-keygen
```

6. 各マネージドノードの IdM **admin** アカウントに SSH 公開鍵をコピーします。

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

これらのコマンドを入力する場合は、IdM **admin** パスワードを入力する必要があります。

**関連情報**

- Ansible Playbook で Identity Management サーバーのインストール
- How to build your inventory

## 6.2. ANSIBLE を使用した IDM サーバーのバックアップの作成

Ansible Playbook の **ipabackup** ロールを使用して、IdM サーバーのバックアップを作成し、それを IdM サーバーに保存できます。

**前提条件**

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - **~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成している (この例の場合)。
  - この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。
- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

**手順**

1. **~/MyPlaybooks/** ディレクトリーに移動します。

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

2. **/usr/share/doc/ansible-freeipa/playbooks** ディレクトリーにある **backup-server.yml** ファイルのコピーを作成します。

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

3. **backup-my-server.yml** Ansible Playbook ファイルを開いて編集します。
4. **hosts** 変数をインベントリーファイルのホストグループに設定して、ファイルを調整します。この例では、**ipaserver** ホストグループに設定します。

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

```
become: true

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

5. ファイルを保存します。
6. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

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

**検証**

1. バックアップした IdM サーバーにログインします。
2. バックアップが **/var/lib/ipa/backup** ディレクトリーにあることを確認します。

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

**関連情報**

- **ipabackup** ロールを使用する他の Ansible Playbook の例は、以下を参照してください。
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** ディレクトリーの **README.md** ファイル
  - **/usr/share/doc/ansible-freeipa/playbooks/** ディレクトリー

## 6.3. ANSIBLE を使用した ANSIBLE コントローラーへの IDM サーバーのバックアップの作成

Ansible Playbook の **ipabackup** ロールを使用して、IdM サーバーのバックアップを作成し、それを Ansible コントローラーに自動的に転送できます。バックアップファイル名は、IdM サーバーのホスト名で始まります。

**前提条件**

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - **~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成している (この例の場合)。
  - この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。
- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

**手順**

1. バックアップを保存するために、Ansible コントローラーのホームディレクトリーにサブディレクトリーを作成します。

```
$ mkdir ~/ipabackups
```

2. ~/**MyPlaybooks**/ ディレクトリーに移動します。

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

3. /**usr**/**share**/**doc**/**ansible-freeipa**/**playbooks** ディレクトリーにある **backup-server-to-controller.yml** ファイルのコピーを作成します。

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

4. **backup-my-server-to-my-controller.yml** ファイルを開いて編集します。

5. 以下の変数を設定してファイルを調整します。

   a. **hosts** 変数を、インベントリーファイルのホストグループに設定します。この例では、**ipaserver** ホストグループに設定します。

   b. **(オプション)** IdM サーバー上にバックアップのコピーを保持するには、次の行のコメントを解除します。

```
# ipabackup_keep_on_server: true
```

6. デフォルトでは、バックアップは Ansible コントローラーの現在の作業ディレクトリーに保存されます。ステップ 1 で作成したバックアップディレクトリーを指定するには、**ipabackup_controller_path** 変数を追加し、それを /**home**/**user**/**ipabackups** ディレクトリーに設定します。

```
---
- name: Playbook to backup IPA server to controller
  hosts: ipaserver
  become: true
  vars:
    ipabackup_to_controller: true
    # ipabackup_keep_on_server: true
    ipabackup_controller_path: /home/user/ipabackups

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

7. ファイルを保存します。

8. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

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

**検証**

- バックアップが Ansible コントローラーの **/home/user/ipabackups** ディレクトリーにあることを確認します。

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

**関連情報**

- **ipabackup** ロールを使用する他の Ansible Playbook の例は、以下を参照してください。
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** ディレクトリーの **README.md** ファイル
  - **/usr/share/doc/ansible-freeipa/playbooks/** ディレクトリー

## 6.4. ANSIBLE を使用した IDM サーバーのバックアップの ANSIBLE コントローラーへのコピー

Ansible Playbook を使用して、IdM サーバーのバックアップを IdM サーバーから Ansible コントローラーにコピーできます。

**前提条件**

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - **~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成している (この例の場合)。
  - この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。
- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

**手順**

1. バックアップを保存するために、Ansible コントローラーのホームディレクトリーにサブディレクトリーを作成します。

```
$ mkdir ~/ipabackups
```

2. **~/MyPlaybooks/** ディレクトリーに移動します。

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

3. **/usr/share/doc/ansible-freeipa/playbooks** ディレクトリーにある **copy-backup-from-server.yml** ファイルのコピーを作成します。

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

4. **copy-my-backup-from-my-server-to-my-controller.yml** ファイルを開いて編集します。
5. 以下の変数を設定してファイルを調整します。
   a. **hosts** 変数を、インベントリーファイルのホストグループに設定します。この例では、**ipaserver** ホストグループに設定します。
   b. **ipabackup_name** 変数を、Ansible コントローラーにコピーする IdM サーバー上の **ipabackup** の名前に設定します。
   c. デフォルトでは、バックアップは Ansible コントローラーの現在の作業ディレクトリーに保存されます。ステップ 1 で作成したディレクトリーを指定するには、**ipabackup_controller_path** 変数を追加し、それを **/home/user/ipabackups** ディレクトリーに設定します。

```
---
- 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: true
    ipabackup_controller_path: /home/user/ipabackups

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

6. ファイルを保存します。
7. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

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

**注記**

**すべて** の IdM バックアップをコントローラーにコピーするには、Ansible Playbook の **ipabackup_name** 変数を **all** に設定します。

```
vars:
  ipabackup_name: all
  ipabackup_to_controller: true
```

たとえば、**/usr/share/doc/ansible-freeipa/playbooks** ディレクトリーの Ansible Playbook **copy-all-backups-from-server.yml** を参照してください。

**検証**

- バックアップが Ansible コントローラーの **/home/user/ipabackups** ディレクトリーにあることを確認します。

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

**関連情報**

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** ディレクトリーの **README.md** ファイル
- **/usr/share/doc/ansible-freeipa/playbooks/** ディレクトリー

## 6.5. ANSIBLE を使用した IDM サーバーのバックアップの ANSIBLE コントローラーから IDM サーバーへのコピー

Ansible Playbook を使用して、IdM サーバーのバックアップを Ansible コントローラーから IdM サーバーにコピーできます。

**前提条件**

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - **~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成している (この例の場合)。
  - この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。
- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

**手順**

1. **~/MyPlaybooks/** ディレクトリーに移動します。

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

2. **/usr/share/doc/ansible-freeipa/playbooks** ディレクトリーにある **copy-backup-from-controller.yml** のコピーを作成します。

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

3. **copy-my-backup-from-my-controller-to-my-server.yml** ファイルを開いて編集します。
4. 以下の変数を設定してファイルを調整します。
   a. **hosts** 変数を、インベントリーファイルのホストグループに設定します。この例では、**ipaserver** ホストグループに設定します。
   b. **ipabackup_name** 変数を、IdM サーバーにコピーする Ansible コントローラー上の **ipabackup** の名前に設定します。

```
---
- 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: true

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

5. ファイルを保存します。

6. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

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

**関連情報**

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** ディレクトリーの **README.md** ファイル
- **/usr/share/doc/ansible-freeipa/playbooks/** ディレクトリー

## 6.6. ANSIBLE を使用した IDM サーバーからのバックアップの削除

Ansible Playbook を使用して、IdM サーバーからバックアップを削除できます。

**前提条件**

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - **~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成している (この例の場合)。
  - この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。
- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

**手順**

1. ~/MyPlaybooks/ ディレクトリーに移動します。

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

2. **/usr/share/doc/ansible-freeipa/playbooks** ディレクトリーにある **remove-backup-from-server.yml** ファイルのコピーを作成します。

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

3. **remove-backup-from-my-server.yml** ファイルを開いて編集します。

4. 以下の変数を設定してファイルを調整します。

   a. **hosts** 変数を、インベントリーファイルのホストグループに設定します。この例では、**ipaserver** ホストグループに設定します。

   b. **ipabackup_name** 変数を、IdM サーバーから削除する **ipabackup** の名前に設定します。

```
---
- 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. ファイルを保存します。

6. Playbook ファイルとインベントリーファイルを指定して Ansible Playbook を実行します。

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

**注記**

IdM サーバーから **すべて** の IdM バックアップを削除するには、Ansible Playbook の **ipabackup_name** 変数を **all** に設定します。

```
  vars:
    ipabackup_name: all
```

たとえば、**/usr/share/doc/ansible-freeipa/playbooks** ディレクトリーの Ansible Playbook **remove-all-backups-from-server.yml** を参照してください。

**関連情報**

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** ディレクトリーの **README.md** ファイル
- **/usr/share/doc/ansible-freeipa/playbooks/** ディレクトリー