Red Hat Enterprise Linux 9

Identity Management を使用した障害復旧の準備

Identity Management デプロイメントに影響する障害を軽減するためのドキュメント

Last Updated: 2022-07-28

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

Identity Management デプロイメントに影響する障害を軽減するためのドキュメント

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本書では、IdM デプロイメントで脅威となる一般的な障害シナリオと、レプリケーション、仮想マシンスナップショット、およびバックアップを使用してこのような状況を軽減する方法を説明します。

目次

オープンソースをより包摂的に

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社 の CTO、Chris Wright のメッセージ を参照してください。

Identity Management では、以下のような用語の置き換えが含まれます。

- **ブラックリスト**から**ブロックリスト**
- **ホワイトリスト**から**許可リスト**
- **スレーブ**から**セカンダリー**
- 単語 **マスター** は、コンテキストに応じて、より正確な言語に置き換えられます。
  - **マスター**から**IdM サーバー**
  - **CA 更新マスター**から**CA 更新サーバー**
  - **CRL マスター**から**CRL パブリッシャーサーバー**
  - **マルチマスター**から**マルチサプライヤー**

RED HAT ドキュメントへのフィードバック (英語のみ)

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。

- 特定の部分についての簡単なコメントをお寄せいただく場合は、以下をご確認ください。
  1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上隅に **Feedback** ボタンがあることを確認してください。
  2. マウスカーソルで、コメントを追加する部分を強調表示します。
  3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
  4. 表示される手順に従ってください。
- Bugzilla を介してフィードバックを送信するには、新しいチケットを作成します。
  1. Bugzilla の Web サイトに移動します。
  2. Component で **Documentation** を選択します。
  3. **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記入してください。
  4. **Submit Bug** をクリックします。

第1章 IDM における障害復旧ツール

適切な障害復旧手順は、データ損失を最小限に抑えてできるだけ早期に障害からの復旧を可能にするために、以下のツールを組み合わせたものです。

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 サーバーが失敗した場合は、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 **サーバーの損失** および **データ損失** と 2 種類があります。

表2.1 サーバー損失対データ損失

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。	• ユーザーが誤ってデータの削除 • 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の準備 • IdM バックアップによるデータ損失の準備

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

以下のガイドラインに従って、サーバーの失われた応答を可能にするレプリカトポロジーを確立します。

本セクションでは、以下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

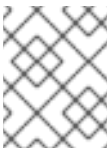
3.1. トポロジー内でレプリカの接続

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行っても、大きな利点はありません。受信レプリカは、一度に 1 つのレプリカによってのみ更新でき、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。

1 台のレプリカに対するレプリケーション合意が 4 つに制限される点について、2 つの例外があります。

- 特定のレプリカがオンラインでないか、応答していない場合はフェールオーバーパスが必要。
- 大規模デプロイメントでは、特定のノード間に追加の直接リンクが必要。

レプリケーション合意を多数構成すると、全体のパフォーマンスに影響を及ぼす場合があります。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、特定のレプリカは、受信更新と送信更新の間で changelog データベースファイルに対して競合が多くなる可能性があります。

レプリカごとにレプリカ合意を使用する場合は、レプリケーションの問題およびレイテンシーが発生しないようにしてください。ただし、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、データセンター間のドメインレプリケーションが保証されます。

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保証されます。

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

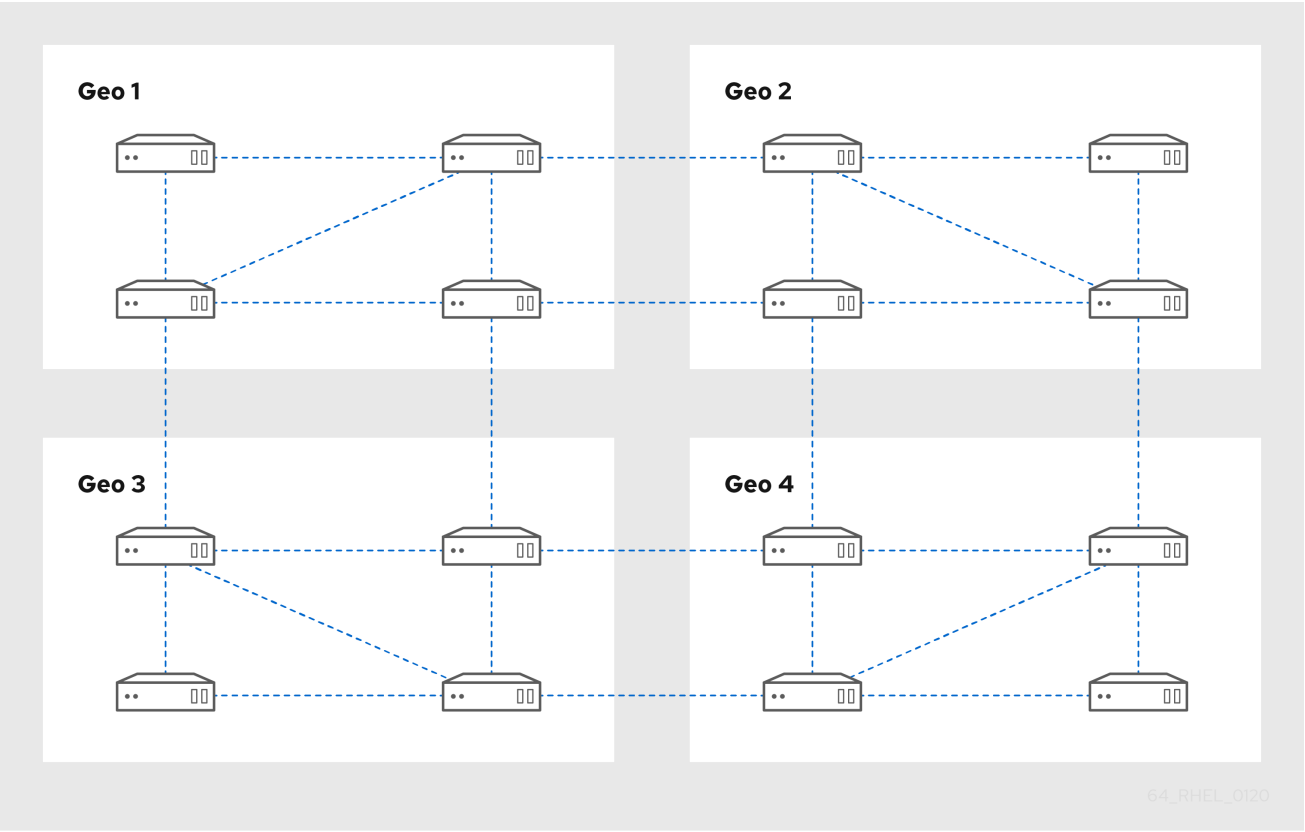
データセンター A および B に、A1 への B1 までのレプリカ合意がある場合は、A2 から B2 へのレプリカ合意があれば、いずれかのサーバーがダウンしても、2 つのデータセンター間でレプリケーションを続行できます。

3.2. レプリカトポロジーの例

以下の図は、信頼できるトポロジーを作成するガイドラインに基づく Identity Management (IdM) トポロジーの例を示しています。

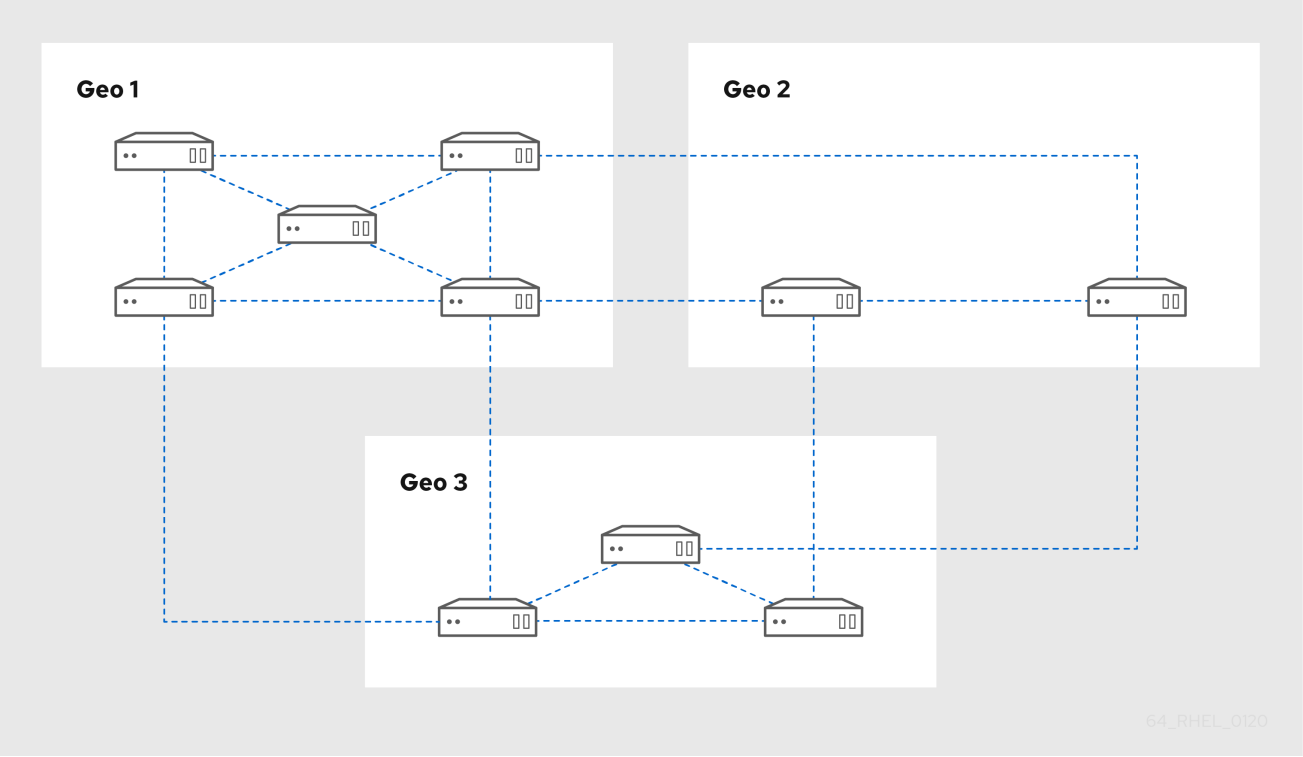
レプリカトポロジー例 1 には 4 つのデータセンターがあり、各データセンターに 4 つのサーバーがあります。このサーバーは、レプリカ合意に接続しています。

図3.1 レプリカトポロジーの例 1



レプリカトポロジー例 2には、所有するサーバー数が異なる 3 つのデータセンターが表示されます。このサーバーは、レプリカ合意に接続しています。

図3.2 レプリカトポロジーの例 2



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 サービスで新規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 レプリカ間の 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

あるサーバーのみが CA サービスを提供し、破損している場合は、環境全体が失われます。IdM CA を使用する場合、Red Hat では、CA サービスがインストールされ、CA サービス間で CA レプリカ合意のあるレプリカを 3 つ以上用意することが **強く推奨** されます。

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の準備

仮想マシンスナップショットは、IdM サーバーの完全な状態を保持するため、データ復旧手順における必須コンポーネントです。

- 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すると、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、この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、そのスナップショットを完全に取得し、オンラインに戻して、レプリケーションの更新を受け取り続けます。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
- 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。

本セクションでは、以下のトピックについて説明します。

- IdM バックアップタイプ
- 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が推奨されます。「 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 バックアップタイプ

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のに **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のに **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 **.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。

```
[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。

```
[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

本セクションでは、**ipa-backup** コマンドの重要な動作と制限を説明します。

- 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するので、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 サービスをオフラインで使用して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、オンラインのサービスで実行できます。
- 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 では、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、IdM クライアントに影響を及ぼさずに、非表示のレプリカで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)、Domain Name System(DNS)、Key Recovery Agent(KRA)などの 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している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 以外のレプリカのバックアップは CA データを取得しません。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お勧めします。

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は、IdM を完全に復元するのに必要な全データが含まれません。

5.4. IDM バックアップの作成

本セクションでは、**ipa-backup** コマンドを使用して、オフラインモードおよびオンラインモードでサーバーのフルバックアップと、データのみのバックアップを作成する方法を説明します。

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宛先を変更します。

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

詳細は「ipa-backup command fails to finish」 を参照してください。

検証手順

- バックアップディレクトリーには、バックアップが含まれるアーカイブが含まれます。

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

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
```

検証手順

- バックアップディレクトリーに **.gpg** ファイル拡張子が付いた暗号化されたアーカイブが含まれるようにします。

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

関連情報

- 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** 権限が必要である。

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** ファイルーのコンテンツに基づいて、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。このパスフレーズを使用して、秘密鍵にアクセスし、復号化します。

```
┌──────────────────────────────────────────────────────┐
│ 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
```

検証手順

- サーバーの GPG キーの一覧を表示します。

```
[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 プライバシーガード

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。

本セクションでは、以下のトピックについて説明します。

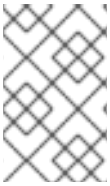
- IdM 管理用の Ansible コントロールノードの準備
- Ansible を使用した IdM サーバーのバックアップの作成
- Ansible を使用した Ansible コントローラーへの IdM サーバーのバックアップの作成
- Ansible を使用した IdM サーバーのバックアップの Ansible コントローラーへのコピー
- Ansible を使用した IdM サーバーのバックアップの Ansible コントローラーから IdM サーバーへのコピー
- Ansible を使用した IdM サーバーからのバックアップの削除

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

管理対象ノードで **root** 権限があれば、**ipaserver**、**ipareplica**、**ipaclient**、および **ipabackup ansible-freeipa** ロールを実行できます。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。

本セクションでは、**~/MyPlaybooks** ディレクトリーを作成し、このディレクトリーに Ansible Playbook を保存して実行できるように設定する方法を説明します。

前提条件

- 管理ノードに 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。

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

[us]
replica.idm.example.com

[ipaserver:children]
eu
us
```

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. (必要に応じて) 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. 各管理対象ノードの 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 サーバーをインストール する。
- インベントリーの構築方法.

6.2. ANSIBLE を使用した IDM サーバーのバックアップの作成

以下の手順では、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、IdM サーバーに保存する方法を説明します。

前提条件

- 以下の要件を満たす Ansible コントロールノードを設定している。
  - Ansible バージョン 2.8 以降を使用している。
  - **ansible-freeipa** パッケージがインストールされている。
  - このオプションを設定する IdM サーバーの完全修飾ドメイン名 (FQDN) でAnsible インベントリーファイルを作成している。
  - Ansible インベントリーファイルは ~/**MyPlaybooks**/ ディレクトリーにあります。

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 変数は、インベントリーファイルから **hosts** 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 -v -i ~/MyPlaybooks/inventory backup-my-server.yml
```

検証手順

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

以下の手順では、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、Ansible コントローラーに自動的に転送する方法を説明します。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

- 以下の要件を満たす Ansible コントロールノードを設定している。
  - Ansible バージョン 2.8 以降を使用している。
  - **ansible-freeipa** パッケージがインストールされている。
  - このオプションを設定する IdM サーバーの完全修飾ドメイン名 (FQDN) でAnsible インベントリーファイルを作成している。
  - Ansible インベントリーファイルは **~/MyPlaybooks/** ディレクトリーにあります。

手順

1. バックアップを保存するには、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** 変数は、インベントリーファイルから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. **(必要に応じて)** IdM サーバーでバックアップのコピーを維持するには、以下の行のコメントを解除します。

```
# ipabackup_keep_on_server: yes
```

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。手順 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、**/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: yes
    # ipabackup_keep_on_server: yes
    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 -v -i ~/MyPlaybooks/inventory backup-my-server-to-my-controller.yml
```

検証手順

- 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

以下の手順では、Ansible Playbook を使用して IdM サーバーのバックアップを Ansible サーバーから Ansible コントローラーにコピーする方法を説明します。

前提条件

- 以下の要件を満たす Ansible コントロールノードを設定している。
  - Ansible バージョン 2.8 以降を使用している。
  - **ansible-freeipa** パッケージがインストールされている。
  - このオプションを設定する IdM サーバーの完全修飾ドメイン名 (FQDN) でAnsible インベントリーファイルを作成している。
  - Ansible インベントリーファイルは ~/**MyPlaybooks**/ ディレクトリーにあります。

手順

1. バックアップを保存するには、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** 変数は、インベントリーファイルから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** 変数は、IdM サーバーの **ipabackup** の名前に設定し、Ansible コントローラーにコピーします。
   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。手順 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、/**home**/**user**/**ipabackups** ディレクトリーに設定します。

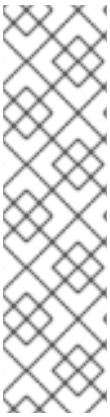
```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_to_controller: yes
    ipabackup_controller_path: /home/user/ipabackups

  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 -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: yes
```

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。

検証手順

- 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

以下の手順では、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 Ansible サーバーにコピーする方法を説明します。

前提条件

- 以下の要件を満たす Ansible コントロールノードを設定している。
  - Ansible バージョン 2.8 以降を使用している。
  - **ansible-freeipa** パッケージがインストールされている。
  - このオプションを設定する IdM サーバーの完全修飾ドメイン名 (FQDN) でAnsible インベントリーファイルを作成している。
  - Ansible インベントリーファイルは **~/MyPlaybooks/** ディレクトリーにあります。

手順

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** 変数は、インベントリーファイルから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** 変数は、Ansible コントローラーの **ipabackup** の名前に設定し、IdM サーバーにコピーします。

```
---
- 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: yes

  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 -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

以下の手順では、Ansible Playbook を使用して IdM サーバーからバックアップを削除する方法を説明します。

前提条件

- 以下の要件を満たす Ansible コントロールノードを設定している。
  - Ansible バージョン 2.8 以降を使用している。
  - **ansible-freeipa** パッケージがインストールされている。
  - このオプションを設定する IdM サーバーの完全修飾ドメイン名 (FQDN) でAnsible インベントリーファイルを作成している。
  - Ansible インベントリーファイルは ~/**MyPlaybooks**/ ディレクトリーにあります。

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** 変数は、インベントリーファイルから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** 変数は、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 -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、 **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。