Red Hat Enterprise Linux 8

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: 2020-09-07

Red Hat Enterprise Linux 8 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

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

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。改善点を報告する場合は、以下のように行います。

- 特定の文章に簡単なコメントを記入する場合は、以下の手順を行います。
    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端に **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。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
    1. Bugzilla の Web サイトにアクセスします。
    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	● *3章 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	● *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* ● *5章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。

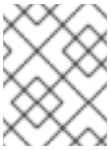
3.1. トポロジー内でレプリカの接続

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、初期レプリカとマスター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。

図3.1「レプリカトポロジーの例 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

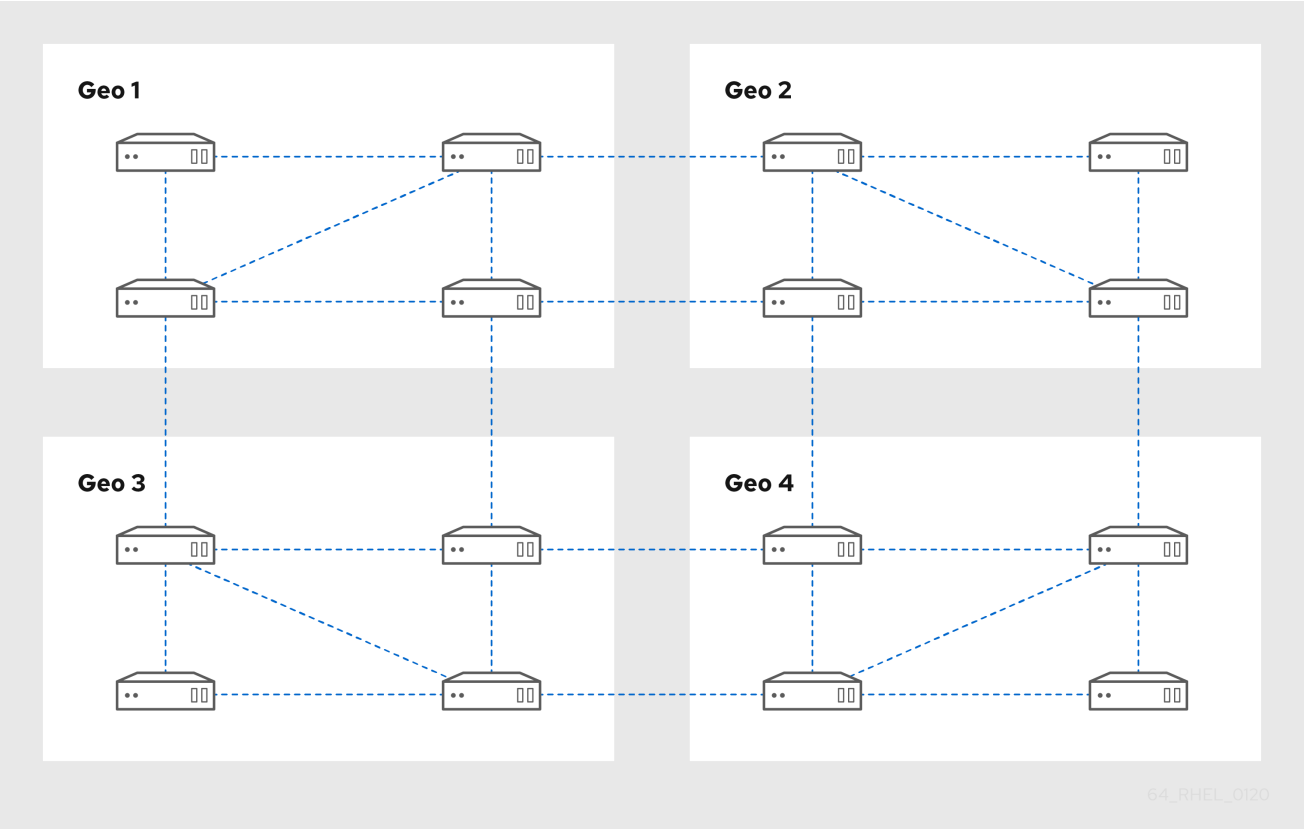
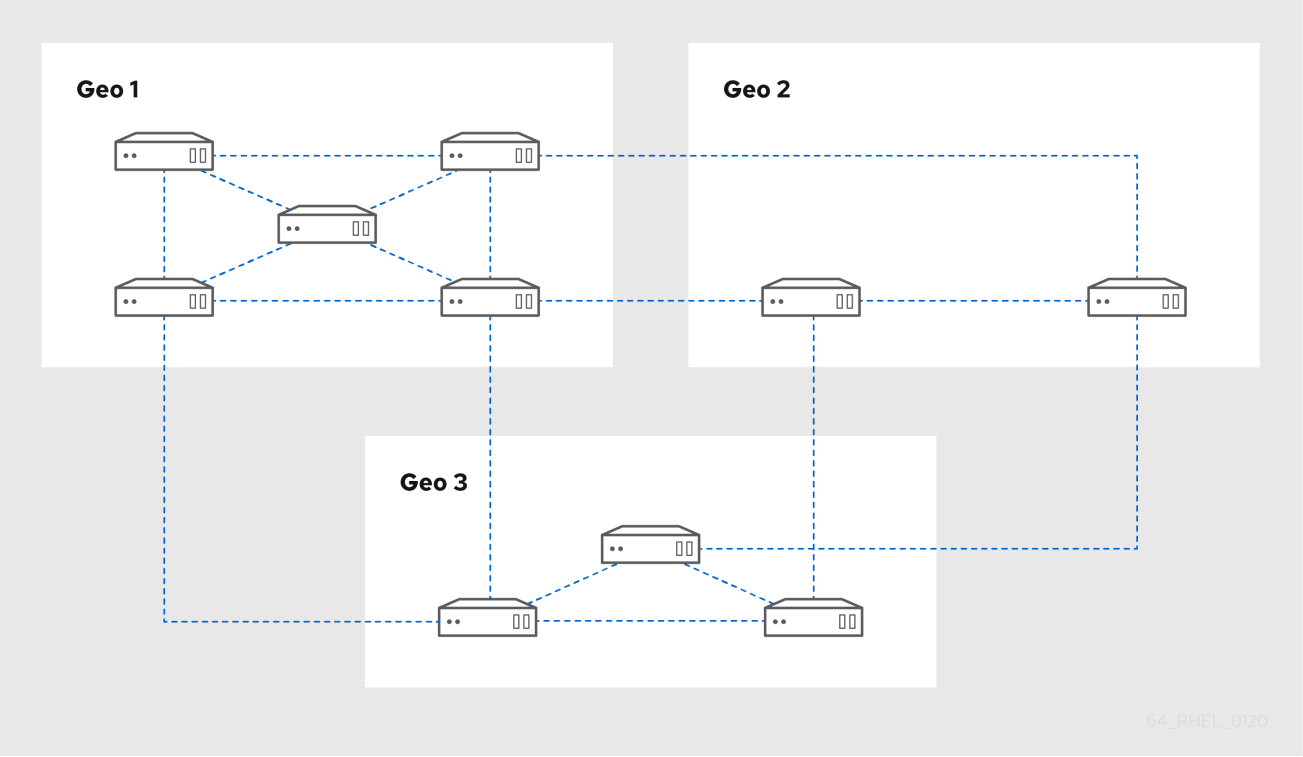


図3.2「レプリカトポロジーの例 2」には、所有するサーバー数が異なる 3 つのデータセンターが表示されます。このサーバーは、レプリカ合意に接続しています。

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: careplica1.example.com
Right node: careplica2.example.com
Segment name [careplica1.example.com-to-careplica2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
```

```
Left node: careplica1.example.com
Right node: careplica2.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

- IdM の CA オプションの詳細は、「CA サービスの計画」を参照してください。
- IdM レプリカのインストールの詳細は、「IdM レプリカのインストール」を参照してください。

3.4. 関連情報

- レプリケーションの詳細は、「レプリカトポロジーの計画」を参照してください。

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

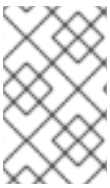
1. デプロイメントの **CA レプリカ** を、仮想マシン内で実行するように設定します。
   a. IdM DNS または KRA が環境で使用されている場合は、このレプリカにも DNS サービスおよび KRA サービスをインストールすることを検討してください。
   b. 必要に応じて、仮想マシンレプリカを 非表示レプリカ として設定します。
2. この仮想マシンを定期的にシャットダウンして、そのスナップショットを完全に取得し、オンラインに戻して、レプリケーションの更新を受け取り続けます。仮想マシンが非表示のレプリカの場合は、この手順中に IdM クライアントが中断することはありません。

関連情報

- Red Hat Enterprise Linux をゲストとして実行することがテストおよび認定された認定ハイパーバイザーの一覧は、「Red Hat Enterprise Linux の実行が認定されているハイパーバイザー」 を参照してください。
- 非表示のレプリカの詳細は、「非表示のレプリカモード」を参照してください。

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。



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。

5.1. IDM バックアップタイプ

IdM は、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という 2 種類のバックアップを提供します。

バックアップタイプ	バックアップのコンテンツ	実行されたオンラインまたはオフライン	実施例
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 • LDAP データ交換形式 (LDIF) の LDAP データ	オフラインのみ。IdM サービスを一時的に停止する必要があります。	IdM デプロイメントのゼロからの再構築
データのみのバックアップ	• LDAP データ交換形式 (LDIF) の LDAP データ • レプリケーション変更ログ	オンラインまたはオフライン。	IdM データを以前の状態に復元

5.2. バックアップファイルの規則

デフォルトでは、IdM はバックアップを **/var/lib/ipa/backup/** ディレクトリーに保存します。このサブディレクトリーの命名規則は以下のとおりです。

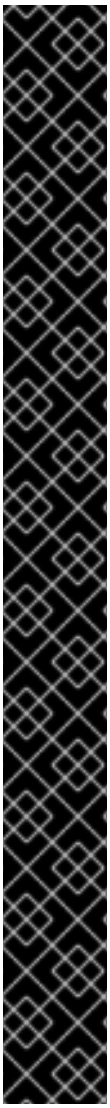
- サーバーのフルバックアップ - GMT 時間で **ipa-full-YEAR-MM-DD-HH-MM-SS**
- データのみのバックアップ - GMT 時間で **ipa-data-YEAR-MM-DD-HH-MM-SS**

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

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。



重要

- デフォルトでは、**ipa-backup** はオフラインモードで実行され、すべての IdM サービスを停止します。バックアップが完了すると、サービスが自動的に起動します。
- 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、バックアップは **/var/lib/ipa/backup/** ディレクトリーを含むファイルシステムに作成されます。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が推奨されます。
- 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。
- サーバーの IdM バックアップは、そのサーバーにインストールされているサーバーロールのみを取得します。
  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**。同様に、KRA が **インストールされていない** レプリカのバックアップも、KRA データを **取得しません**。
- IdM デプロイメントでビルトイン CA を使用する場合、CA なしのレプリカのバックアップでは、IdM デプロイメントを再構築するには不十分です。使用中の IdM サーバーロールがすべてインストールされているレプリカ (CA、KRA、DNS) にバックアップを作成してください。

ipa-backup コマンドの使用例

- 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
```

5.4. 暗号化 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。暗号化した IdM バックアップを作成するには、最初に GPG2 キーを作成する必要があります。

5.4.1. IdM バックアップを暗号化する GPG2 キーの作成

以下の手順では、**ipa-backup** ユーティリティーの GPG2 キーを生成する方法を説明します。

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: IPA Backup
Name-Comment: IPA Backup
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. 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** の内容に基づいて新規の GPG2 キーの生成を開始します。

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

a. GPG2 キーを保護するパスフレーズを入力します。

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: SecretPassphrase42                       │
│                                                      │
│  <OK>                          <Cancel>              │
└──────────────────────────────────────────────────────┘
```

b. 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: SecretPassphrase42                       │
│                                                      │
│  <OK>                          <Cancel>              │
└──────────────────────────────────────────────────────┘
```

c. これで新しい GPG2 キーが作成されました。

```
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] IPA Backup (IPA Backup) <root@example.com>
```

関連情報

- GPG 暗号化とその使用に関する詳細は、GNU Privacy Guard の Web サイトを参照してください。

5.4.2. GPG2 で暗号化した IdM バックアップの作成

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。詳細は「IdM バックアップを暗号化する 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に関する詳細は、「バックアップの作成」を参照してください。

5.5. 関連情報

- IdM のバックアップと復元の詳細は「IdM のバックアップと復元」を参照してください。