Red Hat Enterprise Linux 8

Identity Management を使用した障害復旧の実行

Identity Management デプロイメントに影響する障害から復旧するためのドキュメント

Last Updated: 2020-09-04

Red Hat Enterprise Linux 8 Identity Management を使用した障害復旧の実行

Identity Management デプロイメントに影響する障害から復旧するためのドキュメント

法律上の通知

概要

本書では、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た Identity Management デプロイメント間のサーバーまたはデータの損失に応答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 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1.1 サーバー損失対データ損失

障害タイプ	考えられる原因	応答方法
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	● *2章 レプリケーションによるサーバーの損失からの復旧*
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	● *3章 仮想マシンスナップショットによるデータ損失からの復旧* ● *4章 IdM バックアップを使用したデータ損失からの復旧* ● *5章 データ損失の管理*

第2章 レプリケーションによるサーバーの損失からの復旧

サーバーで深刻な中断や損失が発生した場合は、複数のレプリカを使用すると、レプリカを置き換えて、以前の冗長性レベルを迅速に復元できます。

IdM トポロジーに統合認証局 (CA) が含まれている場合は、CA 更新マスターおよびその他のレプリカで、破損したレプリカを削除して置き換える手順が異なります。

2.1. CA 更新マスターの失われた状態からの復旧

認証局 (CA) 更新マスターが失われた場合は、CA 更新マスターロールを満たすために別の CA レプリカをプロモートしてから、代替 CA レプリカをデプロイする必要があります。

前提条件

- デプロイメントで、IdM の内部認証局 (CA) を使用している。
- 環境内の別のレプリカには CA サービスがインストールされている。

警告

IdM デプロイメントは、以下の場合に修復できません。

1. CA 更新マスターが失われました。
2. CA がインストールされている他のサーバーはありません。
3. CA ロールを持つレプリカのバックアップはありません。
   証明書データが保護されるように、CA ロールでレプリカからのバックアップを作成することが重要です。バックアップの作成および復元に関する詳細は、「IdM バックアップでデータ損失に備える」を参照してください。

手順

1. 失われた CA Renewal Master からレプリカ合意を削除します。「IdM サーバーのアンインストール」を参照してください。
2. 環境内で別の CA レプリカをプロモートして、新しい CA Renewal Master として機能します。「IdM CA Renewal Master の変更およびリセット」を参照してください。
3. 新しい CA レプリカをインストールして、失われた CA レプリカを置き換えます。「CA を使用して IdM レプリカのインストール」を参照してください。
4. DNS を更新して、レプリカトポロジーの変更を反映させます。IdM DNS を使用すると、DNS サービスレコードが自動的に更新されます。
5. IdM クライアントが IdM サーバーに到達できることを確認します。「復旧時に IdM クライアントの調整」を参照してください。

検証手順

1. IdM ユーザーとして Kerberos TGT (Ticket-Granting-Ticket) を正常に取得して、新しいレプリカで Kerberos サーバーをテストします。

```
[root@master ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@master ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/master.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. ユーザー情報を取得して、Directory Server および SSSD 設定をテストします。

```
[root@master ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** コマンドを使用して CA 設定をテストします。

```
[root@master ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

関連情報

- IdM CA Renewal Master の詳細は、「IdM CA Renewal Master の使用」を参照してください。

2.2. 通常のレプリカの失われた状態からの回復

認証局 (CA) 更新マスターではないレプリカを置き換えるには、トポロジーから失われたレプリカを削除し、その場所に新しいレプリカをインストールします。

前提条件

- CA Renewal Master が適切に機能している。CA Renewal Master が失われた場合は、「CA Renewal Master の損失からの復旧」を参照してください。

手順

1. 失われたサーバーにレプリカ合意を削除します。「IdM サーバーのアンインストール」を参照してください。
2. 必要なサービス (CA、KRA、DNS) で新規レプリカをデプロイします。「IdM レプリカのインストール」を参照してください。
3. DNS を更新して、レプリカトポロジーの変更を反映させます。IdM DNS を使用すると、DNS サービスレコードが自動的に更新されます。
4. IdM クライアントが IdM サーバーに到達できることを確認します。「復旧時に IdM クライアントの調整」を参照してください。

検証手順

1. IdM ユーザーとして Kerberos TGT (Ticket-Granting-Ticket) を正常に取得して、新しいレプリカで Kerberos サーバーをテストします。

```
[root@newreplica ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@newreplica ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/master.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. ユーザー情報を取得して、新しいレプリカで Directory Server および SSSD 設定をテストします。

```
[root@newreplica ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

2.3. 複数のサーバーの損失からの復旧

複数のサーバーが同時に失われた場合は、以下のいずれかのシナリオに該当することで、環境を再構築できるかどうかを判断します。

2.3.1. CA なしのデプロイメントで複数のサーバーが失われた状態からの回復

CA なしのデプロイメントでは、サーバーはすべて同等であるとみなされ、失われたレプリカを削除し、置き換えて環境を再構築できます。

手順

- 「通常のレプリカ損失からの復旧」を参照してください。

2.3.2. CA Renewal Master が無効化された場合の複数のサーバー損失からの復旧

前提条件

- デプロイメントで、IdM の内部認証局 (CA) を使用している。

手順

- 「通常のレプリカ損失からの復旧」を参照してください。

2.3.3. CA Renewal Master およびその他のサーバーの損失からの復旧

前提条件

- デプロイメントで、IdM の内部認証局 (CA) を使用している。
- 少なくとも CA レプリカが無効化されている。

手順

1. 別の CA レプリカをプロモートし、CA Renewal Master ロールに対応します。「CA Renewal Master の損失からの復旧」を参照してください。
2. 失われたその他のレプリカをすべて置き換えます。「通常のレプリカ損失からの復旧」を参照してください。

2.3.4. すべての CA レプリカの失われた状態からの復旧

認証局 (CA) レプリカがないと、IdM 環境は、追加のレプリカをデプロイし、そのレプリカを再ビルドする機能がありません。

前提条件

- デプロイメントで、IdM の内部認証局 (CA) を使用している。

手順

- この状況は、完全に失われています。

関連情報

- 完全なインフラストラクチャー損失を準備するには、「仮想マシンスナップショットによるデータ損失の準備」を参照してください。

2.3.5. インフラストラクチャー全体の損失からの復旧

すべてのサーバーが一度にに失われ、復元する仮想マシンスナップショットやデータバックアップがない場合、この状況は復旧できません。

手順

- この状況は、完全に失われています。

関連情報

- 完全なインフラストラクチャー損失を準備するには、「仮想マシンスナップショットによるデータ損失の準備」を参照してください。

第3章 仮想マシンスナップショットによるデータ損失からの復旧

データ損失イベントが発生した場合は、認証局 (CA) のレプリカの仮想マシン (VM) スナップショットを復元して、失われたデータを修復するか、そこから新しい環境をデプロイできます。

3.1. 仮想マシンのスナップショットのみからの復旧

災害がすべての IdM サーバーに影響し、IdM CA レプリカ仮想マシンのスナップショットのみが残っている場合は、失われたサーバーへの参照をすべて削除し、新しいレプリカをインストールすることで、デプロイメントを再作成できます。

前提条件

- CA レプリカ仮想マシン用に仮想マシンのスナップショットを準備している。「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」を参照してください。

手順

1. CA レプリカ仮想マシンで使用するスナップショットを起動します。
2. 失われたレプリカのレプリカ合意を削除します。

```
[root@master ~]# ipa server-del lost-server1.example.com
[root@master ~]# ipa server-del lost-server2.example.com
...
```

3. 次の CA レプリカをインストールします。「CA を使用して IdM レプリカのインストール」を参照してください。
4. VM CA レプリカが CA Renewal Master になりました。Red Hat は、環境内の別の CA レプリカをプロモートして、CA Renewal Master として機能することを推奨します。「IdM CA Renewal Master の変更およびリセット」を参照してください。
5. 必要なサービス (CA、DNS) で追加のレプリカをデプロイし、必要なレプリカトポロジーを再作成します。「IdM レプリカのインストール」を参照してください。
6. DNS を更新して、新しいレプリカトポロジーを反映させます。IdM DNS を使用すると、DNS サービスレコードが自動的に更新されます。
7. IdM クライアントが IdM サーバーにアクセスできることを確認します。「復旧時に IdM クライアントの調整」を参照してください。

検証手順

1. Kerberos TGT (Ticket-Granting-Ticket) を IdM ユーザーとして正常に取得して、すべてのレプリカで Kerberos サーバーをテストします。

```
[root@master ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@master ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM
```

```
Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/master.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. ユーザー情報を取得して、すべてのレプリカで Directory Server および SSSD 設定をテストします。

```
[root@master ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** コマンドを使用して、すべての CA レプリカで CA サーバーをテストします。

```
[root@master ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

関連情報

- レプリケーショントポロジーのベストプラクティスは「レプリカトポロジーの計画」を参照してください。

3.2. 部分的に機能する環境間の仮想マシンのスナップショットからの復旧

障害が複数の IdM サーバーに影響を及ぼし、その他のサーバーが適切に動作している場合は、デプロイメントを仮想マシンスナップショットでキャプチャーされた状態に復元できます。たとえば、他のレプリカが実稼働の状態でもすべての認証局 (CA) レプリカが失われると、CA レプリカを環境に戻す必要があります。

このシナリオでは、失われたレプリカへの参照を削除し、スナップショットから CA レプリカを復元し、レプリケーションを確認し、新規レプリカをデプロイします。

前提条件

- CA レプリカ仮想マシン用に仮想マシンのスナップショットを準備している。「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」を参照してください。

手順

1. すべてのレプリカ合意を失われたサーバーから削除します。「IdM サーバーのアンインストール」を参照してください。
2. CA レプリカ仮想マシンで使用するスナップショットを起動します。
3. 復元したサーバーと失われたサーバー間のレプリカ合意を削除します。

```
[root@restored-CA-replica ~]# ipa server-del lost-server1.example.com
[root@restored-CA-replica ~]# ipa server-del lost-server2.example.com
...
```

4. 復元されたサーバーに、実稼働のサーバーとのレプリカ合意がない場合は、復元されたサーバーをその他のサーバーのいずれかに接続して、復元するサーバーを更新します。

```
[root@restored-CA-replica ~]# ipa topologysegment-add
Suffix name: domain
Left node: restored-CA-replica.example.com
Right node: server3.example.com
Segment name [restored-CA-replica.com-to-server3.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
  Left node: restored-CA-replica.example.com
  Right node: server3.example.com
  Connectivity: both
```

5. **/var/log/dirsrv/slapd-YOUR-INSTANCE/errors** で Directory Server のエラーログを確認し、スナップショットの CA レプリカが残りの IdM サーバーと正しく同期しているかどうかを確認します。
6. データベースが古くて復元されたサーバーのレプリケーションが失敗すると、復元されたサーバーを再初期化します。

```
[root@restored-CA-replica ~]# ipa-replica-manage re-initialize --from
server2.example.com
```

7. 復元されたサーバーのデータベースが正しく同期されている場合は、「IdM レプリカのインストール」に従って、必要なサービス (CA、DNS) で追加のレプリカをデプロイし、続行します。

検証手順

1. Kerberos TGT (Ticket-Granting-Ticket) を IdM ユーザーとして正常に取得して、すべてのレプリカで Kerberos サーバーをテストします。

```
[root@master ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@master ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM
```

```
Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/master.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. ユーザー情報を取得して、すべてのレプリカで Directory Server および SSSD 設定をテストします。

```
[root@master ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** コマンドを使用して、すべての CA レプリカで CA サーバーをテストします。

```
[root@master ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

関連情報

- 復元された CA レプリカのデータベースが同期または再初期化しない場合、復元された CA レプリカから新規デプロイメントを作成し、新しい環境に切り替えます。「仮想マシンのスナップショットからの復元による新規 IdM 環境の確立」を参照します。

3.3. 仮想マシンのスナップショットからの復元による新規 IDM 環境の確立

復元した仮想マシンスナップショットの認証局 (CA) レプリカが他のサーバーと複製できない場合は、仮想マシンスナップショットから新しい IdM 環境を作成します。

新しい IdM 環境を確立するには、仮想マシンサーバーを分離し、そこから追加のレプリカを作成し、IdM クライアントを新しい環境に切り替えます。

前提条件

- CA レプリカ仮想マシン用に仮想マシンのスナップショットを準備している。「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」を参照してください。

手順

1. CA レプリカ仮想マシンで使用するスナップショットを起動します。
2. 現在のデプロイメントの他の部分から復元されたサーバーを分離します。複製トポロジーセグメントがすべて削除されます。
   a. まず、すべての **ドメイン** レプリケーショントポロジーセグメントを表示します。

```
[root@restored-CA-replica ~]# ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: restored-CA-replica.example.com
  Right node: server2.example.com
  Connectivity: both

...

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

   b. 次に、復元されたサーバーに関連するすべての **ドメイン** トポロジーセグメントを削除します。

```
[root@restored-CA-replica ~]# ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
-----------------------------
Deleted segment "new_segment"
-----------------------------
```

   c. 最後に、**ca** トポロジーセグメントを使用して同じアクションを実行します。

```
[root@restored-CA-replica ~]# ipa topologysegment-find
Suffix name: ca
------------------
1 segments matched
------------------
  Segment name: ca_segment
  Left node: restored-CA-replica.example.com
  Right node: server4.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------

[root@restored-CA-replica ~]# ipa topologysegment-del
Suffix name: ca
Segment name: ca_segment
----------------------------
Deleted segment "ca_segment"
----------------------------
```

3. デプロイメントの負荷を処理するために、復元されたサーバーから十分な数の IdM レプリカをインストールします。これで、接続されていない 2 つの IdM デプロイメントが並行して実行するようになりました。

4. 新しい IdM レプリカへの参照をハードコーディングして、IdM クライアントが新しいデプロイメントを使用するようにします。「復旧時に IdM クライアントの調整」を参照してください。

5. 以前のデプロイメントから IdM サーバーを停止し、アンインストールします。「IdM サーバーのアンインストール」を参照してください。

検証手順

1. IdM ユーザーとして Kerberos TGT (Ticket-Granting-Ticket) を正常に取得して、新しいレプリカで Kerberos サーバーをテストします。

```
[root@master ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@master ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/master.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. ユーザー情報を取得して、新しいレプリカごとに Directory Server および SSSD の設定をテストします。

```
[root@master ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** コマンドを使用して、新しい CA レプリカごとに CA サーバーをテストします。

```
[root@master ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

第4章 IDM バックアップを使用したデータ損失からの復旧

ipa-restore ユーティリティーを使用して、IdM サーバーを IdM バックアップでキャプチャーした以前の状態に復元できます。

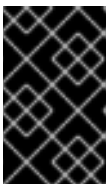
4.1. IDM バックアップから復元するタイミング

IdM バックアップから復元すると、いくつかの障害シナリオに対応できます。

- **LDAP コンテンツに望ましくない変更が加えられた** - エントリーは変更または削除され、デプロイメント全体でそれらの変更が行われ、これらの変更を元に戻すようにします。データのみのバックアップを復元すると、IdM 設定自体に影響を与えずに LDAP エントリーが以前の状態に戻ります。

- **インフラストラクチャーの損失の合計、またはすべての CA インスタンスの損失** - 障害によりすべての認証局レプリカが損傷した場合、デプロイメントは追加のサーバーをデプロイすることで、それ自体を再構築する機能を失うようになりました。この場合は、CA レプリカのバックアップを復元し、そこから新しいレプリカを構築します。

- **分離されたサーバーのアップグレードに失敗** - オペレーティングシステムは機能し続けますが、IdM データが破損するため、IdM システムを既知の正常な状態に復元したい理由になります。Red Hat は、問題を診断し、トラブルシューティングするために、テクニカルサポートをご利用になることが推奨されます。以上の作業にすべて失敗した場合は、サーバーのフルバックアップから復元します。



重要

ハードウェアまたはアップグレードの失敗で推奨されるソリューションは、失われたサーバーをレプリカから再構築することです。詳細は「レプリケーションを使用したサーバーロスからの復旧」を参照してください。

4.2. IDM バックアップから復元する際の注意点

ipa-backup ユーティリティーでバックアップを作成した場合は、IdM サーバーまたは LDAP コンテンツをバックアップ実行時の状態に復元できます。

以下は、IdM バックアップからの復元時の主要な考慮事項です。

- バックアップが作成されたサーバーの設定と一致するサーバー上でのみバックアップを復元できます。サーバーには以下の項目が **必要** です。
  - 同じホスト名
  - 同じ IP アドレス
  - 同じバージョンの IdM ソフトウェア

- マルチマスター環境の IdM サーバーが復元されると、復元されたサーバーは、IdM の唯一の情報ソースになります。他のすべてのマスターサーバーは復元されたサーバーから再度初期化される必要があります。

- 最後のバックアップ後に作成されたデータはすべて失われるため、通常のシステムメンテナンスには、バックアップと復元のソリューションを使用しないでください。

- サーバーが失われた場合は、バックアップから復元するのではなく、レプリカとしてサーバー

を再インストールしてサーバーを再構築することが推奨されます。新規レプリカを作成すると、現在の作業環境のデータが保存されます。詳細は、「サーバーでのレプリケーションによる損失の準備」を参照してください。

- バックアップ機能および復元機能はコマンドラインからのみ管理でき、IdM Web UI では使用できません。

ヒント

バックアップから復元するには、バックアップの実行時にインストールされたものと同じバージョンのソフトウェア (RPM) がターゲットホストに必要になります。このため、Red Hat は、バックアップではなく、仮想マシンのスナップショットからの復元を行うことを推奨します。詳細は「仮想マシンスナップショットによるデータ損失からの復旧」を参照してください。

4.3. バックアップからの IDM サーバーの復元

以下の手順では、IdM バックアップから IdM サーバーまたはその LDAP データを復元する方法を説明します。

図4.1 この例で使用されるレプリケーショントポロジー

64_RHEL_0120

表4.1 この例で使用されるサーバーの命名規則

サーバー名	機能
master1.example.com	バックアップから復元する必要があるサーバー
caReplica2.example.com	Master1.example.com に接続している認証局 (CA) レプリカ。
replica3.example.com	CaReplica2.example.com に接続しているレプリカ。

前提条件

- IdM サーバーの完全なサーバーまたはデータのみのバックアップは、**ipa-backup** ユーティリティーで生成されました。「バックアップの作成」を参照してください。
- 完全なサーバーバックアップからサーバーの完全な復元を実行する前に、サーバーから IdMをアンインストール し、以前と同じサーバー設定を使用して IdM を 再インストール します。

手順

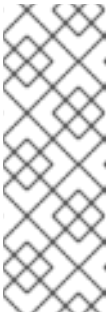
1. **Ipa-restore** ユーティリティーを使用して、完全なサーバーまたはデータのみのバックアップを復元します。

- バックアップディレクトリーがデフォルトの **/var/lib/ipa/backup/** の場合は、ディレクトリーの名前のみを入力します。

```
[root@master1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
```

- バックアップディレクトリーがデフォルトの場所にない場合は、完全パスを入力します。

```
[root@master1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
```



注記

Ipa-restore ユーティリティーは、ディレクトリーに含まれるバックアップのタイプを自動的に検出し、デフォルトで同じタイプの復元を実行します。完全なサーバーバックアップからデータのみの復元を実行するには、**--data** オプションを **ipa-restore** に追加します。

```
[root@master1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
```

2. Directory Manager パスワードを入力します。

```
Directory Manager (existing master) password:
```

3. **Yes** を入力して、現在のデータをバックアップで上書きしていることを確認します。

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
master1.example.com
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. **Ipa-restore** ユーティリティーは、利用可能なすべてのサーバーでレプリケーションを無効にします。

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on master1.example.com to caReplica2.example.com
Disabling CA replication agreement on master1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to master1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to master1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

その後、このユーティリティーは IdM サービスを停止し、バックアップを復元し、サービスを再起動します。

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
```

```
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

5. 復元されたサーバーに接続したすべてのレプリカを再初期化します。

   a. **domain** 接尾辞のレプリカトポロジーセグメントの一覧を表示します。復元されたサーバーに関連するトポロジーセグメントを書き留めます。

```
[root@master1 ~]# ipa topologysegment-find domain
------------------
2 segments matched
------------------
  Segment name: master1.example.com-to-caReplica2.example.com
  Left node: master1.example.com
  Right node: caReplica2.example.com
  Connectivity: both

  Segment name: caReplica2.example.com-to-replica3.example.com
  Left node: caReplica2.example.com
  Right node: replica3.example.com
  Connectivity: both
----------------------------
Number of entries returned 2
----------------------------
```

   b. 復元されたサーバーとともにすべてのトポロジーセグメントの **domain** 接尾辞を再初期化します。
   この例では、**master1** からデータを使用して **caReplica2** の再初期化を実行します。

```
[root@caReplica2 ~]# ipa-replica-manage re-initialize --from=master1.example.com
Update in progress, 2 seconds elapsed
Update succeeded
```

   c. 認証局データに移動し、**ca** 接尾辞のレプリケーショントポロジーセグメントの一覧を表示します。

```
[root@master1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: master1.example.com-to-caReplica2.example.com
  Left node: master1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

   d. 復元されたサーバーに接続されているすべての CA レプリカを再初期化します。

この例では、**master1** からのデータを使用して **caReplica2** の **csreplica** の再初期化を実行します。

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=master1.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

6. 復元されたサーバー **master1.example.com** のデータですべてのサーバーが更新されるまで、レプリケーショントポロジーを介して、後続のレプリカを再初期化します。
この例では、**caReplica2** からのデータで、**replica3** の **domain** 接尾辞を再初期化することのみが必要になります。

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

7. すべてのサーバーで SSSD のキャッシュをクリアし、無効なデータによる認証の問題を回避します。

   a. SSSD サービスを停止します。

   ```
   [root@server ~]# systemctl stop sssd
   ```

   b. SSSD からキャッシュされたコンテンツをすべて削除します。

   ```
   [root@server ~]# sss_cache -E
   ```

   c. SSSD サービスを起動します。

   ```
   [root@server ~]# systemctl start sssd
   ```

   d. サーバーを再起動します。

関連情報

- man ページの **ipa-restore**(1) では、復元中の複雑なレプリケーションシナリオの処理方法が詳細に説明されています。

4.4. 暗号化されたバックアップからの復元

Ipa-restore ユーティリティーは、IdM バックアップが暗号化されているかどうかを自動的に検出し、デフォルトでは GPG2 root キーリングと **gpg-agent** を使用して復元します。

前提条件

- GPG 暗号化 IdM バックアップ。「暗号化 IdM バックアップの作成」を参照してください。
- LDAP Directory Manager のパスワード

- **GPG** キーの作成時に使用されるパスフレーズ

手順

1. GPG2 キーの作成時にカスタムキーリングの場所を使用した場合は、**$GNUPGHOME** 環境変数がそのディレクトリーに設定されていることを確認します。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。

```
[root@server ~]# echo $GNUPGHOME
/root/backup
```

2. **Ipa-restore** ユーティリティーにバックアップディレクトリーの場所を指定します。

```
[root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
```

   a. Directory Manager パスワードを入力します。

```
Directory Manager (existing master) password:
```

   b. GPG キーの作成時に使用した **パスフレーズ** を入力します。

```
┌──────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:        │
│ "IPA Backup (IPA Backup) <root@example.com>"                         │
│ 2048-bit RSA key, ID BF28FFA302EF4557,                               │
│ created 2020-01-13.                                                  │
│                                                                      │
│                                                                      │
│ Passphrase: SecretPassPhrase42                                       │
│                                                                      │
│       <OK>                              <Cancel>                     │
└──────────────────────────────────────────────────────────────────────┘
```

3. 復元されたサーバーに接続されているすべてのレプリカを再初期化します。「バックアップからの IdM サーバーの復元」を参照してください。

第5章 データ損失の管理

データ損失イベントに対する適切な応答は、影響を受けるレプリカの数と失ったデータのタイプにより異なります。

5.1. 分離されたデータ損失への応答

データ損失の発生時に、影響を受けるサーバーをすぐに分離することで、データの損失の複製を最小限に抑えます。次に、環境の残りの部分から置き換えられたレプリカを作成します。

前提条件

- 複数のレプリカを使用した強力な IdM レプリケーショントポロジー。「レプリケーションによるサーバーの損失の準備」を参照してください。

手順

1. データ損失の複製を制限するには、他のトポロジーのレプリカトポロジーセグメントを削除して、影響を受けたレプリカをすべて切断します。

   a. デプロイメント内のすべての **ドメイン** レプリケーショントポロジーセグメントを表示します。

   ```
   [root@server ~]# ipa topologysegment-find
   Suffix name: domain
   ------------------
   8 segments matched
   ------------------
     Segment name: segment1
     Left node: server.example.com
     Right node: server2.example.com
     Connectivity: both

   ...

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

   b. 影響を受けるサーバーに関連するすべての **ドメイン** トポロジーセグメントを削除します。

   ```
   [root@server ~]# ipa topologysegment-del
   Suffix name: domain
   Segment name: segment1
   ----------------------------
   Deleted segment "segment1"
   ----------------------------
   ```

   c. 影響を受けるサーバーに関する **ca** トポロジーセグメントを使用して、同じアクションを実行します。

   ```
   [root@server ~]# ipa topologysegment-find
   Suffix name: ca
   ------------------
   ```

```
1 segments matched
-----------------
  Segment name: ca_segment
  Left node: server.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------

[root@server ~]# ipa topologysegment-del
Suffix name: ca
Segment name: ca_segment
-----------------------------
Deleted segment "ca_segment"
-----------------------------
```

2. データ損失の影響を受けるサーバーは破棄されている必要があります。代替レプリカを作成するには、「複数のサーバーの損失からの復旧」を参照してください。

5.2. すべてのサーバー間の制限されたデータ損失への対応

データ損失イベントは、すべてのサーバー間で誤って削除を実行するなど、環境内のすべてのレプリカに影響する可能性があります。データの損失が認識され、制限されている場合は、手動でデータを再度追加します。

前提条件

- 失われたデータを含む IdM サーバーの仮想マシンスナップショットまたは IdM バックアップ。

手順

1. 失われたデータを確認する必要がある場合は、別のネットワーク上の分離されたサーバーに、仮想マシンのスナップショットまたはバックアップを復元します。
2. **ipa** コマンドまたは **ldapadd** コマンドを使用して、不足している情報をデータベースに追加します。

関連情報

- 仮想マシンのスナップショットからの復元の詳細は「仮想マシンスナップショットによるデータ損失からの復旧」を参照してください。
- 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。

5.3. すべてのサーバー間の未定義のデータ損失への応答

データの損失が深刻な場合または定義されていない場合は、サーバーの仮想マシンスナップショットから新しい環境をデプロイします。

前提条件

- 仮想マシンスナップショットには、失われたデータが含まれます。

手順

1. IdM 認証局 (CA) レプリカを仮想マシンのスナップショットから既知の正常な状態に復元し、そこから新しい IdM 環境をデプロイします。「仮想マシンのスナップショットのみからの復旧」を参照してください。

2. **ipa** コマンドまたは **ldapadd** コマンドを使用して、スナップショットの取得後に作成されたデータを追加します。

関連情報

- 仮想マシンのスナップショットからの復元の詳細は「仮想マシンスナップショットによるデータ損失からの復旧」を参照してください。

第6章 復旧時に IDM クライアントの調整

IdM サーバーが復元している間は、レプリカトポロジーの変更を反映するように IdM クライアントの調整が必要になる場合があります。

手順

1. **DNS 設定を調整** します。

   a. **/etc/hosts** に IdM サーバーの参照が含まれている場合は、ハードコーディングされた IP からホスト名へのマッピングが有効になっていることを確認してください。

   b. IdM クライアントが名前解決に IdM DNS を使用している場合は、**/etc/resolv.conf** の **nameserver** のエントリーが、DNS サービスを提供する IdM レプリカを指していることを確認します。

2. **Kerberos 設定を調整** します。

   a. デフォルトでは、IdM クライアントは Kerberos サーバーの DNS サービスレコードを検索し、レプリカトポロジーの変更に合わせて調整します。

   ```
   [root@client ~]# grep dns_lookup_kdc /etc/krb5.conf
     dns_lookup_kdc = true
   ```

   b. IdM クライアントが **/etc/krb5.conf** で特定の IdM サーバーを使用するようにハードコーディングされている場合は、以下を行います。

   ```
   [root@client ~]# grep dns_lookup_kdc /etc/krb5.conf
     dns_lookup_kdc = false
   ```

   /etc/krb5.conf の **kdc** エントリー、**master_kdc** エントリー、および **admin_server** エントリーが適切に機能する IdM サーバーを参照することを確認します。

   ```
   [realms]
    EXAMPLE.COM = {
     kdc = working-master.example.com:88
     master_kdc = working-master.example.com:88
     admin_server = working-master.example.com:749
     default_domain = example.com
     pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
     pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem
    }
   ```

3. **SSSD 設定を調整** します。

   a. デフォルトでは、IdM クライアントは LDAP サーバーの DNS サービスレコードを検索し、レプリカトポロジーの変更を調整します。

   ```
   [root@client ~]# grep ipa_server /etc/sssd/sssd.conf
   ipa_server = _srv_, master.example.com
   ```

   b. IdM クライアントが **/etc/sssd/sssd.conf** で特定の IdM サーバーを使用するようにハードコーディングされている場合は、**ipa_server** エントリーが適切に動作する IdM サーバーを参照するようにしてください。

```
[root@client ~]# grep ipa_server /etc/sssd/sssd.conf
ipa_server = working-master.example.com
```

4. **SSSD のキャッシュされた情報を消去** します。

   - SSSD キャッシュには、失われたサーバーに関連する古い情報が含まれる場合があります。認証に一貫性がない場合は、SSSD キャッシュをパージします。

     ```
     [root@client ~]# sss_cache -E
     ```

検証手順

1. Kerberos TGT (Ticket-Granting-Ticket) を IdM ユーザーとして取得して、Kerberos 設定を確認します。

```
[root@client ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@client ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 18:44:58  11/25/2019 18:44:55  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. IdM ユーザー情報を取得して、SSSD 設定を確認します。

```
[root@client ~]# id admin
uid=1965200000(admin) gid=1965200000(admins) groups=1965200000(admins)
```