Red Hat Enterprise Linux 8

对身份管理系统进行灾难恢复

在服务器或数据丢失后恢复 IdM

Last Updated: 2024-06-28

Red Hat Enterprise Linux 8 对身份管理系统进行灾难恢复

在服务器或数据丢失后恢复 IdM

法律通告

摘要

服务器和数据丢失场景（例如因为硬件故障）是 IT 环境中的最大风险。如果在 Red Hat Identity Management (IdM)环境中出现这样的事件，恢复过程取决于问题类型、IdM 拓扑以及缓解此类情况所采取的操作。 例如，您可以在 IdM 复制拓扑中恢复单个和多个服务器，您可以使用 IdM 备份和快照恢复数据。在恢复期间或之后，可能需要调整客户端设置，如 DNS 服务器和 Kerberos 配置。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。帮助我们如何进行改进。

通过 Jira 提交反馈（需要帐户）

1. 登录到 Jira 网站。
2. 单击顶部导航栏中的 **Create**。
3. 在 **Summary** 字段中输入描述性标题。
4. 在 **Description** 字段中输入您的建议以改进。包括文档相关部分的链接。
5. 点对话框底部的 **Create**。

第 1 章 IDM 中的灾难情况

灾难情境主要有两种： *服务器丢失*和*数据丢失*。

表 1.1. 服务器丢失和数据丢失

灾难类型	原因示例	如何响应
服务器丢失 ：IdM 部署丢失了一个或多个服务器。	• 硬件故障	• 使用复制恢复单个服务器
数据丢失 ：一个服务器上的 IdM 数据被意外修改，其变化传播到其他服务器中。	• 用户意外删除数据 • 软件错误修改数据	• 使用虚拟机快照恢复数据丢失 • 使用 IdM 备份恢复数据丢失 • 管理数据丢失

第 2 章 使用复制恢复单个服务器

如果单个服务器有严重问题或已丢失，则具有多个副本可确保您创建替换副本，并快速恢复之前冗余级别。

如果您的 IdM 拓扑包含集成的证书颁发机构 (CA)，删除和替换已损坏的副本的步骤因 CA 续订服务器和其它副本而异。

2.1. 恢复丢失 CA 续订服务器

如果证书颁发机构 (CA) 续订服务器丢失，您必须首先推广另一个 CA 副本以满足 CA 续订服务器角色，然后部署替代的 CA 副本。

先决条件

- 您的部署使用 IdM 的内部证书颁发机构 (CA)。
- 环境中的另一个 Replica 已安装了 CA 服务。

警告

如果出现以下情况，IdM 部署是不可恢复的：

1. CA 续订服务器已经丢失。
2. 没有安装 CA。
3. 没有带有 CA 角色的副本备份。
   使用 CA 角色从副本制作备份非常重要，从而使证书数据受到保护。有关创建备份和从备份恢复的更多信息，请参阅 使用 IdM 备份为数据丢失做准备。

流程

1. 从环境中的另一个副本中，升级环境中的另一个 CA 副本，以作为新的 CA 续订服务器。请参阅更改和重置 IdM CA 续订服务器。
2. 从环境中的另一个副本中，将复制协议删除丢失的 CA 续订服务器。请参阅使用 CLI 从拓扑中删除服务器。
3. 安装一个新的 CA Replica 来替换丢失的 CA 副本。请参阅使用 CA 安装 IdM 副本 。
4. 更新 DNS 以反应副本拓扑的更改。如果使用 IdM DNS，则会自动更新 DNS 服务记录。
5. 验证 IdM 客户端可访问 IdM 服务器。请参阅在恢复过程中调整 IdM 客户端。

验证步骤

1. 以 IdM 用户身份成功检索 Kerberos Ticket-Granting-Ticket 在新副本中测试 Kerberos 服务器。

```
[root@server ~]# kinit admin
```

```
Password for admin@EXAMPLE.COM:

[root@server ~]# 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/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 通过检索用户信息，测试 Directory 服务器和 SSSD 配置。

```
[root@server ~]# 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. 使用 **ipa cert-show** 命令测试 CA 配置。

```
[root@server ~]# 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
```

其他资源

- 使用 IdM CA 续订服务器

2.2. 从丢失一个常规副本的情况下进行恢复

要替换不是证书颁发机构 (CA) 续订服务器的副本，请从拓扑中删除丢失的副本，并在该位置安装一个新的副本。

先决条件

- CA 续订服务器正在正确运行。如果 CA 续订服务器丢失，请参阅恢复丢失 CA 续订服务器。

流程

1. 删除丢失的服务器的复制协议。请参阅卸载 IdM 服务器。

2. 使用所需服务（CA、KRA、DNS）部署新副本。请参阅 安装 IdM 副本。
3. 更新 DNS 以反应副本拓扑的更改。如果使用 IdM DNS，则会自动更新 DNS 服务记录。
4. 验证 IdM 客户端可访问 IdM 服务器。请参阅在恢复过程中调整 IdM 客户端。

验证步骤

1. 以 IdM 用户身份成功检索 Kerberos Ticket-Granting-Ticket 在新副本中测试 Kerberos 服务器。

```
[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/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 通过检索用户信息，测试新副本上的 Directory 服务器和 SSSD 配置。

```
[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
```

第 3 章 使用复制恢复多个服务器

如果同时缺少多个服务器，请确定通过查看以下五种情况之一来重建环境。

3.1. 在一个无 CA 的部署中从丢失多个服务器的情况下进行恢复

无 CA 中的服务器都大致相等，因此您可以以任何顺序删除并替换丢失的副本来重建环境。

先决条件

- 您的部署使用了外部证书颁发机构 (CA)。

流程

- 请参阅恢复丢失常规副本。

3.2. 当 CA 续订服务器未被破坏时，从丢失了多个服务器的情况下进行恢复

如果 CA 续订服务器没有问题，您可以按任何顺序替换其他服务器。

先决条件

- 您的部署使用 IdM 内部证书颁发机构 (CA)。

流程

- 请参阅恢复丢失常规副本。

3.3. 从丢失 CA 续订服务器和其它服务器的情况下进行恢复

如果您丢失了 CA 续订服务器和其他服务器，请在替换其他副本前将另一个 CA 服务器提升到 CA 续订服务器角色。

先决条件

- 您的部署使用 IdM 内部证书颁发机构 (CA)。
- 至少一个 CA 副本没有被破坏。

流程

1. 提升另一个 CA 副本以满足 CA 续订服务器角色。请参阅恢复丢失 CA 续订服务器。
2. 替换所有其他丢失的副本。请参阅恢复丢失常规副本。

3.4. 从丢失所有 CA 副本的情况下进行恢复

如果没有任何证书颁发机构 (CA) 副本，IdM 环境将会丢失部署额外副本并重建自身的能力。

先决条件

- 您的部署使用 IdM 内部证书颁发机构 (CA)。

流程

- 这个情形是完全丢失的情况。

其他资源

- 要准备整个基础架构丢失，请参阅准备使用虚拟机快照的数据丢失。

3.5. 从整个基础架构丢失的情况中进行恢复

如果所有服务器同时丢失，且没有用于恢复的虚拟机快照或数据备份，则这种情况无法进行恢复。

流程

- 这个情形是完全丢失的情况。

其他资源

- 准备使用虚拟机快照进行数据丢失。

第 4 章 使用虚拟机快照恢复数据丢失

如果发生数据丢失事件，您可以恢复证书颁发机构 (CA) 副本的虚拟机 (VM) 快照来修复丢失的数据，或者从其中部署新环境。

4.1. 只从虚拟机快照中恢复

如果灾难影响所有 IdM 服务器，且只存在 IdM CA 副本虚拟机 (VM) 的快照，您可以通过删除对丢失的服务器的所有引用并安装新副本来重新创建部署。

先决条件

- 您已准备了 CA 副本虚拟机的虚拟机快照。请参阅使用虚拟机快照准备数据丢失的情况。

流程

1. 引导 CA 副本虚拟机所需的快照。
2. 将复制协议删除任何丢失的副本。

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

3. 安装第二个 CA 副本。请参阅 安装 IdM 副本。
4. VM CA 副本现在是 CA 续订服务器。红帽建议在环境中提升另一个 CA 副本，以充当 CA 续订服务器。请参阅更改和重置 IdM CA 续订服务器。
5. 通过部署带有所需服务（CA、DNS）的额外副本来重新创建所需的副本拓扑。请参阅安装 IdM 副本
6. 更新 DNS 以反应新的副本拓扑。如果使用 IdM DNS，则会自动更新 DNS 服务记录。
7. 验证 IdM 客户端可访问 IdM 服务器。请参阅在恢复过程中调整 IdM 客户端。

验证步骤

1. 以 IdM 用户身份成功检索 Kerberos ticket-granting ticket，在每个副本中测试 Kerberos 服务器。

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

[root@server ~]# 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/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 通过检索用户信息，测试每个副本上的 Directory 服务器和 SSSD 配置。

```
[root@server ~]# 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. 使用 **ipa cert-show** 命令测试每个 CA 副本上的 CA 服务器。

```
[root@server ~]# 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
```

其他资源

- 规划副本拓扑。

4.2. 在部分工作环境中从虚拟机快照中恢复

如果灾难会影响一些 IdM 服务器，而其他 IdM 服务器仍然可以正常工作，您可能需要将部署恢复到虚拟机 (VM) 快照中捕获的状态。例如，如果所有证书颁发机构 (CA) 副本都丢失，其他副本仍在正常工作，则需要将 CA 副本重新置于环境中。

在这种情况下，删除对丢失的副本的引用，从快照中恢复 CA 副本，验证复制和部署新副本。

先决条件

- 您已准备了 CA 副本虚拟机的虚拟机快照。请参阅使用虚拟机快照准备数据丢失的情况。

流程

1. 删除到丢失的服务器的复制协议。请参阅卸载 IdM 服务器。
2. 引导 CA 副本虚拟机所需的快照。
3. 在恢复的服务器和任何丢失的服务器间删除所有复制协议。

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

4. 如果恢复的服务器对仍在生产中的任何服务器没有复制协议，请使用其它一个服务器连接恢复的服务器，以更新恢复的服务器。

```
[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. 查看 **/var/log/dirsrv/slapd-YOUR-INSTANCE/errors** 中的 Directory 服务器错误日志，以查看快照中的 CA 副本是否与剩余的 IdM 服务器正确同步。

6. 如果因为数据库太旧导致在恢复的服务器上复制失败，则重新初始化恢复的服务器。

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

7. 如果恢复的服务器上的数据库已被正确同步，请按照安装 IdM 副本的内容，使用所需服务（CA、DNS）部署额外副本来继续。

验证步骤

1. 以 IdM 用户身份成功检索 Kerberos ticket-granting ticket，在每个副本中测试 Kerberos 服务器。

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

[root@server ~]# 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/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 通过检索用户信息，测试每个副本上的 Directory 服务器和 SSSD 配置。

```
[root@server ~]# 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. 使用 **ipa cert-show** 命令测试每个 CA 副本上的 CA 服务器。

```
[root@server ~]# 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
```

其他资源

- 从虚拟机快照恢复以建立新的 IdM 环境

4.3. 从虚拟机快照恢复以建立新的 IDM 环境

如果来自恢复的虚拟机 (VM) 快照中的证书颁发机构 (CA) 副本无法在其他服务器中复制，请从虚拟机快照创建一个新的 IdM 环境。

要建立新的 IdM 环境，隔离虚拟机服务器，从其中创建额外的副本，并将 IdM 客户端切换到新环境。

先决条件

- 您已准备了 CA 副本虚拟机的虚拟机快照。请参阅使用虚拟机快照准备数据丢失的情况。

流程

1. 引导 CA 副本虚拟机所需的快照。
2. 通过移除所有复制拓扑片段，将恢复的服务器与当前部署的其余部分隔离。
   a. 首先，显示所有 **domain** 复制拓扑片段。

```
[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. 接下来，删除涉及恢复的服务器的每个 **domain** 拓扑片段。

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

c. 最后，在任何 **ca** 拓扑片段中执行相同的操作。

```
[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. 从恢复的服务器安装足够数量的 IdM 副本来处理部署负载。现在，有两个断开连接的 IdM 部署并行运行。

4. 通过对新 IdM 副本进行硬编码引用，将 IdM 客户端切换为使用新部署。请参阅在恢复过程中调整 IdM 客户端。

5. 停止并卸载之前部署中的 IdM 服务器。请参阅卸载 IdM 服务器。

验证步骤

1. 以 IdM 用户身份成功检索 Kerberos ticket-granting ticket，在每个新副本中测试 Kerberos 服务器。

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

[root@server ~]# 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/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 通过检索用户信息，测试每个新副本上的 Directory 服务器和 SSSD 配置。

```
[root@server ~]# 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. 使用 **ipa cert-show** 命令测试每个新 CA 副本上的 CA 服务器。

```
[root@server ~]# 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
```

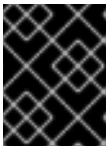
第 5 章 使用 IDM 备份恢复数据丢失

您可以使用 **ipa-restore** 工具将 IdM 服务器恢复到 IdM 备份中捕获的以前的状态。

5.1. 从 IDM 备份中恢复的时间

您可以通过从 IdM 备份中恢复来响应几个灾难情况：

- **对 LDAP 内容进行了不必要的更改**：条目被修改或删除，在整个部署过程中复制这些更改，您希望恢复这些更改。仅恢复数据备份会将 LDAP 条目返回到之前的状态，而不影响 IdM 配置本身。
- **基础架构全部出问题或所有 CA 实例都丢失** ：如果灾难破坏了所有证书颁发机构副本，部署会失去通过部署其他服务器来重建自身的能力。在这种情况下，恢复 CA 副本的备份并从中构建新副本。
- **在隔离服务器上进行升级失败**：操作系统可以正常工作，但 IdM 数据被破坏，因此您想要将 IdM 系统恢复到已知良好状态的原因。红帽建议与技术支持合作，来诊断和排除此问题。如果这些步骤失败，则从全服务器备份中恢复。



重要

硬件或升级失败的首选解决方案是从副本中重建丢失的服务器。如需更多信息，请参阅 使用复制恢复单个服务器。

5.2. 从 IDM 备份中恢复时的注意事项

如果您使用 **ipa-backup** 工具创建的备份，您可以将 IdM 服务器或 LDAP 内容恢复到执行备份时所处的状态。

以下是从 IdM 备份中恢复时的主要注意事项：

- 您只能在符合最初创建备份的服务器配置的服务器中恢复备份。服务器**必**须具有：
  - 相同的主机名
  - 相同的 IP 地址
  - 同一版本的 IdM 软件
- 如果很多 IdM 服务器被恢复，恢复的服务器就成为 IdM 的唯一信息来源。其它服务器**必**须从恢复的服务器中重新初始化。
- 由于上次备份后创建的任何数据都将丢失，请不要使用备份和恢复解决方案进行正常系统维护。
- 如果服务器丢失，红帽建议重新构建服务器，方法是将其重新安装为副本，而不是从备份中恢复。创建新副本可保留当前工作环境中的数据。如需更多信息，请参阅准备使用复制进行服务器丢失。
- 备份和恢复功能只能从命令行管理，且在 IdM Web UI 中不可用。
- 您无法从位于 **/tmp** 或 **/var/tmp** 目录中的备份文件恢复。IdM 目录服务器使用 **PrivateTmp** 目录，且无法访问操作系统通常可用的 **/tmp** 或 **/var/tmp** 目录。

提示

从备份中恢复需要目标主机上安装的软件 (RPM) 版本与执行备份时安装的版本相同。因此，红帽建议从虚拟机快照而不是备份中恢复。如需更多信息，请参阅使用虚拟机快照恢复数据丢失。

5.3. 从备份中恢复 IDM 服务器

从 IdM 备份中恢复 IdM 服务器或其 LDAP 数据。

图 5.1. 本例中使用的复制拓扑

表 5.1. 本例中使用的服务器命名惯例

服务器主机名	功能
server1.example.com	需要从备份中恢复的服务器。
caReplica2.example.com	连接到 **server1.example.com** 主机的证书颁发机构 (CA) 副本。
replica3.example.com	连接到 **caReplica2.example.com** 主机的副本。

先决条件

- 您已使用 **ipa-backup** 工具为 IdM 服务器生成全服务器或者仅数据备份。请参阅 创建备份。
- 您的备份文件不在 **/tmp** 或 **/var/tmp** 目录中。
- 在从全服务器备份中执行全服务器恢复前，请从服务器中 卸载 IdM，并使用之前相同的服务器配置重新安装 IdM。

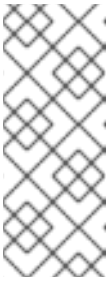
流程

1. 使用 **ipa-restore** 程序恢复全服务器或仅数据备份。
   - 如果备份目录位于默认 **/var/lib/ipa/backup/** 位置，则只输入目录名称：

     ```
     [root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
     ```

   - 如果备份目录不在默认位置，请输入其完整路径：

     ```
     [root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
     ```



注意

ipa-restore 实用程序自动检测该目录包含的备份类型，并且默认执行同类型的恢复。要从全服务器备份中只执行数据恢复，在 **ipa-restore** 命令中添加 **--data** 选项：

```
[root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
```

2. 输入 Directory Manager 密码。

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

3. 输入 **yes** 以确认备份中的当前数据覆盖。

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
server1.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** 工具禁用所有可用服务器的复制：

```
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 server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

然后该工具将停止 IdM 服务，恢复备份并重启服务：

```
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. 重新初始化连接到恢复的服务器的所有副本：

   a. 列出 **domai** 后缀的所有复制拓扑片段，记录涉及恢复的服务器的拓扑片段。

```
[root@server1 ~]# ipa topologysegment-find domain
```

```
------------------
2 segments matched
------------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.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. 使用恢复的服务器重新初始化所有拓扑片段的 **domai** 后缀。
在本例中，使用来自 **server1** 的数据对 **caReplica2** 进行重新初始化。

```
[root@caReplica2 ~]# ipa-replica-manage re-initialize --from=server1.example.com
Update in progress, 2 seconds elapsed
Update succeeded
```

c. 继续到证书颁发机构数据，列出 **ca** 后缀的所有复制拓扑片段。

```
[root@server1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

d. 重新初始化连接到恢复的服务器的所有 CA 副本。
在本例中，使用来自 **server1** 的数据执行 **caReplica2** 的 **csreplica** 重新初始化。

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=server1.example.com
Directory Manager password:

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

6. 继续进入复制拓扑，重新初始化连续的副本，直到所有服务器都已使用恢复的服务器 **server1.example.com** 的数据进行更新。
在本例中，我们只需要使用 **caReplica2** 中的数据在 **replica3** 上重新初始化 **domai** 后缀。

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

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

7. 清除每台服务器上 SSSD 的缓存，以避免因为数据无效而导致的身份验证问题：

   a. 停止 SSSD 服务：

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

   b. 从 SSSD 中删除所有缓存的内容：

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

   c. 启动 SSSD 服务：

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

   d. 重启服务器。

其他资源

- **ipa-restore(1)** man page 还详细介绍了如何在恢复期间处理复杂复制方案。

5.4. 从加密备份中恢复

这个过程从加密的 IdM 备份恢复 IdM 服务器。**ipa-restore** 工具会自动检测 IdM 备份是否已加密，并使用 GPG2 根密钥环恢复它。

先决条件

- GPG 加密的 IdM 备份。请参阅 创建加密的 IdM 备份。
- LDAP Directory Manager 密码
- 创建 GPG 密钥时使用的口令

流程

1. 如果您在创建 GPG2 密钥时使用了自定义密钥环位置，请验证 **$GNUPGHOME** 环境变量是否被设置为该目录。请参阅 创建 GPG2 密钥。

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

2. 为 **ipa-restore** 实用程序提供备份目录位置。

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

   a. 输入 Directory Manager 密码。

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

   b. 输入您创建 GPG 密钥时使用的密码短语。

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

3. 重新初始化连接到恢复的服务器的所有副本。请参阅从备份中恢复 IdM 服务器。

第 6 章 使用 ANSIBLE PLAYBOOK 恢复 IDM 服务器

使用 **ipabackup** Ansible 角色，您可以自动从备份中恢复 IdM 服务器，并在服务器和 Ansible 控制器之间传输备份文件。

本节涵盖了以下主题：

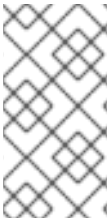
- 准备 Ansible 控制节点来管理 IdM
- 使用 Ansible 从服务器中存储的备份中恢复 IdM 服务器
- 使用 Ansible 从 Ansible 控制器中存储的备份中恢复 IdM 服务器
- 使用 Ansible 将 IdM 服务器的备份复制到 Ansible 控制器
- 使用 Ansible 将 IdM 服务器的备份从 Ansible 控制器复制到 IdM 服务器
- 使用 Ansible 从 IdM 服务器中删除备份

6.1. 准备 ANSIBLE 控制节点来管理 IDM

作为管理身份管理 (IdM) 的系统管理员，在使用 Red Hat Ansible Engine 时，最好执行以下操作：

- 在您的主目录中，创建专用于 Ansible playbook 的子目录，如 **~/MyPlaybooks**。
- 将示例 Ansible playbook 从 **/usr/share/doc/ansible-freeipa/*** 和 **/usr/share/doc/rhel-system-roles/*** 目录以及它们的子目录复制到 **~/MyPlaybooks** 目录中并进行调整。
- 将清单文件包含在 **~/MyPlaybooks** 目录中。

按照这种做法，您可以在一个地方找到所有 playbook，您可以在不调用 root 特权的情况下运行 playbook。



注意

您只需要受管主机上的 **root** 权限来执行 **ipaserver**、**ipareplica**、**ipaclient**、**ipabackup**、**ipasmartcard_server** 和 **ipasmartcard_client ansible-freeipa** 角色。这些角色需要具有目录和 **dnf** 软件包管理器的特权访问权限。

按照以下流程创建 **~/MyPlaybooks** 目录并进行配置，以便您可以使用它来存储和运行 Ansible playbook。

先决条件

- 您已在受管节点上安装了 IdM 服务器 *server.idm.example.com* 和 *replica.idm.example.com*。
- 您已配置了 DNS 和网络，以便您可以直接从控制节点登录到受管节点 *server.idm.example.com* 和 *replica.idm.example.com*。
- 您需要知道 IdM **admin** 密码。

步骤

1. 在主目录中为您的 Ansible 配置和 playbook 创建目录：

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

2. 进入 **~/MyPlaybooks/** 目录：

```
$ cd ~/MyPlaybooks
```

3. 使用以下内容创建 **~/MyPlaybooks/ansible.cfg** 文件：

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

[privilege_escalation]
become=True
```

4. 使用以下内容创建 **~/MyPlaybooks/inventory** 文件：

```
[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
```

此配置定义了两个主机组，即 **eu** 和 **us**，用于这些位置中的主机。此外，此配置定义了 **ipaserver** 主机组，它包含来自 **eu** 和 **us** 组的所有主机。

5. [可选] 创建 SSH 公钥和私钥。要在测试环境中简化访问，请不要在私钥中设置密码：

```
$ ssh-keygen
```

6. 将 SSH 公钥复制到每个受管节点上的 IdM **admin** 帐户：

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

输入这些命令时，您必须输入 IdM **admin** 密码。

其他资源

- 使用 Ansible playbook 安装身份管理服务器。

- 如何构建清单。

6.2. 使用 ANSIBLE 从服务器中存储的备份中恢复 IDM 服务器

您可以使用 Ansible playbook 从该主机上存储的备份中恢复 IdM 服务器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，作为 IdM 客户端、服务器或副本的一部分。
- 您知道 LDAP Directory Manager 密码。

流程

1. 进入 **~/MyPlaybooks/** 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成一个 **restore-server.yml** 文件的副本：

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

3. 打开 **restore-my-server.yml** Ansible playbook 文件以进行编辑。
4. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. 将 **ipabackup_name** 变量设置为要恢复的 **ipabackup** 的名称。
   c. 将 **ipabackup_password** 变量设置为 LDAP Directory Manager 密码。

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

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>
```

```
roles:
- role: ipabackup
  state: restored
```

5. 保存该文件。

6. 运行指定清单文件和 playbook 文件的 Ansible playbook：

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

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.3. 使用 ANSIBLE 从 ANSIBLE 控制器中存储的备份中恢复 IDM 服务器

您可以使用 Ansible playbook 从 Ansible 控制器中存储的备份中恢复 IdM 服务器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，作为 IdM 客户端、服务器或副本的一部分。
- 您知道 LDAP Directory Manager 密码。

流程

1. 进入 **~/MyPlaybooks/** 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成一个 **restore-server-from-controller.yml** 文件的副本：

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

3. 打开 **restore-my-server-from-my-controller.yml** 文件进行编辑。

4. 通过设置以下变量来调整文件：

a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

b. 将 **ipabackup_name** 变量设置为要恢复的 **ipabackup** 的名称。

c. 将 **ipabackup_password** 变量设置为 LDAP Directory Manager 密码。

```
---
- name: Playbook to restore IPA server from controller
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>
    ipabackup_from_controller: true

  roles:
  - role: ipabackup
    state: restored
```

5. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

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

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.4. 使用 ANSIBLE 将 IDM 服务器的备份复制到 ANSIBLE 控制器

您可以使用 Ansible playbook 将 IdM 服务器的备份从 IdM 服务器复制到 Ansible 控制器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，作为 IdM 客户端、服务器或副本的一部分。

流程

1. 若要存储备份，请在 Ansible 控制器上的主目录中创建一个子目录。

```
$ mkdir ~/ipabackups
```

2. 进入 **~/MyPlaybooks/** 目录：

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

3. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **copy-backup-from-server.yml** 文件的副本：

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

4. 打开 **copy-my-backup-from-my-server-to-my-controller.yml** 文件进行编辑。

5. 通过设置以下变量来调整文件：

   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

   b. 将 **ipabackup_name** 变量设置为 IdM 服务器上的 **ipabackup** 的名称，以复制到您的 Ansible 控制器。

   c. 默认情况下，备份存储在 Ansible 控制器的当前工作目录中。要指定在第 1 步中创建的目录，请添加 **ipabackup_controller_path** 变量并将其设置为 **/home/user/ipabackups** 目录。

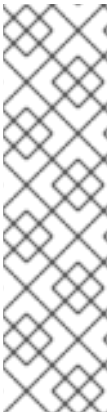
```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_to_controller: true
    ipabackup_controller_path: /home/user/ipabackups

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

6. 保存该文件。

7. 运行 Ansible playbook，指定清单文件和 playbook 文件：

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



注意

要将**所有** IdM 备份复制到控制器，请将 Ansible playbook 中的 **ipabackup_name** 变量设置为 **all** ：

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

例如，请参阅 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **copy-all-backups-from-server.yml** Ansible playbook。

验证步骤

- 验证备份是否位于 Ansible 控制器上的 **/home/user/ipabackups** 目录中：

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

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.5. 使用 ANSIBLE 将 IDM 服务器的备份从 ANSIBLE 控制器复制到 IDM 服务器

您可以使用 Ansible playbook 将 IdM 服务器的备份从 Ansible 控制器复制到 IdM 服务器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，作为 IdM 客户端、服务器或副本的一部分。

流程

1. 进入 **~/MyPlaybooks/** 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **copy-backup-from-controller.yml** 文件的副本：

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

3. 打开 **copy-my-backup-from-my-controller-to-my-server.yml** 文件进行编辑。
4. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. 将 **ipabackup_name** 变量设置为 Ansible 控制器上 **ipabackup** 的名称，以复制到 IdM 服务器。

```
---
- 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. 保存该文件。
6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

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

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

6.6. 使用 ANSIBLE 从 IDM 服务器中删除备份

您可以使用 Ansible playbook 从 IdM 服务器中删除备份。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。

- 目标节点（这是执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，作为 IdM 客户端、服务器或副本的一部分。

流程

1. 进入 ~/MyPlaybooks/ 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **remove-backup-from-server.yml** 文件的副本：

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

3. 打开 **remove-backup-from-my-server.yml** 文件以进行编辑。

4. 通过设置以下变量来调整文件：

   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

   b. 将 **ipabackup_name** 变量设置为 **ipabackup** 的名称，以从 IdM 服务器中删除。

```
---
- 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. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

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

注意

要从 IdM 服务器中删除**所有** IdM 备份，将 Ansible playbook 中的 **ipabackup_name** 变量设置为 **all** ：

```
vars:
  ipabackup_name: all
```

作为一个示例，请参阅 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **remove-all-backups-from-server.yml** Ansible playbook。

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

第 7 章 管理数据丢失

对数据丢失事件的正确响应取决于受影响的副本数量以及丢失数据的副本数。

7.1. 隔离数据丢失

发生数据丢失事件时，通过立即隔离受影响的服务器来最小化数据丢失。然后，从未影响环境的剩余部分创建替代副本。

先决条件

- 带有多个副本的强大 IdM 复制拓扑。请参阅通过使用复制来为服务器丢失的情况做准备。

流程

1. 要限制复制数据丢失，请移除其复制拓扑片段，断开所有受影响的副本与拓扑的其余部分的连接。

   a. 显示不是中的所有 **domain** 复制拓扑片段。

   ```
   [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. 删除所有涉及到受影响服务器的 **domain** 拓扑片段。

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

   c. 对涉及任何受影响的服务器的任何 **ca** 拓扑片段执行同样的操作。

   ```
   [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. 受数据丢失影响的服务器必须被取消。要创建替换副本，请参阅使用复制恢复多个服务器。

7.2. 在所有服务器中的有限数据丢失

数据丢失事件可能会影响环境中的所有副本，如在所有服务器间执行意外删除操作。如果数据丢失是已知的且有限，请手动重新添加丢失数据。

先决条件

- 包含丢失数据的 IdM 服务器的虚拟机 (VM) 快照或 IdM 备份。

流程

1. 如果您需要查看任何丢失数据，请将虚拟机快照或备份到单独的网络上的隔离服务器。
2. 使用 **ipa** 或 **ldapadd** 命令，将缺少的信息添加到数据库中。

其他资源

- 使用虚拟机快照恢复数据丢失。
- 备份和恢复 IdM。

7.3. 在所有服务器中的未定义的数据丢失

如果数据丢失严重或未定义，请从服务器的虚拟机 (VM) 快照部署新环境。

先决条件

- 虚拟机 (VM) 快照包含丢失的数据。

流程

1. 将 IdM 证书颁发机构 (CA) 复制从虚拟机快照恢复到已知良好状态，并从中部署新的 IdM 环境。请参阅只恢复虚拟机快照。
2. 添加在使用 **ipa** 或 **ldapadd** 命令进行快照后创建的任何数据。

其他资源

- 使用虚拟机快照恢复数据丢失。

第 8 章 在恢复过程中调整 IDM 客户端

当 IdM 服务器被恢复时，您可能需要调整 IdM 客户端来反映副本拓扑中的更改。

流程

1. **调整 DNS 配置 ：**

   a. 如果 **/etc/hosts** 包含对 IdM 服务器的任何引用，请确保硬编码的 IP 到主机名映射有效。

   b. 如果 IdM 客户端使用 IdM DNS 进行名称解析，请确保 **/etc/resolv.conf** 中的 **nameserver** 条目指向提供 DNS 服务的工作 IdM 副本。

2. **调整 Kerberos 配置 ：**

   a. 默认情况下，IdM 客户端会查找 Kerberos 服务器的 DNS 服务记录，并将调整到副本拓扑中的更改：

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

   b. 如果 IdM 客户端已被硬编码为使用 **/etc/krb5.conf** 中的特定 IdM 服务器：

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

   确保 **/etc/krb5.conf** 中的 **kdc**、**master_kdc** 和 **admin_server** 条目指向正常工作的 IdM 服务器：

   ```
   [realms]
    EXAMPLE.COM = {
     kdc = functional-server.example.com:88
     master_kdc = functional-server.example.com:88
     admin_server = functional-server.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. **调整 SSSD 配置 ：**

   a. 默认情况下，IdM 客户端会查找 LDAP 服务器的 DNS 服务记录，并调整副本拓扑中的更改：

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

   b. 如果 IdM 客户端已被硬编码为使用 **/etc/sssd/sssd.conf** 中的特定 IdM 服务器，请确保 **ipa_server** 条目指向正常工作的 IdM 服务器：

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

4. **清除 SSSD 的缓存信息 ：**

   - SSSD 缓存可能包含与丢失服务器相关的过时的信息。如果用户遇到不一致的身份验证问

题，请清除 SSSD 缓存：

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

验证步骤

1. 以 IdM 用户身份检索 Kerberos Ticket-Granting-Ticket 来验证 Kerberos 配置。

```
[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. 通过检索 IdM 用户信息来验证 SSSD 配置。

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