Red Hat Enterprise Linux 8

对身份管理系统进行灾难恢复

在影响到身份管理部署的灾难中进行恢复的文档

Last Updated: 2021-06-07

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

在影响到身份管理部署的灾难中进行恢复的文档

法律通告

摘要

本文档论述了使用复制、虚拟机快照和备份对身份管理部署中的服务器或数据丢失的响应。

目录

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。如需了解更多详细信息，请参阅 CTO Chris Wright 信息。

在身份管理中,计划使用的术语替换包括：

- ***块列表*** 替换 *黑名单*
- ***允许列表*** 替换 *白名单*
- ***从属(secondary)***替换 *slave*
- 根据上下文, *master* 将被更精确地替换为更精确的语言：
  - ***IdM 服务器*** 替换 *IdM master*
  - ***CA 续订服务器*** 替换 *CA 续订 master*
  - ***CRL publisher 服务器*** 替换 *CRL master*
  - ***多供应商*** 替换了 *multi-master*

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要提交更复杂的反馈，请创建一个 Bugzilla ticket：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

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	• 第 2 章 *使用复制恢复服务器丢失*
数据丢失: 在服务器中意外修改 IdM 数据,并将更改传播到其他服务器。	• 用户意外删除数据 • 软件错误修改数据	• 第 3 章 *使用虚拟机快照恢复数据丢失* • 第 4 章 *使用 IdM 备份恢复数据丢失* • 第 5 章 *管理数据丢失*

第 2 章 使用复制恢复服务器丢失

如果服务器被严重破坏或丢失,具有多个副本可确保您创建替换副本,并快速恢复以前的冗余级别。

如果您的 IdM 拓扑包含集成证书颁发机构(CA),删除和替换损坏的副本的步骤会因 CA 续订服务器和其他副本的不同。

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,您必须首先提升另一个 CA 副本来满足 CA 续订服务器角色,然后部署替换的 CA 副本。

先决条件

- 您的部署使用 IdM 内部证书颁发机构(CA)。
- 环境中的另一个 Replica 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。
   务必要从带有 CA 角色的副本进行备份,以便保护证书数据。有关创建和恢复备份的更多信息，请参阅准备使用 IdM 备份数据丢失。

流程

1. 将复制协议删除丢失的 CA 续订服务器。请参阅卸载 IdM 服务器。
2. 在环境中升级另一个 CA Replica 以作为新的 CA 续订服务器。请参阅更改和重置 IdM CA Renewal Master。
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. 通过检索用户信息来测试 Directory Server 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
```

其它资源

- 有关 IdM CA 续订服务器的更多信息,请参阅 使用 IdM CA 续订服务器

2.2. 恢复丢失常规副本

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,并安装新副本。

先决条件

- CA 续订服务器可以正常工作。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. 将复制协议删除丢失的服务器。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,在新副本中测试 Directory Server 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
```

2.3. 恢复丢失多个服务器

如果同时丢失多个服务器,请通过查看以下五个场景中的一个适用于您的情况来确定环境是否可以重建。

2.3.1. 在无 CA 部署中恢复丢失多个服务器

无 CA 部署中的服务器都被视为相等,您可以以任何顺序删除和替换丢失的副本来重建环境。

流程

- 请参阅 恢复丢失常规副本。

2.3.2. 当 CA 续订服务器解压时,恢复丢失多个服务器

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。

2.3.3. 恢复丢失 CA 续订服务器和其它服务器

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 副本是不正确的。

流程

1. 提升另一个 CA 副本以实现 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。

2.3.4. 恢复丢失所有 CA 副本

如果没有证书颁发机构(CA)副本,IdM 环境便无法部署额外副本并重建其自身。

先决条件

- 您的部署使用 IdM 内部证书颁发机构(CA)。

流程

- 这种情形是一个完全丢失。

其它资源

- 要准备总基础架构丢失,请参阅 准备使用虚拟机快照数据丢失。

2.3.5. 从基础架构丢失总量中恢复

如果所有服务器都同时丢失,且没有虚拟机(VM)快照或数据备份来恢复,这种情况将无法恢复。

流程

- 这种情形是一个完全丢失。

其它资源

- 要准备总基础架构丢失,请参阅 准备使用虚拟机快照数据丢失。

第 3 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)副本的虚拟机快照(VM)快照来修复丢失的数据,或者从中部署新环境。

3.1. 仅从虚拟机快照中恢复

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

先决条件

- 您已准备 CA 副本虚拟机的虚拟机快照。请参阅 准备使用虚拟机快照数据丢失。

流程

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

```
[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。请参阅使用 CA 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 副本以作为 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 客户端是否可以访问 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,在每个副本上测试 Directory Server 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
```

其它资源

- 有关复制拓扑最佳实践,请参阅 规划副本拓扑。

3.2. 在部分工作的环境中从虚拟机快照中恢复

如果灾难影响一些 IdM 服务器,而其他服务器仍处于正常工作状态,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,其他副本仍在生产中,则需要将 CA 副本放回到环境中。

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 CA 副本虚拟机的虚拟机快照。请参阅 准备使用虚拟机快照数据丢失。

流程

1. 将所有复制协议删除到丢失的服务器中。请参阅卸载 IdM 服务器。
2. 引导 CA 副本虚拟机所需的快照。
3. 删除恢复的服务器和丢失的服务器之间的任何复制协议。

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

4. 如果恢复的服务器没有与仍在生产中的服务器的复制协议,请将恢复的服务器连接到恢复的服务器中,以便更新恢复的服务器。

```
[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** 的 Directory Server 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. 如果恢复的服务器上的复制失败,因为其数据库太过时,请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被正确同步,请根据 安装 IdM 副本来继续使用所需服务（CA、DNS）的额外副本。

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,在每个副本上测试 Directory Server 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
```

其它资源

- 如果恢复的 CA 副本上的数据库没有同步或重新初始化,请从恢复的 CA Replica 创建新部署并切换到新环境。请参阅从虚拟机快照中恢复以建立新的 IdM 环境。

3.3. 从虚拟机快照中恢复以建立新的 IDM 环境

如果恢复的虚拟机(VM)快照中的证书颁发机构(CA)副本无法与其他服务器复制,请从虚拟机快照创建一个新的 IdM 环境。

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

先决条件

- 您已准备 CA 副本虚拟机的虚拟机快照。请参阅 准备使用虚拟机快照数据丢失。

流程

1. 引导 CA 副本虚拟机所需的快照。
2. 通过删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,删除每个涉及恢复的服务器的 **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,使用任何 **ca** 拓扑片段执行相同的操作。

```
[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,以处理部署负载。现在,两个断开连接的 IdM 部署会并行运行。

4. 通过硬编码引用新的 IdM 副本来切换 IdM 客户端使用新的部署。请参阅在恢复过程中调整 IdM 客户端。

5. 从以前的部署停止和卸载 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,在每个新副本中测试 Directory Server 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** 命令在每个新 CA 副本中测试 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
```

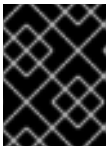
第 4 章 使用 IDM 备份恢复数据丢失

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。

4.1. 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,在整个部署中复制这些更改,并且您要恢复这些更改。只恢复数据备份会将 LDAP 条目返回到之前的状态,而不影响 IdM 配置本身。
- **基础架构丢失或丢失所有 CA 实例：** 如果灾难机构的所有证书颁发机构副本,部署无法通过部署额外的服务器来重建其自身。在这种情况下，恢复 CA 副本的备份并从中构建新副本。
- **隔离服务器的升级失败：** 操作系统仍然可以正常工作,但 IdM 数据被破坏,因此您要将 IdM 系统恢复到已知良好状态。红帽建议您使用技术支持诊断并排除这个问题。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，请参阅恢复使用复制的服务器丢失。

4.2. 从 IDM 备份中恢复时的注意事项

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

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。
- 因为上一次备份后创建的数据都将丢失,所以不要使用备份和恢复解决方案进行正常的系统维护。
- 如果服务器丢失,红帽建议重建服务器,方法是将其重新安装为副本,而不是从备份中恢复。创建一个新的副本会保留来自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 Directory 服务器使用 **PrivateTmp** 目录,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的软件(RPM)版本与执行备份时安装的相同。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。

4.3. 从备份中恢复 IDM 服务器

以下流程描述了从 IdM 备份中恢复 IdM 服务器或者其 LDAP 数据。

图 4.1. 本例中使用的复制拓扑

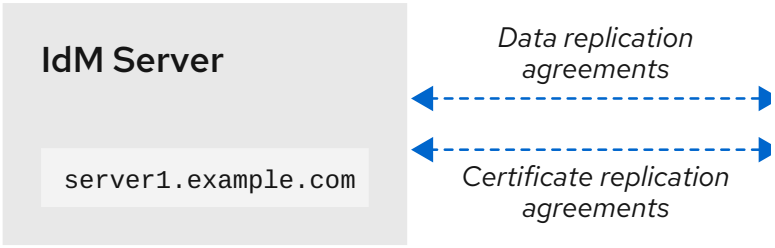


表 4.1. 本例中使用的服务器命名惯例

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

- 您可以使用 **ipa-backup** 程序为 IdM 服务器生成完整服务器或者只使用数据备份。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。

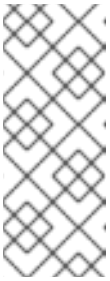
流程

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

     ```
     [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 工具自动检测目录包含的备份类型，并默认执行同一类型的恢复。要从完全服务器备份中只执行对数据的恢复，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已覆盖。

```
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** 实用程序禁用在所有可用的服务器中复制：

```
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 **domain** 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. 使用恢复的服务器为所有拓扑片段重新初始化 **domain** 后缀。
在这个示例中，使用来自 **server1** 的 数据重新初始化 **caReplica2**。

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

c. 移至证书颁发机构数据,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。
在这个示例中，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. 继续通过复制拓扑移至,重新初始化连续副本,直到所有服务器都使用恢复的服务器中的数据进行了更新 **server1.example.com**。
在这个示例中，我们只需要使用来自 **caReplica2** 的数据，在**replica3** 上重新初始化 **domain** 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 SSSD 在每台服务器上的缓存，以避免因为数据无效而导致身份验证问题：

   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。

其它资源

- **ipa-restore (1)** man page 还详细论述了如何在恢复过程中处理复杂复制场景。

4.4. 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 密钥时使用自定义密钥环位置,请确定将 **$GNUPGHOME** 环境变量设置为那个目录。请参阅创建 GPG2 密钥。

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

2. 提供 **ipa-restore** 工具以及备份目录的位置。

   ```
   [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 5 章 管理数据丢失

对数据丢失事件的正确响应将取决于受影响的副本数以及丢失的数据类型。

5.1. 对隔离数据丢失的响应

当发生数据丢失时,通过立即隔离受影响的服务器来最小复制数据丢失。然后,从环境的未受影响剩余部分创建替换副本。

先决条件

- 具有多个副本的强大 IdM 复制拓扑。请参阅 准备使用复制的服务器丢失。

流程

1. 要限制复制数据丢失,请通过删除复制拓扑片段将所有受影响的副本与其余拓扑断开连接。

   a. 显示部署中的所有 **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. 使用任何涉及任何受影响的服务器的 **ca** 拓扑片段执行相同的操作。

```
[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是可根据。要创建替换副本,请参阅 恢复丢失多个服务器。

5.2. 响应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,比如在所有服务器中意外删除数据。如果已知且有限数据丢失,请手动重新添加丢失的数据。

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. 如果您需要查看丢失的数据,请将虚拟机快照或备份恢复到独立网络中的隔离服务器。
2. 使用 **ipa** 或 **ldapadd** 命令在数据库中添加缺少的信息。

其它资源

- 有关从虚拟机快照恢复的信息,请参阅 使用虚拟机快照恢复数据丢失。
- 有关备份和恢复 IdM 的详情,请 参考备份和恢复 IdM。

5.3. 响应所有服务器中的未定义数据丢失

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)从虚拟机快照复制到已知良好状态,并从中部署新的 IdM 环境。请参阅 只从虚拟机快照中恢复。
2. 使用 **ipa** 或 **ldapadd** 命令添加在快照被创建的数据。

其它资源

- 有关从虚拟机快照恢复的信息,请参阅 使用虚拟机快照恢复数据丢失。

第 6 章 在恢复过程中调整 IDM 客户端

在恢复 IdM 服务器时,您可能需要调整 IdM 客户端以反应副本拓扑的更改。

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** 条目指向正常工作的 IdM 副本提供 DNS 服务。

2. **调整 Kerberos 配置**:

   a. 默认情况下,IdM 客户端查找 Kerberos 服务器的 DNS 服务记录,并将调整为副本拓扑的更改：

   ```
   [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** 条目指向可以正常工作的 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 客户端查找 LDAP 服务器的 DNS 服务记录,并调整为副本拓扑的更改：

   ```
   [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特定的 IdM 服务器 **/etc/sssd/sssd.conf**,请确定 **ipa_server** 入口点指向可正常工作的 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的服务器相关的过时信息。如果用户的身份验证问题不一致,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)
```