Red Hat Enterprise Linux 9

管理身份管理中的复制

准备和验证复制环境

Last Updated: 2024-10-12

Red Hat Enterprise Linux 9 管理身份管理中的复制

准备和验证复制环境

法律通告

摘要

在 Red Hat Identity Management (IdM)环境中，复制启用了故障转移和负载平衡。您可以使用命令行、Web UI 和 Ansible Playbook 配置、验证和停止服务器之间的复制。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

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

第 1 章 管理复制拓扑

本章描述了如何管理身份管理(IdM)域中服务器之间的复制。

其他资源

- 规划副本拓扑
- 卸载 IdM 服务器
- IdM 中的故障转移、负载平衡和高可用性

1.1. 解释复制协议、拓扑后缀和拓扑段

当您创建副本时，身份管理(IdM)会在初始服务器和副本之间创建一个复制协议。然后，复制的数据会存储在拓扑后缀中，当两个副本在它们的后缀之间有复制协议时，后缀会形成一个拓扑段。在以下部分中更为详细地解释了这些概念：

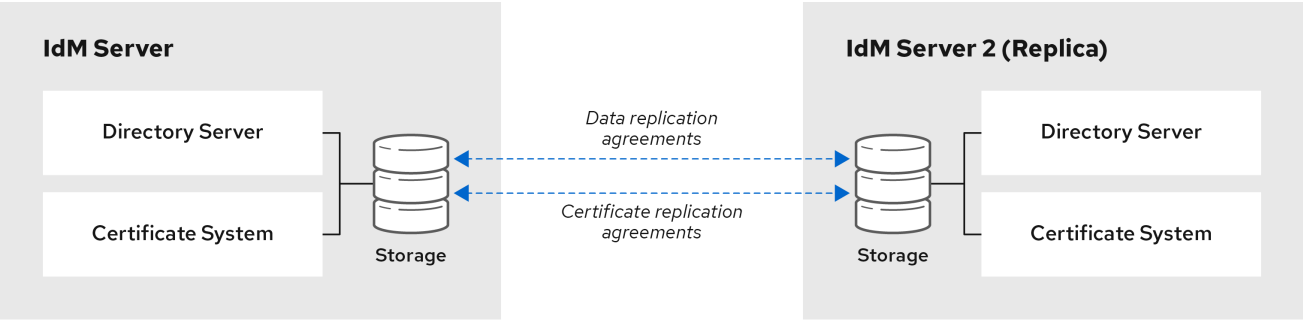
- 复制协议
- 拓扑后缀
- 拓扑段

1.1.1. IdM 副本之间的复制协议

当管理员基于现有服务器创建副本时，身份管理 (IdM) 会在初始服务器和副本之间创建*复制协议*。复制协议确保两个服务器之间不断复制数据和配置。

IdM 使用*多读/写副本复制*。在这种配置中，所有副本都加入到复制协议中接收并提供更新，因此被视为供应商和消费者。复制协议始终是强制的。

图 1.1. 服务器和副本协议



IdM 使用两种复制协议：

- **域复制协议** 复制身份信息。
- **证书复制协议** 复制证书信息。

两个复制频道都是独立的。两个服务器可以有一类或两种类型的复制协议。例如，当服务器 A 和服务器 B 仅配置了域复制协议时，它们之间仅复制身份信息，而不复制证书信息。

1.1.2. 拓扑后缀

*拓扑后缀*存储复制的数据。IdM 支持两种类型的拓扑后缀：**domain** 和 **ca**。每个后缀代表一个单独的服务器，一个独立的复制拓扑。

配置复制协议时，它会在两个不同的服务器上加入同一类型的两个拓扑后缀。

域 后缀：dc=*example*,dc=*com*

域 后缀包含所有域相关的数据。
当两个副本在其 **域** 后缀之间有一个复制协议时，它们将共享目录数据，如用户、组和策略。

ca suffix: o=ipaca

ca 后缀包含证书系统组件的数据。它仅存在于安装有证书颁发机构 (CA) 的服务器上。
当两个副本在其 **ca** 后缀之间有复制协议时，它们将共享证书数据。

图 1.2. 拓扑后缀

在安装新副本时，**ipa-replica-install** 脚本会在两台服务器之间设置初始拓扑复制协议。

例 1.1. 查看拓扑后缀

ipa topologysuffix-find 命令显示拓扑后缀列表：

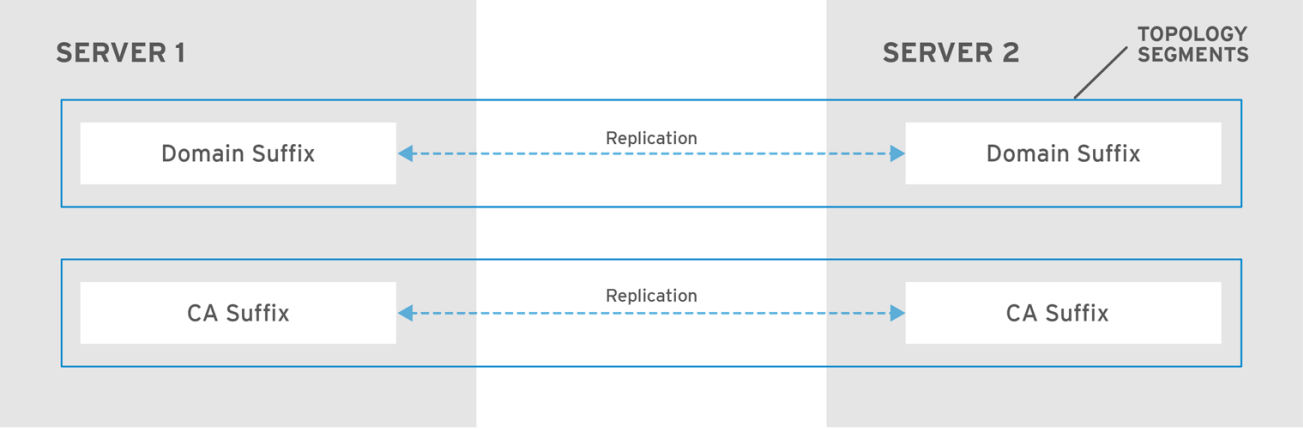
```
$ ipa topologysuffix-find
----------------------------
2 topology suffixes matched
----------------------------
  Suffix name: ca
  Managed LDAP suffix DN: o=ipaca

  Suffix name: domain
  Managed LDAP suffix DN: dc=example,dc=com
----------------------------
Number of entries returned 2
----------------------------
```

1.1.3. 拓扑段

当两个副本在它们的后缀之间有复制协议时，后缀会形成 *拓扑段*。每个拓扑片段由一个 *左节点* 和一个 *右节点* 组成。节点代表加入复制协议的服务器。

IdM 中的拓扑段始终是双向的。每个段代表两种复制协议：从服务器 A 到服务器 B 和从服务器 B 到服务器 A。因此，数据被双向复制。

图 1.3. 拓扑段



例 1.2. 查看拓扑段

ipa topologysegment-find 命令显示为域或 CA 后缀配置的当前拓扑段。例如，对于域后缀：

```
$ ipa topologysegment-find
Suffix name: domain
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

在本例中，域相关的数据仅在两个服务器之间被复制：**server1.example.com** 和 **server2.example.com**。

要仅显示特定段的详情，请使用 **ipa topologysegment-show** 命令：

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: server1.example.com-to-server2.example.com
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

1.2. 使用拓扑图来管理复制拓扑

Web UI 中的拓扑图显示了域中服务器之间的关系。使用 Web UI，您可以操作和转换拓扑表示。

访问拓扑图

要访问拓扑图：

1. 选择 **IPA Server → Topology → Topology Graph**。
2. 如果您对拓扑所做的任何更改没有立即反映在图中，请点击 **Refresh**。

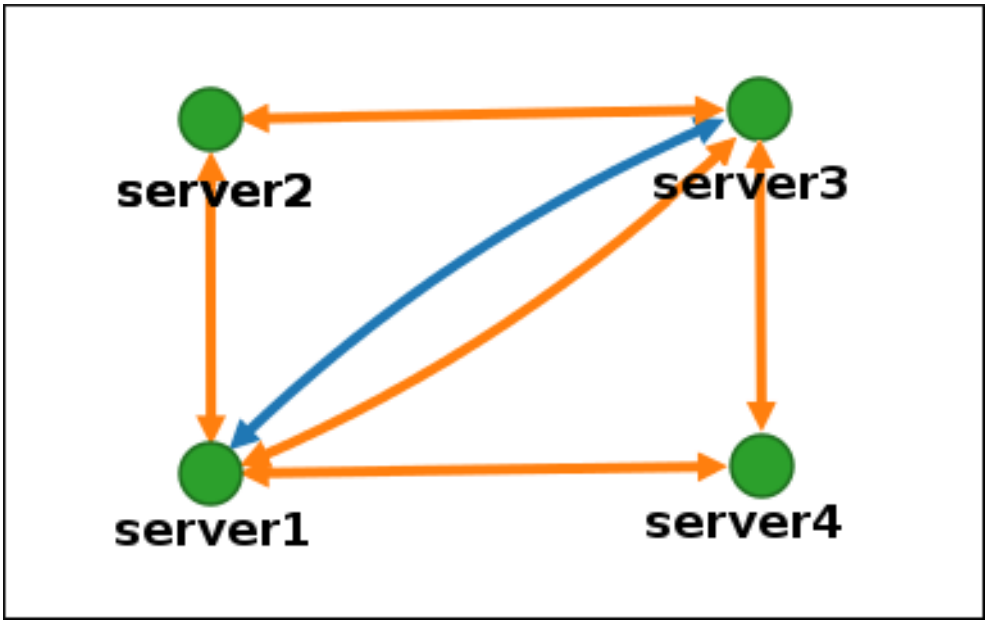
解释拓扑图

加入域复制协议的服务器通过橙色箭头连接。加入 CA 复制协议的服务器通过蓝色箭头连接。

拓扑图示例：推荐的拓扑

以下推荐的拓扑示例显示了四个服务器的可能的推荐拓扑之一：每个服务器至少连接到两个其他服务器，并且多个服务器是 CA 服务器。

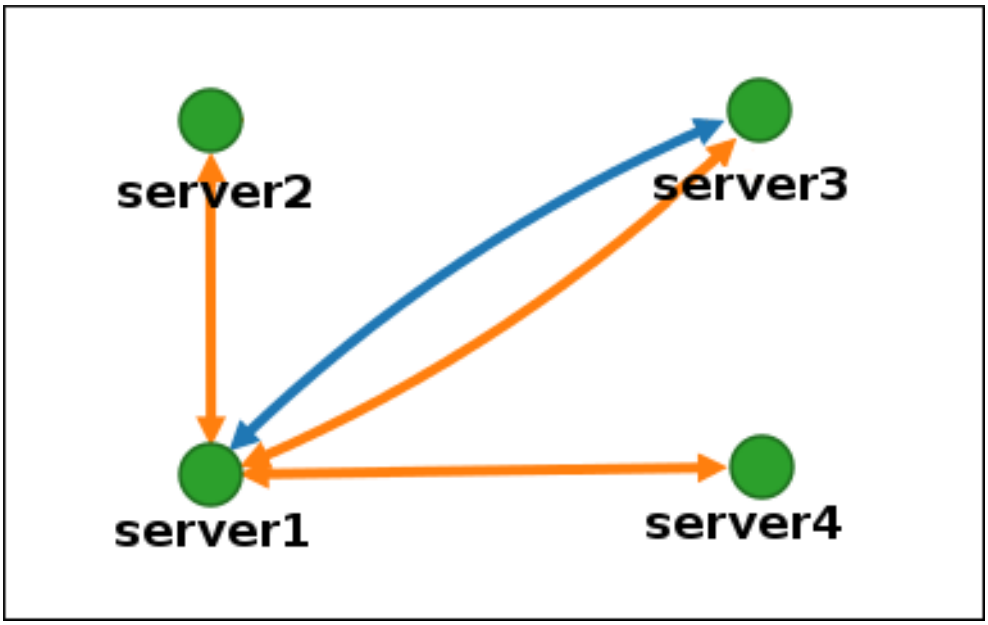
图 1.4. 建议的拓扑示例



拓扑图示例：不推荐的拓扑

在以下不建议的拓扑示例中，**server1** 是一个单点故障。所有其他服务器都与此服务器有复制协议，但与其他任何服务器都没有。因此，如果 **server1** 出现故障，所有其他服务器将被隔离。
避免创建类似这样的拓扑。

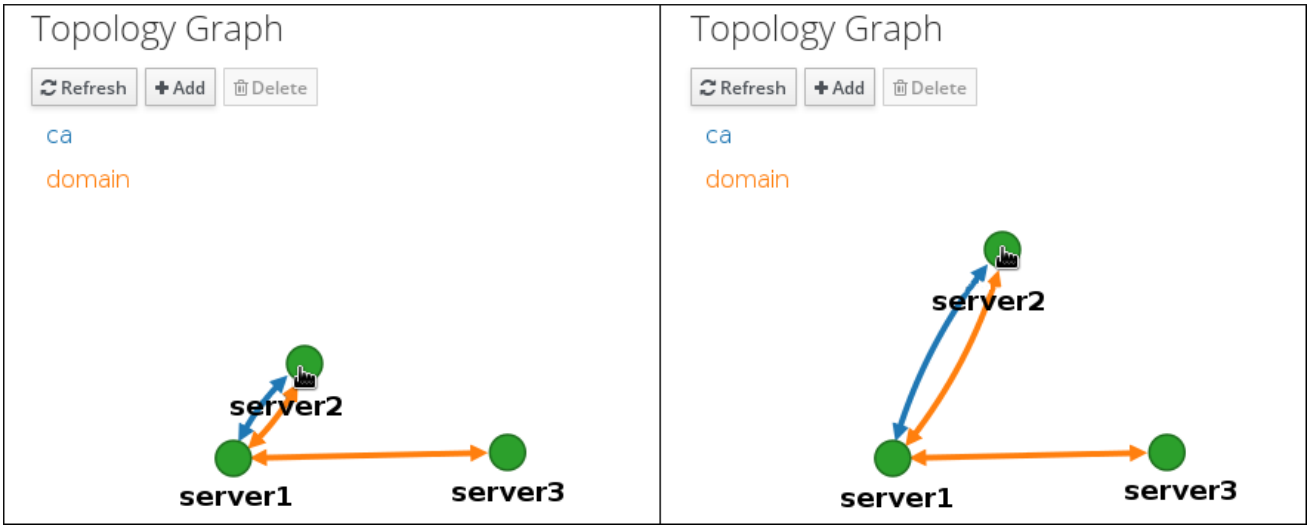
图 1.5. 不鼓励的拓扑示例：单点故障



自定义拓扑视图

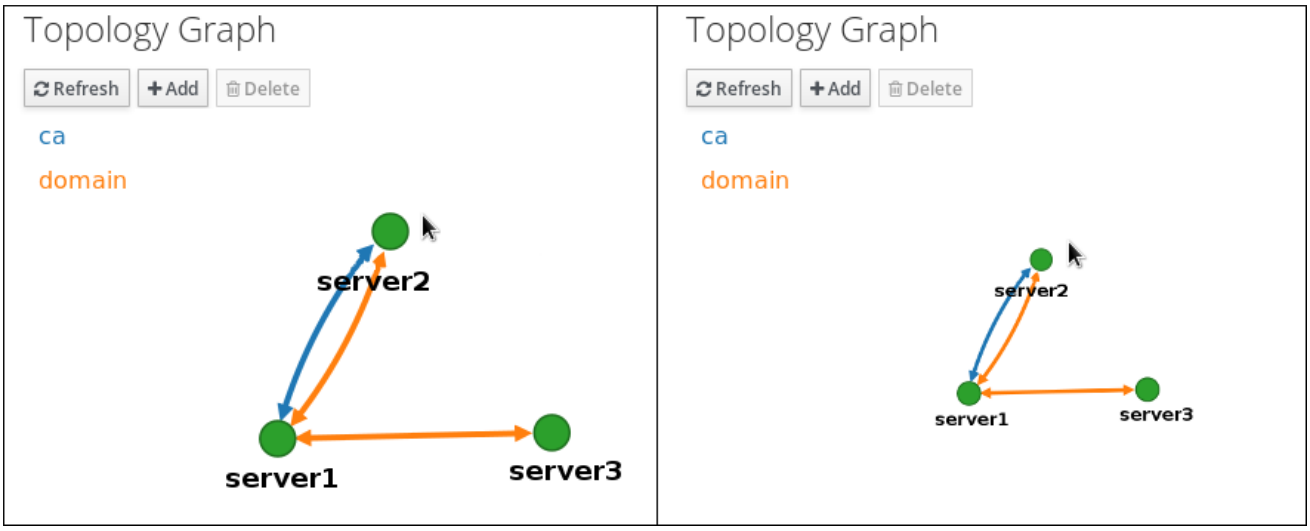
您可以通过按住并拖动鼠标来移动单个拓扑节点：

图 1.6. 移动拓扑图节点



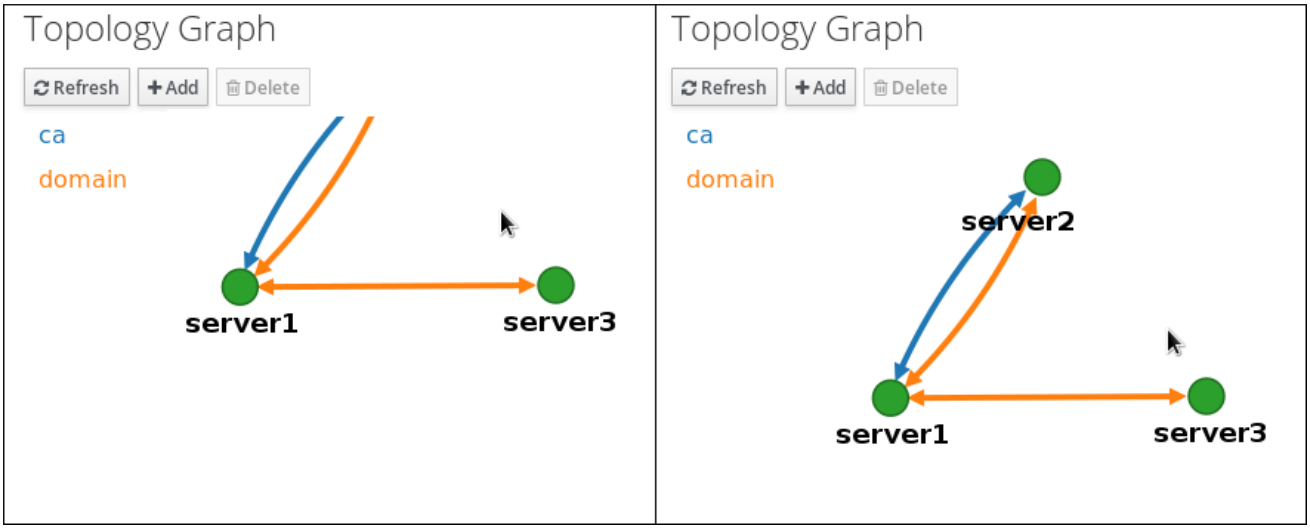
您可以使用鼠标滚轮放大和缩小拓扑图：

图 1.7. 缩放拓扑图



您可以通过按住鼠标左键来移动拓扑图的画布：

图 1.8. 移动拓扑图画布



1.3. 使用 WEB UI 在两台服务器之间设置复制

使用身份管理(IdM) Web UI，您可以选择两个服务器，并在它们之间创建新的复制协议。

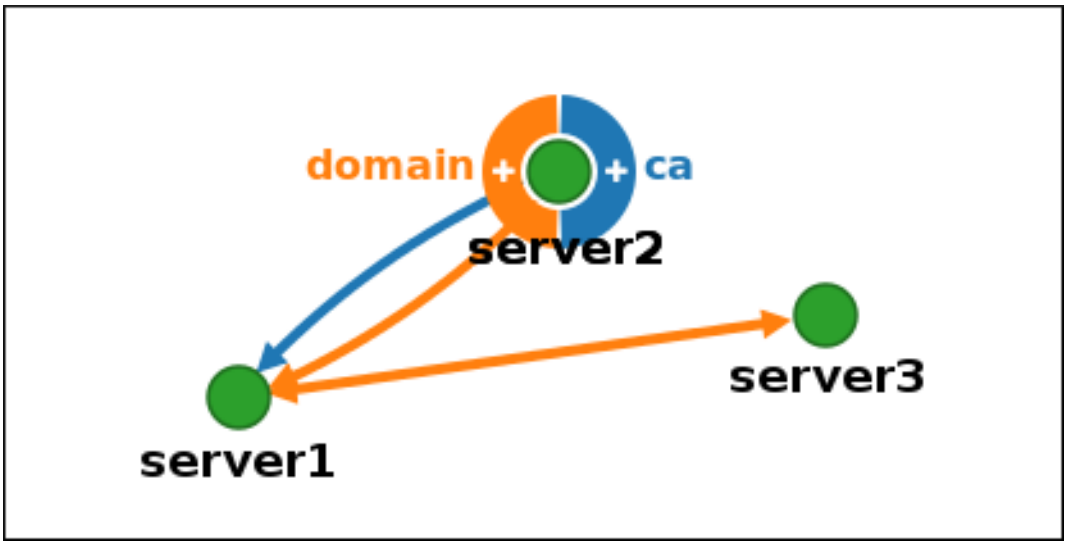
先决条件

- 您以 IdM 管理员身份登录。

步骤

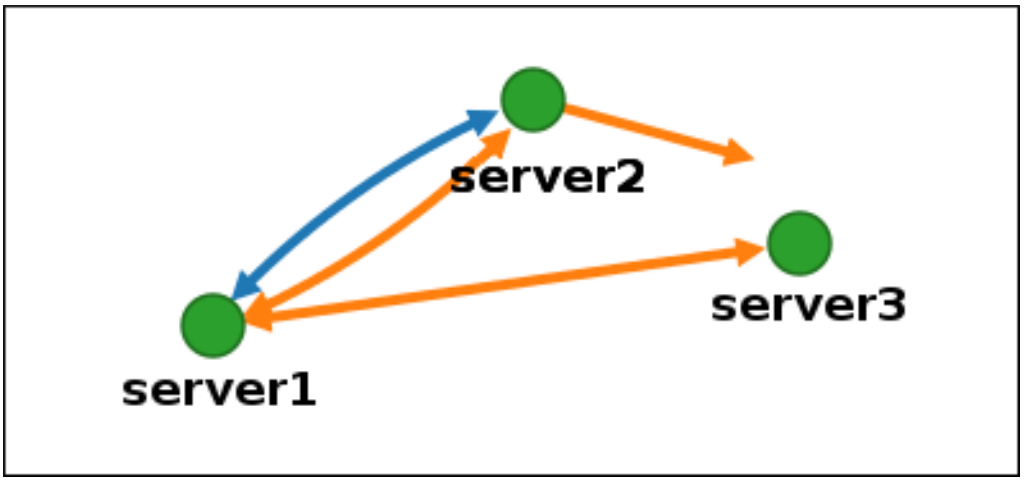
1. 在拓扑图中，将鼠标悬停在其中一台服务器节点上。

图 1.9. 域或 CA 选项



2. 根据您要创建的拓扑段的类型，单击圆圈的 **domain** 或 **ca** 部分。
3. 在鼠标指针下会出现代表新复制协议的新箭头。将鼠标移到其他服务器节点，然后单击该节点。

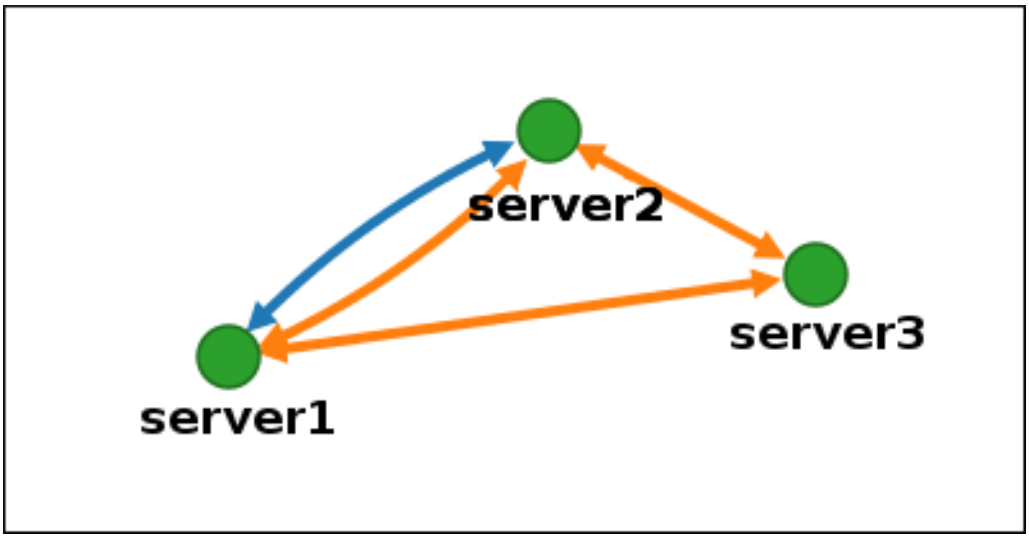
图 1.10. 创建新段



4. 在 **Add topology segment** 窗口中，单击 **Add** 来确认新段的属性。

两个服务器之间的新拓扑段将它们加入复制协议。拓扑图现在显示更新的复制拓扑：

图 1.11. 新段创建好了



1.4. 使用 WEB UI 停止两个服务器之间的复制

使用身份管理(IdM) Web UI，您可以从服务器中删除复制协议。

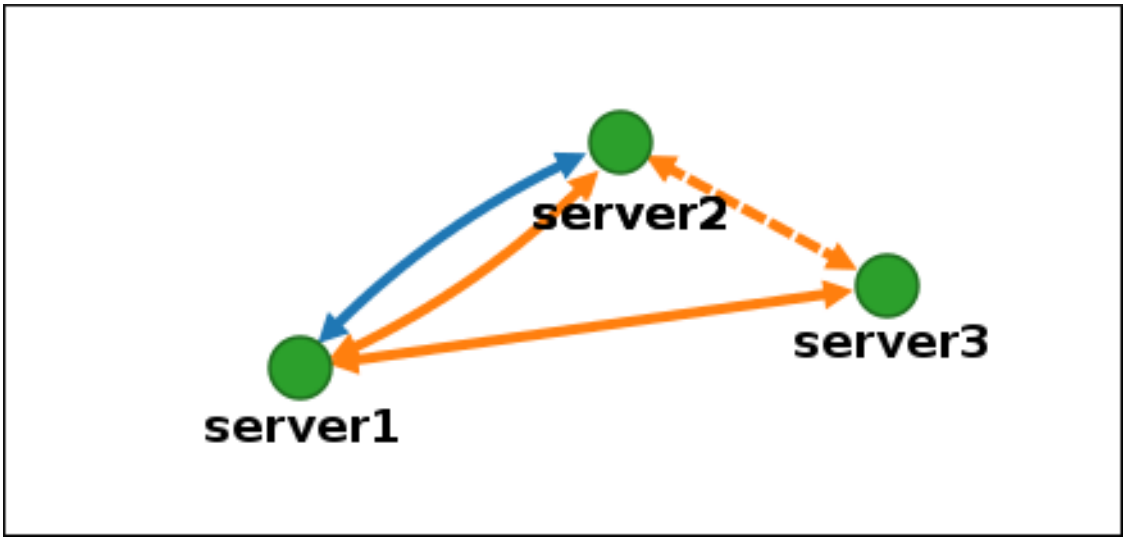
先决条件

- 您以 IdM 管理员身份登录。

步骤

1. 单击代表您要删除的复制协议的箭头。这会高亮显示箭头。

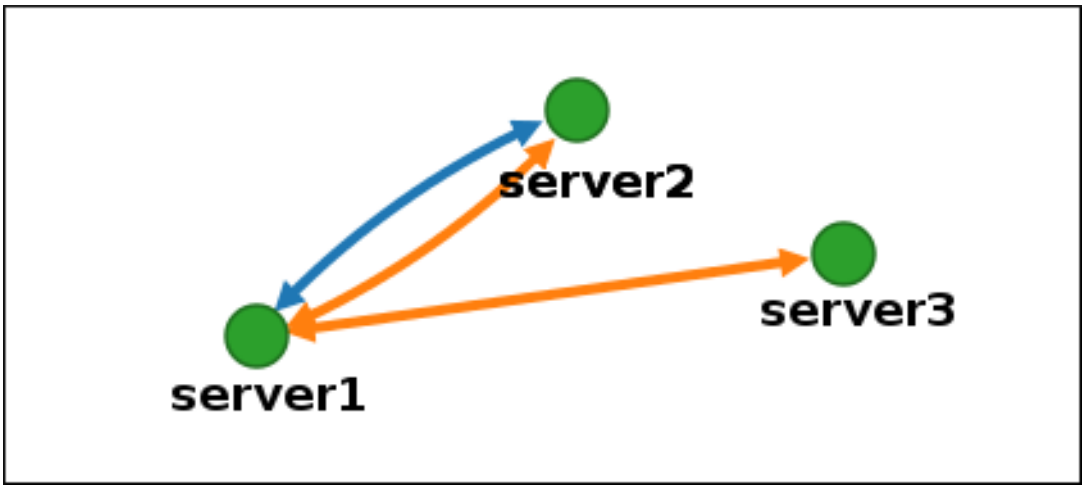
   图 1.12. 拓扑段高亮显示

2. 单击 **Delete**。

3. 在 **Confirmation** 窗口中，单击 **OK**。
   IdM 删除两个服务器之间的拓扑段，这将删除它们的复制协议。拓扑图现在显示更新的复制拓扑：

图 1.13. 拓扑段删除了



1.5. 使用 CLI 在两个服务器之间建立复制

您可以使用 **ipa topologysegment-add** 命令在两个服务器之间配置复制协议。

先决条件

- 您有 IdM 管理员凭证。

步骤

- 为两台服务器创建一个拓扑段。出现提示时，请提供：
  - 所需的拓扑后缀：**domain** 或 **ca**
  - 左侧节点和右侧节点，代表两台服务器
  - [可选] 段的自定义名称
    例如：

```
$ ipa topologysegment-add
Suffix name: domain
Left node: server1.example.com
Right node: server2.example.com
Segment name [server1.example.com-to-server2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

    添加新段来将服务器加入复制协议。

验证

- 验证新段是否已配置：

```
$ ipa topologysegment-show
```

```
Suffix name: domain
Segment name: new_segment
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

1.6. 使用 CLI 停止两个服务器之间的复制

您可以使用 **ipa topology segment-del** 命令从命令行终止复制协议。

先决条件

- 您有 IdM 管理员凭证。

步骤

1. [可选] 如果您不知道要删除的特定复制段的名称，请显示所有可用的段。使用 **ipa topologysegment-find** 命令。出现提示时，请提供所需的拓扑后缀： **domain** 或 **ca**。例如：

```
$ ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both

...

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

   在输出中找到所需的段。

2. 删除连接两台服务器的拓扑段：

```
$ ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
-----------------------------
Deleted segment "new_segment"
-----------------------------
```

   删除段会删除复制协议。

验证

- 验证段是否不再列出：

```
$ ipa topologysegment-find
```

```
Suffix name: domain
------------------
7 segments matched
------------------
  Segment name: server2.example.com-to-server3.example.com
  Left node: server2.example.com
  Right node: server3.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 7
----------------------------
```

1.7. 使用 WEB UI 从拓扑中删除服务器

您可以使用身份管理(IdM)Web 界面从拓扑中删除服务器。此操作不会从主机中卸载服务器组件。

先决条件

- 您以 IdM 管理员身份登录。
- 您要删除的服务器 **不是** 连接其他服务器与拓扑其余部分的唯一服务器；这会导致其他服务器被隔离，这是不允许的。
- 您要删除的服务器 **不是** 您的最后一个 CA 或 DNS 服务器。

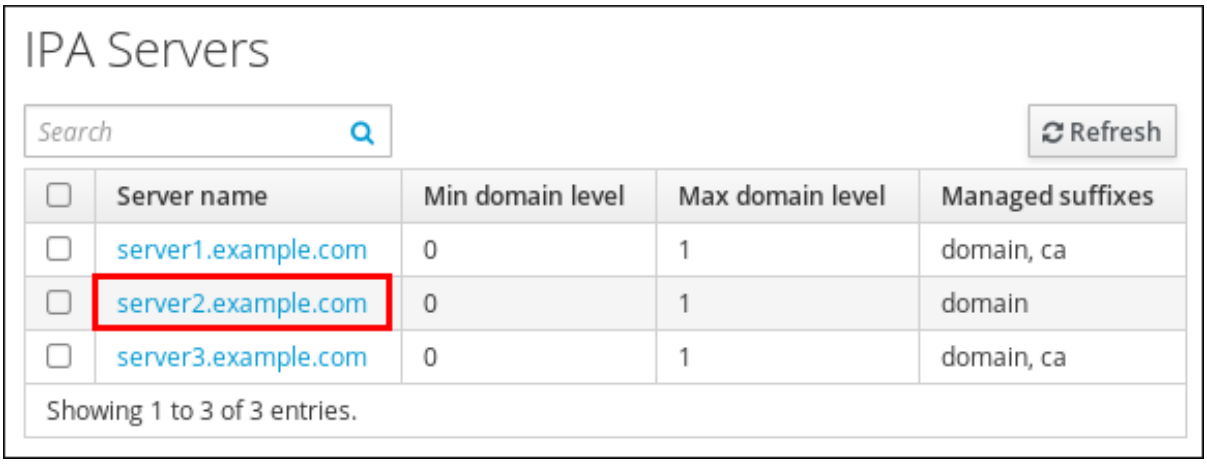
警告

删除服务器是一个不可逆的操作。如果您删除了服务器，将其重新引入回拓扑的唯一方法是在机器上安装一个新副本。

步骤

1. 选择 **IPA Server → Topology → IPA Servers**。
2. 单击要删除的服务器的名称。

图 1.14. 选择服务器



3. 单击 **Delete Server**。

其他资源

- 卸载 IdM 服务器

1.8. 使用 IDM WEB UI 查看 IDM 拓扑中的可用服务器角色

根据安装在 IdM 服务器上的服务，它可以执行各种 *服务器角色*。例如：

- CA 服务器
- DNS 服务器
- 密钥恢复授权(KRA)服务器。

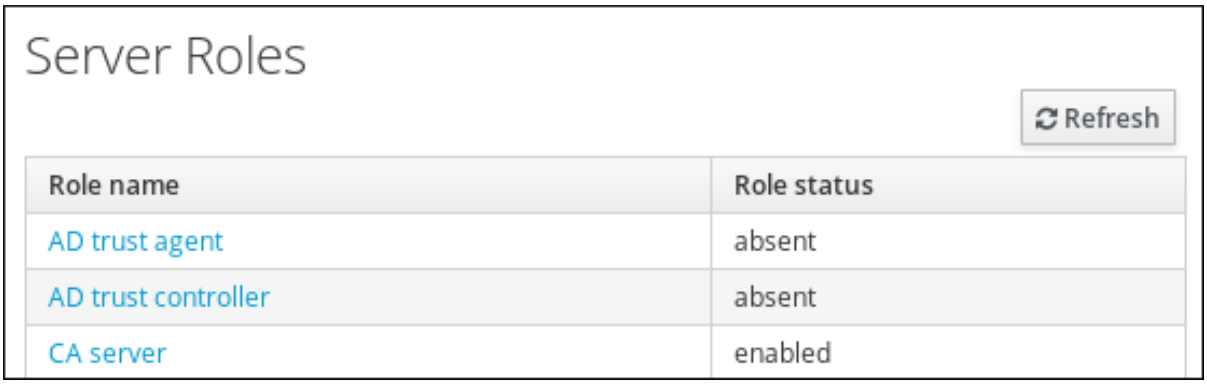
步骤

- 有关支持的服务器角色的完整列表，请参阅 **IPA 服务器 → 拓扑 → 服务器角色**。

注意

- 角色状态 **absent** 意味着拓扑中没有服务器在执行角色。
- 角色状态 **enabled** 意味着拓扑中的一个或多个服务器在执行角色。

图 1.15. Web UI 中的服务器角色



1.9. 使用 IDM CLI 查看 IDM 拓扑中的可用服务器角色

根据安装在 IdM 服务器上的服务，它可以执行各种 *服务器角色*。例如：

- CA 服务器
- DNS 服务器
- 密钥恢复授权(KRA)服务器。

步骤

- 要显示拓扑中的所有 CA 服务器和当前 CA 续订服务器：

```
$ ipa config-show
  ...
  IPA masters: server1.example.com, server2.example.com, server3.example.com
  IPA CA servers: server1.example.com, server2.example.com
  IPA CA renewal master: server1.example.com
```

- 或者，要显示在特定服务器（如 *server.example.com*）上启用的角色的列表：

```
$ ipa server-show
Server name: server.example.com
  ...
  Enabled server roles: CA server, DNS server, KRA server
```

- 或者，使用 **ipa server-find --servrole** 命令搜索启用了特定服务器角色的所有服务器。例如，要搜索所有 CA 服务器：

```
$ ipa server-find --servrole "CA server"
---------------------
2 IPA servers matched
---------------------
  Server name: server1.example.com
  ...

  Server name: server2.example.com
  ...
----------------------------
Number of entries returned 2
----------------------------
```

1.10. 将副本提升为 CA 续订服务器和 CRL 发布者服务器

如果您的 IdM 部署使用嵌入式证书颁发机构(CA)，其中一个 IdM CA 服务器充当 CA 续订服务器（该服务器管理 CA 子系统证书的续订）。其中一个 IdM CA 服务器也充当 IdM CRL 发布者服务器（生成证书撤销列表的服务器）。

默认情况下，CA 续订服务器和 CRL 发布者服务器角色安装在系统管理员使用 **ipa-server-install** 或 **ipa-ca-install** 命令在其上安装 CA 角色的第一个服务器上。但是，您可以将两个角色之一传输到启用了 CA 角色的任何其他 IdM 服务器上。

先决条件

- 您有 IdM 管理员凭证。

1.11. 降级或提升隐藏的副本

流程

安装副本后，您可以配置副本是隐藏还是可见。

有关隐藏副本的详情，请参阅 隐藏副本模式。

先决条件

- 确保副本不是 DNSSEC 密钥主服务器。如果是，在隐藏此副本前将服务移到另一个副本。
- 确保副本不是 CA 续订服务器。如果是，在隐藏此副本前将服务移到另一个副本。详情请查看

流程

- 要隐藏副本：

```
# ipa server-state replica.idm.example.com --state=hidden
```

- 要使副本再次可见：

```
# ipa server-state replica.idm.example.com --state=enabled
```

- 要查看拓扑中所有隐藏副本的列表：

```
# ipa config-show
```

如果所有副本都启用了，则命令输出不会提到隐藏的副本。

第 2 章 准备您的环境以使用 ANSIBLE PLAYBOOK 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。

通过这个方法，您可以在一个位置找到所有 playbook，并可以在不使用 root 特权的前提下运行 playbook。

注意

您只需要在受管节点上具有 **root** 权限来执行 **ipaserver**、**ipareplica**、**ipaclient** 和 **ipabackup 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：

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

```
[us]
replica.idm.example.com

[ipaserver:children]
eu
us
```

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：创建一个 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
```

这些命令要求您输入 IdM **admin** 密码。

其他资源

- 使用 Ansible playbook 来安装身份管理服务器
- 如何构建清单

第 3 章 使用 ANSIBLE 管理 IDM 中的复制拓扑

您可以维护多个身份管理 (IdM) 服务器，并使它们相互复制，以实现冗余目的，以减少或防止服务器丢失。例如，如果一个服务器失败，其他服务器就会为域提供服务。您还可以根据剩余的服务器创建新副本来恢复丢失的服务器。

存储在 IdM 服务器上的数据会根据复制协议复制：当两台服务器配置了复制协议时，它们将共享其数据。复制的数据存储在拓扑**后缀**中。当两个副本在其后缀之间具有复制协议时，后缀组成一个拓扑**片段（segment）**。

本章论述了如何使用 Ansible 管理 IdM 复制协议、拓扑段和拓扑后缀。

3.1. 使用 ANSIBLE 确保 IDM 中存在复制协议

存储在身份管理 (IdM) 服务器上的数据存储基于复制协议：配置了两个服务器时，它们共享其数据。复制协议始终为现实：数据从第一个副本复制到另一个副本，另一个副本复制到第一个副本。

按照以下流程，使用 Ansible playbook 确保 **server.idm.example.com** 和 **replica.idm.example.com** 之间存在 **domain** 类型的复制协议。

先决条件

- 确保您了解设计 在拓扑中连接 IdM 副本的指南 中列出的拓扑的建议。
- 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**，并且您可以访问存储了保护 **secret.yml** 文件的密码的文件。
- 目标节点,也就是在其上执行 **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。

步骤

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 复制 **ansible-freeipa** 软件包提供的 **add-topologysegment.yml** Ansible playbook 文件：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/add-topologysegment.yml
add-topologysegment-copy.yml
```

3. 打开 **add-topologysegment-copy.yml** 文件进行编辑。
4. 通过在 **ipatopologysegment** 任务部分设置以下变量来调整文件：
   - 表示 **ipaadmin_password** 变量的值在 **secret.yml** Ansible vault 文件中定义。

- 根据您要添加的分段类型，将 **suffix** 变量设置为 **domain** 或 **ca**。
- 将 **left** 变量设置为您要作为复制协议左侧节点的 IdM 服务器的名称。
- 将 **right** 变量设置为您要作为复制协议正确节点的 IdM 服务器的名称。
- 确保 **state** 变量设置为 **present**。

这是当前示例修改的 Ansible playbook 文件：

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
- name: Add topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      left: server.idm.example.com
      right: replica.idm.example.com
      state: present
```

5. 保存这个文件。
6. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-
topologysegment-copy.yml
```

其他资源

- 解释复制协议、拓扑后缀和拓扑段
- **/usr/share/doc/ansible-freeipa/README-topology.md**
- **/usr/share/doc/ansible-freeipa/playbooks/topology** 中的 playbook 示例

3.2. 使用 ANSIBLE 确保多个 IDM 副本之间存在复制协议

存储在身份管理 (IdM) 服务器上的数据存储基于复制协议：配置了两个服务器时，它们共享其数据。复制协议始终为现实：数据从第一个副本复制到另一个副本，另一个副本复制到第一个副本。

按照以下流程确保 IdM 中的多个副本对存在复制协议。

先决条件

- 确保您了解拓扑中连接副本中列出的 IdM 拓扑的建议。
- 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**，并且您可以访问存储了保护 **secret.yml** 文件的密码的文件。

- 目标节点,也就是在其上执行 **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。

步骤

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 复制 **ansible-freeipa** 软件包提供的 **add-topologysegments.yml** Ansible playbook 文件：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/add-topologysegments.yml
add-topologysegments-copy.yml
```

3. 打开 **add-topologysegments-copy.yml** 文件进行编辑。
4. 通过在 **vars** 部分中设置以下变量来调整文件：
   - 表示 **ipaadmin_password** 变量的值在 **secret.yml** Ansible vault 文件中定义。
   - 对于每个拓扑片段，在 **ipatopology_segments** 部分添加一个行并设置以下变量：
     - 根据您要添加的分段类型，将 **suffix** 变量设置为 **domain** 或 **ca**。
     - 将 **left** 变量设置为您要作为复制协议左侧节点的 IdM 服务器的名称。
     - 将 **right** 变量设置为您要作为复制协议正确节点的 IdM 服务器的名称。
5. 在 **add-topologysegments-copy.yml** 文件的 **tasks** 部分中，确保 **state** 变量设置为 **present**。这是当前示例修改的 Ansible playbook 文件：

```
---
- name: Add topology segments
  hosts: ipaserver
  gather_facts: false

  vars:
    ipaadmin_password: "{{ ipaadmin_password }}"
    ipatopology_segments:
    - {suffix: domain, left: replica1.idm.example.com , right: replica2.idm.example.com }
    - {suffix: domain, left: replica2.idm.example.com , right: replica3.idm.example.com }
    - {suffix: domain, left: replica3.idm.example.com , right: replica4.idm.example.com }
    - {suffix: domain+ca, left: replica4.idm.example.com , right: replica1.idm.example.com }

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Add topology segment
```

```
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: "{{ item.suffix }}"
      name: "{{ item.name | default(omit) }}"
      left: "{{ item.left }}"
      right: "{{ item.right }}"
      state: present
    loop: "{{ ipatopology_segments | default([]) }}"
```

6. 保存这个文件。

7. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-
topologysegments-copy.yml
```

其他资源

- 解释复制协议、拓扑后缀和拓扑段
- **/usr/share/doc/ansible-freeipa/README-topology.md**
- **/usr/share/doc/ansible-freeipa/playbooks/topology** 中的 playbook 示例

3.3. 使用 ANSIBLE 检查两个副本之间是否存在复制协议

存储在身份管理 (IdM) 服务器上的数据存储基于复制协议：配置了两个服务器时，它们共享其数据。复制协议始终为现实：数据从第一个副本复制到另一个副本，另一个副本复制到第一个副本。

按照以下流程验证 IdM 中多个副本对是否存在复制协议。与 使用 Ansible 确保 IdM 中复制协议存在 不同，这个流程不会修改现有配置。

先决条件

- 确保您了解拓扑中连接副本中列出的 IdM 拓扑的建议。
- 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**，并且您可以访问存储了保护 **secret.yml** 文件的密码的文件。
- 目标节点,也就是在其上执行 **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。

步骤

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 复制 **ansible-freeipa** 软件包提供的 **check-topologysegments.yml** Ansible playbook 文件：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/check-topologysegments.yml
check-topologysegments-copy.yml
```

3. 打开 **check-topologysegments-copy.yml** 文件进行编辑。

4. 通过在 **vars** 部分中设置以下变量来调整文件：

   - 表示 **ipaadmin_password** 变量的值在 **secret.yml** Ansible vault 文件中定义。
   - 对于每个拓扑片段，在 **ipatopology_segments** 部分添加一个行并设置以下变量：
     - 根据您要添加的分段类型，将 **suffix** 变量设置为 **domain** 或 **ca**。
     - 将 **left** 变量设置为您要作为复制协议左侧节点的 IdM 服务器的名称。
     - 将 **right** 变量设置为您要作为复制协议正确节点的 IdM 服务器的名称。

5. 在 **check-topologysegments-copy.yml** 文件的 **tasks** 部分中，确保 **state** 变量设置为 **present**。
   这是当前示例修改的 Ansible playbook 文件：

```
---
- name: Add topology segments
  hosts: ipaserver
  gather_facts: false

  vars:
    ipaadmin_password: "{{ ipaadmin_password }}"
    ipatopology_segments:
    - {suffix: domain, left: replica1.idm.example.com, right: replica2.idm.example.com }
    - {suffix: domain, left: replica2.idm.example.com , right: replica3.idm.example.com }
    - {suffix: domain, left: replica3.idm.example.com , right: replica4.idm.example.com }
    - {suffix: domain+ca, left: replica4.idm.example.com , right:
replica1.idm.example.com }

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Check topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: "{{ item.suffix }}"
      name: "{{ item.name | default(omit) }}"
      left: "{{ item.left }}"
      right: "{{ item.right }}"
      state: checked
    loop: "{{ ipatopology_segments | default([]) }}"
```

6. 保存这个文件。

7. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
-
```

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory check-topologysegments-copy.yml
```

其他资源

- 解释复制协议、拓扑后缀和拓扑段
- **/usr/share/doc/ansible-freeipa/README-topology.md**
- **/usr/share/doc/ansible-freeipa/playbooks/topology** 中的 playbook 示例

3.4. 使用 ANSIBLE 验证 IDM 中是否存在拓扑后缀

在身份管理 (IdM) 中的复制协议中，拓扑后缀存储要复制的数据。IdM 支持两种类型的拓扑后缀：**domain** 和 **ca**。每个后缀代表一个单独的后端，即一个单独的复制拓扑。配置复制协议时，它会在两个不同的服务器上加入同一类型的两个拓扑后缀。

domain 后缀包含与域相关的所有数据，如有关用户、组和策略的数据。**ca** 后缀包含证书系统组件的数据。它仅存在于安装有证书颁发机构 (CA) 的服务器上。

按照以下流程，使用 Ansible playbook 确保 IdM 中存在拓扑后缀。这个示例描述了如何确保 IdM 中存在 **domain** 后缀。

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**，并且您可以访问存储了保护 **secret.yml** 文件的密码的文件。
- 目标节点,也就是在其上执行 **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。

步骤

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 复制 **ansible-freeipa** 软件包提供的 **verify-topologysuffix.yml** Ansible playbook 文件：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/ verify-topologysuffix.yml verify-topologysuffix-copy.yml
```

3. 打开 **verify-topologysuffix-copy.yml** Ansible playbook 文件进行编辑。
4. 通过在 **ipatopologysuffix** 部分中设置以下变量来调整文件：

- 表示 **ipaadmin_password** 变量的值在 **secret.yml** Ansible vault 文件中定义。
- 将 **suffix** 变量设置为 **domain**。如果您要验证 **ca** 后缀是否存在，请将 变量设置为 **ca**。
- 确保 **state** 变量设置为 **verify**。不允许使用其他选项。

这是当前示例修改的 Ansible playbook 文件：

```
---
- name: Playbook to handle topologysuffix
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Verify topology suffix
    ipatopologysuffix:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      state: verified
```

5. 保存这个文件。
6. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory verify-
topologysuffix-copy.yml
```

其他资源

- 解释复制协议、拓扑后缀和拓扑段
- **/usr/share/doc/ansible-freeipa/README-topology.md**
- **/usr/share/doc/ansible-freeipa/playbooks/topology** 中的 playbook 示例

3.5. 使用 ANSIBLE 重新初始化 IDM 副本

如果副本已离线很长时间或者其数据库已损坏，您可以重新初始化它。重新初始化会使用更新的一组数据刷新副本。例如，如果需要从备份进行权威恢复，则可以使用重新初始化。

注意

与复制更新不同，副本仅互相发送更改的条目，重新初始化会刷新整个数据库。

运行命令的本地主机是重新初始化的副本。要指定从中获取数据的副本，请使用 **direction** 选项。

按照以下流程，使用 Ansible playbook 从 **server.idm.example.com** 中重新初始化 **replica.idm.example.com** 上的 **domain** 数据。

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**，并且您可以访问存储了保护 **secret.yml** 文件的密码的文件。

- 目标节点,也就是在其上执行 **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。

步骤

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 复制 **ansible-freeipa** 软件包提供的 **reinitialize-topologysegment.yml** Ansible playbook 文件：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/reinitialize-topologysegment.yml reinitialize-topologysegment-copy.yml
```

3. 打开 **reinitialize-topologysegment-copy.yml** 文件进行编辑。
4. 通过在 **ipatopologysegment** 部分中设置以下变量来调整文件：
   - 表示 **ipaadmin_password** 变量的值在 **secret.yml** Ansible vault 文件中定义。
   - 将 **suffix** 变量设置为 **domain**。如果您要重新初始化 **ca** 数据，请将变量设置为 **ca**。
   - 将 **left** 变量设置为复制协议的左侧节点。
   - 将 **right** 变量设置为复制协议的右节点。
   - 将 **direction** 变量设置为重新初始化数据的方向。**left-to-right** 方向表示数据从左侧节点流到右侧节点。
   - 确保将 **state** 变量设置为 **reinitialized**。
     这是当前示例修改的 Ansible playbook 文件：

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
  - name: Reinitialize topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      left: server.idm.example.com
```

```
right: replica.idm.example.com
direction: left-to-right
state: reinitialized
```

5. 保存这个文件。

6. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory reinitialize-topologysegment-copy.yml
```

其他资源

- 解释复制协议、拓扑后缀和拓扑段
- **/usr/share/doc/ansible-freeipa/README-topology.md**
- **/usr/share/doc/ansible-freeipa/playbooks/topology** 中的 playbook 示例

3.6. 使用 ANSIBLE 确保 IDM 中没有复制协议

存储在身份管理 (IdM) 服务器上的数据存储基于复制协议：配置了两个服务器时，它们共享其数据。复制协议始终为现实：数据从第一个副本复制到另一个副本，另一个副本复制到第一个副本。

按照以下流程确保 IdM 中不存在两个副本之间的复制协议。这个示例描述了如何确保在 **replica01.idm.example.com** 和 **replica02.idm.example.com** IdM 服务器之间不存在 **domain** 类型的复制协议。

先决条件

- 您理解设计 连接拓扑中的副本 中列出的 IdM 拓扑的建议。
- 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**，并且您可以访问存储了保护 **secret.yml** 文件的密码的文件。
- 目标节点,也就是在其上执行 **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。

步骤

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 复制 **ansible-freeipa** 软件包提供的 **delete-topologysegment.yml** Ansible playbook 文件：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/delete-topologysegment.yml
delete-topologysegment-copy.yml
```

3. 打开 **delete-topologysegment-copy.yml** 文件进行编辑。
4. 通过在 **ipatopologysegment** 任务部分设置以下变量来调整文件：
   - 表示 **ipaadmin_password** 变量的值在 **secret.yml** Ansible vault 文件中定义。
   - 将 **suffix** 变量设置为 **domain**。或者，如果您确保 **ca** 数据不在左侧和右侧节点之间复制，请将变量设置为 **ca**。
   - 将 **left** 变量设置为您要作为复制协议左侧节点的 IdM 服务器的名称。
   - 将 **right** 变量设置为 IdM 服务器的名称，该服务器是复制协议的右节点。
   - 确保 **state** 变量设置为 **absent**。

   这是当前示例修改的 Ansible playbook 文件：

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
- name: Delete topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: domain
      left: replica01.idm.example.com
      right: replica02.idm.example.com:
      state: absent
```

5. 保存这个文件。
6. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory delete-
topologysegment-copy.yml
```

其他资源

- 解释复制协议、拓扑后缀和拓扑段
- **/usr/share/doc/ansible-freeipa/README-topology.md**
- **/usr/share/doc/ansible-freeipa/playbooks/topology** 中的 playbook 示例

3.7. 其他资源

- 规划副本拓扑。
- 安装 IdM 副本。

第 4 章 降级或提升隐藏的副本

安装副本后，您可以配置副本是隐藏还是可见。

有关隐藏副本的详情，请参阅 隐藏副本模式。

先决条件

- 确保副本不是 DNSSEC 密钥主服务器。如果是，在隐藏此副本前将服务移到另一个副本。
- 确保副本不是 CA 续订服务器。如果是，在隐藏此副本前将服务移到另一个副本。详情请查看

流程

- 要隐藏副本：

```
# ipa server-state replica.idm.example.com --state=hidden
```

- 要使副本再次可见：

```
# ipa server-state replica.idm.example.com --state=enabled
```

- 要查看拓扑中所有隐藏副本的列表：

```
# ipa config-show
```

如果所有副本都启用了，则命令输出不会提到隐藏的副本。

第 5 章 使用 HEALTHCHECK 检查 IDM 复制

您可以使用 Healthcheck 工具测试身份管理(IdM)复制。

先决条件

- 您在使用 RHEL 版本 8.1 或更新版本。

5.1. 复制健康检查测试

Healthcheck 工具测试身份管理(IdM)拓扑配置，并搜索复制冲突问题。

要列出所有测试，请使用 **--list-sources** 选项运行 **ipa-healthcheck**:

```
# ipa-healthcheck --list-sources
```

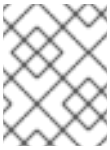
拓扑测试放置在 **ipahealthcheck.ipa.topology** 和 **ipahealthcheck.ds.replication** 源下：

IPATopologyDomainCheck

此测试验证：

- 没有一个服务器与拓扑断开连接。
- 该服务器没有超过推荐的复制协议数。

如果测试成功，则测试会返回配置的域。否则，将报告特定的连接错误。



注意

测试为 **domain** 后缀运行 **ipa topologysuffix-verify** 命令。如果在此服务器上配置了 IdM 证书颁发机构服务器角色，则它也会为 **ca** 后缀运行该命令。

ReplicationConflictCheck

测试搜索 LDAP 中与 **(&(!(objectclass=nstombstone))(nsds5ReplConflict=*))** 匹配的项。

注意

当尝试检查问题时，在所有 IdM 服务器中运行这些测试。

其他资源

- 解决常见的复制问题

5.2. 使用 HEALTHCHECK 检查复制

按照以下流程，使用 Healthcheck 工具对身份管理(IdM)复制拓扑和配置运行独立的手动测试。

Healthcheck 工具包含许多测试。因此，您可以使用以下方法缩短结果：

- 复制冲突测试：**--source=ipahealthcheck.ds.replication**
- 正确拓扑测试：**--source=ipahealthcheck.ipa.topology**

先决条件

- 已以 **root** 用户身份登录。

步骤

- 要运行 Healthcheck 复制冲突和拓扑检查，请输入：

```
# ipa-healthcheck --source=ipahealthcheck.ds.replication --
source=ipahealthcheck.ipa.topology
```

可能有四个不同的结果：

- SUCCESS – 测试成功通过。

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "SUCCESS",
  "kw": {
    "suffix": "domain"
  }
}
```

- WARNING – 测试通过但可能会有问题。
- ERROR – 测试失败。

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "ERROR",
  "uuid": d6ce3332-92da-423d-9818-e79f49ed321f
  "when": 20191007115449Z
  "duration": 0.005943
  "kw": {
    "msg": "topologysuffix-verify domain failed, server2 is not connected
(server2_139664377356472 in MainThread)"
  }
}
```

- CRITICAL – 测试失败，它会影响 IdM 服务器的功能。

其他资源

- **man ipa-healthcheck**

5.3. 其他资源

- IdM 中的 Healthcheck