# Red Hat Enterprise Linux 9

## 在 IdM 和 AD 间安装信任

管理 IdM 和 AD 域之间的跨林信任

Last Updated: 2024-06-26

# Red Hat Enterprise Linux 9 在 IdM 和 AD 间安装信任

管理 IdM 和 AD 域之间的跨林信任

## 法律通告



## 摘要

红帽身份管理(IdM)和活动目录(AD)管理各种核心服务，如 Kerberos、LDAP、DNS 和证书服务。信任关系通过使所有核心服务无缝交互，透明地集成了这两个环境。例如，信任可让 AD 用户认证到 IdM 拓扑中的服务。 准备信任需要在 IdM 和 AD 中使用通用加密类型，在防火墙中打开端口，以及配置 DNS 和 Kerberos 领域设置。如果不再需要信任，您可以将其删除。

# 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. 在顶部导航栏中点 **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 建立信任的先决条件

本文档旨在帮助您在身份管理 IdM 服务器和 Active Directory(AD)之间建立信任，其中两个服务器都位于相同的林。

**先决条件**

- 首先，请阅读 规划身份管理和活动目录之间的跨林信任 文档。
- AD 安装在其中有一个域控制器。
- IdM 服务器已安装并运行。
  详情请参阅 安装身份管理。
- AD 服务器和 IdM 服务器的时钟必须保持同步，因为 Kerberos 在通信中最多需要 5 分钟的延迟。
- 放置在信任中的每个服务器的唯一 NetBIOS 名称，因为 NetBIOS 名称对于识别 Active Directory 域至关重要。
  Active Directory 或 IdM 域的 NetBIOS 名称通常是对应的 DNS 域的第一部分。如果 DNS 域是 **ad.example.com**，则 NetBIOS 名称通常是 **AD**。但这不是必须的。务必要确保 NetBIOS 名称只包括一个词且没有句点。NetBIOS 名称的最大长度为 15 个字符。
- IdM 系统必须在内核中启用 IPv6 协议。
  如果禁用 IPv6，IdM 服务使用的 CLDAP 插件将无法初始化。

**注意**

在 RHEL 7 中，*同步* 和 *信任* 是把 RHEL 系统间接集成到活动目录(AD)的两种可能的方法。在 RHEL 8 中，同步已弃用，在 RHEL 9 中，它不再提供。要集成 IdM 和 AD，请使用信任方法。要在 RHEL 8 中从同步迁移到信任，请参阅 在将 Linux 域与活动目录域集成上下文中将现有环境从同步迁移到信任。

# 第 2 章 WINDOWS 服务器支持的版本

您可以使用以下林和域功能级别与 Active Directory (AD)论坛建立信任关系：

- 林功能级别范围：Windows Server 2012 – Windows Server 2016
- 域功能级别范围：Windows Server 2012 – Windows Server 2016

身份管理 (IdM) 支持与运行以下操作系统的 Active Directory 域控制器建立信任：

- Windows Server 2022（RHEL 9.1 及更新版本）
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

**重要**

身份管理 (IdM) 不支持使用运行 Windows Server 2008 R2 或更早版本的 Active Directory 域控制器建立对 Active Directory 的信任。RHEL IdM 在建立信任关系时需要 SMB 加密，这只在 Windows Server 2012 或更高版本中被支持。

# 第 3 章 信任如何工作

身份管理 IdM 和 Active Directory(AD)之间的信任是建立在跨域 Kerberos 信任上的。这个解决方案使用 Kerberos 功能在不同的身份源间建立信任。因此，所有 AD 用户都可以：

- 登录访问 Linux 系统和资源。
- 使用单点登录（SSO）。

所有 IdM 对象都在 IdM 中的信任中管理。

所有 AD 对象都在信任的 AD 中管理。

在复杂的环境中，单个 IdM 林可以连接到多个 AD 林。这个设置可以为机构的不同功能更好地分离任务。AD 管理员可以专注于用户和与用户相关的策略，而 Linux 管理员对 Linux 基础架构完全控制。在这种情况下，IdM 控制的 Linux 领域类似于 AD 资源域或领域，但其中包含 Linux 系统。

从 AD 的角度来看，身份管理代表一个独立的 AD 域。当 AD 林根域和 IdM 域之间建立了跨林信任时，AD 林域中的用户可以与 IdM 域中的 Linux 机器和服务进行交互。

**注意**

在信任的环境中，IdM 可让您使用 ID 视图来为 IdM 服务器上的 AD 用户配置 POSIX 属性。

# 第 4 章 AD 管理权利

当您要在 AD(Active Directory)和 IdM（身份管理）之间建立信任时，您需要使用具有适当 AD 特权的 AD 管理员帐户。

这样 AD 管理员必须是以下组之一的成员：

- AD 林中的企业管理员组
- AD 林的林根域中的域管理员组

**其他资源**

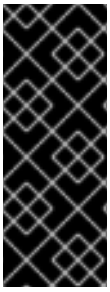
- 有关 Enterprise Admins 的详情，请参考 Enterprise Admins。
- 有关域管理员的详情，请查看 域管理员 。
- 有关 AD 信任的详情，请查看 域和林信任是如何工作的。

# 第 5 章 确保支持 AD 和 RHEL 中的通用加密类型

默认情况下，身份管理建立跨领域信任关系，支持 RC4、AES-128 和 AES-256 Kerberos 加密类型。另外，默认情况下，SSSD 和 Samba Winbind 支持 RC4、AES-128 和 AES-256 Kerberos 加密类型。

RC4 加密已被弃用并默认禁用，因为它被视为不如较新的 AES-128 和 AES-256 加密类型安全。相反，活动目录(AD)用户凭证和 AD 域之间的信任支持 RC4 加密，它们可能不支持所有 AES 加密类型。

如果没有任何常用的加密类型，RHEL 和 AD 域之间的通信可能无法正常工作，或者可能无法对一些 AD 帐户进行身份验证。要解决这种情况，请执行以下部分中列出的配置之一。



**重要**

如果 IdM 处于 FIPS 模式，IdM-AD 集成无法正常工作，因为 AD 只支持使用 RC4 或 AES HMAC-SHA1 加密，而 FIPS 模式中的 RHEL 9 默认只允许 AES HMAC-SHA2。要在 RHEL 9 中启用 AES HMAC-SHA1，请输入 **# update-crypto-policies --set FIPS:AD-SUPPORT**。

IdM 不支持更严格的 **FIPS:OSPP** 加密策略，该策略只应用于通用标准评估的系统。

## 5.1. 在 AD 中启用 AES 加密（推荐）

要确保 AD 林中的活动目录(AD)域间的信任支持强 AES 加密类型，请参阅以下 Microsoft 文章：AD DS：安全：在访问可信域中的资源时，Kerberos "Unsupported etype" 错误

## 5.2. 使用 GPO 在 ACTIVE DIRECTORY 中启用 AES 加密类型

这部分描述了如何使用组策略对象(GPO)在 Active Directory(AD)中启用 AES 加密类型。RHEL 上的某些功能（如在 IdM 客户端上运行 Samba 服务器）需要这个加密类型。

请注意，RHEL 不再支持弱 DES 和 RC4 加密类型。

**先决条件**

- 以可编辑组策略的用户身份登录到 AD。
- 计算机上安装了组**策略管理控制台**。

**流程**

1. 打开组**策略管理控制台**。
2. 右键单击**默认域策略**，然后选择**编辑**。打开组**策略管理编辑器**。
3. 导航到 **计算机配置 → 策略 → Windows 设置 → 安全设置 → 本地策略 → 安全选项**。
4. 双击 **Network security：配置 Kerberos** 策略允许的加密类型。
5. 选择**AES256_HMAC_SHA1**和可选的**未来加密类型**。
6. 点**确定**。
7. 关闭组**策略管理编辑器**。
8. 对**默认域控制器策略**重复上述步骤。

9. 等待 Windows 域控制器(DC)自动应用组策略。或者，如果要在 DC 上手动应用 GPO，请使用具有管理员权限的帐户输入以下命令：

```
C:\> gpupdate /force /target:computer
```

## 5.3. 在 RHEL 中启用 RC4 支持

在针对 AD 域控制器进行身份验证的每个 RHEL 主机上，完成以下概述的步骤。

**流程**

1. 除 **DEFAULT** 加密策略外，使用 **update-crypto-policies** 命令来启用 **AD-SUPPORT-LEGACY** 加密子策略。

```
[root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT-LEGACY
Setting system policy to DEFAULT:AD-SUPPORT-LEGACY
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

2. 重启主机。

## 5.4. 其他资源

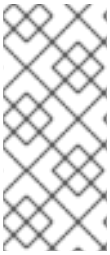
- 请参阅使用系统范围的加密策略。
- 请参阅 信任控制器和信任代理。

# 第 6 章 IDM 和 AD 间的通信所需的端口

要启用 Active Directory(AD)和身份管理(IdM)环境之间的通信，请在 AD 域控制器和 IdM 服务器的防火墙中开放以下端口：

**表 6.1. AD 信任所需的端口**

| 服务 | 端口 | 协议 |
|---|---|---|
| 端点解析端口映射器 | 135 | TCP |
| NetBIOS-DGM | 138 | TCP 和 UDP |
| NetBIOS-SSN | 139 | TCP 和 UDP |
| Microsoft-DS | 445 | TCP 和 UDP |
| Dynamic RPC | 49152-65535 | TCP |
| AD Global Catalog | 3268 | TCP |
| LDAP | 389 | TCP 和 UDP |



**注意**

在 IdM 服务器中不需要为信任打开 TCP 端口 389，但与 IdM 服务器通信的客户端需要这样端口。

DCE RPC 端点映射程序需要 TCP 端口 135 才能正常工作，并在 IdM-AD 信任创建过程中使用。

要打开端口，您可以使用以下方法：

- **firewalld** 服务 – 您可以启用特定的端口，或启用包括端口的以下服务：
  - FreeIPA 信任设置
  - LDAP 的 FreeIPA
  - Kerberos
  - DNS

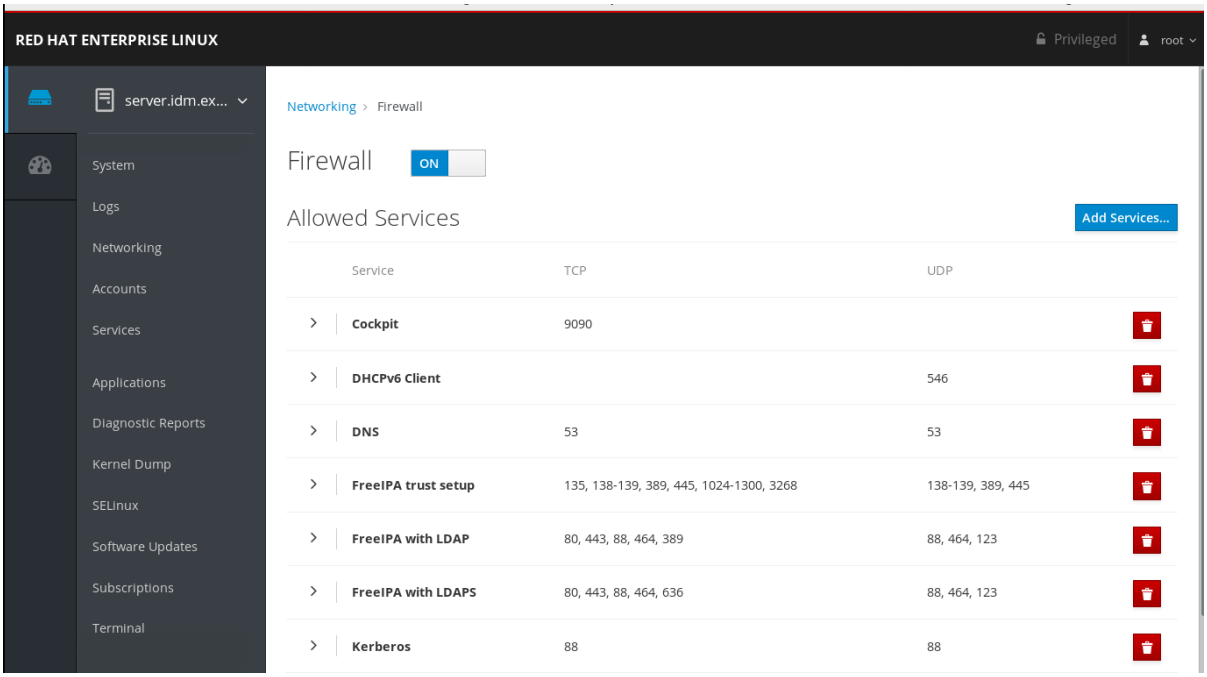
  详情请查看 **firewall-cmd** 手册页。

**注意**

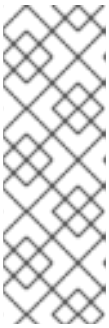
如果您使用 RHEL 8.2 及更早版本，**freeipa-trust** firewalld 服务包含 RPC 端口范围 **1024-1300**，这是不正确的。在 RHEL 8.2 及更早版本上，除了启用 **freeipa-trust** firewalld 服务外，您必须手动打开 TCP 端口范围 **49152-65535**。

这个问题已在 RHEL 8.3 和更新的版本中被解决。（Bug 1850418 - update freeipa-trust.xml definition to include correct dynamic RPC range）

- RHEL web 控制台，是一个基于 **firewalld** 服务的带有防火墙设置的 UI。




有关通过 Web 控制台配置防火墙的详情，请参阅 使用 Web 控制台在防火墙上启用服务



**注意**

如果您使用 RHEL 8.2 及更早版本，则 **FreeIPA Trust Setup** 服务包含 RPC 端口范围 **1024-1300**，这不正确。在 RHEL 8.2 及更早的版本中，除了在 RHEL web 控制台中启用 **FreeIPA Trust Setup** 服务外，您必须手动打开 TCP 端口范围 **49152-65535**。

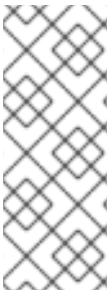
这个问题已在 RHEL 8.3 和更新的版本中被解决。（Bug 1850418 - update freeipa-trust.xml definition to include correct dynamic RPC range）

**表 6.2. 信任中的 IdM 服务器所需的端口**

| 服务 | 端口 | 协议 |
|---|---|---|
| Kerberos | 88, 464 | TCP 和 UDP |
| LDAP | 389 | TCP |
| DNS | 53 | TCP 和 UDP |

**表 6.3. AD 信任中 IdM 客户端所需的端口**

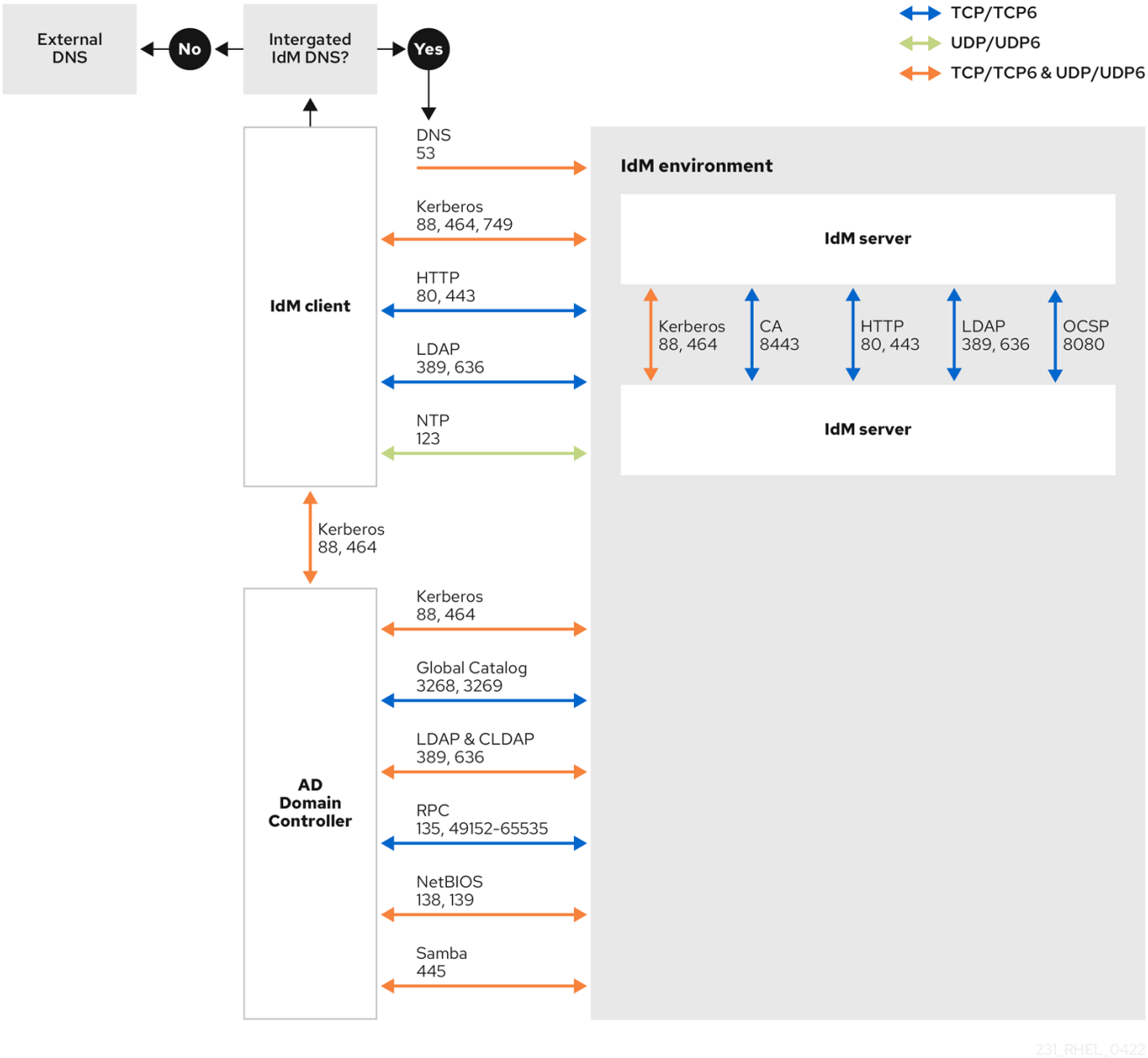
| 服务 | 端口 | 协议 |
| --- | --- | --- |
| Kerberos | 88 | UDP 和 TCP |



**注意**

如果从密钥分发中心(KDC)发送的数据太大，**libkrb5** 库会使用 UDP，并回退到 TCP 协议。Active Directory 将 Privilege Attribute 证书（PAC）附加到 Kerberos 票据上，这会增加大小，需要使用 TCP 协议。为了避免回退和重新发出请求，Red Hat Enterprise Linux 7.4 及之后的版本中的 SSSD 使用 TCP 进行用户身份验证。如果要在 **libkrb5** 使用 TCP 前配置大小，请在 **/etc/krb5.conf** 文件中设置 **udp_preference_limit**。详情请查看 **krb5.conf(5)** 手册页。

下图显示了 IdM 客户端发送的通信，以及 IdM 服务器和 AD 域控制器接收和响应的通信。要在防火墙上设置传入和传出的端口和协议，红帽建议使用 **firewalld** 服务，该服务已有 FreeIPA 服务的定义。




**其他资源**

- 有关 Windows Server 2008 及之后版本中动态 RPC 端口范围的更多信息，请参阅 从 Windows Vista 起和 Windows Server 2008 中已更改的 TCP/IP 的默认动态端口范围。

# 第 7 章 为信任配置 DNS 和域设置

在您连接信任中的身份管理(IdM)和 Active Directory(AD)之前，您需要确保服务器可以互相看到，并能够正确解析域名。要将 DNS 配置为允许使用以下之间的域名：

- 使用集成 DNS 服务器和认证认证机构的主 IdM 服务器。
- 一个 AD Domain Controller。

DNS 设置需要：

- 在 IdM 服务器中配置 DNS 区域
- 在 AD 中配置有条件 DNS 转发
- 验证 DNS 配置的正确性

## 7.1. 唯一的主 DNS 域

在 Windows 中，每个域都是一个 Kerberos 域（realm）和一个 DNS 域（domain）。每个由域控制器管理的域都需要拥有自己的专用 DNS 区。当身份管理(IdM)被 Active Directory(AD)信任为林时也是如此。AD 期望 IdM 有自己的 DNS 域。要使信任设置正常工作，DNS 域需要专用于 Linux 环境。

每个系统都必须配置自己的唯一的主 DNS 域。例如：

- ***ad.example.com*** 用于 AD， ***ldm.example.com*** 用于 IdM。
- ***example.com*** 用于 AD， ***idm.example.com*** 用于 IdM
- AD的 ***ad.example.com*** 和 IdM 的 ***example.com***

最方便的管理解决方案是，每个 DNS 域都由集成的 DNS 服务器管理，但也可以使用任何其他符合标准的 DNS 服务器。

**Kerberos realm 名称作为主 DNS 域名的大写版本**

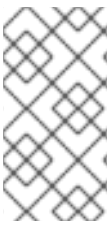
Kerberos realm 名称必须与主 DNS 域名相同，且所有字母都为大写。例如，如果 AD 的域名是 ***ad.example.com***，而 IdM的域名是 ***idm.example.com***，则 Kerberos 领域名称必须是 ***AD.EXAMPLE.COM*** 和 ***IDM.EXAMPLE.COM***。

**DNS 记录可从信任中的所有 DNS 域解析**

所有机器都必须能够从所有涉及信任关系的 DNS 域解析 DNS 记录。

**IdM 和 AD DNS 域**

加入 IdM 的系统可以通过多个 DNS 域进行发布。红帽建议您在与 Active Directory 拥有的 DNS 区域中部署 IdM 客户端。主 IdM DNS 域必须具有正确的 SRV 记录来支持 AD 信任。



**注意**

在 IdM 和 Active Directory 之间具有信任的某些环境中，您可以在作为 Active Directory DNS 域一部分的主机上安装 IdM 客户端。然后，主机可以从基于 Linux 的 IdM 功能中获益。这不是推荐的配置，存在一些限制。如需了解更多详细信息，请参阅在 Active Directory DNS 域中配置 IdM 客户端。

您可以运行以下命令来获取特定于您的系统设置所需的 SRV 记录列表：

```
$ ipa dns-update-system-records --dry-run
```

生成的列表可以类似如下：

```
IPA DNS records:
  _kerberos-master._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
  _kerberos-master._udp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
  _kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
  _kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
  _kerberos.idm.example.com. 86400 IN TXT "IDM.EXAMPLE.COM"
  _kpasswd._tcp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
  _kpasswd._udp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
  _ldap._tcp.idm.example.com. 86400 IN SRV 0 100 389 server.idm.example.com.
  _ipa-ca.idm.example.com. 86400 IN A 192.168.122.2
```

对于同一 IdM 领域一部分的其他 DNS 域，在配置了对 AD 的信任时不需要配置 SRV 记录。原因在于 AD 域控制器不使用 SRV 记录来发现 KDC，而是基于对信任的名称后缀路由信息的 KDC 发现。

## 7.2. 在 IDM WEB UI 中配置 DNS 转发区域

按照以下流程，使用 IdM Web UI 将 DNS 转发区域添加到身份管理(IdM)服务器中。

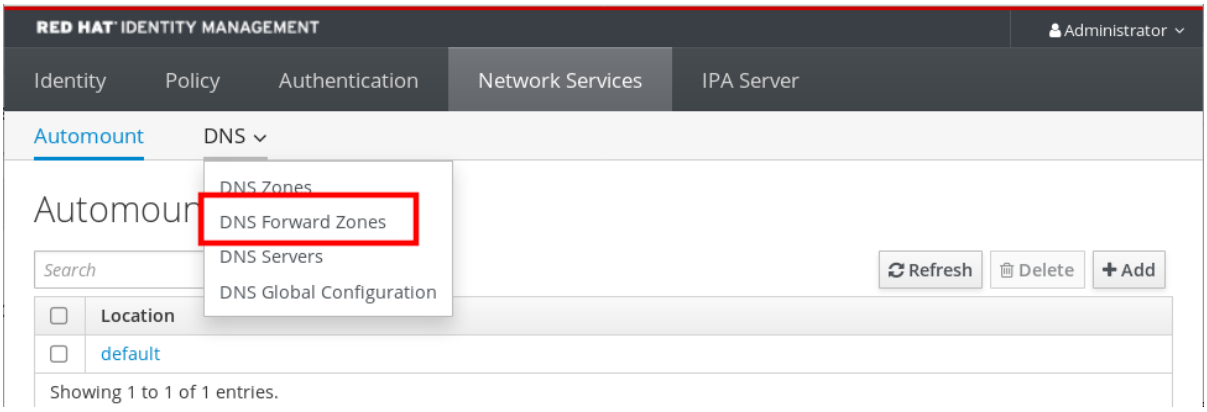
使用 DNS 转发区域，您可以将对特定区域的 DNS 查询转发到不同的 DNS 服务器。例如，您可以将活动目录(AD)域的 DNS 查询转发到 AD DNS 服务器。

**先决条件**

- 使用具有管理员权限的用户帐户访问 IdM Web UI。
- 正确配置了 DNS 服务器。

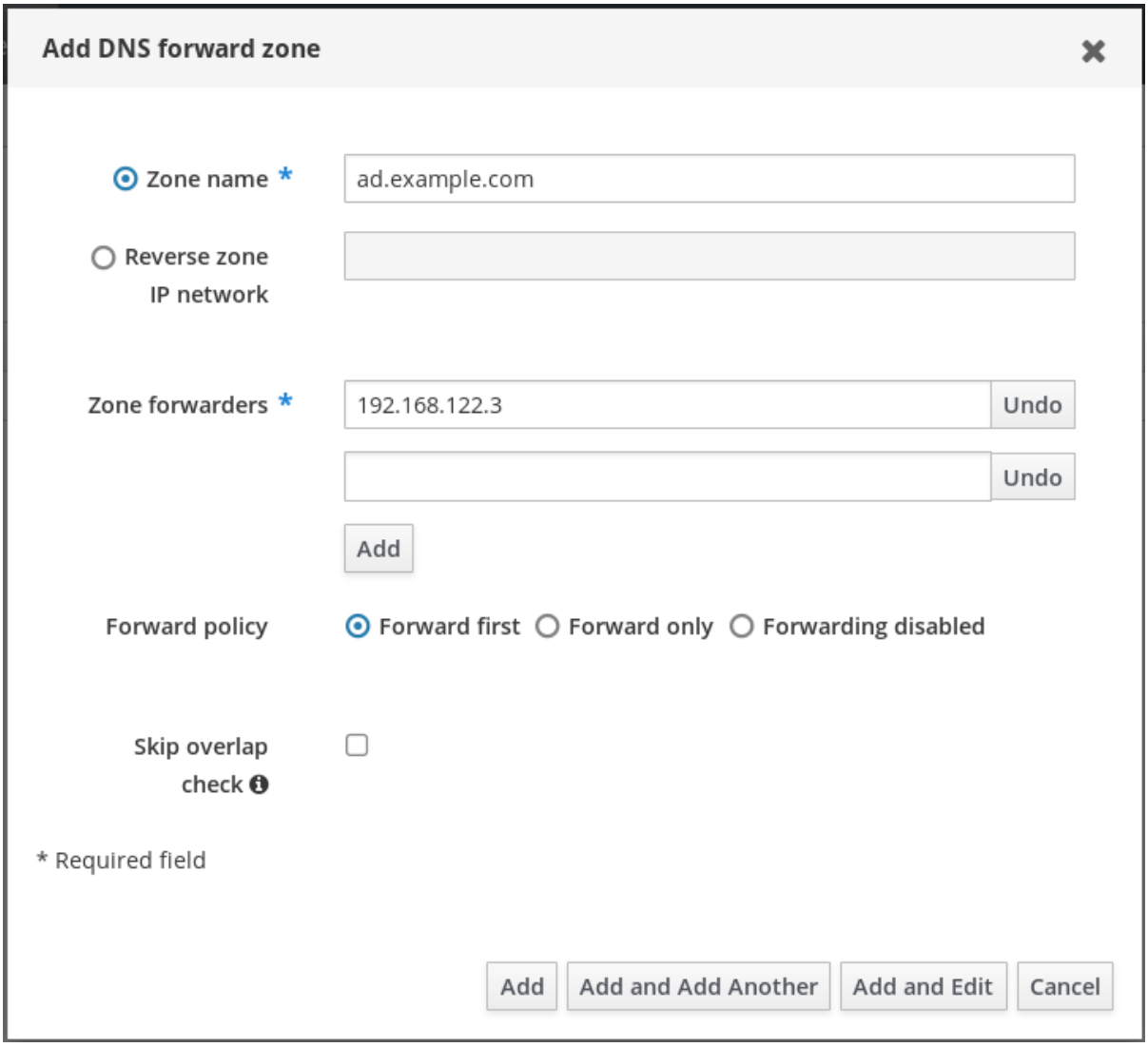
**流程**

1. 使用管理员权限登录到 IdM Web UI。详情请参阅通过 Web 浏览器访问 IdM Web UI 。
2. 点 **Network Services** 标签页。
3. 点 **DNS** 标签页。
4. 在下拉菜单中点击 **DNS Forward Zones** 项。




5. 点击 **Add** 按钮。

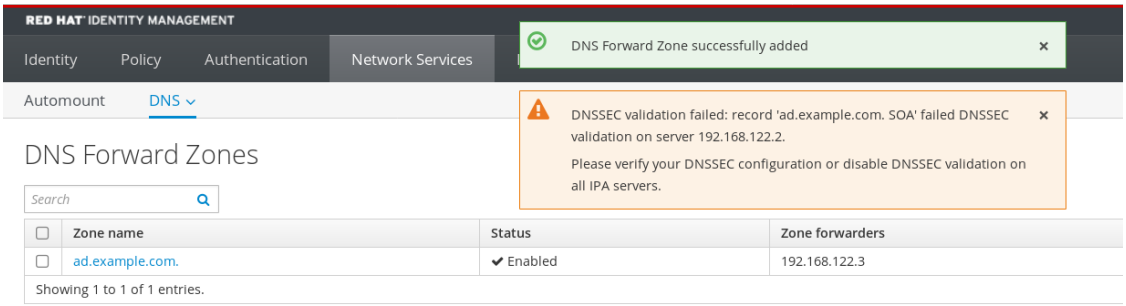
6. 在 **Add DNS forward zone** 对话框中，添加一个区名称。
7. 在**Zone forwarders** 项中，点击 **Add** 按钮。
8. 在 **Zone forwarders** 字段中，添加您要为其创建转发区域的服务器的 IP 地址。
9. 点击 **Add** 按钮。




正向区已添加到 DNS 设置中，您可以在 DNS Forward Zones 设置中进行验证。Web UI 会在以下弹出消息中告知已成功：**DNS Forward Zone successfully added.**

**注意**

在向配置中添加 forward zone 后，Web UI 可能会显示有关 DNSSEC 验证失败的警告。




DNSSEC（域名系统安全扩展）使用数字签名来保护 DNS 数据，使 DNS 免受攻击。在 IdM 服务器中默认启用该服务。出现警告的原因是远程 DNS 服务器没有使用 DNSSEC。红帽建议您在远程 DNS 服务器上启用 DNSSEC。

如果您无法在远程服务器上启用 DNSSEC 验证，您可以在 IdM 服务器中禁用 DNSSEC ：

1. 选择要编辑的合适的配置文件：
   - 如果您的 IdM 服务器使用 RHEL 8.0 或 RHEL 8.1，请打开 **/etc/named.conf** 文件。
   - 如果您的 IdM 服务器使用 RHEL 8.2 或更高版本，请打开 **/etc/named/ipa-options-ext.conf** 文件。
2. 添加以下 DNSSEC 参数：

```
dnssec-enable no;
dnssec-validation no;
```

3. 保存并关闭配置文件。
4. 重启 DNS 服务：

```
# systemctl restart named-pkcs11
```

**验证步骤**

- 将 **nslookup** 命令与远程 DNS 服务器名称一起使用：

```
$ nslookup ad.example.com
Server:         192.168.122.2
Address:        192.168.122.2#53

No-authoritative answer:
Name:           ad.example.com
Address:        192.168.122.3
```

如果您正确配置了域转发，则会显示远程 DNS 服务器的 IP 地址。

## 7.3. 在 CLI 中配置 DNS 转发区域

按照以下流程，使用命令行界面(CLI)将新的 DNS 转发区域添加到身份管理(IdM)服务器中。

使用 DNS 转发区域，您可以将对特定区域的 DNS 查询转发到不同的 DNS 服务器。例如，您可以将活动目录(AD)域的 DNS 查询转发到 AD DNS 服务器。

**先决条件**

- 使用具有管理员权限的用户帐户访问 CLI。
- 正确配置了 DNS 服务器。

**步骤**

- 为 AD 域创建 DNS 转发区域，并使用 **--forwarder** 选项指定远程 DNS 服务器的 IP 地址：

```
# ipa dnsforwardzone-add ad.example.com --forwarder=192.168.122.3 --forward-policy=first
```

**注意**

在向配置添加新的转发区域后，您可能会在 **/var/log/messages** 系统日志中看到有关 DNSSEC 验证失败的警告：

```
named-pkcs11[2572]: no valid DS resolving 'host.ad.example.com/A/IN':
192.168.100.25#53
```

DNSSEC（域名系统安全扩展）使用数字签名来保护 DNS 数据，使 DNS 免受攻击。在 IdM 服务器中默认启用该服务。出现警告的原因是远程 DNS 服务器没有使用 DNSSEC。红帽建议您在远程 DNS 服务器上启用 DNSSEC。

如果您无法在远程服务器上启用 DNSSEC 验证，您可以在 IdM 服务器中禁用 DNSSEC ：

1. 打开 **/etc/named/ipa-options-ext.conf** 文件。
2. 添加以下 DNSSEC 参数：

```
dnssec-enable no;
dnssec-validation no;
```

3. 保存并关闭配置文件。
4. 重启 DNS 服务：

```
# systemctl restart named-pkcs11
```

**验证步骤**

- 将 **nslookup** 命令与远程 DNS 服务器名称一起使用：

```
$ nslookup ad.example.com
Server:         192.168.122.2
Address:        192.168.122.2#53
```

```
No-authoritative answer:
Name:          ad.example.com
Address:       192.168.122.3
```

如果正确配置了域转发，**nslookup** 请求会显示远程 DNS 服务器的 IP 地址。

## 7.4. 在 AD 中配置 DNS 转发

按照以下流程，在活动目录(AD)中为身份管理(IdM)服务器设置 DNS 转发。

**先决条件**

- 已安装 AD 的 Windows Server。
- 在两个服务器中打开 DNS 端口。

**流程**

1. 登录到 Windows 服务器。
2. 打开 **Server Manager**。
3. 打开 **DNS Manager**。
4. 在 **Conditional Forwarders** 中，使用以下内容添加新的条件正向解析器：
   - IdM 服务器 IP 地址
   - 完全限定域名，例如 ***server.idm.example.com***
5. 保存设置。

## 7.5. 验证 DNS 配置

在配置信任前，请验证身份管理（IdM）和 Active Directory（AD）服务器是否可以相互解析。

**先决条件**

- 您需要以 sudo 权限登录。

**流程**

1. 对通过 UDP 的 Kerberos 和通过 TCP 服务记录的 LDAP 运行 DNS 查询。

```
[admin@server ~]# dig +short -t SRV _kerberos._udp.idm.example.com.
0 100 88 server.idm.example.com.

[admin@server ~]# dig +short -t SRV _ldap._tcp.idm.example.com.
0 100 389 server.idm.example.com.
```

这些命令应该列出所有 IdM 服务器。

2. 使用 IdM Kerberos 域名称对 TXT 记录运行 DNS 查询。获得的值应该与您在安装 IdM 时指定的 Kerberos 域匹配。

```
[admin@server ~]# dig +short -t TXT _kerberos.idm.example.com.
"IDM.EXAMPLE.COM"
```

如果前面的步骤没有返回所有预期的记录，请使用缺失的记录更新 DNS 配置：

- 如果您的 IdM 环境使用集成的 DNS 服务器，请输入不带任何选项的 **ipa dns-update-system-records** 命令，来更新您的系统记录：

```
[admin@server ~]$ ipa dns-update-system-records
```

- 如果您的 IdM 环境没有使用集成的 DNS 服务器：

  1. 在 IdM 服务器中，将 IdM DNS 记录导出到文件中：

```
[admin@server ~]$ ipa dns-update-system-records --dry-run --out
dns_records_file.nsupdate
```

     该命令使用相关的 IdM DNS 记录创建一个名为 **dns_records_file.nsupdate** 的文件。

  2. 使用 **nsupdate** 工具和 **dns_records_file.nsupdate** 文件向 DNS 服务器提交 DNS 更新请求。如需更多信息，请参阅 RHEL 7 文档中的 使用 nsupdate 更新外部 DNS 记录。或者，请参阅 DNS 服务器文档来添加 DNS 记录。

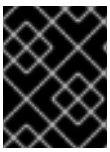
3. 验证 IdM 能够通过一个命令来解析 AD 的服务记录，该命令对 Kerberos 和通过 TCP 服务记录的 LDAP 运行 DNS 查询：

```
[admin@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[admin@server ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

# 第 8 章 在活动目录 DNS 域中配置 IDM 客户端

如果您在由活动目录控制的 DNS 域中有客户端系统，并且您需要这些客户端能够加入 IdM 服务器以从其 RHEL 功能中受益，则可以配置用户，来使用活动目录 DNS 域的主机名访问客户端。



**重要**

这不是推荐的配置，存在一些限制。红帽建议始终将 IdM 客户端部署在与活动目录拥有的区域不同的 DNS 区域中，并通过其 IdM 主机名访问 IdM 客户端。

您的 IdM 客户端配置取决于您是否需要使用 Kerberos 单点登录。

## 8.1. 配置没有 KERBEROS 单点登录的 IDM 客户端

如果 IdM 客户端位于活动目录 DNS 域中，密码身份验证是唯一可供用户访问 IdM 客户端上资源的身份验证方法。按照以下流程配置没有 Kerberos 单点登录的客户端。

**步骤**

1. 使用 **--domain=IPA_DNS_Domain** 选项安装 IdM 客户端，来确保系统安全服务守护进程(SSSD)可以与 IdM 服务器进行通信：

```
[root@idm-client.ad.example.com ~]# ipa-client-install --domain=idm.example.com
```

   这个选项禁用了活动目录 DNS 域的 SRV 记录自动检测。

2. 打开 **/etc/krb5.conf** 配置文件，并在 **[domain_realm]** 部分中找到活动目录域的现有映射。

```
.ad.example.com = IDM.EXAMPLE.COM
ad.example.com = IDM.EXAMPLE.COM
```

3. 将这两个行替换为将活动目录 DNS 区域中 Linux 客户端的完全限定域名(FQDN)映射到 IdM 域的条目：

```
idm-client.ad.example.com = IDM.EXAMPLE.COM
```

   通过替换默认映射，您可以防止 Kerberos 将其对活动目录域的请求发送到 IdM Kerberos 分发中心(KDC)。相反，Kerberos 使用通过 SRV DNS 记录的自动发现来定位 KDC。

## 8.2. 请求没有单点登录的 SSL 证书

基于 SSL 的服务需要带有 **dNSName** 扩展记录的证书，该扩展记录涵盖所有系统主机名，因为原始(A/AAAA)和 CNAME 记录都必须在证书里。目前，IdM 只对 IdM 数据库中的主机对象颁发证书。

在描述的没有单点登录的设置中，IdM 已在数据库中有 一个 FQDN 主机对象，并且 **certmonger** 可以使用此名称来请求证书。

**先决条件**

- 按照 配置没有 Kerberos 单点登录的 IdM 客户端 中的流程来安装和配置 IdM 客户端。

**步骤**

- 使用 **certmonger** 来请求使用 FQDN 的证书：

```
[root@idm-client.ad.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=ipa-client.ad.example.com \
    -D ipa-client.ad.example.com \
    -K host/idm-client.ad.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

**certmonger** 服务使用存储在 **/etc/krb5.keytab** 文件中的默认主机密钥来验证 IdM 证书颁发机构(CA)。

## 8.3. 配置带有 KERBEROS 单点登录的 IDM 客户端

如果您需要 Kerberos 单点登录来访问 IdM 客户端上的资源，则该客户端必须在 IdM DNS 域中，如 **idm-client.idm.example.com**。您必须在指向 IdM 客户端的 A/AAAA 记录的活动目录 DNS 域中创建一个 CNAME 记录 **idm-client.ad.example.com** 。

对于基于 Kerberos 的应用服务器，MIT Kerberos 支持一种方法，来允许接受应用程序的 keytab 中任何基于主机的主体。

**步骤**

- 在 IdM 客户端上，通过在 **/etc/krb5.conf** 配置文件的 **[libdefaults]** 部分中设置以下选项，来禁用针对 Kerberos 服务器的 Kerberos 主体的严格检查：

```
ignore_acceptor_hostname = true
```

## 8.4. 请求带有单点登录的 SSL 证书

基于 SSL 的服务需要带有 **dNSName** 扩展记录的证书，该扩展记录涵盖所有系统主机名，因为原始(A/AAAA)和 CNAME 记录都必须在证书里。目前，IdM 只对 IdM 数据库中的主机对象颁发证书。

按照以下流程，在 IdM 中为 **ipa-client.example.com** 创建主机对象，并确保实际的 IdM 机器的主机对象可以管理此主机。

**先决条件**

- 您已禁用了针对 Kerberos 主机的 Kerberos 主体的目严格检查，如 配置带有 Kerberos 单点登录的 IdM 客户端 中所述。

**步骤**

1. 在 IdM 服务器上创建一个新的主机对象：

```
[root@idm-server.idm.example.com ~]# ipa host-add idm-client.ad.example.com --force
```

使用 **--force** 选项，因为主机名是 CNAME，而不是 A/AAAA 记录。

2. 在 IdM 服务器上，允许 IdM DNS 主机名来管理 IdM 数据库中的活动目录主机条目：

```
[root@idm-server.idm.example.com ~]# ipa host-add-managedby idm-client.ad.example.com
\
    --hosts=idm-client.idm.example.com
```

3. 现在，您可以为您的 IdM 客户端请求一个 SSL 证书，并带有在活动目录 DNS 域中其主机名称的 **dNSName** 扩展记录：

```
[root@idm-client.idm.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=`hostname --fqdn` \
    -D `hostname --fqdn` \
    -D idm-client.ad.example.com \
    -K host/idm-client.idm.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

# 第 9 章 设置信任

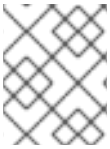
本节描述了如何使用命令行在 IdM 端上配置身份管理(IdM)/Active Directory(AD)信任。

**先决条件**

- 正确配置了 DNS。IdM 和 AD 服务器必须能够解析其他名称。详情请参阅为信任配置 DNS 和领域设置。
- 部署了 AD 和 IdM 的支持版本。详情请查看 支持的 Windows Server 版本。
- 您已获得 Kerberos ticket。详情请参阅 使用 kinit 手动登录到 IdM 。

## 9.1. 为信任准备 IDM 服务器

在与 AD 建立信任前，您必须在 IdM 服务器上使用 **ipa-adtrust-install** 工具来准备 IdM 域。



**注意**

在其上运行 **ipa-adtrust-install** 命令的所有系统都会自动成为 AD 信任控制器。但是，您必须在 IdM 服务器上只运行一次 **ipa-adtrust-install** 。

**先决条件**

- IdM 服务器已安装。
- 您需要 root 权限才能安装软件包并重新启动 IdM 服务。

**步骤**

1. 安装所需的软件包：

```
[root@ipaserver ~]# dnf install ipa-server-trust-ad samba-client
```

2. 以 IdM 管理用户身份进行身份验证：

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

3. 运行 **ipa-adtrust-install** 工具：

```
[root@ipaserver ~]# ipa-adtrust-install
```

如果 IdM 安装了集成的 DNS 服务器，则会自动创建 DNS 服务记录。

如果您在没有集成 DNS 服务器的情况下安装了 IdM，**ipa-adtrust-install** 会打印一个服务记录列表，您必须手动将它们添加到 DNS，然后才能继续操作。

4. 该脚本提示您 **/etc/samba/smb.conf** 已存在，并将被重写：

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your existing
Samba configuration.

Do you wish to continue? [no]: yes
```

5. 该脚本提示您配置 **slapi-nis** 插件，这是一个兼容插件，允许旧的 Linux 客户端与受信任的用户一起工作：

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted users.

Enable trusted domains support in slapi-nis? [no]: yes
```

6. 系统会提示您运行 SID 生成任务，以便为任何现有用户创建 SID：

```
Do you want to run the ipa-sidgen task? [no]: yes
```

这是一个资源密集型任务，因此如果您有大量的用户，您可以在其他时间运行此操作。

7. **（可选）** 默认情况下，对于 Windows Server 2008 及更高版本，动态 RPC 端口范围定义为 **49152-65535**。如果需要为您的环境定义一个不同的动态 RPC 端口范围，请将 Samba 配置为使用不同的端口，并在防火墙设置中开放这些端口。以下示例将端口范围设置为 **55000-65000**。

```
[root@ipaserver ~]# net conf setparm global 'rpc server dynamic port range' 55000-65000
[root@ipaserver ~]# firewall-cmd --add-port=55000-65000/tcp
[root@ipaserver ~]# firewall-cmd --runtime-to-permanent
```

8. 确保正确配置了DNS，如 验证信任的 DNS 配置 中所述。

**重要**

红帽强烈建议您在每次运行完 **ipa-adtrust-install** 后，验证 DNS 配置，如 验证信任的 DNS 配置 中所述，特别是如果 IdM 或 AD 不使用集成的 DNS 服务器。

9. 重启 **ipa** 服务：

```
[root@ipaserver ~]# ipactl restart
```

10. 使用 **smbclient** 工具来验证 Samba 是否会对 IdM 端的 Kerberos 身份验证做出响应：

```
[root@ipaserver ~]# smbclient -L ipaserver.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
   Sharename       Type      Comment
   ---------       ----      -------
   IPC$            IPC       IPC Service (Samba 4.15.2)
...
```

## 9.2. 使用命令行设置信任协议

按照以下流程使用命令行设置信任协议。身份管理(IdM)服务器允许您配置三种类型的信任协议：

- **One-way trust** – 默认选项。单向信任使 Active Directory（AD）的用户和组可以访问 IdM 中的资源，但不允许反向访问。IdM 域信任 AD 林，但 AD 林不信任 IdM 域。

- **双向信任** - 双向信任使 AD 用户和组可以访问 IdM 中的资源。
  您必须为像 Microsoft SQL Server 这样的解决方案配置双向信任，该解决方案希望 Kerberos 协

议的 **S4U2Self** 和 **S4U2Proxy** Microsoft 扩展能够跨信任边界工作。RHEL IdM 主机上的应用可能会向 Active Directory 域控制器请求有关 AD 用户的 **S4U2Self** 或 **S4U2Proxy** 信息，双向信任提供了这一特性。

请注意，这个双向信任功能并不允许 IdM 用户登录到 Windows 系统，IdM 中的双向信任并不为用户授予与 AD 中的单向信任解决方案相比的任何额外权利。

  - 要创建双向信任，请向命令中添加以下选项：**--two-way=true**

- **外部信任** - 不同林中的 IdM 和 AD 域之间的信任关系。虽然林信任总是需要在 IdM 和 Active Directory 林的根域之间建立信任，但可以从 IdM 到林中的域建立外部信任只有由于管理或组织方面的原因而无法在林根域之间建立林信任时，才推荐这么做。

  - 要创建外部信任，请在命令中添加以下选项：**--external=true**

以下步骤演示了如何创建单向信任协议。

**先决条件**

- Windows 管理员的用户名和密码。
- 您已为信任准备了 IdM 服务器。

**步骤**

- 使用 **ipa trust-add** 命令为 AD 域和 IdM 域创建信任协议：

  - 要让 SSSD 根据其 SID 自动为 AD 用户生成 UID 和 GID，请使用 **活动目录域** ID 范围类型创建一个信任协议。这是最常见的配置。

    ```
    [root@server ~]# ipa trust-add --type=ad ad.example.com --admin
    <ad_admin_username> --password --range-type=ipa-ad-trust
    ```

  - 如果您已经为 Active Directory 中的用户配置了 POSIX 属性（如 **uidNumber** 和 **gidNumber**），并且希望 SSSD 处理此信息，请使用 **POSIX 属性 ID 范围类型创建与 Active Directory 域的** 信任协议：

    ```
    [root@server ~]# ipa trust-add --type=ad ad.example.com --admin
    <ad_admin_username> --password --range-type=ipa-ad-trust-posix
    ```

**警告**

如果您在创建信任时没有指定 ID Range 类型，IdM 会尝试通过在林根域中请求 AD 域控制器的详情来自动选择适当的范围类型。如果 IdM 没有检测到任何 POSIX 属性，则信任安装脚本选择 **Active Directory 域** ID 范围。

如果 IdM 检测到林根域中的任何 POSIX 属性，则信任安装脚本选择 **带有 POSIX 属性 ID 范围的 Active Directory 域**，并假定 AD 中正确配置了 UID 和 GID。如果 AD 中没有正确设置 POSIX 属性，您将无法解析 AD 用户。

例如，如果需要访问 IdM 系统的用户和组不是林根域的一部分，而是位于林域的子域中，安装脚本可能不会检测到子 AD 域中定义的 POSIX 属性。在这种情况下，红帽建议您在创建信任时显式选择 POSIX ID 范围类型。

## 9.3. 在 IDM WEB UI 中设置信任协议

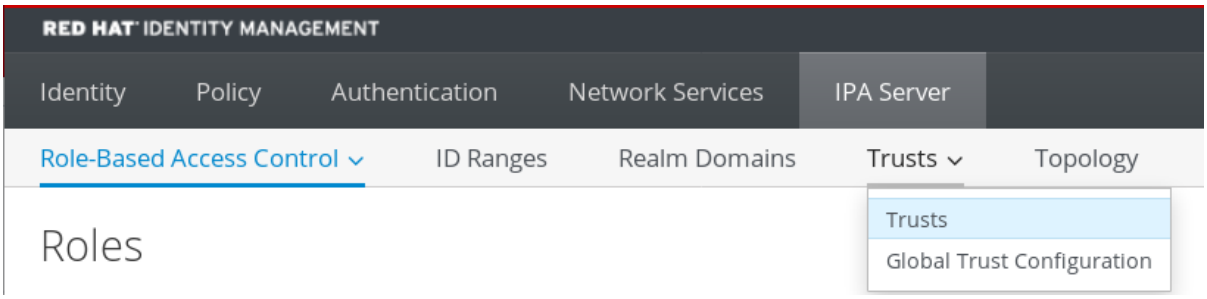
按照以下流程，使用 IdM Web UI 在 IdM 端配置身份管理(IdM)/活动目录(AD)信任协议。

**先决条件**

- 正确配置了 DNS。IdM 和 AD 服务器必须能够解析其他名称。
- 部署了 AD 和 IdM 的支持版本。
- 您已获得 Kerberos ticket。
- 在 Web UI 中创建信任前，为信任准备 IdM 服务器，如下所述：为信任准备 IdM 服务器。
- 您需要以 IdM 管理员身份登录。

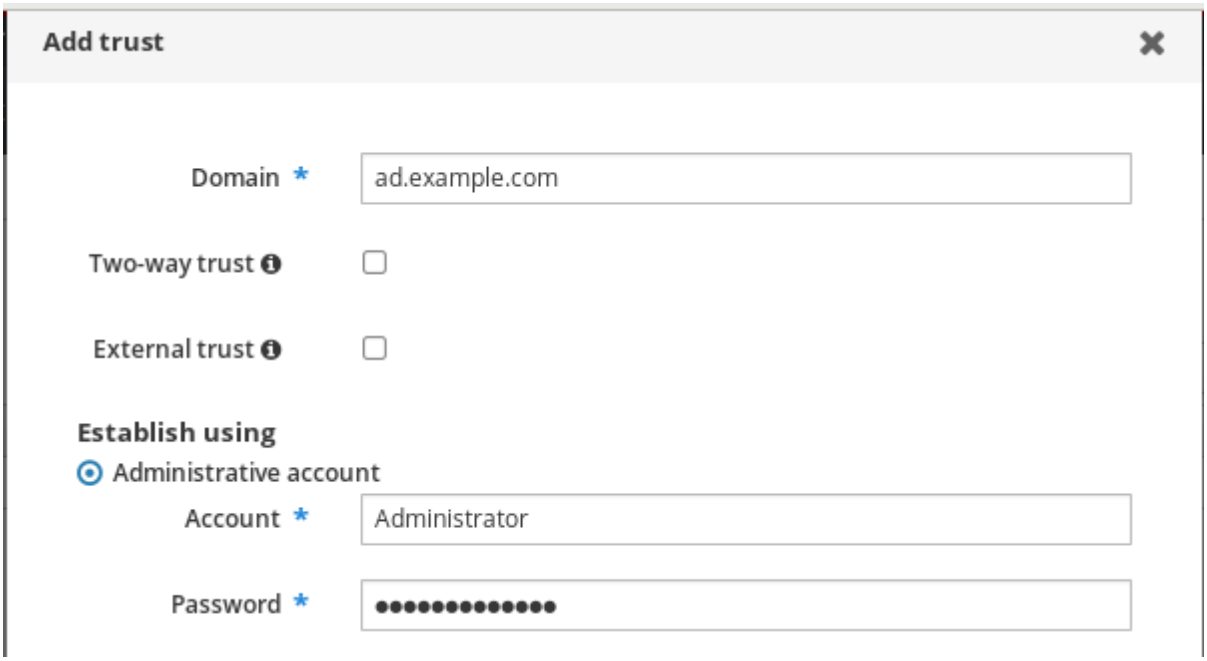
**流程**

1. 使用管理员权限登录到 IdM Web UI。详情请参阅通过 Web 浏览器访问 IdM Web UI 。
2. 在 IdM Web UI 中点 **IPA Server** 标签页。
3. 在 **IPA Server** 选项卡中，点 **Trusts** 标签页。
4. 在下拉菜单中选择 **Trusts** 选项。




5. 点击 **Add** 按钮。
6. 在 **Add Trust** 对话框中，输入 Active Directory 域的名称。

7. 在 **Account** 和 **Password** 字段中，添加 Active Directory 管理员的管理员凭证。



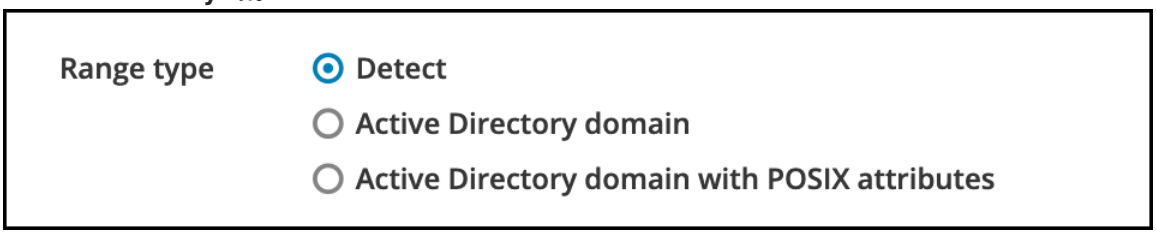

8. *（可选）* 如果要启用 AD 用户和组访问 IdM 中的资源，请选择 **双向信任**。但是，IdM 中的双向信任并不为用户授予与 AD 中的单向信任解决方案相比的额外权利。由于默认的跨林信任 SID 过滤设置，这两个解决方案被视为同等安全。

9. *（可选）* 如果您要为 AD 域配置不是 AD 林的根域的信任，请选择 **External trust**。虽然林信任始终需要在 IdM 和 Active Directory 林的根域之间建立一个信任，但您可以在 AD 林内建立一个外部信任。

10. *（可选）* 默认情况下，信任安装脚本会尝试检测适当的 ID 范围类型。您还可以通过选择以下选项之一来显式设置 ID 范围类型：

    a. 要使 SSSD 根据其 SID 自动为 AD 用户生成 UID 和 GID，请选择 **Active Directory 域** ID 范围类型。这是最常见的配置。

    b. 如果您已经为 Active Directory 中的用户配置了 POSIX 属性（如 **uidNumber** 和 **gidNumber**），并且希望 SSSD 处理此信息，请选择 **具有 POSIX 属性 ID 范围类型的 Active Directory 域**。



**警告**

如果您在默认 **Detect** 选项上保留 **Range 类型** 设置，IdM 会尝试通过在林根域中请求 AD 域控制器的详情来自动选择适当的范围类型。如果 IdM 没有检测到任何 POSIX 属性，则信任安装脚本选择 **Active Directory 域** ID 范围。

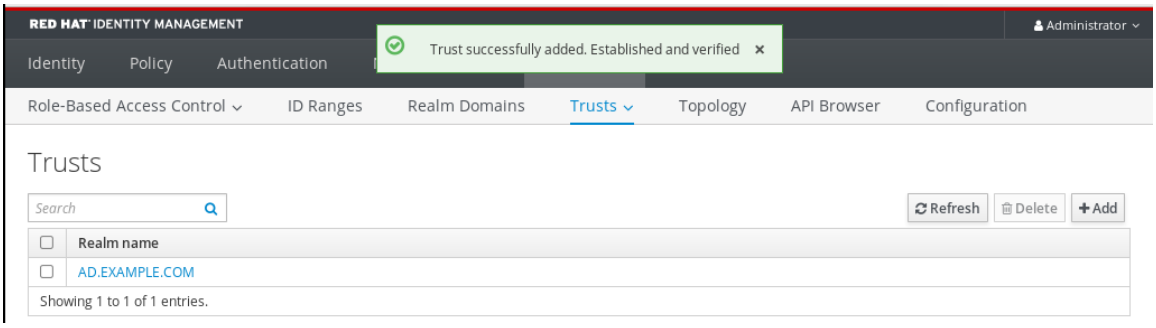
如果 IdM 检测到林根域中的任何 POSIX 属性，则信任安装脚本选择 **带有 POSIX 属性 ID 范围的 Active Directory 域**，并假定 AD 中正确配置了 UID 和 GID。如果 AD 中没有正确设置 POSIX 属性，您将无法解析 AD 用户。

例如，如果需要访问 IdM 系统的用户和组不是林根域的一部分，而是位于林域的子域中，安装脚本可能不会检测到子 AD 域中定义的 POSIX 属性。在这种情况下，红帽建议您在创建信任时显式选择 POSIX ID 范围类型。

11. 点击 **Add**。

**验证步骤**

- 如果信任成功添加到了 IdM 服务器，您可以在 IdM Web UI 中看到绿色的弹出窗口。这意味着：
  - 域名存在
  - 正确添加了 Windows 服务器的用户名和密码。




现在，可以继续测试信任连接和 Kerberos 身份验证。

## 9.4. 使用 ANSIBLE 设置信任协议

按照以下流程，使用 Ansible playbook 在身份管理(IdM)和活动目录(AD)之间建立单向信任协议。您可以配置三种类型的信任协议：

- **One-way trust** – 默认选项。单向信任使 Active Directory（AD）的用户和组可以访问 IdM 中的资源，但不允许反向访问。IdM 域信任 AD 林，但 AD 林不信任 IdM 域。
- **双向信任** - 双向信任使 AD 用户和组可以访问 IdM 中的资源。
  您必须为像 Microsoft SQL Server 这样的解决方案配置双向信任，该解决方案希望 Kerberos 协议的 **S4U2Self** 和 **S4U2Proxy** Microsoft 扩展能够跨信任边界工作。RHEL IdM 主机上的应用可能会向 Active Directory 域控制器请求有关 AD 用户的 **S4U2Self** 或 **S4U2Proxy** 信息，双向信任提供了这一特性。

请注意，这个双向信任功能并不允许 IdM 用户登录到 Windows 系统，IdM 中的双向信任并不为用户授予与 AD 中的单向信任解决方案相比的任何额外权利。

  - 要创建双向信任，请在 playbook 任务中添加以下变量： **two_way: true**

- **外部信任** - 不同林中的 IdM 和 AD 域之间的信任关系。虽然林信任总是需要在 IdM 和 Active Directory 林的根域之间建立信任，但可以从 IdM 到林中的域建立外部信任只有由于管理或组织方面的原因而无法在林根域之间建立林信任时，才推荐这么做。

  - 要创建外部信任，请在 playbook 任务中添加以下变量：**external: true**

**先决条件**

- Windows 管理员的用户名和密码。
- IdM **admin** 密码。
- 您已为信任准备了 IdM 服务器。
- 您可以使用 IdM 的 4.8.7 版本或更高版本。要查看您安装在服务器上的 IdM 版本，请运行 **ipa --version**。
- 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,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. 根据您的用例选择以下场景之一：

   - 要创建 ID 映射信任协议，其中 SSSD 会根据其 SID 自动为 AD 用户和组群生成 UID 和 GID，请创建一个带有以下内容的 **add-trust.yml** playbook：

```
---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is present
      ipatrust:
```

```
    ipaadmin_password: "{{ ipaadmin_password }}"
    realm: ad.example.com
    admin: Administrator
    password: secret_password
    range_type: ipa-ad-trust
    state: present
```

在示例中：

- **realm** 定义 AD 领域名称字符串。
- **admin** 定义 AD 域管理员字符串。
- **password** 定义 AD 域管理员密码字符串。

- 要创建 POSIX 信任协议，其中 SSSD 会处理存储在 AD 中的 POSIX 属性，如 **uidNumber** 和 **gidNumber**，请创建一个包含以下内容的 **add-trust.yml** playbook：

```
---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        range_type: ipa-ad-trust-posix
        state: present
```

- 要通过请求林根域中 AD 域控制器的详情来创建信任协议，其中 IdM 试图自动选择适当的范围类型、**ipa-ad-trust** 或 **ipa-ad-trust-posix**，请创建一个带有以下内容的 **add-trust.yml** playbook：

```
---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        state: present
```

**警告**

如果您在创建信任时没有指定 ID 范围类型，且 IdM 没有在 AD 林根域中检测到任何 POSIX 属性，则信任安装脚本会选择 **Active Directory domain** ID 范围。

如果 IdM 检测到林根域中的任何 POSIX 属性，则信任安装脚本选择 **带有 POSIX 属性 ID 范围的 Active Directory 域**，并假定 AD 中正确配置了 UID 和 GID。

但是，如果 POSIX 属性没有在 AD 中正确设置，则您将无法解析 AD 用户。例如，如果需要访问 IdM 系统的用户和组不是林根域的一部分，而是位于林域的子域中，安装脚本可能不会检测到子 AD 域中定义的 POSIX 属性。在这种情况下，红帽建议您在创建信任时显式选择 POSIX ID 范围类型。

3. 保存该文件。
4. 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-trust.yml
```

**其他资源**

- /usr/share/doc/ansible-freeipa/README-trust.md
- /usr/share/doc/ansible-freeipa/playbooks/trust

## 9.5. 验证 KERBEROS 配置

要验证 Kerberos 配置，请测试是否可以获取身份管理(IdM)用户的单子，以及 IdM 用户是否可以请求服务单。

**流程**

1. 为 Active Directory（AD）用户请求一个 ticket（票据）：

```
[root@ipaserver ~]# kinit user@AD.EXAMPLE.COM
```

2. 为 IdM 域中的服务请求 ticket：

```
[root@server ~]# kvno -S host server.idm.example.com
```

如果 AD 服务单被成功授予了，则会列出一个跨领域单据授予单（TGT），以及所有其他请求的单子。TGT 命名为 krbtgt/IPA.DOMAIN@AD.DOMAIN。

```
[root@server ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.EXAMPLE.COM
```

```
Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/server.idm.example.com@IDM.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IDM.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
```

**localauth** 插件将 Kerberos 主体映射到本地系统安全服务守护进程(SSSD)用户名。这允许 AD 用户使用 Kerberos 身份验证并访问 Linux 服务，这些服务直接支持 GSSAPI 身份验证。

## 9.6. 验证 IDM 上的信任配置

在配置信任前，请验证身份管理（IdM）和 Active Directory（AD）服务器是否可以相互解析。

**先决条件**

- 您需要使用管理员权限登录。

**流程**

1. 对通过 UDP 的 MS DC Kerberos 和通过 TCP 服务记录的 LDAP 运行 DNS 查询。

```
[root@server ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.idm.example.com.
0 100 88 server.idm.example.com.

[root@server ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.idm.example.com.
0 100 389 server.idm.example.com.
```

这些命令列出了在其上执行 **ipa-adtrust-install** 的所有 IdM 服务器。如果 **ipa-adtrust-install** 没有在任何 IdM 服务器上执行，则输出为空，这通常是在建立第一个信任关系之前。

2. 对 Kerberos 和通过 TCP 服务记录的 LDAP 运行 DNS 查询，来验证 IdM 是否能够为 AD 解析服务记录：

```
[root@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

.

## 9.7. 验证 AD 上的信任配置

配置信任后，验证：

- 身份管理（IdM）托管的服务可从 Active Directory（AD）服务器解析。
- AD 服务可从 AD 服务器解析。

**先决条件**

- 您需要使用管理员权限登录。

**步骤**

1. 在 AD 服务器上，设置 **nslookup.exe** 工具来查找服务记录。

```
C:\>nslookup.exe
> set type=SRV
```

2. 通过 UDP 和 LDAP 通过 TCP 服务记录输入 Kerberos 的域名。

```
> _kerberos._udp.idm.example.com.
_kerberos._udp.idm.example.com.       SRV service location:
    priority              = 0
    weight                = 100
    port                  = 88
    svr hostname   = server.idm.example.com
> _ldap._tcp.idm.example.com
_ldap._tcp.idm.example.com       SRV service location:
    priority              = 0
    weight                = 100
    port                  = 389
    svr hostname   = server.idm.example.com
```

3. 将服务类型改为 TXT，并使用 IdM Kerberos 域名运行对 TXT 记录的 DNS 查询。

```
C:\>nslookup.exe
> set type=TXT
> _kerberos.idm.example.com.
_kerberos.idm.example.com.        text =

    "IDM.EXAMPLE.COM"
```

4. 对通过 UDP 的 MS DC Kerberos 和通过 TCP 服务记录的 LDAP 运行 DNS 查询。

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.idm.example.com.
_kerberos._udp.dc._msdcs.idm.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = server.idm.example.com
> _ldap._tcp.dc._msdcs.idm.example.com.
_ldap._tcp.dc._msdcs.idm.example.com.       SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = server.idm.example.com
```

Active Directory 只希望发现能够响应 AD 特定协议请求的域控制器，如其他 AD 域控制器和 IdM 信任控制器。使用 **ipa-adtrust-install** 工具将 IdM 服务器提升为信任控制器，您可以使用 **ipa server-role-find --role 'AD trust controller'** 命令来验证哪些服务器是信任控制器。

5. 验证 AD 服务是否可以从 AD 服务器解析。

```
C:\>nslookup.exe
> set type=SRV
```

6. 通过 UDP 和 LDAP 通过 TCP 服务记录输入 Kerberos 的域名。

```
> _kerberos._udp.dc._msdcs.ad.example.com.
_kerberos._udp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = addc1.ad.example.com
> _ldap._tcp.dc._msdcs.ad.example.com.
_ldap._tcp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = addc1.ad.example.com
```

## 9.8. 创建信任代理

信任代理是一个可以对 AD 域控制器执行身份查找的IdM 服务器。

例如，如果您要创建一个与 Active Directory 信任的 IdM 服务器的副本，您可以将副本设置为信任代理。副本不会自动安装 AD 信任代理角色。

**先决条件**

- 已安装了带有 Active Directory 信任的 IdM 。
- **sssd-tools** 软件包已安装。

**步骤**

1. 在现有的信任控制器上，运行 **ipa-adtrust-install --add-agents** 命令：

```
[root@existing_trust_controller]# ipa-adtrust-install --add-agents
```

该命令启动一个交互式配置会话，并提示您设置代理所需的信息。

2. 重启信任代理上的 IdM 服务。

```
[root@new_trust_agent]# ipactl restart
```

3. 从信任代理上的 SSSD 缓存中删除所有条目：

```
[root@new_trust_agent]# sssctl cache-remove
```

4. 验证副本是否安装了 AD 信任代理角色：

```
[root@existing_trust_controller]# ipa server-show new_replica.idm.example.com
...
Enabled server roles: CA server, NTP server, AD trust agent
```

**其他资源**

- 有关 **--add-agents** 选项的详情，请参考 **ipa-adtrust-install(1)** 手册页。
- 有关信任代理的更多信息，请参阅规划身份管理指南中的 信任控制器和信任代理 。

## 9.9. 在 CLI 上为 POSIX ID 范围启用自动私有组映射

默认情况下，如果您建立了依赖于存储在 AD 数据的 POSIX 数据的 POSIX 信任，SSSD 不会为 Active Directory(AD)用户映射私有组。如果任何 AD 用户没有配置主组，IdM 将无法解析它们。

此流程解释了如何在命令行中为 **auto_private_groups** SSSD 参数设置 **hybrid** 选项来为 ID 范围启用自动专用组映射。因此，IdM 可以解析在 AD 中没有配置主组的 AD 用户。

**先决条件**

- 您已成功在 IdM 和 AD 环境间成功建立了 POSIX 跨林信任。

**步骤**

1. 显示所有 ID 范围并记录您要修改的 AD ID 范围。

```
[root@server ~]# ipa idrange-find
----------------
2 ranges matched
----------------
  Range name: IDM.EXAMPLE.COM_id_range
  First Posix ID of the range: 882200000
  Number of IDs in the range: 200000
  Range type: local domain range

  Range name: AD.EXAMPLE.COM_id_range
  First Posix ID of the range: 1337000000
  Number of IDs in the range: 200000
  Domain SID of the trusted domain: S-1-5-21-4123312420-990666102-3578675309
  Range type: Active Directory trust range with POSIX attributes
----------------------------
Number of entries returned 2
----------------------------
```

2. 使用 **ipa idrange-mod** 命令调整 AD ID 范围的自动专用组行为。

```
[root@server ~]# ipa idrange-mod --auto-private-groups=hybrid
AD.EXAMPLE.COM_id_range
```

3. 重置 SSSD 缓存以启用新的设置。

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

**其他资源**

- 为 AD 用户自动映射私有组的选项

## 9.10. 在 IDM WEBUI 中为 POSIX ID 范围启用自动私有组映射

默认情况下，如果您建立了依赖于存储在 AD 数据的 POSIX 数据的 POSIX 信任，SSSD 不会为 Active Directory(AD)用户映射私有组。如果任何 AD 用户没有配置主组，IdM 将无法解析它们。

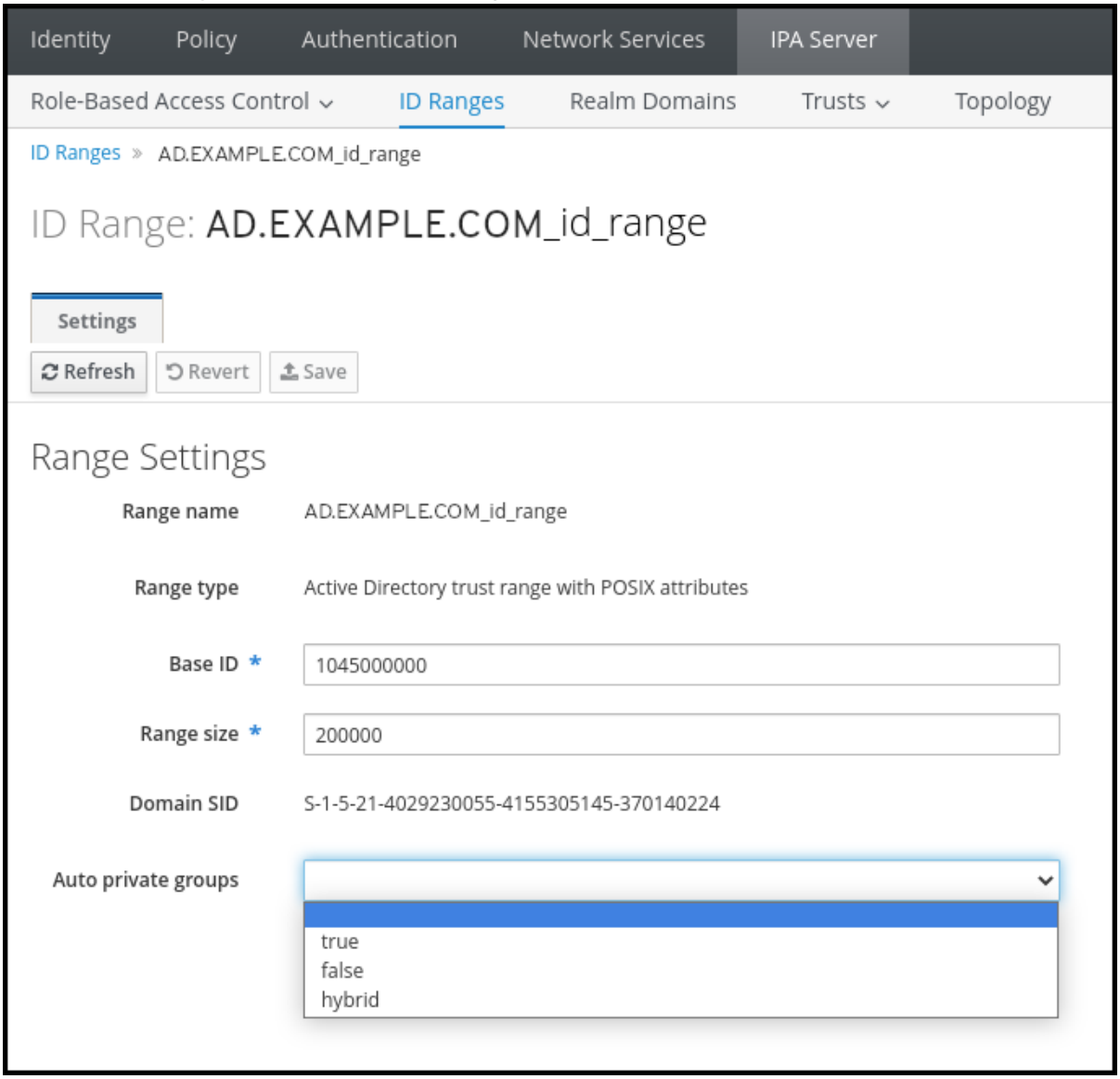
此流程解释了如何在 Identity Management(IdM)WebUI 中设置 **auto_private_groups** SSSD 参数的 **hybrid** 选项来为 ID 范围启用自动专用组映射。因此，IdM 可以解析在 AD 中没有配置主组的 AD 用户。

**先决条件**

- 您已成功在 IdM 和 AD 环境间成功建立了 POSIX 跨林信任。

**步骤**

1. 使用您的用户名和密码登录到 IdM Web UI。
2. 打开 **IPA Server → ID Ranges** 选项卡。
3. 选择要修改的 ID 范围，如 **AD.EXAMPLE.COM_id_range**。
4. 从 **Auto private groups** 下拉菜单中选择 **hybrid** 选项。




5. 点 **Save** 按钮保存您的更改。

**其他资源**

- 为 AD 用户自动映射私有组的选项

# 第 10 章 对设置跨林信任进行故障排除

了解更多有关在身份管理(IdM)环境和活动目录(AD)林之间配置跨林信任过程的故障排除。

## 10.1. 使用 AD 建立跨林信任时事件序列

当您使用 **ipa trust-add** 命令建立与活动目录(AD)域控制器(DC)的跨林信任时，命令代表运行命令的用户进行操作，并在 IdM 服务器上执行以下操作。如果您在建立跨林信任时遇到问题，您可以使用此列表来帮助缩小并排除您的问题。

**第 1 部分：命令会验证设置和输入**

1. 验证 IdM 服务器是否具有 **Trust Controller** 角色。
2. 验证传递给 **ipa trust-add** 命令的选项。
3. 验证与可信林根域关联的 ID 范围。如果您没有将 ID 范围类型和属性指定为 **ipa trust-add** 命令的选项，则从 Active Directory 发现它们。

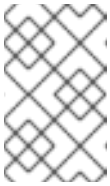
**第 2 部分：命令尝试建立对 Active Directory 域的信任**

4. 为每个信任方向创建单独的信任对象。每个对象都会在两端（IdM 和 AD）中创建。如果您要建立单向信任，每个都只创建一个对象。
5. IdM 服务器使用 Samba 套件处理 Active Directory 的域控制器功能，并在目标 AD PDC 中创建信任对象：
   a. IdM 服务器建立了一个到目标 DC 上 **IPC$** 共享的安全连接。从 RHEL 8.4 开始，连接至少需要使用 Windows Server 2012 及以上的 SMB3 协议，以确保连接足够安全用于会话的 AES 加密。
   b. IdM 服务器使用 **LSA QueryTrustedDomainInfoByName** 调用来查询是否存在可信域对象(TDO)。
   c. 如果已存在 TDO，则使用 **LSA DeleteTrustedDomain** 调用将其删除。

**注意**

如果用来建立信任的 AD 用户帐户没有最佳根的完整 **Enterprise Admin(EA)** 或 **Domain Admin(DA)** 权限，如 **Incoming Forest Trust Builders** 组的成员，这个调用会失败。如果没有自动删除旧的 TDO，则必须从 AD 手动删除它。

   d. IdM 服务器使用 **LSA CreateTrustedDomainEx2** 调用创建新 TDO。TDO 凭证使用 Samba 提供的密码生成器以及 128 个随机字符随机生成。
   e. 然后，使用 **LSA SetInformationTrustedDomain** 调用修改新的 TDO，以确保正确设置信任支持的加密类型：
      i. 启用了 **RC4_HMAC_MD5** 加密类型，即使还没有使用 RC4 密钥，因为 Active Directory 的设计方式。
      ii. **AES128_CTS_HMAC_SHA1_96** 和 **AES256_CTS_HMAC_SHA1_96** 加密类型已启用。

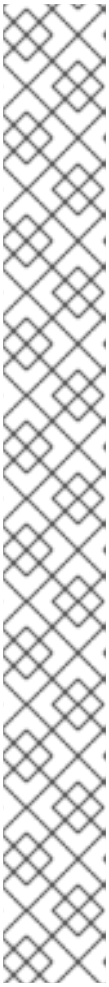


**注意**

默认情况下，RHEL 9 不允许 SHA-1 加密，这是 AD 所需的算法。确保启用了 **AD-SUPPORT** 系统范围的加密策略，以便 RHEL 9 IdM 服务器中的 SHA-1 加密以便与 AD Domain Controller 进行通信。请参阅 <link TBA>。

6. 对于林信任，请验证可使用 **LSA SetInformationTrustedDomain** 调用来传输中的域。

7. 使用 **LSA RSetForestTrustInformation** 调用，添加与其他林通信（IdM 在与 AD 通信时 AD）的信任拓扑信息。



**注意**

此步骤可能会导致以下 3 个原因冲突：

1. SID 命名空间冲突，报告为 **LSA_SID_DISABLED_CONFLICT** 错误。无法解决此冲突。
2. NetBIOS 命名空间冲突，报告为 **LSA_NB_DISABLED_CONFLICT** 错误。无法解决此冲突。
3. DNS 命名空间与顶级名称(TLN)冲突，报告为 **LSA_TLN_DISABLED_CONFLICT** 错误。如果 TLN 因另一林原因造成的，IdM 服务器可以自动解决它。

要解决 TLN 冲突，IdM 服务器执行以下步骤：

1. 检索冲突林的林信任信息。
2. 将 IdM DNS 命名空间的排除条目添加到 AD 林中。
3. 为我们所冲突的林林信任信息设置林信任信息。
4. 重新尝试建立对原始林的信任。

如果您通过 **ipa trust-add** 命令进行身份验证，IdM 服务器只能解决这些冲突，该附加组件具有可更改的 AD 管理员的权限。如果您没有这些权限的访问权限，则原始林的管理员必须手动执行 Windows UI 的 **Active Directory Domains 和 Trusts** 部分中上面的步骤。

8. 如果不存在，为可信域创建 ID 范围。

9. 对于林信任，请从林根查询 Active Directory 域控制器以获取有关林拓扑的详细信息。IdM 服务器使用此信息为来自可信林中的任何其他域创建额外的 ID 范围。

**其他资源**

- 信任控制器和信任代理
- 概述文档 (Microsoft)
- 技术文件 (Microsoft)
- 活动目录中的特权帐户和组 (微软)

## 10.2. 建立 AD 信任的先决条件列表

您可以使用以下清单查看创建 AD 域的信任的先决条件。

**表 10.1. 表**

| 组件 | Configuration | 其它详情 |
| --- | --- | --- |
| 产品版本 | 您的 Active Directory 域使用受支持的 Windows 服务器版本。 | Windows 服务器支持的版本 |
| AD Administrator 权限 | Active Directory 管理帐户必须是以下组之一的成员：<br>• AD 林中的 **Enterprise Admin (EA)** 组<br>• AD 林的 **Domain Admins (DA)** 组 | |
| Networking | 所有 IdM 服务器的 Linux 内核中都启用了 IPv6 支持。 | IdM 中的 IPv6 要求 |
| 日期和时间 | 验证两个服务器上的日期和时间设置是否匹配。 | IdM 的时间服务要求 |
| 加密类型 | 以下 AD 帐户具有 AES 加密密钥：<br>• AD Administrator<br>• AD 用户帐户<br>• AD 服务<br>如果您最近在 AD 中启用了 AES 加密，请使用以下步骤生成新的 AES 密钥：<br>1. 重新建立您的林中任何 AD 域的信任关系。<br>2. 更改 AD Administrator、用户帐户和服务的密码。 | • 支持 IdM 中的加密类型<br>• 使用 GPO 在 Active Directory 中启用 AES 加密类型 |
| firewall | 您已在 IdM 服务器和 AD 域控制器中打开了所有必要的端口，用于双向通信。 | IdM 和 AD 间的通信所需的端口 |

| 组件 | Configuration | 其它详情 |
| --- | --- | --- |
| DNS | • IdM 和 AD 各自有唯一的主 DNS 域。<br>• IdM 和 AD DNS 域不重叠。<br>• LDAP 和 Kerberos 服务的正确 DNS 服务(SRV)记录。<br>• 您可以从信任中的所有 DNS 域解析 DNS 记录。<br>• Kerberos realm 名称作为主 DNS 域名的大写版本例如，DNS 域 **example.com** 具有对应的 Kerberos 域 **EXAMPLE.COM** | 为信任配置 DNS 和域设置 |
| Topology | 确保您试图使用您配置为信任控制器的 IdM 服务器建立信任。 | 信任控制器和信任代理 |

## 10.3. 收集尝试建立 AD 信任的调试日志

如果您在 IdM 环境和 AD 域间建立信任时遇到问题，请使用以下步骤启用详细的错误记录，以便您可以收集日志来尝试建立信任。您可以查看这些日志以帮助您的故障排除工作，或者您可以在红帽技术支持问题单中提供它们。

**先决条件**

- 您需要 root 权限来重启 IdM 服务。

**步骤**

1. 要为 IdM 服务器启用调试，请使用以下内容创建文件 **/etc/ipa/server.conf**。

```
[global]
debug=True
```

2. 重启 **httpd** 服务以载入调试配置。

```
[root@trust_controller ~]# systemctl restart httpd
```

3. 停止 **smb** 和 **winbind** 服务。

```
[root@trust_controller ~]# systemctl stop smb winbind
```

4. 为 **smb** 和 **winbind** 服务设置调试日志级别。

```
[root@trust_controller ~]# net conf setparm global 'log level' 100
```

5. 要为 IdM 框架使用的 Samba 客户端代码启用调试日志记录，请编辑 **/usr/share/ipa/smb.conf.empty** 配置文件使其包含以下内容。

```
[global]
log level = 100
```

6. 删除以前的 Samba 日志。

```
[root@trust_controller ~]# rm /var/log/samba/log.*
```

7. 启动 **smb** 和 **winbind** 服务。

```
[root@trust_controller ~]# systemctl start smb winbind
```

8. 打印时间戳，在您试图建立启用了详细模式的信任时。

```
[root@trust_controller ~]# date; ipa -vvv trust-add --type=ad ad.example.com
```

9. 查看以下错误日志文件，以了解有关失败请求的信息：

   a. **/var/log/httpd/error_log**

   b. **/var/log/samba/log.***

10. 禁用调试。

```
[root@trust_controller ~]# mv /etc/ipa/server.conf /etc/ipa/server.conf.backup
[root@trust_controller ~]# systemctl restart httpd
[root@trust_controller ~]# systemctl stop smb winbind
[root@trust_controller ~]# net conf setparm global 'log level' 0
[root@trust_controller ~]# mv /usr/share/ipa/smb.conf.empty
/usr/share/ipa/smb.conf.empty.backup
[root@trust_controller ~]# systemctl start smb winbind
```

11. *（可选）* 如果无法确定身份验证问题的原因：

   a. 收集和归档您最近生成的日志文件。

```
[root@trust_controller ~]# tar -cvf debugging-trust.tar /var/log/httpd/error_log
/var/log/samba/log.*
```

   b. 创建一个红帽技术支持问题单，并在尝试中提供时间戳和调试日志。

**其他资源**

- IPA - AD Trust Troubleshooting

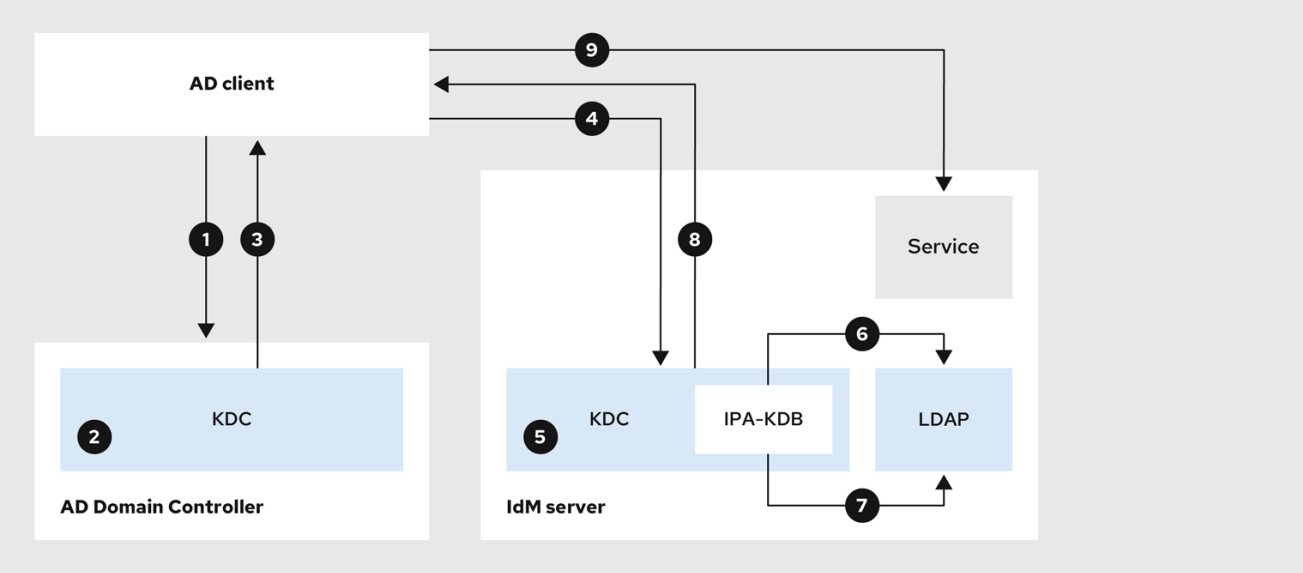
# 第 11 章 对其他林中的服务进行客户端访问进行故障排除

在 Identity Management(IdM)和 Active Directory(AD)环境之间配置信任后，您可能会遇到以下问题：一个域中的客户端无法访问其他域中的服务。使用以下示意图对问题进行故障排除。

## 11.1. 当 AD 林根域请求来自 IDM 服务器的主机请求时，信息流

下图显示了当 Active Directory(AD)客户端请求 Identity Management(IdM)域中服务时的信息流。

如果您在 AD 客户端访问 IdM 服务时遇到问题，您可以使用此信息缩小故障排除工作并识别问题源。




1. AD 客户端联系 AD Kerberos 分发中心(KDC)以在 IdM 域中为该服务执行 TGS 请求。
2. AD KDC 识别该服务属于可信 IdM 域。
3. AD KDC 将客户端发送跨域票据(TGT)，以及引用可信 IdM KDC。
4. AD 客户端使用跨域 TGT 向 IdM KDC 请求 ticket。
5. IdM KDC 验证通过跨域 TGT 传输的权限属性证书(MS-PAC)。
6. IPA-KDB 插件可能会检查 LDAP 目录，以查看是否允许外部主体获取所请求服务的票据。
7. IPA-KDB 插件对 MS-PAC、验证和过滤数据进行解码。它会在 LDAP 服务器中执行查找，以检查是否需要使用附加信息（如本地组）增加 MS-PAC。
8. IPA-KDB 插件随后对 PAC 进行编码，为它签名，将其附加到服务票据，并将其发送到 AD 客户端。
9. AD 客户端现在可以使用 IdM KDC 发布的服务票据联系 IdM 服务。

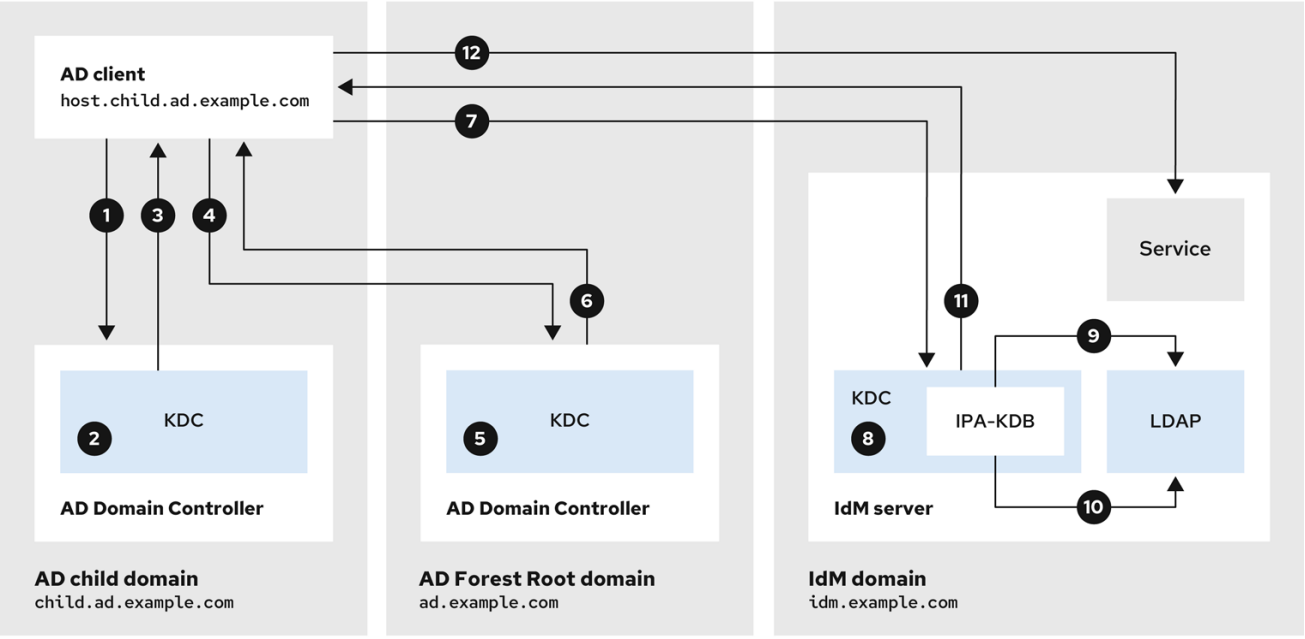
**其他资源**

- 当来自 IdM 服务器的 AD 子域请求服务时的信息流

## 11.2. 当来自 IDM 服务器的 AD 子域请求服务时的信息流

下图显示了当子域中的 Active Directory(AD)主机请求 Identity Management(IdM)域中的服务时的信息流。在这种情况下，AD 客户端联系子域中的 Kerberos 分发中心(KDC)，然后联系 AD 林根中的 KDC，最后联系 IdM KDC 以请求对 IdM 服务的访问。

如果您在 AD 客户端访问 IdM 服务时遇到问题，并且您的 AD 客户端属于 AD 林根的子域，您可以使用这些信息缩小故障排除工作并识别问题源。




1. AD 客户端在其自己的域中联系 AD Kerberos Distribution Center(KDC)，以执行 IdM 域中该服务的 TGS 请求。
2. **child.ad.example.com** 中的 AD KDC（子域）可识别该服务所属的可信 IdM 域。
3. 子域中的 AD KDC 向客户端发送 AD 林根域 **ad.example.com** 的推荐票据。
4. AD 客户端与 IdM 域中服务的 AD 林根域中的 KDC 联系。
5. 林根域中的 KDC 识别该服务属于可信 IdM 域。
6. AD KDC 将客户端发送跨域票据(TGT)，以及引用可信 IdM KDC。
7. AD 客户端使用跨域 TGT 向 IdM KDC 请求 ticket。
8. IdM KDC 验证通过跨域 TGT 传输的权限属性证书(MS-PAC)。
9. IPA-KDB 插件可能会检查 LDAP 目录，以查看是否允许外部主体获取所请求服务的票据。
10. IPA-KDB 插件对 MS-PAC、验证和过滤数据进行解码。它会在 LDAP 服务器中执行查找，以检查是否需要使用附加信息（如本地组）增加 MS-PAC。
11. IPA-KDB 插件随后对 PAC 进行编码，为它签名，将其附加到服务票据，并将其发送到 AD 客户端。
12. AD 客户端现在可以使用 IdM KDC 发布的服务票据联系 IdM 服务。

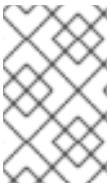
**其他资源**

- 当 AD 林根域请求来自 IdM 服务器的主机请求时，信息流

## 11.3. IDM 客户端从 AD 服务器请求服务时的信息流

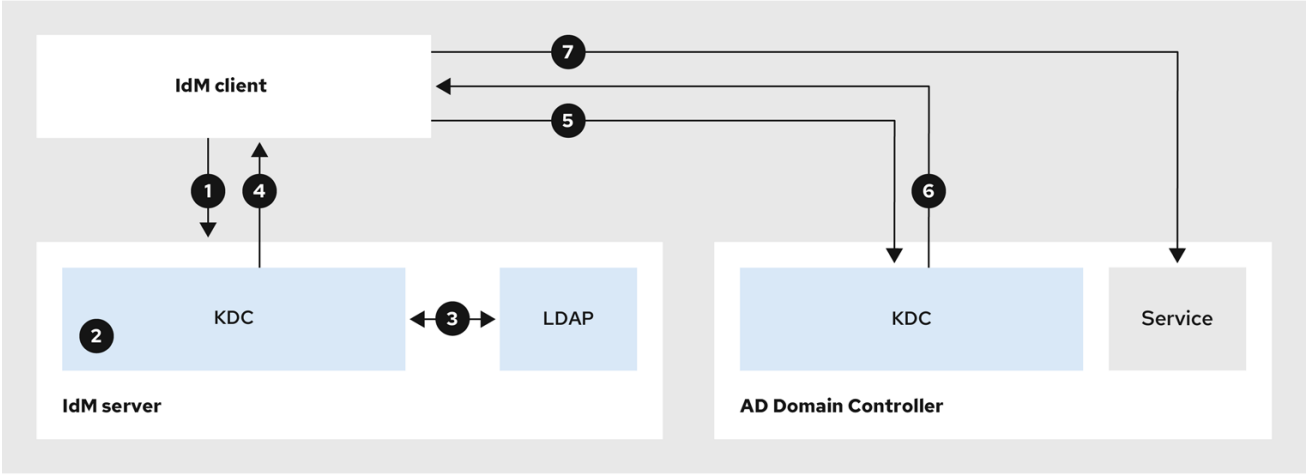
下图显示了当您在 IdM 和 AD 之间配置了双向信任时，Identity Management(IdM)客户端请求 Active Directory(AD)域中的服务时的信息流。

如果您从 IdM 客户端访问 AD 服务时遇到问题，您可以使用此信息缩小故障排除工作并识别问题源。



**注意**

默认情况下，IdM 为 AD 建立单向信任，这意味着无法为 AD 林中的资源发出跨 realm ticket-granting ticket(TGT)。为了能够向来自可信 AD 域的服务请求 ticket，请配置双向信任。




1. IdM 客户端从 IdM Kerberos 分发中心(KDC)请求一个 ticket-granting ticket(TGT)用于所需的 AD 服务。
2. IdM KDC 识别该服务属于 AD 域，验证域是否已知并可信，以及客户端是否允许从该域请求服务。
3. 使用 IdM Directory Server 关于用户主体的信息，IdM KDC 创建一个跨域 TGT，其中包含有关用户主体的 Privileged Attribute 证书(MS-PAC)记录。
4. IdM KDC 向 IdM 客户端发送跨域 TGT。
5. IdM 客户端联系 AD KDC 来请求 AD 服务的票据，显示包含 IdM KDC 提供的 MS-PAC 的跨域 TGT。
6. AD 服务器验证和过滤 PAC，并返回 AD 服务的 ticket。
7. IPA 客户端现在可以联系 AD 服务。

**其他资源**

- 单向信任和双向信任

# 第 12 章 使用命令行删除信任

按照以下流程使用命令行界面删除 IdM 端的身份管理(IdM)/活动目录(AD)信任。

**先决条件**

- 您已作为 IdM 管理员获得了 Kerberos 单。详情请查看 Web UI 中的 Logging 到 IdM：使用 Kerberos ticket。

**步骤**

1. 使用 **ipa trust-del** 命令从 IdM 中删除信任配置。

```
[root@server ~]# ipa trust-del ad_domain_name
-----------------------------
Deleted trust "ad_domain_name"
-----------------------------
```

2. 从 Active Directory 配置中删除信任对象。

**注意**

删除信任配置不会自动删除已为 AD 用户创建的 ID 范围 IdM。这样，如果您再次添加信任，则重新使用现有的 ID 范围。另外，如果 AD 用户已在 IdM 客户端上创建了文件，则其 POSIX ID 会在文件元数据中保留。

要删除与 AD 信任相关的所有信息，请在删除信任配置和信任对象后删除 AD 用户 ID 范围：

```
# ipa idrange-del AD.EXAMPLE.COM_id_range
# systemctl restart sssd
```

**验证步骤**

- 使用 **ipa trust-show** 命令来确认信任已删除。

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

**其他资源**

- 删除对 AD 的信任后删除 ID 范围

# 第 13 章 使用 IDM WEB UI 删除信任

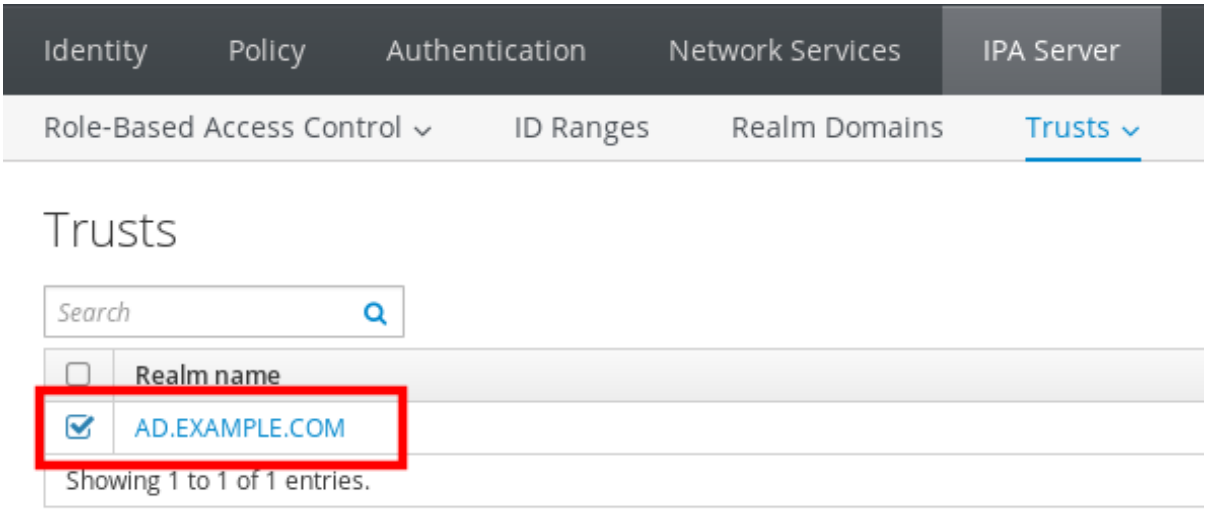
按照以下流程，使用 IdM Web UI 删除身份管理(IdM)/活动目录(AD)信任。

**先决条件**

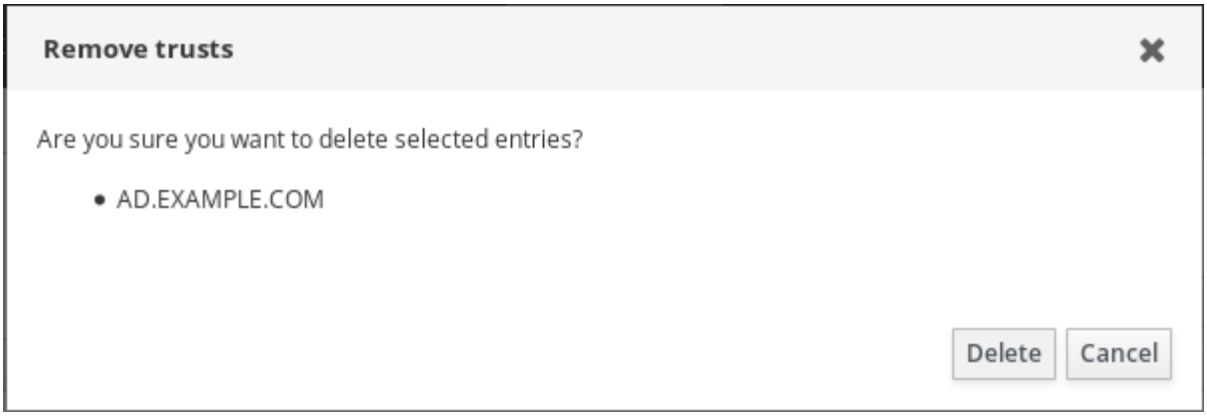
- 您已获得 Kerberos ticket。详情请查看 Web UI 中的 Logging 到 IdM：使用 Kerberos ticket 。

**步骤**

1. 使用管理员权限登录到 IdM Web UI。详情请参阅通过 Web 浏览器访问 IdM Web UI 。
2. 在 IdM Web UI 中点 **IPA Server** 标签页。
3. 在 **IPA Server** 选项卡中，点 **Trusts** 标签页。
4. 选择您要删除的信任。




5. 点击 **Delete** 按钮。
6. 在 **Remove trusts** 对话框中点击 **Delete**。




7. 从 Active Directory 配置中删除信任对象。

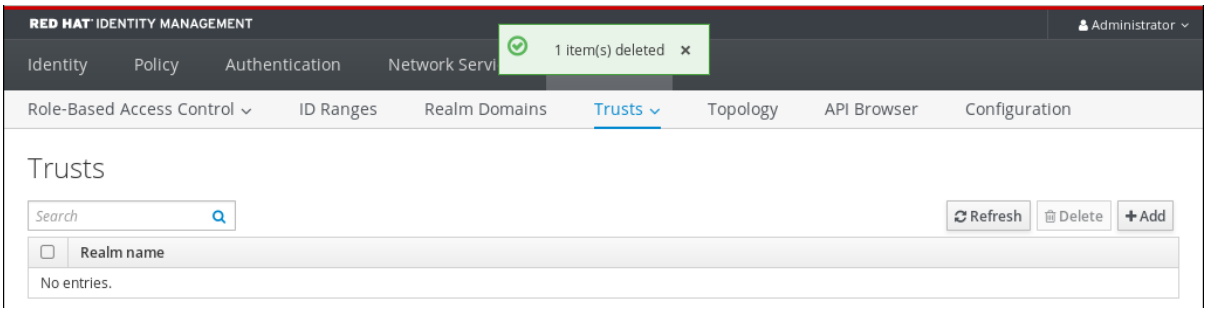
**注意**

删除信任配置不会自动删除已为 AD 用户创建的 ID 范围 IdM。这样，如果您再次添加信任，则重新使用现有的 ID 范围。另外，如果 AD 用户已在 IdM 客户端上创建了文件，则其 POSIX ID 会在文件元数据中保留。

要删除与 AD 信任相关的所有信息，请在删除信任配置和信任对象后删除 **ID Ranges** 选项卡中的 AD 用户 ID 范围。

**验证步骤**

- 如果信任被成功删除，Web UI 会显示一个带有以下文字的绿色弹框：




**其他资源**

- 删除对 AD 的信任后删除 ID 范围

# 第 14 章 使用 ANSIBLE 删除信任

按照以下流程，使用 Ansible playbook 删除 IdM 端的身份管理(IdM)/活动目录(AD)信任。

**先决条件**

- 您已作为 IdM 管理员获得了 Kerberos 单。详情请查看 Web UI 中的 Logging 到 IdM：使用 Kerberos ticket。
- 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,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. 使用以下内容创建 **del-trust.yml** playbook：

```
---
- name: Playbook to delete trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is absent
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        state: absent
```

在示例中，**realm** 定义 AD 领域名称字符串。

3. 保存该文件。
4. 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 del-trust.yml
```

**注意**

删除信任配置不会自动删除已为 AD 用户创建的 ID 范围 IdM。这样，如果您再次添加信任，则重新使用现有的 ID 范围。另外，如果 AD 用户已在 IdM 客户端上创建了文件，则其 POSIX ID 会在文件元数据中保留。

要删除与 AD 信任相关的所有信息，请在删除信任配置和信任对象后删除 AD 用户 ID 范围：

```
# ipa idrange-del AD.EXAMPLE.COM_id_range
# systemctl restart sssd
```

**验证步骤**

- 使用 **ipa trust-show** 命令来确认信任已删除。

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

**其他资源**

- /usr/share/doc/ansible-freeipa/README-trust.md
- /usr/share/doc/ansible-freeipa/playbooks/trust
- 删除对 AD 的信任后删除 ID 范围

# 第 15 章 删除对 AD 的信任后删除 ID 范围

如果您已删除了 IdM 和活动目录(AD)环境之间的信任，则您可能想要删除与其关联的 ID 范围。

**警告**

分配给与可信域相关联的 ID 范围的 ID，可能仍然用于注册到 IdM 的系统上的文件和目录的所有权。

如果您删除了与已删除的 AD 信任对应的 ID 范围，则您将无法解析 AD 用户所拥有的任何文件和目录的所有权。

**先决条件**

- 您已删除了对 AD 环境的信任。

**步骤**

1. 显示所有当前正在使用的 ID 范围：

```
[root@server ~]# ipa idrange-find
```

2. 识别与您删除的信任相关联的 ID 范围的名称。ID 范围名称的第一部分是信任的名称，如 **AD.EXAMPLE.COM_id_range**。

3. 删除范围：

```
[root@server ~]# ipa idrange-del AD.EXAMPLE.COM_id_range
```

4. 重启 SSSD 服务，来删除对您已删除的 ID 范围的引用。

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

**其他资源**

- 请参阅 使用命令行删除信任。
- 请参阅 使用 IdM Web UI 删除信任 。