Red Hat Enterprise Linux 7

Windows 集成指南

将 Linux 系统与 Active Directory 环境集成

Last Updated: 2023-04-06

Red Hat Enterprise Linux 7 Windows 集成指南

将 Linux 系统与 Active Directory 环境集成

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

异构 IT 环境通常包含各种需要无缝通信的不同领域和操作系统。红帽企业 Linux 提供了多种方式，可以将 Linux 域与 Microsoft Windows 上的 Active Directory(AD)紧密集成。集成可以在包括用户、组、服务或系统在内的不同域对象上实现。本指南还包括不同的集成场景，从轻量级 AD 直通身份验证到功能齐全的 Kerberos 可信域。 除了本指南外，您还可以在以下指南中找到与 Red Hat Enterprise Linux Identity Management 相关的其他功能和服务文档： Linux 域身份、身份验证和策略指南记录了红帽身份管理，此解决方案提供了在基于 Linux 的域中管理身份存储以及身份验证和授权

策略的集中统一方式。 系统级身份验证指南记录了在本地系统上配置身份验证的不同应用程序和服务，包括 authconfig实用程序、系统安全服务守护进程(SSSD)服务、可插拔验证模块(PAM)框架、Kerberos、certmonger 实用程序和用于应用程序的单点登录(SSO)。

目录

第 1 章 集成 ACTIVEACTIVE DIRECTORYNBSP;DIRECTORY 和 LINUX 环境的方法

IT 环境具有.它们中的系统具有某种目的。集成两个单独的基础架构需要评估每种环境的用途，并了解它们如何和在哪里交互。

1.1. 定义 WINDOWS 集成

Windows 集成可能意味着完全不同，具体取决于 Linux 环境和 Windows 环境之间的必要交互。这可能意味着单个 Linux 系统已加入 Windows 域，这可能意味着 Linux 域已配置为 Windows 域的对等点，或者可能只是意味着在环境间复制信息。

Windows 域和 Linux 系统之间存在多个联系人。这些要点各自围绕识别不同域对象（用户、组、系统、服务）以及该标识中使用的服务。

用户身份和身份验证

- 位于什么位置的用户帐户；位于 Windows（AD 域）或中央身份和身份验证服务器上运行的中央身份验证系统，或在 Linux 上运行的中央身份和身份验证服务器？
- 用户在 Linux 系统上如何进行身份验证；如何通过本地 Linux 身份验证系统或在 Windows 上运行的中央身份验证系统？
- 如何为用户配置组成员资格？如何确定组成员身份？
- 用户是否会使用用户名/密码对、Kerberos 票据、证书或方法组合进行身份验证？
- 访问 Linux 计算机上的服务需要 POSIX 属性。这些属性是如何存储的：它们是在 Windows 域中设置、在本地 Linux 系统上配置，还是动态映射（用于 UID/GID 编号和 Windows SID）？
- 哪些用户将访问哪些资源？Windows 定义的用户是否会访问 Linux 资源？Linux 定义的用户是否会访问 Windows 资源？

在大多数环境中，ActiveActive Directorynbsp;Directory 域是用户信息的核心中心，这意味着，Linux 系统需要某种方式来访问该用户信息以进行身份验证。*然后，真正的问题是如何获取该用户信息*，以及该信息中有多少可供外部系统使用。Linux 系统（POSIX 属性）和 Linux 用户（认证应用程序管理员）所需的信息与如何管理该信息之间也需要平衡。

主机和服务主体

- 将访问哪些资源？
- 需要哪些身份验证协议？
- 如何获取 Kerberos 票据？如何请求或验证 SSL 证书？
- 用户是否需要访问单个域或 Linux 和 Windows 域？

DNS 域、查询和名称解析

- DNS 配置是什么？
- 是否存在单个 DNS 域？是否有子域？
- 系统主机名将如何解析？

- 如何配置服务发现？

安全策略

- 访问控制指令在哪里设置？
- 每个域配置了哪些管理员？

更改管理

- 系统添加到域中的频率如何？
- 如果更改了与 Windows 集成相关的底层配置（如 DNS 服务），这些更改是如何传播的？
- 配置是通过域相关的工具还是调配系统维护的？
- 集成路径是否需要在 Windows 服务器上进行其他应用程序或配置？

与域中哪些元素集成同样重要，是如何维护集成的。如果特定的集成工具是手动的，但环境有许多系统频繁更新，那么从维护角度来看，一个工具可能无法用于该环境。

以下小节概述了与 Windows 集成的主要场景。在直接集成中，Linux 系统连接到 Active Directory，无需任何额外的压力。另一方面，间接集成涉及集中管理 Linux 系统并将整个环境连接到服务器到服务器级别的 Active Directory 的身份服务器。

1.2. 直接集成

您需要两个组件才能将 Linux 系统连接到 Active Directory(AD)。个组件与中央身份和身份验证源交互，本例中为 AD。其他组件检测到可用的域，并将第一个组件配置为处理正确的身份源。有不同的选项可用于检索信息和对 AD 进行身份验证。其中包括：

原生 LDAP 和 Kerberos PAM 和 NSS 模块

这些模块包括nss_ldap、pam_ldap 和 pam_krb5。由于 PAM 和 NSS 模块被加载到每个应用程序进程中，它们直接影响执行环境。如果没有缓存、离线支持或对访问凭证的充分保护，则不鼓励在 NSS 和 PAM 中使用基本 LDAP 和 Kerberos 模块，因为其功能有限，不鼓励使用 PAM。

Samba Winbind

Samba Winbind 一直是将 Linux 系统连接到 AD 的传统方式。winbind 模拟 Linux 系统上的 Windows 客户端，并可与 AD 服务器通信。

请注意：

- **如果您将 Samba 配置为域成员，则必须运行 Winbind 服务。**
- **在多林 AD 设置中直接与 Winbind 集成需要双向信托。**

- 远程林必须信任本地林，以确保 idmap_ad 插件正确处理远程林用户。

系统安全性服务守护进程（SSSD）

SSSD 的主要功能是通过通用框架访问远程身份和身份验证资源，为系统提供缓存和离线支持。SSSD 高度可配置；它提供 PAM 和 NSS 集成，以及用于存储本地用户的数据库，以及从中央服务器检索到的核心和扩展用户数据。SSSD 是将 Linux 系统与您选择的身份服务器连接的建议组件，可以是 Active Directory、Red Hat Enterprise Linux 中的 Identity Management(IdM)，或者任何通用 LDAP 或 Kerberos 服务器。

请注意：

- 默认情况下，直接与 SSSD 集成只能在单个 AD 林中正常工作。
- 远程林必须信任本地林，以确保 idmap_ad 插件正确处理远程林用户。

从 Winbind 转换到 SSSD 的主要原因是，SSSD 可用于直接和间接集成，并允许在无需大量迁移成本的情况下从一种集成方法切换到另一种集成方法。为直接将 Linux 系统与 AD 集成，配置 SSSD 或 Winbind 的最简便方法是使用 realmd 服务。它允许调用者以标准的方式配置网络身份验证和域成员资格。realmd 服务自动发现有关可访问域和域的信息，不需要高级配置加入域或域。

直接集成是将 Linux 系统引入 AD 环境的简单方法。但是，随着 Linux 系统份额的增长，部署通常会看到更好地集中管理身份相关策略（如基于主机的访问控制、sudo 或 SELinux 用户映射）的需求。首先，可以在本地配置文件中维护 Linux 系统这些方面的配置。然而，随着越来越多的系统，配置文件的分发和管理借助红帽卫星等调配系统更易于分发和管理。这种方法可产生更改配置文件并分发配置文件的开销。当直接集成不再扩展时，考虑下一节中描述的间接集成更为有用。

1.2.1. 支持的用于直接集成的 Windows 平台

您可以使用以下林和域功能级别将您的 Linux 机器直接与 Active Directory 域集成：

- 林功能级别范围：Windows Server 2008 - Windows 服务器 2016[1]
- 域功能级别范围：Windows Server 2008 - Windows Server 2016[1]

在以下支持的操作系统中使用上述功能级别测试直接集成：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

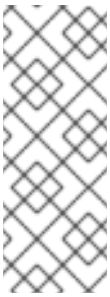
1.3. 间接集成

间接集成的主要优点是集中管理与这些系统相关的 Linux 系统和策略，同时使来自 Active Directory(AD)域的用户能够透明地访问 Linux 系统和服务。间接集成有两种不同的方法：

基于信任的解决方案

建议的做法是利用红帽企业 Linux 中的身份管理(IdM)作为中央服务器来控制 Linux 系统，然后使用 AD 建立跨域 Kerberos 信任，使 AD 中的用户能够登录并使用单点登录来访问 Linux 系统和资源。这个解决方案使用 Kerberos 功能在不同的身份源间建立信任。IdM 作为一个独立的林，利用了 AD 支持的林级信任。

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 管理员可以专注于与用户相关的用户和策略，而 Linux 管理员完全控制 Linux 基础架构。在这种情况下，IdM 控制的 Linux 域类似于 AD 资源域或域，但其中包含 Linux 系统。



注意

在 Windows 中，每个域都是一个 Kerberos 域（realm）和一个 DNS 域（domain）。由域控制器管理的每个域都需要拥有自己的专用 DNS 区域。IdM 作为林受 AD 信任时也是如此。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。

请注意，在信任环境中，IdM 允许您使用 *ID 视图*为 IdM 服务器上的 AD 用户配置 POSIX 属性。详情请查看：

- 第 8 章 *在 Active Directory 环境中使用 ID 视图*

- *系统级身份验证指南中的 SSSD 客户端 视图*

基于同步的解决方案

基于信任的解决方案的另一种方法是利用用户同步功能（IdM 或 Red Hat Directory Server(RHDS)），允许用户帐户（以及 RHDS 以及组帐户）从 AD 同步到 IdM 或 RHDS，但不会朝着相反的方向同步。用户同步有一些限制，包括：

- 用户重复
- 需要同步密码，这需要 AD 域中所有域控制器上有一个特殊组件
- 要捕获密码，所有用户必须首先手动更改密码
- 同步只支持单个域
- AD 中只能有一个域控制器用于将数据同步到 IdM 或 RHDS 的一个实例

在某些集成场景中，用户同步可能是唯一可用的选项，但通常不鼓励使用同步方法，而是偏向于基于跨域信任的集成。

---

[1] Windows Server 2019 没有引入新的功能级别。功能级别最高的 Windows Server 2019 使用是 Windows Server 2016。

部分 I. 将单一 LINUX 系统添加到 ACTIVE DIRECTORY 域

这部分论述了系统安全服务守护进程(SSSD)如何与 Active Directory(AD)域一起工作，如何使用 realmd 系统实现直接域集成，最后，如何使用 Samba 进行 AD 集成。

第 2 章 使用 ACTIVE DIRECTORY 作为 SSSD 的身份提供程序

系统安全服务后台程序(SSSD)是一种用于访问远程目录和身份验证机制的系统服务。它将本地系统（SSSD 客户端）连接到外部后端系统（域）。这为 SSSD 客户端提供了使用 SSSD 供应商访问身份和身份验证远程服务的权限。例如，这些远程服务包括：LDAP 目录、身份管理(IdM)或 Active Directory(AD)域，或者 Kerberos 域。

当用作 AD 集成的身份管理服务时，SSSD 是 NIS 或 Winbind 等服务的替代选择。本章论述了 SSSD 如何与 AD 配合工作。有关 SSSD 的详情，请查看 系统级身份验证指南。

2.1. AD 提供程序如何处理受信任的域

本节论述了当您在 /etc/sssd/sssd.conf 文件中设置 id_provider = ad 时，SSSD 如何处理可信域。

- SSSD 只支持单个 ActiveActive Directorynbsp 中的域，Directory 林。如果 SSSD 需要从多个地区访问多个域，请考虑使用带有信任（首选）的 IdM 或 winbindd 服务而不是 SSSD。

- 默认情况下，SSSD 会发现林中的所有域，如果可信域中的对象请求到达，SSSD 会尝试解析它。

  如果可信域无法访问或在地理位置上造成速度较慢，您可以在 /etc/sssd/sssd.conf 中设置 ad_enabled_domains 参数来限制从哪些可信域 SSSD 解析对象。

- 默认情况下，您必须使用完全限定用户名从可信域解析用户。

2.2. 为 SSSD 配置 AD 提供程序

AD 供应商可让 SSSD 使用 LDAP 身份供应商和 Kerberos 身份验证供应商，并对 AD 环境进行优化。

2.2.1. 集成选项概述

Linux 和 Windows 系统为用户和组群使用不同的标识符：

- Linux 使用用户 ID (UID) 和组 ID (GID)。请参阅 系统管理员 指南中的 管理用户和组。

Linux UID 和 GID 符合 POSIX 标准。

- *Windows 使用安全 ID (SID)。*

重要

不要在 Windows 和 ActiveActive Directorynbsp;Directory 中使用相同的用户名。

向 Red Hat Enterprise Linux 系统进行身份验证的用户（包括 AD 用户）必须分配有 UID 和 GID。为此，SSSD 提供以下集成选项：

为 AD 用户自动生成新的 UID 和 GID

SSSD 可以使用 AD 用户的 SID 在名为 ID 映射的进程中计算生成 POSIX ID。ID 映射会在 AD 中的 SID 和 Linux 中的 ID 之间创建一个映射。

- *当 SSSD 检测到新的 AD 域时，它会为新域分配一系列可用 ID。因此，每个 AD 域在每个 SSSD 客户端机器上都有相同的 ID 范围。*
- *当 AD 用户第一次登录 SSSD 客户端机器时，SSSD 在 SSSD 缓存中为用户创建一个条目，包括基于用户的 SID 以及该域的 ID 范围的 UID。*
- *因为 AD 用户的 ID 是以一致的方式从同一 SID 生成，所以用户在登录到任何 Red Hat Enterprise Linux 系统时具有相同的 UID 和 GID。*

请参阅 第 2.2.2 节 “使用 ID 映射配置 AD 域作为 SSSD 的提供程序”。

注意

当所有客户端系统都使用 SSSD 将 SID 映射到 Linux ID 时，映射是一致的。如果有些客户端使用不同的软件，请选择以下之一：

- 确定所有客户端都使用相同的映射算法。
- 使用显式 POSIX 属性，如 使用 AD 中定义的 POSIX 属性 所述。

使用 AD 中定义的 POSIX 属性

AD 可以创建并存储 POSIX 属性，如 uidNumber、gidNumber、unixHomeDirectory 或 loginShell。

使用 为 AD 用户自动生成新的 UID 和 GID 中描述的 ID 映射时，SSSD 会创建新的 UID 和 GID，这将覆盖 AD 中定义的值。要保留 AD 定义的值，必须在 SSSD 中禁用 ID 映射。

请参阅 第 2.2.3 节 “配置 SSSD 使用 AD 中定义的 POSIX 属性”。

2.2.2. 使用 ID 映射配置 AD 域作为 SSSD 的提供程序

先决条件

确保 AD 系统和 Linux 系统都已正确配置：

- 验证名称解析配置。特别是，验证 DNS SRV 记录。例如，对于名为 ad.example.com 的域：
  - 验证 DNS SRV LDAP 记录：

```
# dig -t SRV _ldap._tcp.ad.example.com
```

  - 验证 AD 记录：

```
# dig -t SRV _ldap._tcp.dc._msdcs.ad.example.com
```

如果您稍后将 SSSD 连接到特定的 AD 域控制器，则不需要验证 DNS SRV 记录。

- 验证两个系统上的系统时间是否同步。这样可确保 Kerberos 能够正常工作。

- 确保 AD 域控制器上的以下端口已打开并可以被 RHEL 主机访问。

表 2.1. 使用 SSSD 将 Linux 系统直接集成到 AD 所需的端口

服务	端口	协议	备注
DNS	53	UDP 和 TCP	
LDAP	389	UDP 和 TCP	
Kerberos	88	UDP 和 TCP	
Kerberos	464	UDP 和 TCP	kadmin 用来设置和更改密码
LDAP 全局目录	3268	TCP	如果使用 id_provider = ad 选项
NTP	123	UDP	可选
Samba	445	UDP 和 TCP	对于 AD 组策略对象 (GPO)

配置本地系统

红帽建议使用 realm join 命令来配置系统。请参阅 第 3 章 使用 realmd 连接到 Active Directory 域。realmd 套件自动编辑所有必要的配置文件。例如：

```
# realm join ad.example.com
```

如果您不想使用 realmd，您可以手动配置系统。请参阅在 Red Hatnbsp 中手动将 SSSD 客户端连接

到 Active Directory 域;Hat Knowledgebase.

可选：配置用户主目录和 Shell

当用户首次登录 Linux 系统时，pam_oddjob_mkhomedir.so 库会自动创建主目录。默认情况下，SSSD 从 AD 身份提供程序检索主目录的格式。在 Linux 客户端中自定义目录格式：

1. *打开 /etc/sssd/sssd.conf 文件：*
2. *在 [domain] 部分，使用以下选项之一：*
   - *fallback_homedir 设置回退主目录格式，只有在 AD 中未定义主目录时才使用*
   - *override_homedir 设置主目录模板，始终覆盖 AD 中定义的主目录*

   例如，要始终使用格式 /home/domain_name/user_name:

```
[domain/EXAMPLE]
[... file truncated ...]
override_homedir = /home/%d/%u
```

   详情请查看 sssd.conf(5) man page。

默认情况下，SSSD 从 AD 中配置的 loginShell 参数检索用户 shell 的信息。在 Linux 客户端中自定义用户 shell 设置：

1. *打开 /etc/sssd/sssd.conf 文件：*
2. *使用这些选项定义所需的用户 shell 设置：*
   - *shell_fallback 设置回退值，仅在 AD 中没有定义 shell 时才使用*

- override_shell 设置始终覆盖 AD 中定义的 shell 的值
- default_shell 设置默认 shell 值
- allowed_shells 和 vetoed_shells 设置允许或黑名单的 shell 列表

详情请查看 sssd.conf(5) man page。

加载新配置

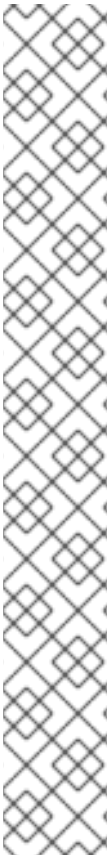
- 更改配置文件后重启 SSSD。

```
# systemctl restart sssd.service
```

其它资源

- 有关 LDAP 和 Kerberos 供应商的其它配置选项请查看 sssd-ldap(5) 和 sssd-krb5(5) man page。
- 有关 AD 供应商的其它配置选项请查看 sssd-ad(5) man page。

2.2.3. 配置 SSSD 使用 AD 中定义的 POSIX 属性



注意

在以前的版本中，UNIX 扩展的 Identity Management 可用于为用户帐户提供 POSIX 属性。扩展现已被弃用。详情请查看 Microsoft Developer Network。

如果您正在使用 UNIX 的 Identity Management for UNIX，请参阅知识库文章以了解常见问题解答。

有关引用 Unix 身份管理以及 Unix 软件包的服务的旧流程，请查看这些 Red Hatnbsp; 推荐的知识库文章：

- 使用 POSIX 属性配置 Active Directory 域
- 将 Active Directory 配置为 LDAP 域

建议

为获得最佳性能，请将 POSIX 属性发布到 AD 全局目录。如果全局目录中没有 POSIX 属性，SSSD 会直接连接到 LDAP 端口上的单个域控制器。

将 Linux 系统加入 AD 域

按照 第 2.2.2 节 “使用 ID 映射配置 AD 域作为 SSSD 的提供程序” 中的步骤操作。

在 SSSD 中禁用 ID 映射

1. 打开 /etc/sssd/sssd.conf 文件：
2. 在 AD 域部分，添加 ldap_id_mapping = false 设置。

注意

如果您使用 realm 实用程序加入域并添加 --automatic-id-mapping=no 参数，则 realm 实用程序已使用 ldap_id_mapping = false 设置 SSSD。

3. 如果您之前请求的任何用户使用默认 ID 映射配置的用户，请删除 SSSD 缓存：

```
rm -f /var/lib/sss/db/*
```

SSSD 现在将使用 AD 中的 POSIX 属性，而不是在本地创建它们。

其它资源

有关 ID 映射和 ldap_id_mapping 参数的详情，请查看 sssd-ldap(8) man page。

2.3. 自动 KERBEROS 主机密钥选项卡续订

如果安装了 adcli 软件包，SSSD 会在 AD 环境中自动续订 Kerberos 主机 keytab 文件。如果机器帐户密码早于配置的值，守护进程会每天检查并在需要时更新它。

默认续订间隔为 30 天。更改默认选项：

1. 在 /etc/sssd/sssd.conf 文件中向 AD 供应商添加以下参数：

```
ad_maximum_machine_account_password_age = value_in_days
```

2. 重启 SSSD：

```
# systemctl restart sssd
```

要禁用自动 Kerberos 主机 keytab 续订，请设置 ad_maximum_machine_account_password_age = 0。

2.4. 启用动态 DNS 更新

AD 允许其客户端自动刷新其 DNS 记录。AD 还主动维护 DNS 记录，以确保这些记录已更新，包括超时（粘贴）和删除（过期）不活动记录。默认情况下，AD 端不启用 DNS 清理功能。

SSSD 允许 Linux 系统通过刷新其 DNS 记录来模仿 Windows 客户端，这也阻止其记录标记为不活动并从 DNS 记录中删除。启用动态 DNS 更新时，客户端的 DNS 记录会被刷新：

- 身份提供商在线时（始终）
- Linux 系统重新启动（始终）
- 在指定的时间间隔（可选配置）；默认情况下，AD 供应商每 24 小时更新 DNS 记录

  您可以将此行为设置为与 DHCP 租期相同的间隔。在这种情况下，Linux 客户端会在租期续订后续订。

DNS 更新使用 Kerberos/GSSAPI 作为 DNS(GSS-TSIG)发送到 AD 服务器。这意味着，只需要启用安全连接。

为每个域设置动态 DNS 配置。例如：

```
[domain/ad.example.com]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad

ldap_schema = ad

dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600
```

有关这些选项的详情，请查看 sssd-ad(5) man page。

2.5. 在 SSSD 中使用 RANGE RETRIEVAL SEARCHES

SSSD 支持使用 Range Retrieval 功能进行 AD 搜索。有关范围检索搜索的详情，请查看 Microsoft Developer Network。

重要

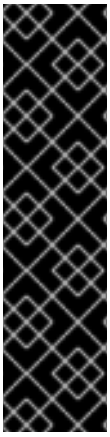
如果您在组或搜索库中设置自定义过滤器，过滤器可能无法与非常大的组配合工作。

2.6. 组策略对象访问控制

组策略是一种 Microsoft Windows 功能，使管理员能够集中管理 Active Directory(AD)环境中的用户和计算机的策略。组策略对象 (GPO)是存储在域控制器(DC)上的策略设置集合，可应用于策略目标，如计算机和用户。与 Windows 登录权限相关的 GPO 策略设置通常用于管理 AD 环境中的基于计算机的访问控制。

2.6.1. SSSD 如何使用 GPO 访问控制工作

当您将 SSSD 配置为应用 GPO 访问控制时，SSSD 会检索适用于主机系统和 AD 用户的 GPO。根据检索的 GPO 配置，SSSD 确定是否允许用户登录到特定的主机。这样，管理员可以定义 AD 域控制器上集中的 Linux 和 Windows 客户端遵守的登录策略。



重要

安全过滤功能允许您通过在安全过滤器中列出特定用户、组或主机来进一步限制 GPO 访问控制的范围。但是，SSSD 只支持安全过滤器中的用户和组。SSSD 忽略安全过滤器中的主机条目。

为确保 SSSD 将 GPO 访问控制应用到特定系统，请在 AD 域中创建新 OU，将系统移到 OU，然后将 GPO 链接到这个 OU。

2.6.2. SSSD 支持的 GPO 设置

表 2.2. SSSD 检索的 GPO 访问控制选项

GPO 选项 [a]	对应的 sssd.conf 选项 [b]
允许本地登录 拒绝本地登录	***ad_gpo_map_interactive***
允许通过远程桌面服务登录 通过远程桌面服务拒绝登录	***ad_gpo_map_remote_interactive***
从网络访问此计算机 拒绝从网络访问此计算机	***ad_gpo_map_network***

GPO 选项 [a]	对应的 sssd.conf 选项 [b]
允许以批处理任务身份登录 拒绝以批处理任务身份登录	*ad_gpo_map_batch*
允许作为服务登录 拒绝作为服务登录	*ad_gpo_map_service*
[a] 如 Windows 上的组策略管理编辑器中的名称。 [b] 有关这些选项的详情，请查看 sssd-ad(5) man page，以及默认将 GPO 选项映射到的可插入验证模块(PAM)服务列表。	

2.6.3. 为 SSSD 配置基于 GPO 的访问控制

基于 GPO 的访问控制可以在 /etc/sssd/sssd.conf 文件中配置。ad_gpo_access_control 选项指定基于 GPO 的访问控制运行的模式。它可以设置为以下值：

ad_gpo_access_control = permissive

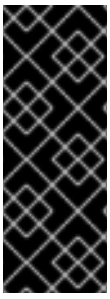
permissive 值指定基于 GPO 的访问控制会被评估但不强制实施；每次访问都会被拒绝时都会记录 syslog 信息。这是默认的设置。

ad_gpo_access_control = enforcing

enforcing 值指定评估并实施基于 GPO 的访问控制。

ad_gpo_access_control = disabled

disabled 值指定基于 GPO 的访问控制不会被评估，也不会强制执行。



重要

在开始使用基于 GPO 的访问控制并将 ad_gpo_access_control 设置为 enforcing 模式前，建议确保将 ad_gpo_access_control 设置为 permissive 模式并检查日志。通过查看 syslog 消息，您可以在最终设置 enforcing 模式前，根据需要测试和调整当前的 GPO 设置。

以下与基于 GPO 的访问控制相关的参数也可以在 sssd.conf 文件中指定：

- *ad_gpo_map_* 选项和 ad_gpo_default_right 选项配置哪些 PAM 服务映射到特定的 Windows 日志权限。*

  要将 PAM 服务添加到映射到特定 GPO 设置的默认 PAM 服务列表中，或者从列表中删除该服务，请使用 ad_gpo_map_* 选项。例如，要从映射到交互式登录的 PAM 服务列表中删除 su 服务（GPO 设置允许在本地登录和拒绝本地登录）：

```
ad_gpo_map_interactive = -su
```

- *ad_gpo_cache_timeout 选项指定后续访问控制请求可以重复使用缓存中存储的文件的时间间隔，而不是从 DC 中检索它们。*

有关可用 GPO 参数及其描述和默认值的详情，请查看 sssd-ad(5) man page。

2.6.4. 其它资源

- *有关配置 SSSD 以用于 GPO 的更多详细信息，请参阅 配置 SSSD 以处理 Red Hatnbsp 中的 Active Directory SSH 或 Console/GUI GPOs ；Hat 知识库。*

2.7. 使用 SSSD 自动创建用户私有组

直接集成到 AD 中的 SSSD 客户端可为每个 AD 用户自动创建一个用户私人组，确保其 GID 与用户的 UID 匹配，除非已经获取了 GID 号。为避免冲突，请确保服务器上不存在 GID 与用户 UID 相同的组。

GID 不存储在 AD 中。这样可确保 AD 用户从组功能中受益，而 LDAP 数据库不包含不必要的空组。

2.7.1. 为 AD 用户激活自动创建用户专用组

为 AD 用户激活自动创建用户私有组：

1. *编辑 /etc/sssd/sssd.conf 文件，在 [domain/LDAP] 部分添加：*

```
auto_private_groups = true
```

2. 重启 sssd 服务，删除 sssd 数据库：

```
# service sssd stop ; rm -rf /var/lib/sss/db/* ; service sssd start
```

执行此步骤后，每个 AD 用户都有一个与 UID 相同的 GID：

```
# id ad_user1
uid=121298(ad_user1) gid=121298(ad_user1) groups=121298(ad_user1),10000(Group1)
# id ad_user2
uid=121299(ad_user2) gid=121299(ad_user2) groups=121299(ad_user2),10000(Group1)
```

2.7.2. 取消激活 AD 用户的自动创建用户专用组

要取消激活为 AD 用户自动创建用户私有组：

1. 编辑 /etc/sssd/sssd.conf 文件，在 [domain/LDAP] 部分添加：

```
auto_private_groups = false
```

2. 重启 sssd 服务，删除 sssd 数据库：

```
# service sssd stop ; rm -rf /var/lib/sss/db/* ; service sssd start
```

执行此步骤后，所有 AD 用户都有相同的通用 GID：

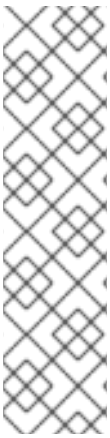
```
# id ad_user1
uid=121298(ad_user1) gid=10000(group1) groups=10000(Group1)
# id ad_user2
uid=121299(ad_user2) gid=10000(group1) groups=10000(Group1)
```

2.8. SSSD 客户端和 ACTIVE DIRECTORY DNS SITE AUTODISCOVERY

Active Directory林可能非常大，拥有许多不同的域控制器、域和子域，以及物理站点。Active Directory 使用站点的概念来识别其域控制器的物理位置。这使得客户端能够连接在地理上最接近的域控制器，从而提高客户端性能。

默认情况下，SSSD 客户端使用自动发现来查找其 AD 站点并连接到最接近的域控制器。这个过程由这些步骤组成：

1. SSSD 从 AD 林中的 DNS 服务器查询 SRV 记录。返回的记录在林中包含 DC 的名称。
2. SSSD 将 LDAP ping 发送到每个 DC。如果 DC 在配置的时间间隔内没有响应，则请求超时，SSSD 将 LDAP ping 发送到下一个间隔。如果连接成功，响应会包含 SSSD 客户端所属的 AD 站点的信息。
3. 然后，SSSD 从 DNS 服务器查询 SRV 记录以查找所属站点内的 DC，并连接到其中一个。



注意

SSSD 记住它默认属于的 AD 站点。这样，SSSD 可以在自动发现过程中将 LDAP ping 直接发送到本站点的 DC，以刷新站点信息。因此，自动发现的过程非常快速，因为通常不会发生超时。

如果站点不再存在或者同时将客户端分配到不同的站点，SSSD 会开始查询林中的 SRV 记录，然后再次进行整个过程。

要覆盖自动发现，使用 /etc/sssd/sssd.conf 文件的 [domain] 部分中的 ad_site 选项指定您要连接到的 AD 站点。

其它资源

- *有关 sssd-ad(5) 的详情，请查看 ad_site man page。*

- *有关 Identity Management 和 Active Directory 之间具有信任的环境，请参阅 第 5.6 节 “将身份管理或 SSSD 限制为受信任的 Active Directory 域中的选定 Active Directory 服务器或站点”。*

2.9. SSSD 故障排除

有关对 SSSD 故障排除 的详情，请参考系统级 身份验证指南中的 故障排除 SSSD 附录。

第 3 章 使用 REALMD 连接到 ACTIVE DIRECTORY 域

realmd 系统提供了一种清晰、简单的方式，可以发现和加入身份域，从而实现直接域集成。它将底层 Linux 系统服务（如 SSSD 或 Winbind）配置为连接到该域。

第 2 章 使用 Active Directory 作为 SSSD 的身份提供程序 描述如何在本地系统和 Active Directory 中使用系统安全服务守护进程(SSSD)作为后端身份提供程序。确保为此系统正确配置可能是一项复杂的任务：每个可能的身份供应商和 SSSD 本身都有许多不同的配置参数。此外，所有域信息必须提前提供，然后在 SSSD 配置中正确格式化，以便 SSSD 将本地系统与 AD 集成。

realmd 系统简化了该配置。它可以运行发现搜索来识别可用的 AD 和身份管理域，然后将系统加入到该域，并设置用于连接给定身份域并管理用户访问权限所需的客户端服务。另外，由于 SSSD 作为底层服务支持多个域，因此 realmd 也可以发现和支持多个域。

3.1. 支持的域类型和客户端

realmd 系统支持以下域类型：

- Microsoft Active Directory
- Red Hat Enterprise Linux Identity Management

realmd 支持以下域客户端：

- Red Hat Enterprise Linux Identity Management 和 Microsoft Active Directory 的 SSSD
- 适用于 Microsoft Active Directory 的 winbind

3.2. 使用 REALMD的先决条件

要使用 realmd 系统，请安装 realmd 软件包。

```
# yum install realmd
```

另外，请确保安装了 oddjob、oddjob-mkhomedir、sssd 和 adcli 软件包。需要这些软件包才能使用 realmd 管理系统。

注意

如 第 3.4 节 “发现和加入身份域” 所述，您只需使用 realmd 来查找要安装的软件包。

3.3. REALMD 命令

realmd 系统有两个主要的任务领域：

- 在域中管理系统注册
- 设置哪些域用户可以访问本地系统资源

realmd 中的中央实用程序称为 realm。大多数 realm 命令要求用户指定实用程序应执行的操作，以及要执行该操作的实体（如域或用户帐户）：

```
realm command arguments
```

例如：

```
realm join ad.example.com
realm permit user_name
```

表 3.1. realmd 命令

命令	描述
realm 命令	
discover	对网络中的域运行发现扫描。
join	将系统添加到指定的域中。
leave	从指定的域中删除系统。
list	列出系统的所有配置域，或者所有发现和配置的域。

命令	描述
登录命令	
permit	为指定用户或配置域中的所有用户启用访问权限，以访问本地系统。
deny	限制指定用户或配置域中所有用户的访问权限，以访问本地系统。

有关 realm 命令的详情请参考 realm(8) man page。

3.4. 发现和加入身份域

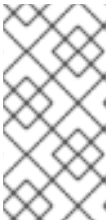
realm discovery 命令返回完整的域配置，以及必须安装的软件包列表，才能在域中注册系统。

然后，realm join 命令通过配置本地系统服务和身份域中的条目来设置本地计算机以用于指定域。由 realm 运行的进程遵循以下步骤 ：

1. *对指定的域运行发现扫描.*

2. *自动安装将系统加入域所需的软件包。*

   这包括 SSSD 和 PAM 主目录作业软件包。请注意，自动安装软件包需要运行 PackageKit 套件。

   注意

   如果禁用 PackageKit，系统会提示您输入缺少的软件包，您需要使用 yum 实用程序手动安装它们。

3. *通过在 目录中为系统创建帐户条目来加入域。*

4. *创建 /etc/krb5.keytab 主机 keytab 文件。*

5. 在 SSSD 中配置域并重新启动服务。

6. 在 PAM 配置和 /etc/nsswitch.conf 文件中为系统服务启用域用户。

发现域

不带任何选项运行时，realm discover 命令将显示有关默认 DNS 域的信息，即通过 Dynamic Host Configuration Protocol(DHCP)分配的域：

```
# realm discover
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common
```

也可以为特定域运行发现。要做到这一点，运行 realm discover 并添加您要发现的域名称：

```
# realm discover ad.example.com
```

域系统随后将使用 DNS SRV 查找来自动查找此域中的域控制器。

注意

域发现命令要求 NetworkManager 正在运行；特别是，它依赖于 NetworkManager 的 D-Bus 接口。如果您的系统没有使用 NetworkManager，请始终在 realm discovery 命令中指定域名。

realmd 系统可以发现 Active Directory 和 Identity Management 域。如果您的环境中两个域都存在，您可以使用 --server-software 选项将发现结果限制为特定的服务器类型。例如：

```
# realm discover --server-software=active-directory
```

发现搜索返回的其中一个属性是 login-policy，它显示域用户是否允许域用户在加入完成后立即登录。如果默认情况下不允许登录，您可以使用 realm allow 命令手动允许登录。详情请查看 第 3.7 节 “管理域用户的登录权限”。

有关 realm discover 命令的详情请参考 realm(8) man page。

加入域

重要

请注意，Active Directory 域需要使用唯一的计算机名称。NetBIOS 计算机名称及其 DNS 主机名应唯一定义并相互对应。

要将系统加入身份域，请使用 realm join 命令并指定域名：

```
# realm join ad.example.com
realm: Joined ad.example.com domain
```

默认情况下，连接以域管理员身份执行。对于 AD，管理员帐户名为 Administrator ；对于 IdM，它名为 admin。要以其他用户身份连接，请使用 -U 选项：

```
# realm join ad.example.com -U user
```

命令首先尝试在没有凭据的情况下进行连接，但是如果需要，它会提示输入密码。

如果在 Linux 系统上正确配置了 Kerberos，则也可以使用 Kerberos 票据进行身份验证。要选择 Kerberos 主体，请使用 -U 选项。

```
# kinit user
  # realm join ad.example.com -U user
```

realm join 命令接受其他几个配置选项。有关 realm join 命令的详情请参考 realm(8) man page。

例 3.1. 将系统注册到域中的过程示例

1. 运行 realm discovery 命令，以显示有关域的信息。

```
# realm discover ad.example.com
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
  configured: no
  server-software: active-directory
  client-software: sssd
```

2. 运行 **realm join** 命令，并将域名传递到 命令。如果系统提示输入密码，请提供管理员密码。

```
# realm join ad.example.com
Password for Administrator: password
```

请注意，当发现或加入域时，**realmd** 会检查 **DNS SRV** 记录：

- **_ldap._tcp.domain.example.com. for Identity Management records**
- **_ldap._tcp.dc._msdcs.domain.example.com. for Active Directory records**

在配置了 **AD** 时会默认创建 记录，这允许通过服务发现发现它。

在加入域后测试系统配置

要测试系统是否已成功加入域中，请验证您是否可以以用户身份从域中登录，并是否正确显示用户信息：

1. 运行 **id user@domain_name** 命令，以显示域中用户的信息。

```
# id user@ad.example.com
uid=1348601103(user@ad.example.com) gid=1348600513(domain
group@ad.example.com) groups=1348600513(domain group@ad.example.com)
```

2. 使用 **ssh** 实用程序，以同一用户身份登录。

```
# ssh -l user@ad.example.com linux-client.ad.example.com
user@ad.example.com@linux-client.ad.example.com's password:
Creating home directory for user@ad.example.com.
```

3. 验证**pwd** 实用程序是否打印用户的主目录。

```
$ pwd
/home/ad.example.com/user
```

4. 验证 **id** 实用程序是否在第一步中显示与 **id user@domain_name** 命令相同的信息。

```
$ id
uid=1348601103(user@ad.example.com) gid=1348600513(domain
group@ad.example.com) groups=1348600513(domain group@ad.example.com)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

在测试域加入是否成功时，**kinit** 实用程序也很有用。请注意，要使用该工具，必须安装 **krb5-workstation** 软件包。

3.5. 从身份域中删除系统

若要从身份域中删除系统，可使用 **realm left** 命令。该命令从 **SSSD** 和本地系统中删除域配置。

```
# realm leave ad.example.com
```

默认情况下，删除将以默认管理员身份执行。对于 **AD**，管理员帐户名为 **Administrator** ；对于 **IdM**，它名为 **admin**。如果使用其他用户加入域，则可能需要以该用户身份执行删除操作。要指定其他用户，请使用 **-U** 选项：

```
# realm leave ad.example.com -U 'AD.EXAMPLE.COM\user'
```

命令首先尝试在没有凭据的情况下进行连接，但是如果需要，它会提示输入密码。

请注意，当客户端离开某个域时，计算机帐户不会从 目录中删除；仅删除本地客户端配置。如果要删除计算机帐户，请在指定 **--remove** 选项的情况下运行 命令。

有关 **realm leave** 命令的详情请参考 **realm(8) man page**。

3.6. 列出域

realm list 命令列出系统的每个配置域，以及该域的完整详情和默认配置。这与 realm discovery 命令返回的信息相同，仅适用于已在系统配置中的域。

```
# realm list --all --name-only
ad.example.com
```

realm list 接受的最显著选项有：

--all

all 选项列出了所有已发现的域，包括已配置和未配置的域。

--name-only

name-only 选项将结果限制为域名，不显示域配置详情。

有关 realm list 命令的详情请参考 realm(8) man page。

3.7. 管理域用户的登录权限

默认情况下会应用域端访问控制，这意味着域用户的登录策略在域本身中定义。此默认行为可以被覆盖，以便使用客户端访问控制。使用客户端访问控制时，登录权限仅由本地策略定义。

如果域应用客户端访问控制，您可以使用 realmd 系统为来自该域的用户配置基本的允许或拒绝访问规则。请注意，这些访问规则允许或拒绝访问系统上的所有服务。必须在特定系统资源或域中设置更具体的访问规则。

要设置访问规则，请使用以下两个命令：

realm deny

realm deny 命令只是拒绝对域内所有用户的访问。使用此命令及 --all 选项。

域允许

realm allow 命令可用于：

- 使用 --all 选项授予所有用户的访问权限，例如：

```
$ realm permit --all
```

- 向指定用户授予访问权限，例如：

```
$ realm permit user@example.com
$ realm permit 'AD.EXAMPLE.COM\user'
```

- 使用 -x 选项拒绝对指定用户的访问，例如：

```
$ realm permit -x 'AD.EXAMPLE.COM\user'
```

请注意，当前仅允许主域中的用户进行访问，不适用于可信域中的用户。这是因为虽然用户登录必须包含域名，但 SSSD 当前无法提供有关可用子域的信息。

重要

更为安全的一点是，仅允许特定选定用户或组进行访问，而不是拒绝访问某些用户或组，同时让其他用户均可访问。因此，我们不建议默认允许访问 all，而仅拒绝域允许 -x 的指定用户访问。相反，红帽建议为所有用户维护默认无访问权限策略，仅使用域允许向选定的用户授予访问权限。

有关 realm deny 和 realm allow 命令的详情请参考 realm(8) man page。

3.8. 更改默认用户配置

realmd 系统支持修改默认用户主目录和 shell POSIX 属性。例如，如果 Windows 用户帐户中没有设置某些 POSIX 属性，或者这些属性与本地系统上其他用户的 POSIX 属性不同，这可能是必需的。

重要

只有 realm join 命令尚未运行时才可以更改本节中描述的配置。如果系统已经加入，请更改 /etc/sssd/sssd.conf 文件中的默认主目录和 shell，如 “可选：配置用户主目录和 Shell”一节 所述。

要覆盖默认主目录和 shell POSIX 属性，请在 /etc/realmd.conf 文件中的 [users] 部分指定以下选项：

default-home

default-home 选项设置一个模板，用于为未明确设置主目录的帐户创建主目录。常用的格式为 /home/%d/%u，其中 %d 是域名，%u 是用户名。

default-shell

default-shell 选项定义默认用户 shell。它接受任何受支持的系统 shell。

例如：

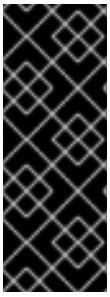
```
[users]
default-home = /home/%u
default-shell = /bin/bash
```

有关选项的详情请参考 realmd.conf(5) man page。

3.9. ACTIVEACTIVE DIRECTORYNBSP 的额外配置;DIRECTORY 域条目

每个域的自定义设置可以在 /etc/realmd.conf 文件中定义。每个域可以有自己的配置部分；部分的名称必须与域名匹配。例如：

```
[ad.example.com]
attribute = value
attribute = value
```



重要

只有 realm join 命令尚未运行时才可以更改本节中描述的配置。如果系统已经加入，更改这些设置不会有任何影响。在这种情况下，您必须离开域，如 第 3.5 节 “从身份域中删除系统” 所述，然后再次加入，如 “加入域”一节 所述。请注意，加入需要域管理员的凭据。

要更改域的配置，请编辑 /etc/realmd.conf 中的对应部分。以下示例禁用 ad.example.com 域的 ID 映射，设置主机主体，并将系统添加到指定的子树中：

```
[ad.example.com]
computer-ou = ou=Linux Computers,DC=domain,DC=example,DC=com
user-principal = host/linux-client@AD.EXAMPLE.COM
automatic-id-mapping = no
```

请注意，在最初使用 realm join 命令将系统加入域时，也可以设置相同的配置，如 “加入域”一节 所述。

```
# realm join --computer-ou="ou=Linux Computers,dc=domain,dc=com" --automatic-id-mapping=no --
user-principal=host/linux-client@AD.EXAMPLE.COM
```

表 3.2 “域配置选项” 列出 /etc/realmd.conf 的 domain default 部分中可设置的最重要选项。有关可用配置选项的完整信息，请查看 realmd.conf(5) man page。

表 3.2. 域配置选项

选项	描述
computer-ou	设置将计算机帐户添加到域中的目录位置。这可以是完整 DN 或 RDN，相对于 root 条目。子树必须已经存在。
user-principal	将计算机帐户的 **userPrincipalName** 属性值设置为提供的 Kerberos 主体。
automatic-id-mapping	设置是启用动态 ID 映射还是禁用映射并使用 Active Directory 中配置的 POSIX 属性。

第 4 章 使用 SAMBA 进行 ACTIVE DIRECTORY 集成

Samba 在红帽企业 Linux 中实施服务器消息块(SMB)协议。SMB 协议用于访问服务器上的资源，如文件共享和共享打印机。

您可以使用 Samba 将 Active Directory(AD)域用户验证到域控制器(DC)。此外，您可以使用 Samba 向网络中的其他 SMB 客户端共享打印机和本地目录。

4.1. 使用 WINBINDD AUTHENTICATE DOMAIN USERS

Samba 的 winbindd 服务为名称服务交换机(NSS)提供接口，并让域用户在登录本地系统时对 AD 进行身份验证。

使用 winbindd 的优势在于，您可以增强共享目录和打印机的配置，而无需安装其他软件。详情请查看《红帽系统管理员指南》中有关 Samba 的章节。

4.1.1. 加入 AD 域

如果要加入 AD 域并使用 Winbind 服务，请使用 realm join --client-software=winbind domain_name 命令。realm 实用程序自动更新配置文件，例如用于 Samba、Kerberos 和 PAM 的配置文件。

如需更多详细信息和示例，请参阅《红帽系统管理员指南》中的将 Samba 设置为域成员部分。

4.2. 将 SMB 共享与 SSSD 和 WINBIND 搭配使用

这部分论述了如何使用 SSSD 客户端根据服务器消息块(SMB)协议（也称为通用 Internet 文件系统(CIFS)协议）访问和充分利用共享。

重要

在 IdM 或 ActiveActive Directorynbsp 中使用 SSSD 作为客户端;Directory 域有一些限制，红帽不推荐将 SSSD 用作 ID 映射插件作为 Winbind。详情请查看在“IdM 客户端上运行的 Samba 文件服务器的支持状态是什么，或直接注册了 SSSD 用作客户端守护进程的 AD 客户端”。

SSSD 不支持 Winbind 提供的所有服务。例如，SSSD 不支持使用 NT LAN Manager(NTLM)或 NetBIOS 名称查找进行身份验证。如果您需要这些服务，请使用 Winbind。请注意，在身份管理域中，Kerberos 身份验证和 DNS 名称查找可用于相同目的。

4.2.1. SSSD 如何使用 SMB 工作

SMB 文件共享协议在 Windows 机器上广泛使用。在身份管理和 Active Directory 之间信任的红帽企业 Linux 环境中，SSSD 可以像标准 Linux 文件系统一样无缝使用 SMB。

要访问 SMB 共享，系统必须能够将 Windows SID 转换为 Linux POSIX UID 和 GID。SSSD 客户端使用 SID 到 ID 或 SID 至名称算法，这将启用这个 ID 映射。

4.2.2. 在 SSSD 和 Winbind 间切换以用于 SMB 共享访问

这个步骤描述了如何在 SSSD 和 Winbind 插件间切换，这些插件用于从 SSSD 客户端访问 SMB 共享。要使 Winbind 能够访问 SMB 共享，您需要在客户端上安装 cifs-utils 软件包。确保您的机器上安装了 cifs-utils ：

```
$ rpm -q cifs-utils
```

1. 可选。了解您当前是否使用 SSSD 或 Winbind 从 SSSD 客户端访问 SMB 共享：

```
# alternatives --display cifs-idmap-plugin
cifs-idmap-plugin - status is auto.
 link currently points to /usr/lib64/cifs-utils/cifs_idmap_sss.so
/usr/lib64/cifs-utils/cifs_idmap_sss.so - priority 20
/usr/lib64/cifs-utils/idmapwb.so - priority 10
Current `best' version is /usr/lib64/cifs-utils/cifs_idmap_sss.so.
```

如果安装了 SSSD 插件(cifs_idmap_sss.so)，则默认其优先级高于 Winbind 插件(idmapwb.so)。

2. 在切换到 Winbind 插件前，请确保 Winbind 在系统中运行：

```
# systemctl is-active winbind.service
active
```

在切换到 SSSD 插件前，请确保 SSSD 在系统中运行：

```
# systemctl is-active sssd.service
active
```

3. 要切换到其他插件，请使用 **alternatives --set cifs-idmap-plugin** 命令，并指定所需插件的路径。例如，切换到 Winbind:

```
# alternatives --set cifs-idmap-plugin /usr/lib64/cifs-utils/idmapwb.so
```

注意

32 位版本平台（如 RHEL 7 中的 i686）使用 /usr/lib/cifs-utils/ 目录，而不是 /usr/lib64/cifs-utils/。

4.3. 其它资源

有关 Samba 的详情，请查看《红帽系统管理员指南》中的相应章节。

部分 II. 将 LINUX 域与 ACTIVE DIRECTORY 域集成：跨林信任

这部分提供了通过创建、配置和管理跨林信任环境将 Linux 域与 Active Directory 域集成的推荐做法。

第 5 章 使用 ACTIVEACTIVE DIRECTORYNBSP;DIRECTORY 和 IDENTITYIDENTITY MANAGEMENTNBSP;MANAGEMENT 创建 CROSS-FOREST TRUSTS

本章论述了 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp 间创建跨林信任;Management.跨林信任是间接集成身份管理和 Active Directory(AD)环境的两个方法之一。另一种方法是同步。如果您不确定要为您的环境选择哪一种方法，请参阅 第 1.3 节 “间接集成”。

Kerberos 实施信任的概念。在信任中，一个 Kerberos 域的主体可向另一个 Kerberos 域中的服务请求一个票据。使用此票据时，主体可以针对属于其他域的计算机上的资源进行身份验证。

Kerberos 也可以在另外两个单独的 Kerberos 域之间创建关系：跨域信任。属于信任的域使用一对票据和密钥；一个域的成员然后计算为两个域的成员。

红帽身份管理支持在 IdM 域和 Active Directory 域之间配置跨林信任。

5.1. 跨林信任简介

Kerberos 域仅涉及身份验证。其他服务和协议用于为 Kerberos 域中的计算机上运行的资源补充身份和授权。

因此，建立 Kerberos 跨域信任不足以让一个域的用户访问另一域中的资源；在其他通信级别也需要支持。

5.1.1. 信任关系的架构

ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 管理各种核心服务，如 Kerberos、LDAP、DNS 或证书服务。为了以透明的方式集成这两种多样化环境，所有核心服务必须彼此无缝交互。

Active Directory Trusts、林和跨林信任

Kerberos 跨域信任在 Active Directory 环境之间身份验证方面扮演着重要角色。无论如何执行访问权限，解析可信 AD 域中用户和组名称的所有活动都需要身份验证：使用 LDAP 协议或作为服务器消息块(SMB)协议基础上分布式计算环境/远程过程调用(DCE/RPC)的一部分。由于在两个不同的 Active Directory 域之间组织访问涉及更多协议，因此信任关系具有更为通用的名称，Active Directory 信任。

可以将多个 AD 域组织到 Active Directory 林中。林的根域是林中创建的第一个域。身份管理域不能是现有 AD 林的一部分，因此它总是被视为一个单独的林。

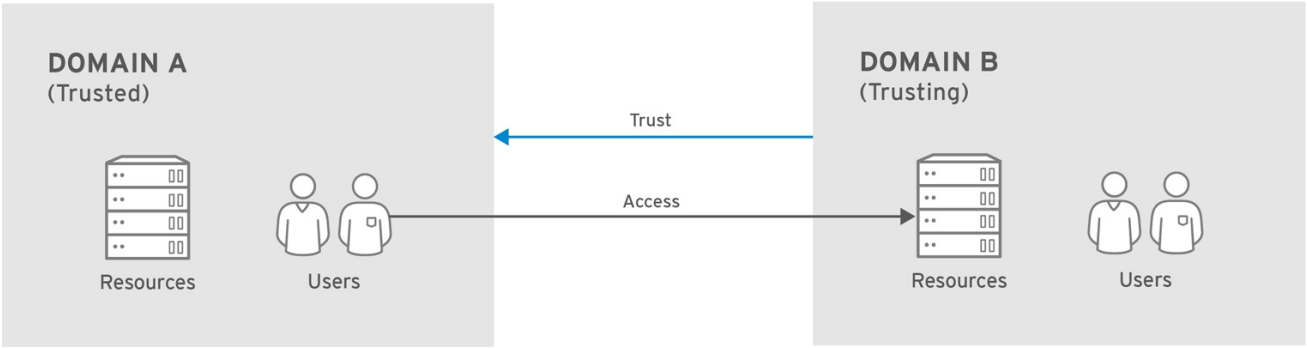
当两个单独的林根域之间建立了信任关系时，允许来自不同 AD 地区的用户和服务进行通信，则信任称为 Active Directory 跨林信任。

信任流和单向信任

信任在两个域之间建立访问关系。Activeactive Directorynbsp;Directory 环境可能比较复杂，因此 ActiveActive Directorynbsp 的可能类型和排序;Directory 信任、在子域、根域或林之间。信任是指从一个域到另一个域的路径。在域之间移动身份和信息的方式称为信任流。

受信任的域包含用户，信任域则允许访问资源。在单向信任中，信任流向一个方向：用户可以访问信任域的资源，但信任域的用户无法访问受信任的域中的资源。在 图 5.1 “单向信任” 中，Domain A 被 Domain B 信任，但 Domain B 不被 Domain A 信任。

图 5.1. 单向信任

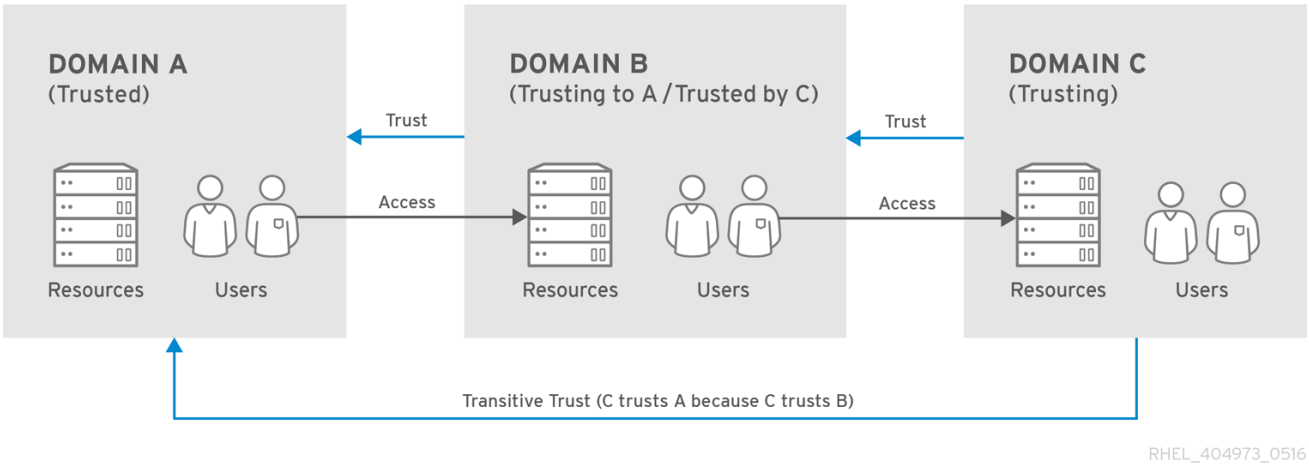


IdM 允许管理员配置单向和双向信任。详情请查看 第 5.1.4 节 “一次性和双向信任”。

传输和非转换信任

信任可以是传递的，以便域信任另一个域和被该第二个域信任的任何其他域。

图 5.2. 传输信任



信任也可以是非转换性的，这意味着信任仅限于明确包含的域。

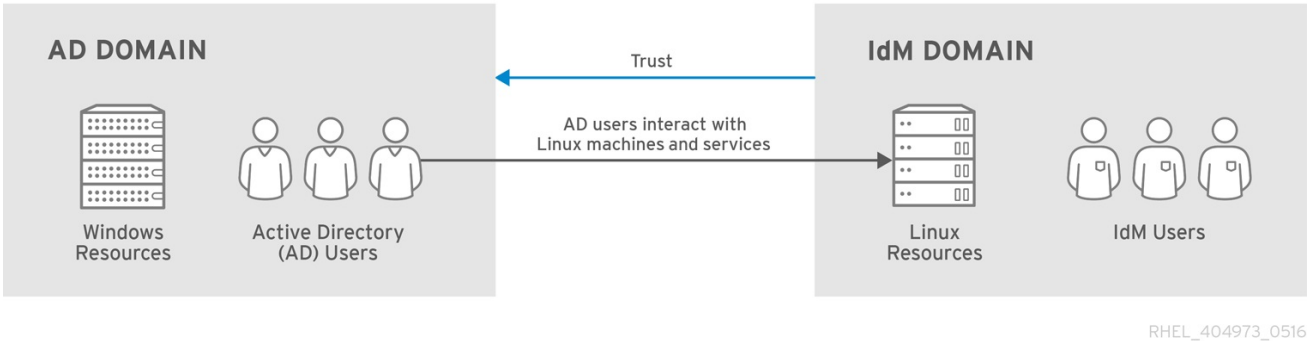
Active Directory 和 Identity Management 中的跨林信任

在 Active Directory 林内，域之间的信任关系在默认情况下通常是双向和传递的。

因为两个 AD 林之间的信任是两个林根域之间的信任，所以它也可以是双向或单向的。跨林信任的传递很明确：任何在 AD 林内导致林根域的域信任正在被跨林信任传递。但是，单独的跨林信任不是传递的。必须在每个 AD 林根域与另一个 AD 林根域之间建立显式跨林信任。

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 域之间建立跨林信任时，来自 AD 林域中的用户可以与 IdM 域中的 Linux 计算机和服务交互。

图 5.3. 信任方向



5.1.2. Active Directory 安全对象和信任

Active Directory 全局目录

全局目录包含有关 ActiveActive Directorynbsp;Directory 对象的信息。它将对象的完整副本存储在

自己的域中。来自 ActiveActive Directorynbsp 中其他域的对象；Directory 林，通常最多搜索属性的部分副本存储在全局目录中。此外，某些类型的组仅在特定范围内有效，且可能不属于全局目录。

请注意，跨林信任上下文比单个域宽松。因此，来自可信林的这些服务器本地或域范围内安全组成员资格对 IdM 服务器可能不可见。

全局目录和 POSIX 属性

Activeactive Directorynbsp;Directory 不使用默认设置复制 POSIX 属性。如果需要使用 AD 中定义的 POSIX 属性，请强烈建议将它们复制到全局目录服务。

5.1.3. IdM 中的信任架构

在 IdentityIdentity Managementnbsp;Management side 中，IdM 服务器必须能够识别 ActiveActive Directorynbsp;Directory 身份并相应地处理访问控制的组成员资格。Microsoft PAC（MS-PAC、Privilege Account 证书）包含用户所需的信息、其安全 ID、域名和组成员身份。IdentityIdentity Managementnbsp;Management 有两个组件来分析 Kerberos ticket 中 PAC 中的数据：

- SSSD，要在 ActiveActive Directorynbsp 上执行身份查找，并检索用于授权的用户和组安全标识符(SID)。SSSD 还缓存用户、组和票据信息，以及映射 Kerberos 和 DNS 域的用户、组和票据信息，
- IdentityIdentity Managementnbsp;Management（Linux 域管理）将 ActiveActive Directorynbsp;Directory 用户与 aan IdMnbsp;IdM 组关联，用于 IdM 策略和访问。

注意

Linux 域管理（如 SELinux、sudo 和基于主机的访问控制）的访问控制规则和策略通过 IdentityIdentity Managementnbsp;Management 进行定义和应用。在 ActiveActive Directorynbsp;Directory 一侧设置的任何访问控制规则没有被 IdM 评估或使用；唯一的 ActiveActive Directorynbsp;Directory 配置是组成员资格。

使用不同的 Active Directory Forests 信任

IdM 也可以是与不同 AD 林的信任关系的一部分。建立信任后，可以按照相同的命令和程序在以后添加与其他林之间的额外信任。IdM 可以同时信任多个完全不相关的林，允许来自这些不相关 AD 的用户访问同一共享 IdM 域中的资源。

5.1.3.1. Activeactive Directorynbsp;Directory PACs 和 IdM Tickets

ActiveActive Directorynbsp 中的组信息存储在 Privilege Attribute 证书 （MS-PAC 或 PAC）数据集中的标识符列表中。PAC 包含各种授权信息，如组成员身份或其他凭据信息。它还包括 Active Directory 域中用户和组的安全标识符 (SID)。SIDS 是创建时分配给 Active Directory 用户和组的标识符。在信任环境中，组成员由 SID 标识，而不是名称或 DN。

Active Directory 用户的 Kerberos 服务请求票据中嵌入了 PAC，作为将实体识别到 Windows 域中其他 Windows 客户端和服务器的一种方式。IdM 将 PAC 中的组信息映射到 ActiveActive Directorynbsp;Directory 组，然后到对应的 IdM 组来确定访问权限。

当 ActiveActive Directorynbsp;Directory 用户在 IdM 资源中请求一个 ticket 请求时，此过程如下：

1. 服务请求包含用户的 PAC。IdM Kerberos 分发中心(KDC)通过比较 Active Directory 组列表和 IdM 组中的成员资格来分析 PAC。

2. 对于 MS-PAC 中定义的 Kerberos 主体的 SID，IdM KDC 评估 IdM LDAP 中定义的外部组成员资格。如果 SID 有可用的其他映射，MS-PAC 记录将使用 SID 所属 IdM 组的其他 SID 扩展。生成的 MS-PAC 由 IdM KDC 签名。

3. 服务票据返回给用户，其更新的 PAC 由 IdM KDC 签名。属于 IdM 域的 AD 组的用户现在可以被 IdM 客户端上的 SSSD 根据服务票据的 MS-PAC 内容识别。这允许减少身份流量来发现 IdM 客户端的组成员资格。

当 IdM 客户端评估服务票据时，该进程包括以下步骤：

1. 评估流程中使用的 Kerberos 客户端库将 PAC 数据发送到 SSSD PAC 响应器。

2. PAC 响应器验证 PAC 中的组 SID，并将用户添加到 SSSD 缓存中的对应组。当访问新服务时，SSSD 会为每个用户存储多个 TGT 和票据。

3. 属于已验证组的用户现在可以访问 IdM 端所需的服务。

5.1.3.2. Active Directory 用户和身份管理组

在管理 Active Directory 用户和组时，您可以将单独的 AD 用户和整个 AD 组添加到身份管理组中。

有关如何为 AD 用户配置 IdM 组的描述，请参阅 第 5.3.3 节 “为 ActiveActive Directorynbsp 创建 IdM 组;Directory 用户”。

非POSIX 外部组和 SID 映射

IdM LDAP 中的组成员资格通过指定属于组成员的 LDAP 对象的区分名称(DN)来表示。AD 条目不会同步或复制到 IdM，这意味着 AD 用户和组在 IdM LDAP 中没有 LDAP 对象。因此，它们不能直接用于在 IdM LDAP 中表达组成员资格。

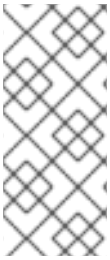
因此，IdM 会创建非POSIX 外部组 ：代理 LDAP 对象，其中包含 AD 用户和组的 SID 作为字符串的引用。然后，非POSIX 外部组被引用为普通 IdM LDAP 对象，以代表 IdM 中的 AD 用户和组的组成员资格。

非POSIX 外部组的 SIDS 由 SSSD 处理；SSSD 映射 AD 用户属于 IdM 中的 POSIX 组的 SID。AD 端的 SID 与用户名关联。当用户名用于访问 IdM 资源时，IdM 中的 SSSD 会将该用户名解析为其 SID，然后在 AD 域中查找该 SID 的信息，如 第 5.1.3.1 节 “Activeactive Directorynbsp;Directory PACs 和 IdM Tickets” 所述。

ID 范围

在 Linux 中创建用户时，会为其分配用户 ID 号。此外，也为用户创建一个专用组。私有组 ID 号与用户 ID 号相同。在 Linux 环境中，这不会造成冲突。但是，在 Windows 上，安全 ID 号必须为域中的每个对象唯一。

受信任的 AD 用户需要在 Linux 系统中使用 UID 和 GID 号。IdM 可以生成这个 UID 和 GID 号，但如果 AD 条目已分配了 UID 和 GID 号，则分配不同的数字会导致冲突。为避免此类冲突，可以使用 AD 定义的 POSIX 属性，包括 UID 和 GID 号以及首选的登录 shell。



注意

AD 将林内所有对象的信息子集存储在全局目录中。全局目录包括林中的每个域的所有条目。如果要使用 AD 定义的 POSIX 属性，红帽强烈建议您首先将这些属性复制到全局目录。

创建信任时，IdM 会自动检测要使用的 ID 范围，并为添加到信任的 AD 域创建一个唯一 ID 范围。您还可以通过将以下选项之一传递给 ipa trust-add 命令来手动选择：

ipa-ad-trust

此范围选项用于 IdM 根据 SID 生成 ID 算法。

如果 IdM 使用 SID-to-POSIX ID 映射生成 SID，AD 和 IdM 用户和组的 ID 范围必须具有唯一、非覆盖的 ID 范围。

ipa-ad-trust-posix

此范围选项用于 AD 条目中 POSIX 属性中定义的 ID。

IdM 从 AD 的全局目录或目录控制器获取 POSIX 属性，包括 uidNumber 和 gidNumber。如果 AD 域正确管理且没有 ID 冲突，则以这种方式生成的 ID 号是唯一的。在这种情况下，不需要验证 ID 或 ID 范围。

例如：

```
[root@ipaserver ~]# ipa trust-add name_of_the_trust --range-type=ipa-ad-trust-posix
```

重新创建其他 ID 范围的信任

如果所创建信任的 ID 范围不适合您的部署，您可以使用 other --range-type 选项重新创建信任：

1. 查看当前使用的所有 ID 范围：

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

在列表中，标识 ipa trust-add 命令创建的 ID 范围的名称。ID 范围名称的第一部分是 trust: name_of_the_trust _id_range的名称，如 ad.example.com。

2. （可选）如果您不知道在创建信任时使用了哪个 --range-type 选项 ipa-ad -trust 或 ipa-ad-trust-posix，请识别该选项：

```
[root@ipaserver ~]# ipa idrange-show name_of_the_trust_id_range
```

记录 类型，以便您在第 5 步中为新信任选择相反类型。

3. 删除 ipa trust-add 命令创建的范围：

```
[root@ipaserver ~]# ipa idrange-del name_of_the_trust_id_range
```

4. 删除信任：

```
[root@ipaserver ~]# ipa trust-del name_of_the_trust
```

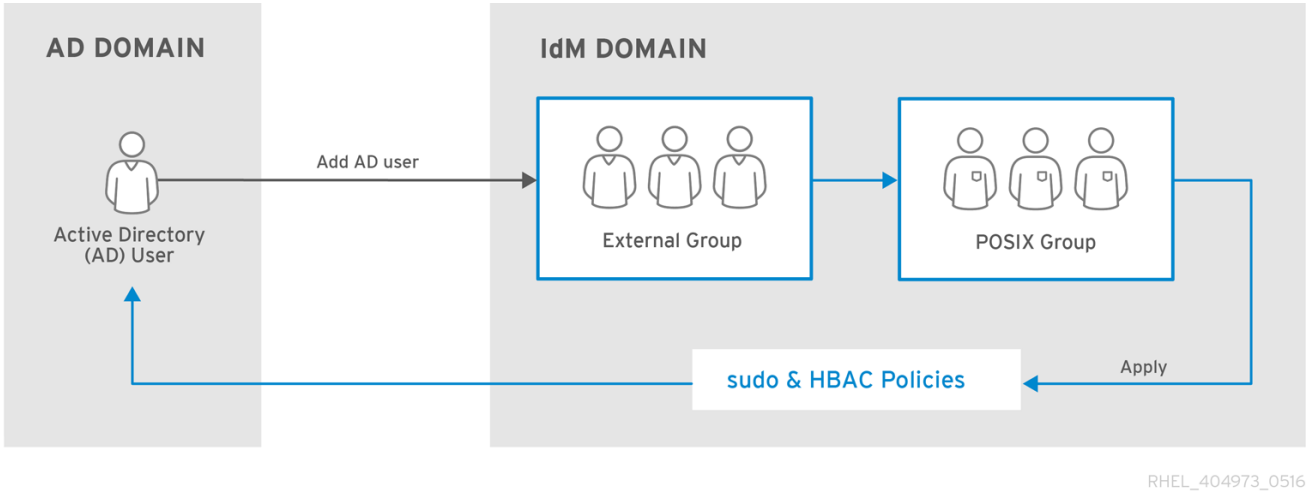
5. 使用正确的 --range-type 选项创建新信任。例如：

```
[root@ipaserver ~]# ipa trust-add name_of_the_trust --range-type=ipa-ad-trust
```

5.1.3.3. Active Directory 用户以及 IdM 策略和配置

几个 IdM 策略定义（如 SELinux、基于主机的访问控制、sudo 和 netgroups）依赖于用户组来识别策略的应用方式。

图 5.4. ActiveActive Directorynbsp;Directory Users and IdM Groups and Policies



Active Directory 用户在 IdM 域外部，但仍可作为组成员添加到 IdM 组，只要这些组配置为外部组，如 第 5.1.3.2 节 “Active Directory 用户和身份管理组” 所述。在这种情况下，sudo、基于主机的访问控制和其他策略会应用到外部 POSIX 组，最终在访问 IdM 域资源时应用到 AD 用户。

ticket 中的 PAC 中的用户 SID 被解析为 AD 身份。这意味着，ActiveActive

Directorynbsp;Directory 用户可使用其完全限定的用户名或其 SID 作为组成员来添加。

5.1.4. 一次性和双向信任

IdM 支持两种类型的信任协议，具体取决于能够建立与 IdM 中服务连接的实体是仅限于 AD，也可以包含 IdM 实体。

单向信任

单向信任可让 AD 用户和组访问 IdM 中的资源，但不能通过另一种方式访问。IdM 域信任 AD 林，但 AD 林不信任 IdM 域。

单向信任是创建信任的默认模式。

双向信任

双向信任可让 AD 用户和组访问 IdM 中的资源。您必须为 Microsoft SQL Server 等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 扩展在信任范围内工作。RHEL IdM 主机上的应用可能会从 Active Directory 域控制器请求 S4U2Self 或 S4U2Proxy 信息，并提供一个双向信任来提供此功能。

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。

有关单向和双向信任的常规信息，请参阅 第 5.1.1 节 “信任关系的架构”。

建立信任后，就无法修改其类型。如果您需要其他类型的信任，请再次运行 ipa trust-add 命令；这样做，您可以删除现有信任并创建新信任。

5.1.5. 外部 Trusts 到 ActiveActive Directorynbsp;Directory

外部信任是指位于不同地区的域之间的信任关系。虽然林信任始终需要在 ActiveActive Directorynbsp 根域间建立信任；Directory 林，您可以建立对林内任何域的信任。

外部信任是非转换的。因此，来自其他 ActiveActive Directorynbsp 的用户和组无法访问 IdM 资源。如需更多信息，请参阅 “传输和非转换信任”一节。

5.1.6. 信任控制器和信任代理

IdM 提供以下支持对 ActiveActive Directorynbsp;Directory 信任的 IdM 服务器：

信任控制器

可以控制信任并对 ActiveActive Directorynbsp;Directory 域控制器(DC)执行身份查找的 IdM 服务器。Activeactive Directorynbsp;Directory 域控制器在建立和验证对 ActiveActive Directorynbsp 的信任时联系信任控制器。配置信任时会创建第一个信任控制器。

有关将 IdM 服务器配置为信任控制器的详情，请参考 第 5.2.2 节 “创建信任”。

与信任代理相比，信任控制器运行更多的面向网络的服务，因而为潜在的入侵者提供了更大的攻击面。

信任代理

可针对 ActiveActive Directorynbsp;Directory 域控制器执行身份查找的 IdM 服务器。

有关将 IdM 服务器配置为信任代理的详情，请参考 第 5.2.2.1.1 节 “为信任准备 IdM 服务器”。

除了信任控制器和代理外，IdM 域还可以包含不带任何角色的副本。但是，这些服务器并不与 ActiveActive Directorynbsp;Directory 进行通信。因此，与这些服务器通信的客户端无法解决 ActiveActive Directorynbsp;Directory 用户和组或验证或授权 ActiveActive Directorynbsp;Directory 用户。

表 5.1. 信任控制器和信任代理提供的功能比较

功能	信任控制器	信任代理
解决 ActiveActive Directorynbsp;Directory 用户和组	是	是
注册运行来自可信 ActiveActive Directorynbsp 的用户访问的 IdM 客户端；Directory 林	是	是
管理信任（例如，添加信任协议）	是	否

在规划部署信任控制器和信任代理时，请考虑以下指南：

- 每个身份管理部署至少配置两个信任控制器。
- 在每个数据中心中至少配置两个信任控制器。

如果您希望创建额外的信任控制器，或者现有信任控制器失败，请通过提升信任代理或副本来创建新的信任控制器。要做到这一点，在 IdM 服务器中使用 ipa-adtrust-install 工具，如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述。

重要

您不能将现有信任控制器降级到信任代理。信任控制器服务器角色安装后，就无法从拓扑中删除。

5.2. 创建跨林信任

5.2.1. 环境和机器要求

在配置信任协议前，请确保 ActiveActive Directorynbsp;Directory 和身份管理服务器、机器和环境满足本节中描述的要求和设置。

5.2.1.1. 支持的 Windows 平台

您可以建立与 ActiveActive Directorynbsp 的信任关系;Directory 林和域功能级别：

- 林功能级别范围：Windows Server 2008 - Windows 服务器 2016
- 域功能级别范围：Windows Server 2008 - Windows 服务器 2016

支持并测试以下操作系统，以便使用上述功能级别建立信任：

- Windows Server 2012 R2

- *Windows Server 2016*

之前版本的 Windows Server 不支持建立信任。

5.2.1.2. DNS 和 Realm 设置

要建立信任，Active Directory 和 Identity Management 需要特定的 DNS 配置：

唯一的主 DNS 域

每个系统都必须配置自己的唯一的主 DNS 域。例如：

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

重要

如果 IdM 域是 AD 域的父域，IdM 服务器必须在 Red Hat Enterprise Linux 7.5 或更高版本中运行。

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

AD 或 IdM 无法将主 DNS 域与另一个身份管理系统共享。如需更多信息，请参阅 Linux 域身份、身份验证和策略指南中的 主机名和 DNS 配置要求文档。

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，如果域名是 AD 的 ad.example.com，而 idm.example.com for IdM，则需要 Kerberos 域名称为 AD.EXAMPLE.COM 和 IDM.EXAMPLE.COM。

DNS 记录可从信任中的所有 DNS 域解析

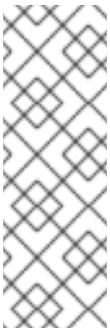
所有机器都必须能够从涉及信任关系的所有 DNS 域解析 DNS 记录：

- 在配置 IdM DNS 时，请参阅有关在 IdM 域中配置 DNS 服务 的部分，以及管理 Linux 域身份、身份验证和策略指南中的 DNS 转发 部分的内容。

- 如果您在没有集成 DNS 的情况下使用 IdM，请按照 章节描述在 Linux 域身份、身份验证和策略指南 中不集成 DNS 的服务器安装 的说明。

IdM 和 AD DNS 域之间没有重叠

加入 IdM 的系统可以通过多个 DNS 域进行发布。包含 IdM 客户端的 DNS 域不得与包含加入 AD 的机器的 DNS 域重叠。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 ActiveActive Directorynbsp;Directory 之间信任的一些环境中，您可以在属于 ActiveActive Directorynbsp 的主机上安装 IdM 客户端；Directory DNS 域。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。红帽建议始终在与 ActiveActive Directorynbsp 拥有的 DNS 区域中部署 IdM 客户端；Directory 并通过 IdM 主机名访问 IdM 客户端。

您可以通过运行 $ ipa dns-update-system-records --dry-run 命令来获取特定于系统设置所需的 SRV 记录列表。

生成的列表可以类似如下：

```
$ ipa dns-update-system-records --dry-run
 IPA DNS records:
 _kerberos-master._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos-master._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
 _kerberos.example.com. 86400 IN TXT "EXAMPLE.COM"
 _kpasswd._tcp.example.com. 86400 IN SRV 0 100 464 server.example.com.
 _kpasswd._udp.example.com. 86400 IN SRV 0 100 464 server.example.com.
 _ldap._tcp.example.com. 86400 IN SRV 0 100 389 server.example.com.
 _ntp._udp.example.com. 86400 IN SRV 0 100 123 server.example.com.
```

对于同一 IdM 域一部分的其他 DNS 域，在配置对 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，而是基于信任名称后缀路由信息的 KDC 发现。

验证 DNS 配置

在配置信任前，请验证身份管理和 Active Directory 服务器是否可以自行解析，也可以互相解析。

如果运行下面描述的命令没有显示预期的结果，请检查主机上执行命令的 DNS 配置。如果主机配置看起来正确，请确保 DNS 从父域到子域的设置正确无误。

请注意，AD 会缓存 DNS 查找的结果，因此有时无法立即看到您在 DNS 中所做的更改。您可以通过运行 ipconfig /flushdns 命令来删除当前的缓存。

验证 IdM 托管的服务是否可以从用于建立信任的 IdM 域服务器解析

1. 通过 UDP 和 LDAP 通过 TCP 服务记录运行对 Kerberos 的 DNS 查询。

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.ipa.example.com.
0 100 88 ipamaster1.ipa.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.ipa.example.com.
0 100 389 ipamaster1.ipa.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。获取的值应该与您在安装 IdM 时指定的 Kerberos 域匹配。

```
[root@ipaserver ~]# dig +short -t TXT _kerberos.ipa.example.com.
IPA.EXAMPLE.COM
```

3. 执行 ipa-adtrust-install 工具后（如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述），通过 UDP 和 LDAP 运行对 MS DC Kerberos 的 DNS 查询，通过 TCP 服务记录运行 LDAP。

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.ipa.example.com.
0 100 88 ipamaster1.ipa.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ipa.example.com.
0 100 389 ipamaster1.ipa.example.com.
```

命令应该会列出已在其上执行 **ipa-adtrust-install** 的所有 IdM 服务器。请注意，如果 **ipa-adtrust-install** 没有在任何 IdM 服务器上执行，则输出为空（通常在建立第一个信任关系前）。

验证 **IdM 能够解析 AD 的服务记录**

通过 **UDP 和 LDAP 通过 TCP 服务记录运行对 Kerberos 的 DNS 查询。**

```
[root@ipaserver ~]# dig +short -t SRV _kerberos._udp.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.
```

这些命令应当返回 **AD 域控制器的名称。**

验证 **IdM-hosted 服务是否可以从 AD 服务器解析**

1. 在 **AD 服务器上，设置 thenslookup.exe 实用程序来查找服务记录。**

```
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.ipa.example.com.
_kerberos._udp.ipa.example.com.       SRV service location:
    priority             = 0
    weight               = 100
    port                 = 88
    svr hostname   = ipamaster1.ipa.example.com
> _ldap._tcp.ipa.example.com
_ldap._tcp.ipa.example.com       SRV service location:
    priority             = 0
    weight               = 100
    port                 = 389
    svr hostname   = ipamaster1.ipa.example.com
```

预期的输出包含与 *验证 **IdM 托管的服务是否可以从用于建立信任的 IdM 域服务器解析*** 中显示相同的 **IdM 服务器集合。**

3. 将服务类型更改为 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.ipa.example.com.
_kerberos.ipa.example.com.        text =

    "IPA.EXAMPLE.COM"
```

输出应该包含与 验证 IdM 托管的服务是否可以从用于建立信任的 IdM 域服务器解析 中显示相同的值。

4. 执行 ipa-adtrust-install 工具后（如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述），通过 UDP 和 LDAP 运行对 MS DC Kerberos 的 DNS 查询，通过 TCP 服务记录运行 LDAP。

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.ipa.example.com.
_kerberos._udp.dc._msdcs.ipa.example.com.        SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = ipamaster1.ipa.example.com
> _ldap._tcp.dc._msdcs.ipa.example.com.
_ldap._tcp.dc._msdcs.ipa.example.com.        SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = ipamaster1.ipa.example.com
```

命令应该会列出已在其上执行 ipa-adtrust-install 工具的所有 IdM 服务器。请注意，如果 ipa-adtrust-install 没有在任何 IdM 服务器上执行，则输出为空（通常在建立第一个信任关系前）。

验证 AD 服务是否可以从 AD 服务器解析

1. 在 AD 服务器上，设置 thenslookup.exe 实用程序来查找服务记录。

```
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.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
```

预期的输出包含与 验证 IdM 能够解析 AD 的服务记录 中显示的相同的 AD 服务器集合。

5.2.1.3. NetBIOS 名称

NetBIOS 名称对于识别 ActiveActive Directorynbsp;Directory(AD)域（如果 IdM 配置了信任）时，用来识别 IdM 域和服务至关重要。因此，您必须对 IdM 域使用不同的 NetBIOS 名称，而不是您要建立林信任的 AD 域中使用的 NetBIOS 名称。

ActiveActive Directorynbsp 的 NetBIOS 名称;Directory 或 IdM 域通常是对应 DNS 域的最左侧组件。例如，如果 DNS 域是 ad.example.com，则 NetBIOS 名称通常是 AD。

注意

NetBIOS 名称的最大长度为 15 个字符。

5.2.1.4. 防火墙和端口

要启用 AD 域控制器和 IdM 服务器之间的通信，请确定您满足以下端口要求：

- 打开 AD 信任和 IdM 服务器在 IdM 服务器和所有 AD 域控制器两个方向上所需的端口 ：从 IdM 服务器到 AD 域控制器，然后返回。
- 在 AD 信任的可信 AD 林的所有 AD 域控制器上打开 IdM 客户端所需的端口。在 IdM 客户端中，确保端口在传出方向打开（请参阅 Linux 域身份、身份验证和策略指南中的安装客户端）的先决条件。

表 5.2. AD 信任需要的端口

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
端点映射器侦听器范围	1024-1300	TCP
AD Global Catalog	3268	TCP
LDAP	389	TCP [a] 和 UDP

[a] 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。

表 5.3. Trust 中 IdM 服务器所需的端口

服务	端口	协议
Kerberos	请参阅 *Linux 域身份、身份验证和策略指南* 中的端口要求。	
LDAP		
DNS		

表 5.4. AD 信任中 IdM 客户端所需的端口

服务	端口	协议	备注
Kerberos	88	UDP 和 TCP	如果从 Kerberos 分发中心(KDC) **发送的数据过大，libkrb5** 库将使用 UDP 并退回到 TCP 协议。Activeactive Directorynbsp;Directory 将 Privilege Attribute Certificate(PAC)附加到 Kerberos 票据中，这会增加大小，多数情况下需要使用 TCP 协议。为避免回退和重新发送请求，默认情况下，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。要在 **libkrb5** 使用 TCP 前配置大小，请在 **/etc/krb.5.conf** 文件中设置 ***udp_preference_limit***。详情请查看 krb5.conf(5) man page。

其它资源

- ***有关如何打开所需端口的建议，请参阅 Linux 域身份、身份验证和策略指南 中的端口 要***

求。

5.2.1.5. IPv6 设置

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。

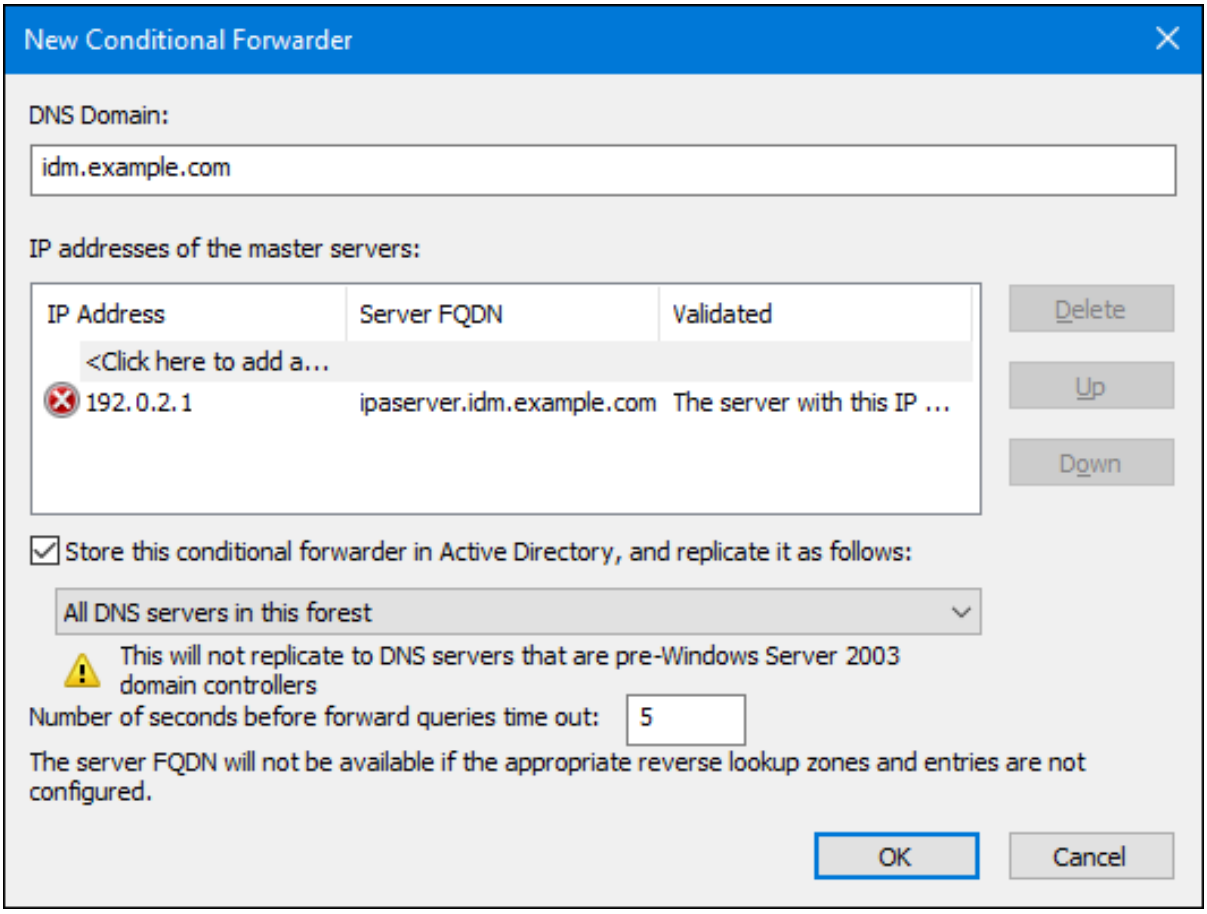
5.2.1.6. 时钟设置

ActiveActive Directorynbsp;Directory 服务器和 IdM 服务器都必须有其时钟同步。

5.2.1.7. 在 AD 中为 IdM 域创建条件 Forwarder

准备 AD DNS 服务器，以将 IdM 域的查询转发到 IdM DNS 服务器：

1. 在 Windows AD 域控制器上，打开 Active Directory(AD) DNS 控制台。
2. 右键单击 Conditional Forwarders，再选择 New Conditional Forwarder。
3. 输入 IdM DNS 域名和 IdM DNS 服务器的 IP 地址
4. 在 Active Directory 中选择 Store this conditional forwarder 并将其复制如下，然后选择与您的环境匹配的复制设置。
5. 点确定。



6. *要验证 AD 域控制器(DC)是否可以解析 IdM 域中的 DNS 条目，请打开命令提示并输入：*

```
C:\> nslookup server.idm.example.com
```

如果命令返回 IdM 服务器的 IP 地址，条件转发器可以正常工作。

5.2.1.8. 在 IdM 中为 AD 域创建转发区

准备 IdM DNS 服务器，以将 AD 域的查询转发到 AD DNS 服务器：

1. *在 IdM 服务器上，为 AD DNS 域创建一个正向区条目。有关在 IdM 中创建 DNS 转发区的详情，请参考 Linux 域身份、身份验证和策略指南 中的配置转发区部分。*

2. *如果 AD DNS 服务器不支持 DNSSEC，在 IdM 服务器上禁用 DNSSEC 验证：*

a. 编辑 /etc/named.conf 文件，将 dnssec-validation 参数设置为 no ：

```
dnssec-validation no;
```

b. 重启 named-pkcs11 服务：

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

3. 要验证 IdM 服务器是否可以解析 AD 域中的 DNS 条目，请输入：

```
# host server.ad.example.com
```

如果命令返回 AD DC 的 IP 地址，则 forward 区域可以正常工作。

5.2.1.9. 支持的用户名格式

IdM 在本地 SSSD 客户端中执行用户名映射。SSSD 支持的来自可信域的用户的默认输出用户名格式是 user_name@domain。Activeactive Directorynbsp;Directory 支持几种不同类型的名称格式：user_name、user_name@DOMAIN_NAME 和 DOMAIN_NAME\user_name。

用户只能使用其用户名(user_name)或其完全限定用户名(user_name@domain_name)，例如在系统身份验证时。

警告

最好使用完全限定用户名以避免在多个域中存在相同用户名时发生冲突。

如果用户只指定带有域的用户名，SSSD 会在 /etc/sssd/sssd.conf 文件和可信域中配置的所有域中搜索帐户。如果您配置了一个域解析顺序，如 第 8.5.3 节 “在 IdM 客户端中配置域解析顺序” 所述，SSSD 会按照定义的顺序搜索用户。不管怎样，SSSD 会使用找到的第一个条目。如果多个域中存在相同的用户名，而找到的第一个条目不是预期的条目，这可能会导致问题或混淆。

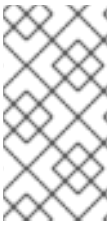
默认情况下，SSSD 会始终以完全限定格式显示用户名。有关更改格式的详情请参考 第 5.5 节 “更改 SSSD 显示的用户名格式”。

要识别用户名以及用户名所属的域，SSSD 使用 re_expression 选项中定义的正则表达式。正则表达式用于 IdM 后端或 AD 后端，并支持所有上述格式：

```
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
```

5.2.2. 创建信任

以下小节描述了在不同配置场景中创建信任关系。第 5.2.2.1 节 “从命令行创建信任” 包含从命令行配置信任的完整步骤。其他小节描述了与这种基本配置场景不同的步骤，并引用所有其他步骤的基本步骤。



注意

如果您在现有信任环境中设置副本，则副本不会自动配置为信任控制器。要将副本配置为额外的信任控制器，请按照本节中的步骤操作。

创建信任后，请参阅 第 5.2.3 节 “跨林信任的安装后注意事项”。

5.2.2.1. 从命令行创建信任

在 IdM 和 Active Directory Kerberos 域间创建信任关系涉及以下步骤：

1. 为信任准备 IdM 服务器，如下所述 第 5.2.2.1.1 节 “为信任准备 IdM 服务器”
2. 创建信任协议，如 第 5.2.2.1.2 节 “创建信任协议”
3. 验证 Kerberos 配置，如 所述 第 5.2.2.1.3 节 “验证 Kerberos 配置”

5.2.2.1.1. 为信任准备 IdM 服务器

要为与 AD 的信任关系设置 IdM 服务器，请按照以下步骤执行：

1. 安装所需的 IdM、信任和 Samba 软件包：

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

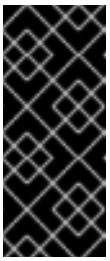
2. 配置 IdM 服务器以启用信任服务。如果您使用 ipa-replica-install --setup-adtrust 命令安装服务器，您可以跳过这一步。

   a. 运行 ipa-adtrust-install 工具：

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

   实用程序添加 AD 信任所需的 DNS 服务记录。如果 IdM 安装了集成的 DNS 服务器，则会自动创建这些记录。

   如果 IdM 安装时没有集成 DNS 服务器，ipa-adtrust-install 会输出您必须手动添加到 DNS 的服务记录列表，然后才能继续。



   重要

   红帽强烈建议在每次运行 ipa-adtrust-install 后验证 DNS 配置，如 “验证 DNS 配置”一节 所述，特别是在 IdM 或 AD 不使用集成 DNS 服务器时。

   b. 脚本会提示配置 slapi-nis 插件，这是一个兼容插件，允许较旧的 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]: y
```

   c. 首次安装 目录时，至少有一个用户（IdM 管理员）存在。SID 生成任务可以为任何现有用户创建一个 SID，以支持信任环境。这是一个资源密集型任务；对于大量用户而言，这可以单独运行。

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

3. 确保正确配置了 DNS，如 第 5.2.1.2 节 “DNS 和 Realm 设置” 所述。

4. 启动 smb 服务：

```
[root@ipaserver ~]# systemctl start smb
```

5. 另外，还可在系统引导时配置 smb 服务自动启动：

```
[root@ipaserver ~]# systemctl enable smb
```

6. （可选）使用 smbclient 实用程序验证 Samba 是否从 IdM 端响应 Kerberos 身份验证。

```
[root@ipaserver ~]# smbclient -L ipaserver.ipa.example.com -k
lp_load_ex: changing to config backend registry

 Sharename       Type      Comment
 ---------       ----      -------
 IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.

 Server               Comment
 ---------            -------

 Workgroup            Master
 ---------            -------
```

5.2.2.1.2. 创建信任协议

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

```
# ipa trust-add --type=type ad_domain_name --admin ad_admin_username --password
```

ipa trust-add 命令默认设置单向信任。在 RHEL 7 中无法建立双向信任。

要建立外部信任，请将 --external=true 选项传递给 ipa trust-add 命令。详情请查看 第 5.1.5 节 “外部 Trusts 到 ActiveActive Directorynbsp;Directory”。

注意

ipa trust-add 命令默认将服务器配置为信任控制器。详情请查看 第 5.1.6 节 “信任控制器和信任代理”。

以下示例使用 --two-way=true 选项建立了双向信任：

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --admin Administrator --password --
two-way=true
Active Directory domain administrator's password:
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-
5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11, S-1-5-10, S-1-3,
S-1-2, S-1-1, S-1-0, S-1-5-19,
                    S-1-5-18
  SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6, S-1-5-5, S-1-5-4, S-1-
5-9, S-1-5-8, S-1-5-17, S-1-5-16, S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11, S-1-5-10, S-1-3,
S-1-2, S-1-1, S-1-0, S-1-5-19,
                    S-1-5-18
  Trust direction: Two-way trust
  Trust type: Active Directory domain
  Trust status: Established and verified
```

5.2.2.1.3. 验证 Kerberos 配置

要验证 Kerberos 配置，测试是否可以获取 IdM 用户的票据，以及 IdM 用户是否可以请求服务票据。

验证双向信任：

1. **为 IdM 用户请求一个 ticket：**

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

2. **为 IdM 域中的服务请求 ticket：**

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

3. *为 **AD 域中的服务请求服务票据：***

```
[root@ipaserver ~]# kvno -S cifs adserver.example.com
```

如果 AD 服务票据被成功授予，则会使用其他所有请求的票据列出跨域票据(TGT)。TGT 命名为 krbtgt/AD.DOMAIN@IPA.DOMAIN。

```
[root@ipaserver ]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: user@IPA.DOMAIN

Valid starting     Expires            Service principal
06/15/12 12:13:04  06/16/12 12:12:55  krbtgt/IPA.DOMAIN@IPA.DOMAIN
06/15/12 12:13:13  06/16/12 12:12:55  host/ipaserver.ipa.example.com@IPA.DOMAIN
06/15/12 12:13:23 06/16/12 12:12:55 krbtgt/AD.DOMAIN@IPA.DOMAIN
06/15/12 12:14:58  06/15/12 22:14:58  cifs/adserver.ad.example.com@AD.DOMAIN
```

从 IdM 端验证单向信任：

1. *为 **ActiveActive Directorynbsp 请求一个 ticket:Directory 用户：***

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

2. *为 **IdM 域中的服务请求 ticket：***

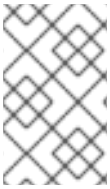
```
[root@ipaserver ~]# kvno -S host ipaserver.example.com
```

如果 AD 服务票据被成功授予，则会使用其他所有请求的票据列出跨域票据(TGT)。TGT 命名为 krbtgt/IPA.DOMAIN@AD.DOMAIN。

```
[root@ipaserver ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.DOMAIN

Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/ipaserver.ipa.example.com@IPA.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IPA.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
```

localauth 插件将 Kerberos 主体映射到本地 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。



注意

有关插件的详情请参考 第 5.3.7.2 节 “使用 SSH 不带密码”。

5.2.2.2. 使用共享 Secret 创建信任

共享 secret 是一种密码，它为受信任的同级服务器所知，可供其他域用于加入信任。共享 secret 可以在 Active Directory(AD)中配置单向和双向信任。在 AD 中，共享 secret 作为信任配置中的可信域对象 (TDO)存储。

IdM 支持使用共享 secret 而不是 AD 管理员凭证创建单向或双向信任。设置这种信任需要管理员在 AD 中创建共享 secret，并在 AD 端手动验证信任关系。

5.2.2.2.1. 使用共享 secret 创建双向信任

使用 Microsoft Windows Server 2012 R2 或 2016 的共享 secret 创建双向信任：

1. *为信任准备 IdM 服务器，如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述。*
2. *如果 IdM 和 AD 主机使用无法解析这两个域的 DNS 服务器，请为 DNS 区域设置转发：*
   a. *准备 AD DNS 服务器，以将 IdM 域的查询转发到 IdM DNS 服务器。详情请查看 第 5.2.1.7 节 “在 AD 中为 IdM 域创建条件 Forwarder”。*
   b. *准备 IdM DNS 服务器，以将 AD 域的查询转发到 AD DNS 服务器。详情请查看 第 5.2.1.8 节 “在 IdM 中为 AD 域创建转发区”。*
3. *配置 Active Directory 域和信任控制台的信任。特别是：*
   - *创建新信任.*

- 为信任的 IdM 域名指定，如 idm.example.com。
- 指定这是林类型的信任。
- 指定这是双向信任类型。
- 指定这是林范围的身份验证。
- 设置信任密码。

注意

在配置 IdM 中的信任时，必须使用相同的密码。

当系统要求确认进入的信任时，请选择 **No**。

4. 创建信任协议，如 第 5.2.2.1.2 节 “创建信任协议” 所述。运行 **ipa trust-add** 命令时，请使用 **--type**、**--trust-secret** 和 **--two-way=True** 选项，并省略 **--admin** 选项。例如：

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --trust-secret --two-way=True
Shared secret for the trust:
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19, S-1-5-18
  SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12, S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-1-5-19, S-1-5-18
  Trust direction: Trusting forest
  Trust type: Active Directory domain
  Trust status: Waiting for confirmation by remote side
```

5. 检索域列表：

```
[root@ipaserver ~]# ipa trust-fetch-domains ad_domain
```

6. 在 IdM 服务器上，使用 ipa trust-show 命令验证是否已建立信任关系。

```
[root@ipaserver ~]# ipa trust-show ad.example.com

  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  Trust direction: Trusting forest
  Trust type: Active Directory domain
```

7. 另外，还可搜索可信域：

```
[root@ipaserver ~]# ipa trustdomain-find ad.example.com
Domain name: ad.example.com
Domain NetBIOS name: AD
Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
Domain enabled: True
```

8. 验证 Kerberos 配置，如 第 5.2.2.1.3 节 “验证 Kerberos 配置” 所述。

5.2.2.2.2. 使用共享 secret 创建一Way Trust

使用 Microsoft Windows Server 2012 R2 或 2016 的共享 secret 创建单向信任：

1. 为信任准备 IdM 服务器，如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述。

2. 如果 IdM 和 AD 主机使用无法解析这两个域的 DNS 服务器，请为 DNS 区域设置转发：

   a. 准备 AD DNS 服务器，以将 IdM 域的查询转发到 IdM DNS 服务器。详情请查看 第 5.2.1.7 节 “在 AD 中为 IdM 域创建条件 Forwarder”。

   b. 准备 IdM DNS 服务器，以将 AD 域的查询转发到 AD DNS 服务器。详情请查看 第 5.2.1.8 节 “在 IdM 中为 AD 域创建转发区”。

3. 配置 Active Directory 域和信任控制台的信任 ：

   a. 右键单击域名，然后选择 Properties。

   b. 在 Trusts 选项卡上，单击 New Trust。

   c. 输入 IdM 域名，点 Next。

   d. 选择 Forest trust，然后单击 Next。

   e. 选择单向：传入 ，然后单击"下一步"。

   f. 选择"仅此域 "，然后单击"下一步"。

   g. 输入共享 secret（信任密码），然后单击 Next。

   h. 验证设置，再单击 Next。

   i. 当系统询问您是否要确认传入的信任时，请选择 No，不要确认传入的信任，然后单击 Next。

   j. 点 Finish。

4. 创建信任协议：

```
[root@ipaserver ~]# ipa trust-add --type=ad --trust-secret ad.example.com
Shared secret for the trust: password
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-1762709870-351891212-3141221786
```

```
Trust direction: Trusting forest
Trust type: Active Directory domain
Trust status: Waiting for confirmation by remote side
```

输入您在 AD 域和信任控制台中设置的共享机密。

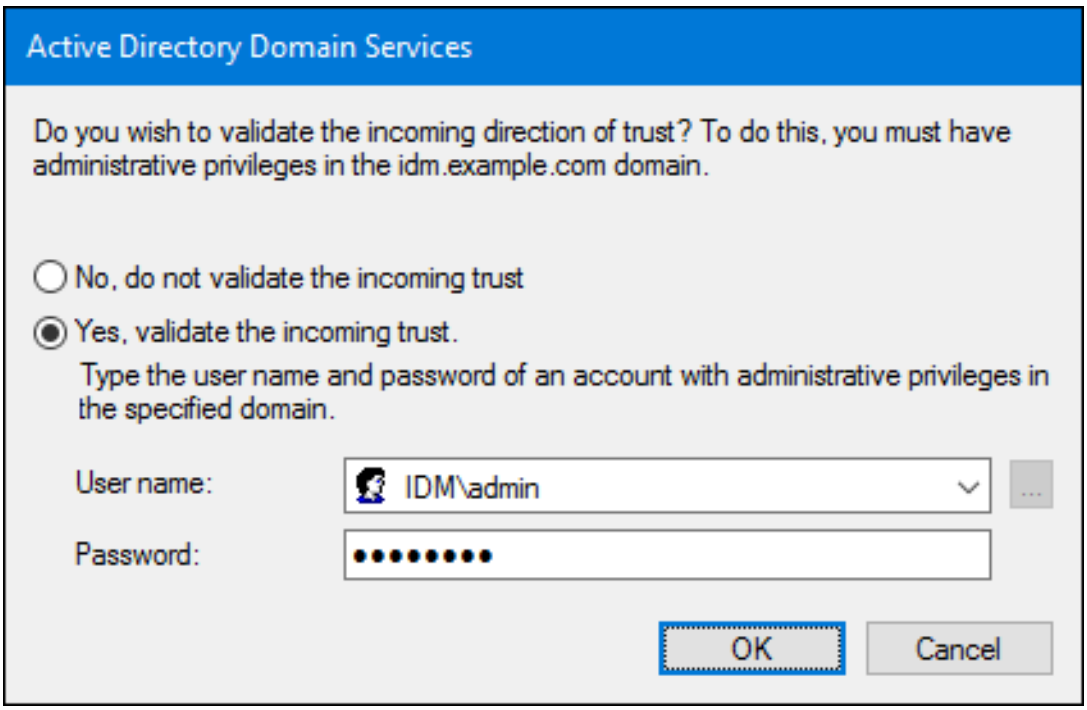
5. **验证 Active Directory 域和信任控制台的信任 ：**

   a. **右键单击域名，然后选择 Properties。**

   b. **在 Trusts 选项卡上，选择域中信任此域（传入信任）窗格中的域，然后单击 Properties。**

   c. **单击 Validate 按钮。**

   d. **选择 Yes，验证进入的信任，并输入 IdM admin 用户的凭据。**



6. **更新可信域列表：**

```
[root@ipaserver ~]# ipa trust-fetch-domains ad.example.com
---------------------------------------------------------------------------------------
List of trust domains successfully refreshed. Use trustdomain-find command to list them.
```

```
---------------------------------------------------------------------------------------
----------------------------
Number of entries returned 0
----------------------------
```

7. ***列出可信域：***

```
[root@ipaserver ~]# ipa trustdomain-find ad.example.com
  Domain name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-1762709870-351891212-3141221786
  Domain enabled: True
----------------------------
Number of entries returned 1
----------------------------
```

8. ***（可选）验证 IdM 服务器是否可以从 AD 域检索用户信息：***

```
[root@ipaserver ~]# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:610600500:610600500:Administrator:/home/ad.example.co
m/administrator:
```

5.2.2.3. 验证 ID 映射

验证 ID 映射：

1. ***在 Windows ActiveActive Directorynbsp;Directory 域控制器(DC)上运行以下命令，以列出最高 ID：***

```
C:\> dcdiag /v /test:ridmanager /s:ad.example.com
...
Available RID Pool for the Domain is 1600 to 1073741823
...
```

2. ***列出 IdM 服务器上的 ID 范围：***

```
[root@ipaserver ~]# ipa idrange-find
----------------
1 range matched
----------------
  Range name: AD.EXAMPLE.COM_id_range
  First Posix ID of the range: 610600000
  Number of IDs in the range: 200000
  First RID of the corresponding RID range: 0
```

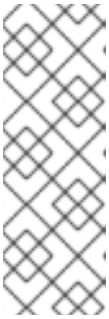
```
Domain SID of the trusted domain: S-1-5-21-796215754-1239681026-23416912
Range type: Active Directory domain range
----------------------------
Number of entries returned 1
----------------------------
```

在后续步骤中，您需要第一个 POSIX ID 值。

3. **在 ActiveActive Directorynbsp;Directory DC 上，显示安全标识符(SID)或用户。例如，显示管理员的 SID：**

```
C:\> wmic useraccount where name="administrator" get sid
S-1-5-21-796215754-1239681026-23416912-500
```

SID 的最后一部分是相对标识符(RID)。在下一步中，您需要用户的 RID。



注意

如果 RID 大于默认 ID 范围(200000)，请使用 ipa idrange-mod 命令扩展范围。例如：

```
# ipa idrange-mod --range-size=1000000 AD.EXAMPLE.COM_id_range
```

4. **显示 IdM 服务器中同一用户的用户 ID：**

```
[root@ipaserver ~]# id ad\\administrator
uid=610600500(administrator@ad.example.com)...
```

5. **如果您将第一个 POSIX ID 值(610600000)添加到 RID(500)，它必须与 IdM 服务器中显示的用户 ID(610600500)匹配。**

5.2.2.4. 在现有 IdM 实例上创建信任

当为现有 IdM 实例配置信任时，IdM 服务器及其域中条目的某些设置已被配置。但是，您必须设置 Active Directory 域的 DNS 配置，并将 Active Directory SID 分配给所有现有的 IdM 用户和组。

1. **为信任准备 IdM 服务器，如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述。**

2. 创建信任协议，如 第 5.2.2.1.2 节 “创建信任协议” 所述。

3. 为每个 IdM 用户生成 SID。

注意

如果使用 ipa-adtrust-install 实用程序建立信任时生成 SID，则不要执行这个步骤。

a. 通过在后端 LDAP 目录中运行 ipa-sidgen-task 操作，为每个条目自动添加新的 ipaNTSecurityIdentifier 属性，其中包含 SID。

```
[root@ipaserver ]# ldapmodify -x -H ldap://ipaserver.ipa.example.com:389 -D
"cn=directory manager" -w password

dn: cn=sidgen,cn=ipa-sidgen-task,cn=tasks,cn=config
changetype: add
objectClass: top
objectClass: extensibleObject
cn: sidgen
nsslapd-basedn: dc=ipadomain,dc=com
delay: 0

adding new entry "cn=sidgen,cn=ipa-sidgen-task,cn=tasks,cn=config"
```

b. 任务成功完成后，会在 SID 生成任务（Sidgen 任务）结束状态为零(0)的错误日志中记录一条消息。

```
[root@ipaserver ]# grep "sidgen_task_thread" /var/log/dirsrv/slapd-IDM-EXAMPLE-
COM/errors
[20/Jul/2012:18:17:16 +051800] sidgen_task_thread - [file ipa_sidgen_task.c, line 191]:
Sidgen task starts ...
[20/Jul/2012:18:17:16 +051800] sidgen_task_thread - [file ipa_sidgen_task.c, line 196]:
Sidgen task finished [0].
```

4. 验证 Kerberos 配置，如 第 5.2.2.1.3 节 “验证 Kerberos 配置” 所述。

5.2.2.5. 添加第二个信任

当在已配置了一个或多个信任协议的 IdM 服务器上添加信任时，不再需要某些常规 IdM 信任设置，如安装与信任相关的软件包或配置 SID。要添加额外的信任，您只需要配置 DNS 并建立信任协议。

1. 确保正确配置了 DNS，如 第 5.2.1.2 节 “DNS 和 Realm 设置” 所述。

2. 创建信任协议，如 第 5.2.2.1.2 节 “创建信任协议” 所述。

5.2.2.6. 在 Web UI 中创建信任

在创建 Web UI 信任之前，请为信任准备 IdM 服务器。这个信任配置最容易从命令行执行，如 第 5.2.2.1.1 节 “为信任准备 IdM 服务器” 所述。

设定了初始配置后，可以在 IdM Web UI 中添加信任协议：

1. 打开 IdM Web UI：

```
https://ipaserver.example.com
```

2. 打开 IPA 服务器主选项卡，然后选择"信任"子选项卡。

3. 在 Trusts 子选项卡中，单击 Add 以打开新的信任配置窗口。

4. 填写有关信任的所需信息：

   a. 在 Domain 字段中提供 AD 域名。

   b. 要将信任设置为双向，请选择双向信任复选框。要将信任设置为单向，请不要选择双向信任。

      有关单向和双向信任的更多信息，请参阅 第 5.1.4 节 “一次性和双向信任”。

   c. 要在另一个林中建立对某个域的外部信任，请选中 External Trust 复选框。

如需更多信息，请参阅 第 5.1.5 节 “外部 Trusts 到 ActiveActive Directorynbsp;Directory”。

d. 使用 的 Establish 部分定义如何建立信任：

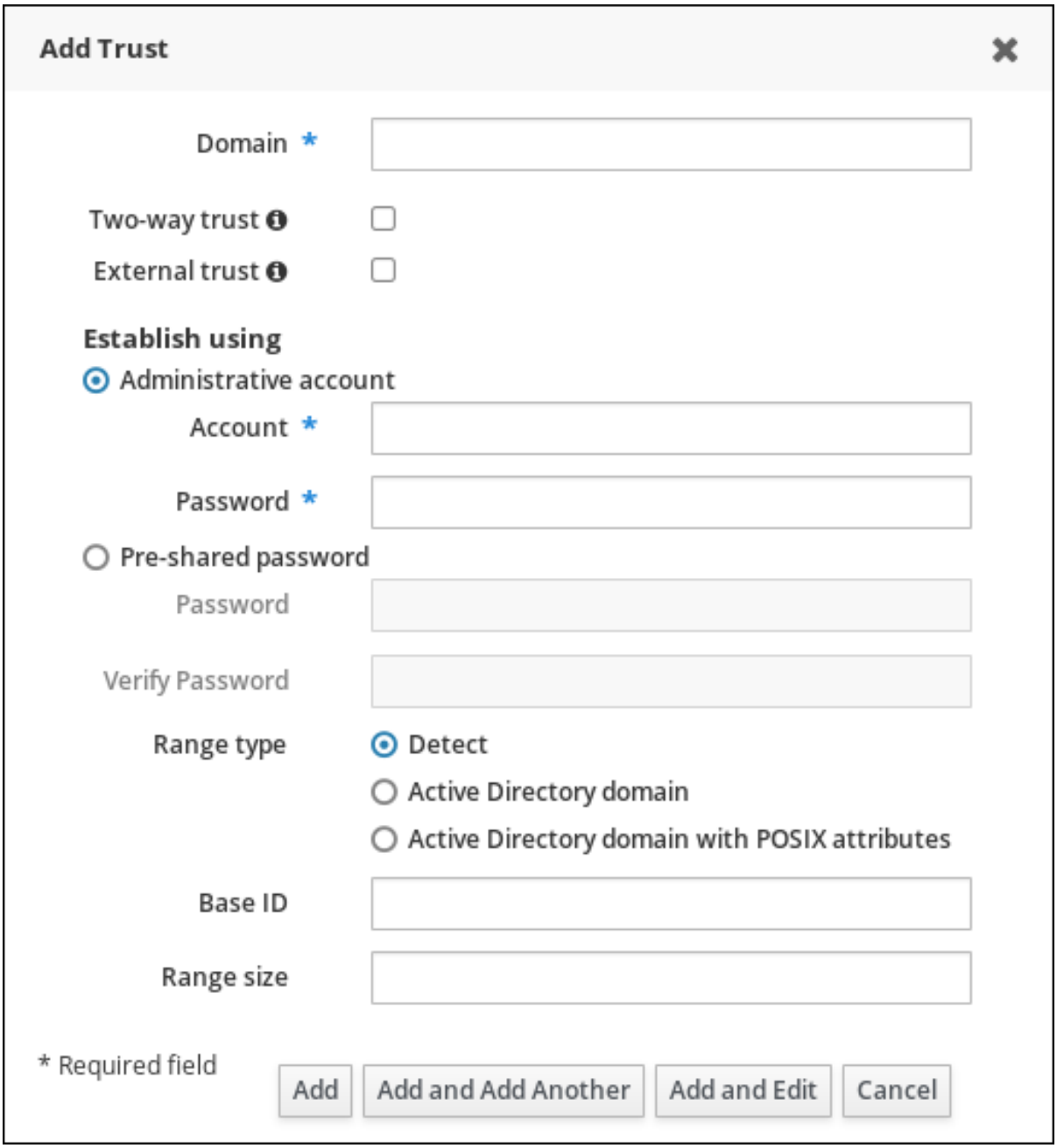
- 要使用 AD 管理员的用户名和密码建立信任，请选择管理帐户并提供所需的凭证。
- 或者，若要通过共享密码建立信任，请选择 Pre-shared password 并提供信任密码。

e. 为信任定义 ID 配置：

- Range 类型选项允许您选择 ID 范围类型。如果您希望 IdM 自动检测要使用的 ID 范围，请选择 Detect。
- 要定义 ID 范围的起始 ID，请使用 Base ID 字段。要定义 ID 范围的大小，请使用 Range size 字段。如果您希望 IdM 在 ID 范围中使用默认值，请不要指定这些选项。

有关 ID 范围的详情请参考 “ID 范围”一节。

图 5.5. 在 Web UI 中添加信任



5. *单击 **Add** 以保存新信任关系。*

*之后，验证 **Kerberos** 配置，如 第 5.2.2.1.3 节 “验证 Kerberos 配置” 所述。*

5.2.3. 跨林信任的安装后注意事项

5.2.3.1. Active Directory Trust 的潜在行为问题

5.2.3.1.1. Active Directory 用户和 IdM 管理

目前，Active Directory(AD)用户和管理员只能在登录 IdM Web UI 后查看其自助服务页面。AD 管

理员无法访问 IdM Web UI 的管理员视图。详情请参阅 Linux 域身份、身份验证和策略指南中的 验证 IdM Web UI 作为 AD 用户 部分。

另外，AD 用户目前无法管理自己的 ID 覆盖。只有 IdM 用户才能添加和管理 ID 覆盖。

5.2.3.1.2. 验证 Deleted ActiveActive Directorynbsp;Directory 用户

默认情况下，每个 IdM 客户端使用 SSSD 服务缓存用户身份和凭证。如果 IdM 或 AD 后端供应商暂时不可用，SSSD 可让本地系统为已经成功登录一次的用户引用身份。

因为 SSSD 会在本地维护一个用户列表，所以后端上所做的更改可能不会立即对运行 SSSD 的客户端可见。在这样的客户端中，之前登录 IdM 资源且哈希密码存储在 SSSD 缓存中的用户能够再次登录，即使其用户帐户已在 AD 中删除。

如果满足上述条件，则会将用户身份缓存在 SSSD 中，即使删除了用户帐户，AD 用户也可以登录到 IdM 资源。在 SSSD 在线并能够针对 AD 域控制器验证 AD 用户登录前，此问题会一直存在。

如果客户端系统在线运行 SSSD，则用户提供的密码由 AD 域控制器验证。这样可保证不允许已删除的 AD 用户登录。

5.2.3.1.3. credential Cache Collections 和 Selecting ActiveActive Directorynbsp;Directory Principals

Kerberos 凭证缓存尝试根据以下标识符将客户端主体与服务器主体匹配：

1. 服务名称
2. 主机名
3. realm name

当客户端和服务器映射基于主机名或真实名称和凭据缓存集合时，可能会作为 AD 用户绑定发生意外行为。这是因为 ActiveActive Directorynbsp 的 realm 名称与 IdM 系统的域名称不同。

如果 AD 用户使用 kinit 实用程序获取 ticket，然后使用 SSH 连接到一个 IdMnbsp;IdM 资源，则这个主体不会被选择用于资源票据。一个 IdMnbsp;IdM 主体会被使用，因为 IdM 主体与资源名称匹配。

例如，如果 AD 用户是 Administrator，且域是 ADEXAMPLE.ADREALM，则主体是 Administrator@ADEXAMPLE.ADREALM。

```
[root@server ~]# kinit Administrator@ADEXAMPLE.ADREALM
Password for Administrator@ADEXAMPLE.ADREALM:
[root@server ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@ADEXAMPLE.ADREALM

Valid starting       Expires              Service principal
27.11.2015 11:25:23  27.11.2015 21:25:23
krbtgt/ADEXAMPLE.ADREALM@ADEXAMPLE.ADREALM
 renew until 28.11.2015 11:25:16
```

在 ActiveActive Directorynbsp;Directory ticket 缓存中设置为默认主体。但是，如果任何 IdM 用户也具有 Kerberos ticket（如 admin），则有一个单独的 IdM 凭证缓存，并有一个 IdMnbsp;IdM 默认主体。如果 ActiveActive Directorynbsp;Directory 用户使用 SSH 连接到资源，则 IdM 默认主体会被选择为主机 ticket。

```
[root@vm-197 ~]# ssh -l Administrator@adexample.adrealm ipaclient.example.com
Administrator@adexample.adrealm@ipaclient.example.com's password:

[root@vm-197 ~]# klist -A
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@ADEXAMPLE.ADREALM

Valid starting       Expires              Service principal
27.11.2015 11:25:23  27.11.2015 21:25:23
krbtgt/ADEXAMPLE.ADREALM@ADEXAMPLE.ADREALM
 renew until 28.11.2015 11:25:16

Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EXAMPLE.COM >>>>> IdM user

Valid starting       Expires              Service principal
27.11.2015 11:25:18  28.11.2015 11:25:16  krbtgt/EXAMPLE.COM@EXAMPLE.COM
27.11.2015 11:25:48 28.11.2015 11:25:16 host/ipaclient.example.com@EXAMPLE.COM >>>>> host
principal
```

这是因为 IdM 主体的域名与 IdM 资源域匹配。

5.2.3.1.4. 解析组 SID

丢失 Kerberos 票据

运行 命令从 Samba 服务获取 SID（如 net getlocalsid 或 net getdomainsid），会从 Kerberos 缓存中删除任何现有的管理票据。

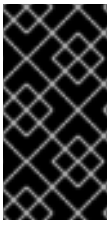
注意

您不需要为使用 Active Directory 信任而运行命令，如 net getlocalsid 或 net getdomainsid。

无法为用户验证组成员身份

无法验证特定可信用户是否与特定的 IdM 组（外部或 POSIX）关联。

无法为 ActiveActive Directorynbsp;Directory 组成员资格显示 Remote ActiveActive Directorynbsp;Directory User



重要

请注意，如果 IdM 服务器和客户端在 Red Hat Enterprise Linux 7.1 或更高版本上运行，则此问题不再会发生。

id 实用程序可用于显示 Linux 系统用户的本地组关联。但是，id 不显示 Active Directory 用户的 Active Directory 组成员资格，即使 Samba 工具确实显示了这些用户。

要临时解决这个问题，您可以使用 ssh 工具作为给定的 AD 用户登录到 anan IdMnbsp;IdM 客户端机器。在 AD 用户第一次成功登录后，id 搜索会检测并显示 AD 组成员资格：

```
[root@ipaserver ~]# id ADDOMAIN\user
uid=1921801107(user@ad.example.com) gid=1921801107(user@ad.example.com)
groups=1921801107(user@ad.example.com),129600004(ad_users),1921800513(domain
users@ad.example.com)
```

5.2.3.2. 配置信任代理

在信任环境中设置了新副本后，副本不会自动安装 AD 信任代理角色。将副本配置为信任代理：

1. 在现有的信任控制器中运行 ipa-adtrust-install --add-agents 命令：

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

命令启动一个交互式配置会话，并提示您输入设置代理所需的信息。

有关 **--add-agents** 选项的详情请参考 **ipa-adtrust-install(1) man page**。

2. 在新副本中：

a. 重启 IdM 服务：

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

b. 从 SSSD 缓存中删除所有条目：

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

注意

要使用 **sssctl** 命令，必须安装 **sssd-tools** 软件包。

c. （可选）验证副本是否安装了 AD 信任代理角色 ：

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

5.3. 管理和配置跨林信任环境

5.3.1. 可信域环境中的用户主体名称

IdM 支持使用用户主体名称(UPN)登录。UPN 是用于进行身份验证的用户名的替代选择，格式为 **username@KERBEROS-REALM**。在 ActiveActive Directorynbsp;Directory 林中可以配置额外的 UPN 后缀。这些企业主体名称用于提供默认 UPN 的替代登录。

例如，如果公司使用 Kerberos 域 **AD.EXAMPLE.COM**，用户的默认 UPN 为 **user@ad.example.com**。然而，公司常常希望其用户能够使用其电子邮件地址（如

user@example.com ）登录。在这种情况下，管理员将额外的 UPN 后缀 example.com 添加到 ActiveActive Directorynbsp;Directory 林，并在用户的帐户属性中设置新后缀。

只有在 AD 林根目录中定义时，UPN 后缀才对 IdM 可见。作为 AD 管理员，您可以使用 Active Directory 域和 Trust utility 或 PowerShell 命令行工具来定义 UPN。

注意

要为用户配置 UPN 后缀，红帽建议使用执行错误验证的工具，如 Active Directory 域和 Trust 实用程序。

红帽建议不要通过低级修改来配置 UPN，例如使用 ldapmodify 命令为用户设置 userPrincipalName 属性，因为 Active Directory 不验证这些操作。

当您在可信 AD 林中添加或删除 UPN 后缀时，您必须刷新 IdM master 上可信林的信息：

```
[root@ipaserver ~]# ipa trust-fetch-domains
Realm-Name: ad.example.com
--------------------------------
No new trust domains were found
--------------------------------
----------------------------
Number of entries returned 0
----------------------------
```

运行以下命令验证是否获取了替代 UPN：

```
[root@ipaserver ~]# ipa trust-show
Realm-Name: ad.example.com
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-23416912
  Trust direction: Two-way trust
  Trust type: Active Directory domain
  UPN suffixes: example.com
```

域的 UPN 后缀存储在 cn=trusted_domain_name,cn=ad,cn=trusts,dc=idm,dc=example,dc=com 子树中的多值属性 ipaNTAdditionalSuffixes 中。

5.3.2. ActiveActive Directorynbsp 中的 IdM 客户端;Directory DNS 域

在 IdM 和 ActiveActive Directorynbsp;Directory 之间信任的一些环境中，您可以在属于 ActiveActive Directorynbsp 的主机上安装 IdM 客户端；Directory DNS 域。然后，主机可以从基于 Linux 的 IdM 功能中获益。

重要

这不是推荐的配置，存在一些限制。红帽建议始终在与 ActiveActive Directorynbsp 拥有的 DNS 区域中部署 IdM 客户端；Directory 并通过 IdM 主机名访问 IdM 客户端。

5.3.2.1. 不要求使用 Kerberos 单点登录 IdM 客户端

对于在 ActiveActive Directorynbsp;Directory DNS 域中设置的 IdM 客户端，只有密码验证可用于访问这个 IdM 主机上的资源。针对这种情况配置客户端：

1. 要确保客户端中的系统安全服务守护进程(SSSD)可以与 IdM 服务器通信，请使用 --domain=IPA_DNS_Domain 选项安装 IdM 客户端：

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

这个选项禁用 ActiveActive Directorynbsp;Directory DNS 域的 SRV 记录自动探测。

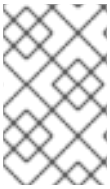
2. 在 /etc/krb5.conf 配置文件的 [domain_realm] 部分找到 ActiveActive Directorynbsp;Directory 域的现有映射：

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

将这两个行替换为 ActiveActive Directorynbsp 中的 Linux 客户端完全限定域名(FQDN)的映射条目；Directory DNS 区到 IdM 域：

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

替换默认映射可防止 Kerberos 将其对 ActiveActive Directorynbsp 的请求发送到 IdM Kerberos 发布中心(KDC)。相反，Kerberos 使用 SRV DNS 记录自动发现来查找 KDC。仅针对添加的主机 idm-client.ad.example.com 设置 IdM KDC。



注意

只有使用用户名和密码才能对不属于 IdM 拥有 DNS 区的客户端进行身份验证。

处理 SSL 证书

基于 SSL 的服务需要一个包含所有系统主机名的 dNSName 扩展记录的证书，因为证书中必须同时存在原始(A/AAAA)和 CNAME 记录。目前，IdM 只发布证书来托管 IdM 数据库中的对象。

在没有可用单点登录的设置中，IdM 在数据库中已具有 FQDN 的主机对象，certmonger 可以为此名称请求证书 ：

```
[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
```

认证器服务使用 /etc/krb5.keytab 文件中存储的默认主机密钥来向 IdM 证书颁发机构(CA)进行身份验证。

5.3.2.2. 需要 Kerberos 单点登录 IdM 客户端

如果您需要 Kerberos 单点登录才能访问 IdM 客户端上的资源，客户端必须位于 IdM DNS 域中，如 idm-client.idm.example.com。您必须在 ActiveActive Directorynbsp 中创建 CNAME 记录 idm-client.ad.example.com ；Directory DNS 域指向 IdM 客户端的 A/AAAA 记录。

对于基于 Kerberos 的应用程序服务器，MIT Kerberos 支持一种方法，允许接受应用的 key 选项卡中任何基于主机的主体。要禁用对将 Kerberos 主体作为 Kerberos 服务器的目标的严格检查，请在 /etc/krb5.conf 配置文件的 [libdefaults] 部分中设置以下选项：

```
ignore_acceptor_hostname = true
```

处理 SSL 证书

基于 SSL 的服务需要一个包含所有系统主机名的 dNSName 扩展记录的证书，因为证书中必须同时存在原始(A/AAAA)和 CNAME 记录。目前，IdM 只发布证书来托管 IdM 数据库中的对象。

在没有可用单点登录的设置中，IdM 在数据库中已具有 FQDN 的主机对象，certmonger 可以为此名

称请求证书 ：

1. *创建新主机对象 ：*

```
[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. *允许 IdM DNS 主机名管理 IdM 数据库中的 ActiveActive Directorynbsp;Directory 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
```

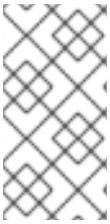
通过这个设置，IdM 客户端可以在 ActiveActive Directorynbsp 中为其主机名请求带有 dNSName 扩展记录的 SSL 证书；Directory DNS 域 ：

```
[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
```

5.3.3. 为 ActiveActive Directorynbsp 创建 IdM 组;Directory 用户

需要用户组来设置 IdM 用户的访问权限、基于主机的访问控制、sudo 规则和其他控制。这些组是授予 IdM 域资源访问权限并限制访问的方式。

AD 用户和 AD 组都可以直接添加到 IdM 用户组中。为此，首先将 AD 用户或组添加到非POSIX IdM 外部组中，然后添加到本地 IdM POSIX 组。然后，POSIX 组可用于 AD 用户的用户和角色管理。IdM 中处理非POSIX 组的原则请参考 第 5.1.3.2 节 “Active Directory 用户和身份管理组”。



注意

也可以将 AD 用户组添加为 IdM 外部组的成员。通过在单个 AD 域内保持用户和组管理，这可以更加轻松地为 Windows 用户定义策略。

1. 可选。在 AD 域中创建或选择要用于管理 IdM 域中的 AD 用户的组。多个组可用于 IdM 端的不同组并添加到不同的组中。

2. 通过将 **--external** 选项添加到 **ipa group-add** 命令，在 IdM 域中为 ActiveActive Directorynbsp;Directory 用户创建一个外部组。**external** 选项表示此组旨在包含 IdM 域外的成员。例如：

```
[root@ipaserver ~]# ipa group-add --desc='AD users external map' ad_users_external --
external
-------------------------------
Added group "ad_users_external"
-------------------------------
  Group name: ad_users_external
  Description: AD users external map
```

注意

外部组必须链接到一组其他用户，而不是用户的主组。Activeactive Directorynbsp;Directory 将组成员存储在组的 **member** 属性中，IdM 使用此属性来解析成员。但是，ActiveActive Directorynbsp;Directory 将用户的主组群保存在用户条目的 **primaryGroupID** 属性中，该属性没有被解决。

3. 创建一个新的 IdM POSIX 组，或选择一个现有组来管理 IdM 策略。例如，要创建新组：

```
[root@ipaserver ~]# ipa group-add --desc='AD users' ad_users
-----------------------
Added group "ad_users"
-----------------------
  Group name: ad_users
  Description: AD users
  GID: 129600004
```

4. 将 AD 用户或组作为外部成员添加到 IdM 外部组中。AD 成员通过其完全限定名称标识，如 **DOMAIN\group_name** 或 **DOMAIN\username**。然后，AD 身份被映射到用户或组的 ActiveActive Directorynbsp;Directory SID。

例如，对于 AD 组：

```
[root@ipaserver ~]# ipa group-add-member ad_users_external --external "AD\Domain
Users"
 [member user]:
 [member group]:
  Group name: ad_users_external
  Description: AD users external map
  External member: S-1-5-21-3655990580-1375374850-1633065477-513
SID_DOM_GROUP (2)
-------------------------
Number of members added 1
-------------------------
```

5. *将外部 IdM 组作为成员添加到 POSIX IdM 组。例如：*

```
[root@ipaserver ~]# ipa group-add-member ad_users --groups ad_users_external
  Group name: ad_users
  Description: AD users
  GID: 129600004
  Member groups: ad_users_external
-------------------------
Number of members added 1
-------------------------
```

5.3.4. 维护信任

信任管理涉及多个领域，如全局信任配置、Kerberos 信任配置、DNS 域配置或向 Active Directory 用户分配的 ID 范围。

5.3.4.1. 编辑全局信任配置

ipa-adtrust-install 程序自动为 IdM 域配置后台信息，这是使用 ActiveActive Directorynbsp;Directory 域创建信任所需要的信息。

全局信任配置包含五个属性：

- *Windows 样式的安全 ID(SID)；此属性是自动生成且无法修改*
- *域 GUID；此属性是自动生成且无法修改*

- Kerberos 域名；此属性来自 IdM 配置，且无法修改
- 要添加 IdM 用户的默认组；可以修改此属性
- NetBIOS 名称；不建议修改此属性

信任配置存储在 cn=域,cn=ad,cn=etc,dc=example,dc=com 子树中。

5.3.4.1.1. 更改 NetBIOS 名称

重要

在大多数情况下，更改 NetBIOS 名称需要重新建立所有现有的信任。因此，红帽建议不要更改属性。

在运行 ipa-adtrust-install 实用程序时，为 IdM 服务器配置兼容 Active Directory 拓扑中的 NetBIOS 名称。要稍后更改，请再次运行 ipa-adtrust-install，并使用 --netbios-name 选项指定新的 NetBIOS 名称：

```
[root@ipaserver ]# ipa-adtrust-install --netbios-name=NEWBIOSNAME
```

5.3.4.1.2. 更改 Windows 用户的默认组

当 Identity Management 配置为信任 Active Directory 林时，MS-PAC 记录会添加到 IdM 用户的 Kerberos 票据中。MS-PAC 记录包含 IdM 用户所属组的安全标识符(SID)。如果 IdM 用户的主要组没有分配 SID，则将使用为默认 SMB Group 定义的安全标识符值。当 AD 域控制器请求来自 IdM 信任控制器的用户信息时，Samba 套件也应用同样的逻辑。

默认 SMB 组是由 ipa-adtrust-install 实用程序自动创建的回退组。默认组无法被删除，但您可以使用全局信任配置指定另一个 IdM 组用作 IdM 用户主组的回退。

要从命令行设置默认组，请使用 ipa trustconfig-mod 命令：

```
[root@server ~]# kinit admin
[root@server ~]# ipa trustconfig-mod --fallback-primary-group="Example Windows Group"
```

从 IdM Web UI 设置默认组：

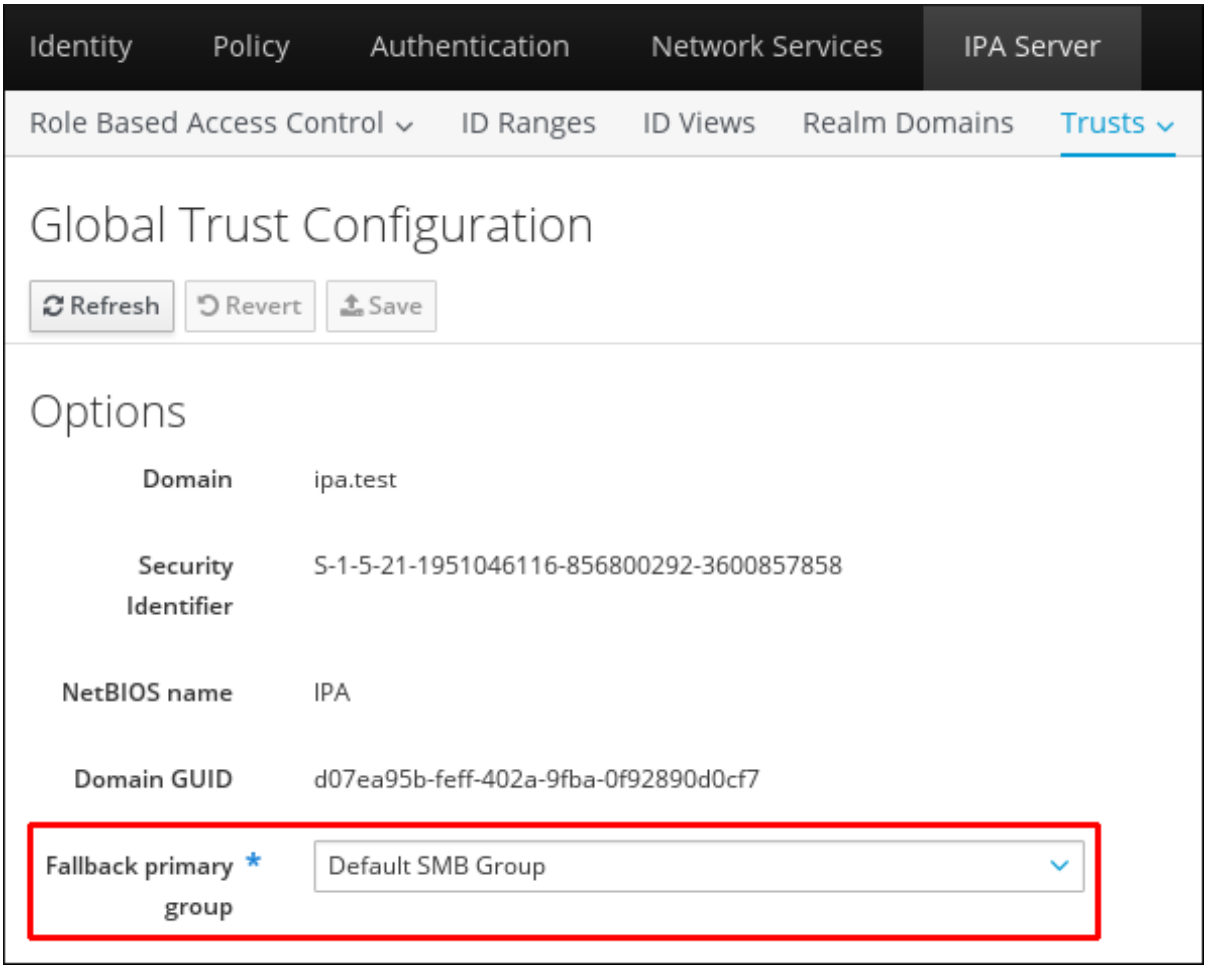
1. **打开 IdM Web UI。**

```
https://ipaserver.example.com
```

2. **在 IPA 服务器主选项卡下，选择信任子选项卡，然后打开 Global Configuration 部分。**

3. **从 Fallback 主组下拉列表中的所有 IdM 组中，选择一个新组。**

图 5.6. 为 Windows 用户配置默认组



4. **单击 Save 以保存新配置。**

5.3.4.2. 发现、启用和禁用受信任域

传递信任意味着信任路径可以跟随一系列域。它在 第 5.1.1 节 “信任关系的架构” 中进行了更详细的

描述。

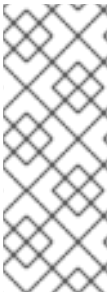
IdM 对林中的根域充满信任，并且由于传递性，它来自同一林的所有子域和来自同一林的其他域都会隐式包含在该信任中。IdM 遵循这个拓扑，因为 Windows 用户从林中的任何位置试图访问 IdM 资源。每个域和子域都是 IdM 信任配置中的信任域。每个域存储在自己的条目 cn=子域,cn=trust_name,cn=ad,cn=trusts,dc=example,dc=com 中的 trusts 子树中。

当配置信任时，IdM 会尝试发现并映射完整的 ActiveActive Directorynbsp;Directory 拓扑，但在某些情况下需要 或 useful 来手动检索该拓扑。这可以通过 trust-fetch-domains 命令完成：

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trust-fetch-domains ad.example.com
-----------------------------------------
List of trust domains successfully refreshed
-----------------------------------------
  Realm name: test.ad.example.com
  Domain NetBIOS name: TEST
  Domain Security Identifier: S-1-5-21-87535643-5658642561-5780864324

  Realm name: users.ad.example.com
  Domain NetBIOS name: USERS
  Domain Security Identifier: S-1-5-21-91314187-2404433721-1858927112

  Realm name: prod.ad.example.com
  Domain NetBIOS name: PROD
  Domain Security Identifier: S-1-5-21-46580863-3346886432-4578854233
----------------------------
Number of entries returned 3
----------------------------
```



注意

当使用共享 secret 添加信任时，您需要手动检索 AD 林的拓扑。运行 ipa trust-add ad.domain --trust-secret 命令后，使用 AD 域和信任工具中的林信任属性验证在 AD 端的传入信任。然后，运行 ipa trust-fetch-domains ad.domain 命令。IdM 将接收关于信任的信息，这些信息将随后可用。

且检索拓扑（通过自动或手动发现），就可以在 IdM 信任配置中完全启用、禁用或删除该拓扑中的个别域和子域。

例如，要禁止特定子域中用户使用 IdM 资源，请禁用该信任域：

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trustdomain-disable test.ad.example.com
```

```
----------------------------------------
Disabled trust domain "test.ad.example.com"
----------------------------------------
```

可以使用 **trustdomain-enable** 命令重新启用该信任域。

如果某个域应该从拓扑中永久删除，而不是将它从 IdM 信任配置中删除。

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa trustdomain-del prod.ad.example.com
------------------------------------------------------------------
Removed information about the trusted domain " "prod.ad.example.com"
------------------------------------------------------------------
```

5.3.4.3. 查看和管理与 IdM Kerberos 域关联的域

与 IdM Kerberos 域关联的域存储在 IdM 目录中的 **cn=Realm Domains,cn=ipa,cn=etc,dc=example,dc=com** 子树中。IdM 在与 Active Directory 建立信任时会使用域列表。知道由 IdM 管理的域的完整列表，使 AD 域控制器能够知道将哪些身份验证请求路由到 IdM KDC。使用 **realmdomains-show** 命令显示与 IdM 域关联的域列表：

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa realmdomains-show
Domain: ipa.example.org, ipa.example.com, example.com
```

在带有集成 DNS 的 IdM 设置中：

- 在使用 **ipa dnszone-add** 命令将新 DNS 区域添加到 IdM 后，域会自动添加到域列表中。运行 **ipa realmdomains-show** 在 IdM KDC 控制的域列表中显示新域：

  ```
  # kinit admin
  # ipa dnszone-add ipa2.example.com
  # ipa realmdomains-show
  Domain: ipa.example.org, ipa.example.com, example.com, ipa2.example.com
  ```

  与 IdM Kerberos 域关联的域删除和其他类型的修改也会自动处理。

在没有集成 DNS 的 IdM 设置中：

- 如果添加了属于 IdM Kerberos 域一部分的 DNS 区域，则必须手动将新域添加到 IdM KDC 控制的 IdM 域列表中。使用 **ipa realmdomains-mod** 命令及 **--add-domain** 选项添加新域：

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa realmdomains-mod --add-domain=ipa2.example.com
Domain: ipa.example.org, ipa.example.com, example.com, ipa2.example.com
```

如果删除了 DNS 区域，您需要手动删除与 IdM Kerberos 域关联的域，同时：

```
[root@ipaserver ~]# kinit admin
[root@ipaserver ~]# ipa realmdomains-mod --del-domain=ipa2.example.com
Domain: ipa.example.org, ipa.example.com, example.com
```

如果要对域列表进行多项更改，可以使用 **--domain** 选项修改和替换列表本身。

```
[root@ipaserver ~]# ipa realmdomains-mod --domain={ipa.example.org,ipa2.example.com}
```

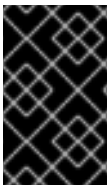
5.3.4.4. 在透明信任中为 UID 和 GID 号添加范围

"ID 范围"一节 中描述了在最初配置信任时创建 ID 范围。要在以后添加 ID 范围，请使用 **ipa idrange-add** 命令及以下选项：

- **base-id** 选项设置 POSIX 范围的基本 ID，即起始数
- **range-size** 选项设置 IdM 使用的 POSIX ID 范围的大小。IdM 将可信 AD 域中的用户和组的 RID 映射到 POSIX ID。**--range-size** 选项定义 IdM 创建的最大 ID 数。AD 对您创建的每个用户和组使用一个新的 RID。如果您删除了用户或组，AD 不会为将来的 AD 条目重复使用 RID。因此，范围必须足够大，以便 IdM 为每个现有的 AD 用户和组分配 ID，以及您以后创建的 ID。例如，如果管理员删除了 50000 个 AD 用户并且在此期间将创建 10000 个新帐户，则范围必须至少设置为 60000 个。但是，重要的是，范围中还包含足够的预留。在您期望默认(200000)范围大小不足的大型环境中，将 **--range-size** 设置为更高的值。
- **rid-base** 选项设置 RID 的起始数，这是 SID 中最右侧的数字；该值表示要添加到基本 ID 的范围，以防止冲突
- **dom-sid** 选项设置域 SID，因为可能会为信任配置了多个域

在以下示例中，基本 ID 是 1,200,000，RID 为 1,000。得到的 ID 号为 1,201,000。

```
[root@server ~]$ kinit admin
[root@server ~]$ ipa idrange-add --base-id=1200000 --range-size=200000 --rid-base=0 --dom-
sid=S-1-5-21-123-456-789 trusted_dom_range
```



重要

确保手动定义的 ID 范围与 IdM 使用的 ID 范围不重叠。

5.3.4.5. 手动调整 DNA ID 范围

在某些情况下，您可能需要手动调整现有副本的分布式 Numeric Assignment（强制）ID 范围，例如恢复分配给非有效副本的 DNA ID 范围，或者扩展已耗尽 ID 的范围。

在手动调整 DNA ID 范围时，请确保新调整后的范围包含在 IdM ID 范围内。您可以使用 ipa idrange-find 命令检查它。如果 IdM ID 范围内没有包含新调整的范围，命令会失败。

要从非破坏性副本恢复 DNA ID 范围，请使用 ipa-replica-manage dnarange-show 命令来查看当前分配的 DNA 范围。要查看当前分配的 on-deck DNA 范围，请使用 ipa-replica-manage dnanextrange-show 命令。

重要

不要创建重叠的 ID 范围。如果您分配给服务器或副本重叠的任何 ID 范围，可能会导致两个不同的服务器分配相同的 ID 值到不同的条目。

要为指定服务器定义当前的 DNA ID 范围，请使用 ipa-replica-manage dnarange-set 命令：

```
# ipa-replica-manage dnarange-set masterA.example.com 1250-1499
```

要为指定服务器定义下一个 DNA ID 范围，请使用 ipa-replica-manage dnanextrange-set 命令：

```
# ipa-replica-manage dnanextrange-set masterB.example.com 1500-5000
```

5.3.4.6. 用于服务和主机的 Kerberos 标记

访问可信域中的服务或主机可能需要 Kerberos 票据(TGT)的特殊标志。例如，如果要使用单点登录与带有 ActiveActive Directorynbsp;Directory(AD)帐户的 IdM 客户端登录，则需要 Kerberos TGT 标

志 OK_AS_DELEGATE。

如需更多信息以及如何设置 Kerberos 标记，请参阅 Linux 域身份、身份验证和策略指南 中的服务及主机的 Kerberos 标记。

5.3.5. 为服务设置 PAC 类型

在 IdM 资源中，如果 ActiveActive Directorynbsp;Directory 用户请求一个服务的 ticket，则 IdM 会将请求转发到 ActiveActive Directorynbsp;Directory 以检索用户信息。与 ActiveActive Directorynbsp 关联的访问数据;Directory 组分配由用户发送，由 ActiveActive Directorynbsp 发送；Directory 并嵌入到 Kerberos ticket 中。

ActiveActive Directorynbsp 中的组信息；Directory 存储在 ActiveActive Directorynbsp 的每个 Kerberos 票据列表中；Directory 用户存储在称为 特权访问证书 或 MS-PAC 的特殊数据集中。PAC 中的组信息必须映射到 ActiveActive Directorynbsp;Directory 组，然后指向对应的 IdM 组来帮助确定访问权限。

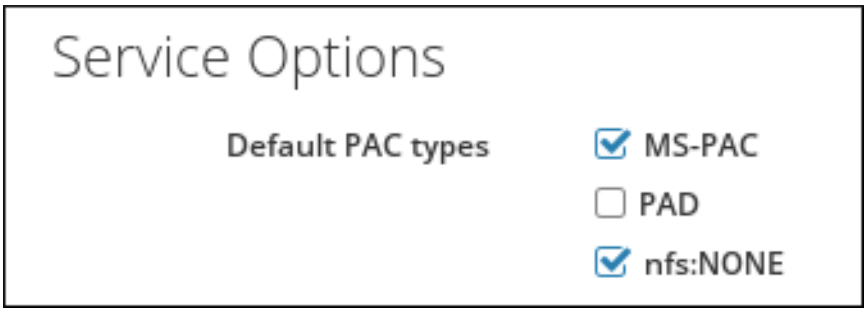
当用户第一次尝试对域服务进行身份验证时，IdM 服务可以配置为为每个身份验证请求生成 PAC。

5.3.5.1. 设置默认 PAC 类型

IdM 服务器配置定义服务默认生成哪些 PAC 类型。可以通过更改特定服务的本地设置来覆盖全局设置。

1. 打开 IPA Server 选项卡。
2. 选择 Configuration 子选项卡。
3. 滚动到 Service Options 区域。

图 5.7. Service Options 区域



4. *要使用 PAC，请选中 MS-PAC 复选框，该复选框会添加一个可供 AD 服务使用的证书。如果没有选择复选框，则不会在 Kerberos 票据中添加任何 PAC。*

   如果您选中 nfs:NONE 复选框，则 MS-PAC 记录不会添加到针对 NFS 服务器发布的服务票据中。

   注意

   您可以忽略PAD 复选框。IdM 中尚不提供此功能。

5. *单击页面顶部的更新链接，以保存更改。*

5.3.5.2. 为服务设置 PAC 类型

如果没有为该服务明确设置任何设置，全局策略会设置要用于服务的 PAC 类型。但是，全局设置可以在本地服务配置中覆盖。

要从命令行更改 PAC 设置，请使用 ipa service-mod 命令和 --pac-type 选项。有关如何使用该命令的详情，请在添加 --help 选项的情况下运行该命令：

```
$ ipa service-mod --help
Usage: ipa [global-options] service-mod PRINCIPAL [options]

Modify an existing IPA service.
Options:
-h, --help            show this help message and exit
...
```

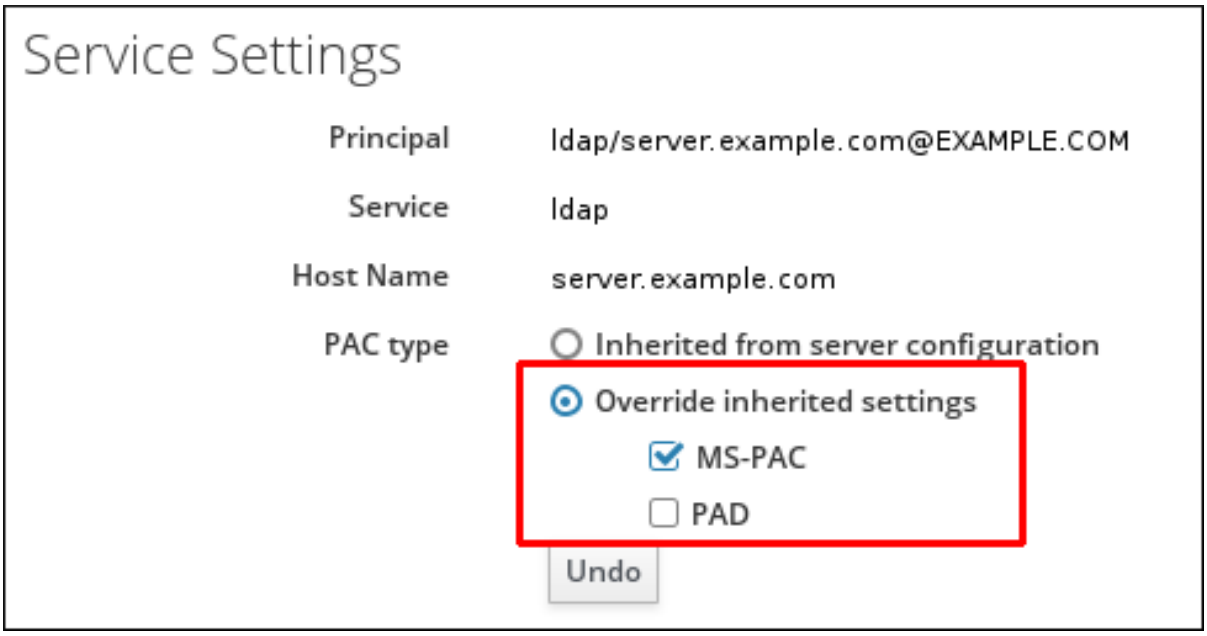
更改 Web UI 中的 PAC 设置：

1. 打开"身份 "选项卡，然后选择"服务 "子选项卡。

2. 单击要编辑的服务的名称。

3. 在 Service Settings 区域，选中覆盖继承的 settings 选项，然后选择 MS-PAC 复选框来添加可供 AD 服务使用的证书。

图 5.8. Service Settings 区域



如果没有选择复选框，则不会在 Kerberos 票据中添加任何 PAC。

注意

您可以忽略PAD 复选框。IdM 中尚不提供此功能。

4. 单击页面顶部的更新链接，以保存更改。

5.3.6. 使用在 Active Directory 中定义的 POSIX Attributes

5.3.6.1. 为 Active Directory 用户定义 UID 和 GID 属性

如果 Windows 管理员手动为用户定义了 POSIX UID 和 GID 属性，请在 IdM 服务器上为用户创建具有相同 GID 的匹配组。

创建组可确保该用户与主要用户组关联。如果这样的组不存在，IdM 服务器将无法查找用户所属的所有组。

5.3.6.2. 传输登录 Shell 和主目录属性

重要

该客户端必须注册到一个基于 Red Hat Enterprise Linuxnbsp 的 IdM 服务器 ;Hat Enterprise Linuxnbsp;Linux 7.1 或更高版本才能从此功能中受益。

SSSD 可以从与 IdM 信任关系的 Active Directory 服务器读取以下属性值：

- loginShell 属性，用于指定 AD 用户的 shell
- unixHomeDirectory 属性，它指定 AD 用户的主目录

当使用这些属性在 AD 服务器上定义自定义 shell 或主目录值时，会将自定义值显示给 AD 用户的 IdM 客户端。因此，AD 用户和 IdM 端会显示相同的用户 shell。

请注意，要将 AD 用户主目录显示 IdM 客户端，IdM 服务器中的 /etc/sssd/sssd.conf 文件的 [domain] 部分中的 subdomain_homedir 选项必须设置为 %o。%o 值表示从身份提供程序检索的主目录。例如：

```
[domain/example.com]
subdomain_homedir = %o
```

如果 AD 管理员修改 AD 端的 loginShell 或 unixHomeDirectory，则更改也会自动反映在 IdM 端。如果 AD 服务器上未定义这些属性，SSSD 会使用模板默认值。然后，这个默认值被显示到 IdM 客户端。

5.3.7. 从 ActiveActive Directorynbsp 使用 SSH;Directory Machine for IdM 资源

配置信任后，ActiveActive Directorynbsp;Directory 用户可以使用 SSH 及其 AD 凭证访问 IdM 主机上的机器、服务和文件。

5.3.7.1. 缓存注意事项

IdM 客户端没有直接连接到 ActiveActive Directorynbsp;Directory 域控制器(DC)以检索用户属性。客户端会连接到缓存此信息的 IdM 服务器。因此，如果您在 ActiveActive Directorynbsp;Directory 中禁用用户，用户仍然可以使用 SSH 密钥身份验证对 IdM 客户端进行身份验证，直到用户记录在 IdM 数据库中过期。

IdM 在以下情况下更新用户记录：

- 该条目已自动过期。
- 使用 sss_cache 实用程序手动使用户条目在缓存中过期：

```
# sss_cache --user user_name
```

- 用户使用 kinit 实用程序或 Web UI 向 IdM 服务器进行身份验证。

5.3.7.2. 使用 SSH 不带密码

用于本地授权的 localauth Kerberos 插件确保 Kerberos 主体自动映射到本地 SSSD 用户名。通过 localauth，在使用 Kerberos 登录时不会提示来自可信 AD 域的 Windows 用户输入密码，因此无需密码即可使用 SSH。

插件提供跨多个域和信任的可靠映射机制：当 sssd 连接到 Kerberos 库以将主体映射到本地 POSIX 身份时，SSSD 插件会根据 IdM 中定义的信任协议对其进行映射。

在某些情况下，用户可以使用 SSH 堡垒主机访问其他 Red Hat Enterprise Linuxnbsp;Hat Enterprise Red Hat Enterprise Linuxnbsp;Linux 机器。默认情况下，如果您使用 Kerberos 验证堡垒主机上的 SSH，则无法使用 Kerberos 向其他 Red Hat Enterprise Linuxnbsp 转发到其他 Red Hat Enterprise Linuxnbsp;Hat Enterprise Linuxnbsp;Linux 主机。要启用这样的转发身份验证，请在 bastions 主机主体中添加 OK_AS_DELEGATE Kerberos 标志：

```
# ipa host-mod bastion_host.idm.example.com --ok-as-delegate=true
```

Red Hat Enterprise Linuxnbsp 上的 AD 用户 Kerberos 身份验证;Hat Enterprise Red Hat Enterprise Linuxnbsp;Linux 7.1 and newer Systems

在 Red Hat Enterprise Linuxnbsp;Hat Enterprise Linuxnbsp;Linux 7.1 和更新的系统中，SSSD 自动配置 localauth Kerberos 插件。

SSSD 允许使用 user@AD.DOMAIN、ad.domain\user 和 AD\user 格式的用户名。

注意

在具有 localauth 的系统中，不需要在 /etc/krb5.conf 文件中设置 auth_to_local 选项，或者在.k5login 文件中列出 Kerberos 主体。localauth 插件使得之前用于登录的配置不会过时的密码。

为 AD 用户手动配置 Kerberos 身份验证

在没有 localauth 插件的系统中，SSH 提示输入 ActiveActive Directorynbsp 的用户密码 ;Directory 域用户即使用户获取正确的 Kerberos ticket。

要启用 Active Directory 用户在这种情况下使用 Kerberos 进行身份验证，请在 /etc/krb5.conf 文件中配置 auth_to_local 选项，或在用户主目录中的.k5login 文件中列出用户 Kerberos 主体。

配置 /etc/krb5.conf

以下流程描述了如何在 Kerberos 配置中配置域映射。

1. 打开 /etc/krb5.conf 文件。

2. 在 [realms] 部分中，按名称标识 IdM 域，然后添加两个 auth_to_local 行来定义 Kerberos 主体名称映射：

   - 在一个规则中，包含用于映射不同 Active Directory 用户名格式和特定 Active Directory 域的规则。
   - 在另一条规则中，为标准 Unix 用户名设置 DEFAULT 值。

   例如：

```
[realms]
IDM = {
....
```

```
auth_to_local = RULE:[1:$1@$0](^.*@ADDOMAIN$)s/@ADDOMAIN/@addomain/
auth_to_local = DEFAULT
}
```

3. 重新启动 KDC 服务。

```
[root@server ~]# systemctl restart krb5kdc.service
```

请注意，如果您使用 auth_to_local 选项配置 Kerberos 身份验证，用于 SSH 访问的用户名必须满足以下条件：

- 用户名必须具有格式 ad_user@ad_domain。
- 域名必须是小写。
- 用户名的大小写必须与 ActiveActive Directorynbsp;Directory 中的用户名匹配。例如，用户和用户 被视为不同的用户，因为存在不同的情况。

有关设置 auth_to_local 的详情，请查看 krb5.conf(5) man page。

configure.k5login

以下步骤将系统配置为查找本地用户名的 Kerberos 主体名称。

1. 在用户的主目录中创建.k5login 文件。
2. 列出用户在 文件中使用的 Kerberos 主体。

如果身份验证用户与现有 Kerberos 票据中的主体匹配，则允许用户使用票据登录，而且不会提示用户输入密码。

请注意，如果您使用.k5login 配置配置 Kerberos 身份验证，用于 SSH 访问的用户名必须具有 ad_user@ad_domain 格式。

有关配置 .k5login 文件的详情请参考 .k5login(5) man page。

无论哪种配置过程都会导致 AD 用户能够使用 Kerberos 登录。

5.3.8. 使用启用了 Kerberos 的 Web 应用程序的信任

任何现有的 Web 应用程序都可配置为使用 Kerberos 身份验证，该身份验证引用可信 ActiveActive Directorynbsp;Directory 和 IdM Kerberos 域。有关完整的 Kerberos 配置指令，请参阅 mod_auth_kerb 模块的配置页面。

注意

更改 Apache 应用程序配置后，重启 Apache 服务：

```
[root@ipaserver ~]# systemctl restart httpd.service
```

例如，对于 Apache 服务器，有几个选项可定义 Apache 服务器如何连接到 IdM Kerberos 域：

KrbAuthRealms

KrbAuthRealms 选项为 IdM 域的名称提供应用程序位置。这是必需的。

Krb5Keytab

Krb5Keytab 选项提供 IdM 服务器 keytab 的位置。这是必需的。

KrbServiceName

KrbServiceName 选项设置用于 keytab(HTTP)的 Kerberos 服务名称。这是推荐的。

KrbMethodK5Passwd 和 KrbMethodNegotiate

KrbMethodK5Passwd Kerberos 方法选项为有效用户启用基于密码的身份验证。如果有一个有效的 Kerberos ticket 可用，该 KrbMethodNegotiate 选项启用单点登录(SSO)。

建议为许多用户使用这些选项。

KrbLocalUserMapping

KrbLocalUserMapping 选项允许常规 Web 登录（通常是帐户的 UID 或通用名称）映射到完全限定的用户名（其格式为 user@REALM.COM）。

强烈建议使用这个选项。如果没有域名/登录名映射， Web 登录似乎与域用户不同。这意味着用户无法查看其预期数据。

有关支持的用户名格式的详情请参考 第 5.2.1.9 节 “支持的用户名格式”。

例 5.1. Apache Web 应用程序中的 Kerberos 配置

```
<Location "/mywebapp">
  AuthType Kerberos
  AuthName "IPA Kerberos authentication"
  KrbMethodNegotiate on
  KrbMethodK5Passwd on
  KrbServiceName HTTP
  KrbAuthRealms IDM_DOMAIN
  Krb5Keytab /etc/httpd/conf/ipa.keytab
  KrbLocalUserMapping on
  KrbSaveCredentials off
  Require valid-user
</Location>
```

5.3.9. 将 IdM 服务器配置为用于 Active Directory Kerberos 通讯的 Kerberos 分发中心代理

在某些情况下，网络限制或防火墙规则阻止身份管理(IdM)客户端将 Kerberos 流量发送到 Active Directory(AD)域控制器上的端口 88。解决方法是设置 Kerberos 代理，如身份管理服务器上，以将来自 IdM 客户端的流量中继到 AD。

1. 在 IdM 客户端上，将 Active Directory 域添加到 /etc/krb5.conf 文件的 [realms] 部分。将 kdc 和 kpasswd_server 参数设置为指向 IdM 服务器的完全限定域名，后接 /KdcProxy':

```
AD.EXAMPLE.COM = {
        kdc = https://server.idm.example.com/KdcProxy
        kpasswd_server = https://server.idm.example.com/KdcProxy
    }
```

2.

在 IdM 客户端上，禁用创建 /var/lib/ss/pubconf/kdcinfo.* 文件，这些文件可覆盖上一步中的 /etc/krb5.conf 规格。编辑 /etc/sssd/sssd.conf 文件，将 krb5_use_kdcinfo 设置为 False:

```
[domain/example.com]
krb5_use_kdcinfo = False
```

3.

在 IdM 服务器中，将 /etc/ipa/kdcproxy/kdcproxy.conf 文件中的 use_dns 选项设置为 true，以利用 DNS 服务(SRV)记录来查找 AD 服务器以便与之通信：

```
use_dns = true
```

另外，如果您不想使用 DNS SRV 记录，在 /etc/krb5.conf 文件的 [realms] 部分添加显式 AD 服务器：

```
AD.EXAMPLE.COM = {
    kdc = ad-server.ad.example.com
    kpasswd_server = ad-server.ad.example.com
  }
```

注意

您可以通过运行脚本来执行流程的第 2 和 3 步，例如 Ansible 脚本。这在多个系统上进行更改时特别有用。

4.

在 IdM 服务器中，重启 IPA 服务：

```
# ipactl restart
```

5. 要验证这个过程是否成功，请在 IdM 客户端中运行以下命令：

```
# rm /var/lib/sss/pubconf/kdcinfo*
# kinit ad_user@AD.EXAMPLE.COM
Password for ad_user@AD.EXAMPLE.COM:
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: ad_user@AD.EXAMPLE.COM

Valid starting     Expires            Service principal
[... output truncated ...]
```

5.4. 更改受信任的 ACTIVE DIRECTORY 域中的用户和组的 LDAP 搜索库

作为管理员，您可以在可信 Active Directory 域中为用户和组设置不同的搜索基础。例如，这可让您从不活跃的组织单元中过滤用户，以便只有活跃的 Active Directory 用户和组对 SSSD 客户端系统可见。

5.4.1. 先决条件

- 为确保 SSSD 不解析用户所属的所有组，请考虑在 Active Directory 端禁用对 tokenGroups 属性的支持。

  启用 tokenGroups 时，SSSD 会解析用户所属的所有组，因为 属性包含 SID 的扁平列表。有关属性的详情，请参阅 Microsoft Developer Network 上的 Token-Groups 属性。

5.4.2. 配置 LDAP 搜索基础以限制搜索

这个步骤描述了通过编辑 /etc/sssd/sssd.conf 文件将 SSSD 中的搜索限制为特定的子树。

注意事项

- 如果您的 SSSD 客户端直接加入 Active Directory 域，请对所有客户端执行此步骤。

- 如果您的 SSSD 客户端位于与 Active Directory 信任的身份管理域中，则仅在身份管理服务器上执行此步骤。

流程

1. 确保受信任的域在 sssd.conf 中有一个单独的 [domain] 部分。可信域部分的标题遵循此模板：

```
[domain/main_domain/trusted_domain]
```

例如：

```
[domain/idm.example.com/ad.example.com]
```

2. 编辑 sssd.conf 文件，将搜索基础限制为特定的组织单元(OU)。例如： ldap_search_base 选项会更改所有对象的搜索基础。

```
[domain/idm.example.com/ad.example.com]
ldap_search_base = ou=finance,dc=ad,dc=example,dc=com
```

您还可以使用 ldap_user_search_base、ldap_group_search_base、ldap_netgroup_search_base 和 ldap_service_search_base 选项。有关这些选项的详情请参考 sssd-ldap(5) man page。

3. 重启 SSSD。

```
# systemctl restart sssd.service
```

4. 要验证，请在 SSSD 客户端上解析几个 Active Directory 用户。例如，测试用户搜索库和组群搜索库的更改：

```
# getent passwd ad_user@ad.example.com
# getent group ad_group@ad.example.com
```

如果正确配置了 SSSD，您可以只从配置的搜索库解析对象。

如果您能够从其他搜索域解析用户，请通过检查 SSSD 日志对问题进行故障排除：

1. SSSD 缓存过期。

```
# sss_cache --everything
```

2. 在 sssd.conf 的常规 [domain] 部分，将 debug_level 选项设置为 9。

3. 重复 命令以解析用户。

4. 在 /var/log/sssd/ 的 SSSD 日志中，查找来自sdap_get_generic_* 功能的消息。功能记录用户搜索中使用的过滤器和搜索基础。

其它资源

- 有关您可以在 sssd.conf 的可信域部分使用的选项列表，请查看 sssd.conf(5) man page 中的 TRUSTED SECTION。

5.5. 更改 SSSD 显示的用户名格式

默认情况下，SSSD 在显示用户名时使用 user_name@domain_name 格式。在更改格式前，请参阅 第 5.2.1.9 节 “支持的用户名格式” 了解这个默认值的原因。

要配置 SSSD 仅显示没有域的用户名：

1. 在 /etc/sssd/sssd.conf 文件中的域部分添加以下条目：

```
full_name_format = %1$s
```

2. 重启 SSSD：

```
# systemctl restart sssd
```

5.6. 将身份管理或 SSSD 限制为受信任的 ACTIVE DIRECTORY 域中的选定 ACTIVE DIRECTORY 服务器或站点

作为管理员，您可以在可信 Active Directory 域中禁用自动发现 Active Directory 服务器和站点，并手动列出服务器、站点或两者，以便您可以限制 SSSD 与之通信的 Active Directory 服务器列表。例

如，这可让您避免联系无法访问的网站。

5.6.1. 配置 SSSD 以联系特定活动目录服务器

这个步骤描述了通过编辑 /etc/sssd/sssd.conf 文件手动设置 SSSD 连接到的 Active Directory 服务器。

注意事项

- 如果您的 SSSD 客户端直接加入 Active Directory 域，请对所有客户端执行此步骤。

  在这个设置中，限制 Active Directory 域控制器(DC)或站点也会将 SSSD 客户端配置为连接到特定服务器或站点进行身份验证。

- 如果您的 SSSD 客户端位于与 Active Directory 信任的身份管理域中，则仅在身份管理服务器上执行此步骤。

  在此设置中，限制 Active Directory DC 或站点不会将身份管理客户端配置为连接到特定服务器或站点以进行身份验证。虽然可信 Active Directory 用户和组通过身份管理服务器解析，但身份验证直接针对 Active Directory DC 执行。从 Red Hat Enterprise Linux 7.6 和 sssd-1.16.2-5.el7 开始，您可以在 IdM 客户端中使用 SSSD 使用 ad_server 和 ad_site 选项的特定 AD 服务器或站点。在之前的 Red Hat Enterprise Linux 7 版本中，通过在客户端上的 /etc/krb5.conf 文件中定义所需的 Active Directory DC 来限制身份验证。

流程

1. 确保受信任的域在 sssd.conf 中有一个单独的 [domain] 部分。可信域部分的标题遵循此模板：

   ```
   [domain/main_domain/trusted_domain]
   ```

   例如：

   ```
   [domain/idm.example.com/ad.example.com]
   ```

2. 编辑 sssd.conf 文件，以列出 Active Directory 服务器或您要连接到的站点的主机名。

使用 ad_server，以及 Active Directory 服务器的 ad_server_backup 选项（可选）。在 Active Directory 站点使用 ad_site 选项。有关这些选项的详情请参考 sssd-ad(5) man page。

例如：

```
[domain/idm.example.com/ad.example.com]
ad_server = dc1.ad.example.com
```

3. 重启 SSSD。

```
# systemctl restart sssd.service
```

4. 要在 SSSD 客户端上，通过配置的服务器或站点以 Active Directory 用户身份解析或身份验证。例如：

```
# id ad_user@ad.example.com
```

如果您无法解析用户或验证，请使用这些步骤排除此问题：

1. 在 sssd.conf 的常规 [domain] 部分，将 debug_level 选项设置为 9。

2. 检查 /var/log/sssd/ 中的 SSSD 日志，以查看 SSSD 联系了哪些服务器。

其它资源

- 有关您可以在 sssd.conf 的可信域部分使用的选项列表，请查看 sssd.conf(5) man page 中的 TRUSTED SECTION。

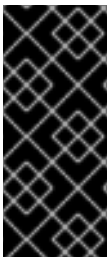
5.7. 为传统 LINUX 客户端提供 ACTIVE DIRECTORY 信任

运行 Red Hat Enterprise Linuxnbsp 的 Linux 客户端;Hat Enterprise Linuxnbsp;带有 SSSD 版本 1.8 或更早版本（传统客户端）不会为 IdM 跨林信任提供 IdM 跨林信任。因此，要使 AD 用户能够访问 IdM 服务器提供的服务，必须正确配置旧的 Linux 客户端和 IdM 服务器。

旧客户端不需要使用 SSSD 版本 1.9 或更高版本与 IdM 服务器通信来获取 LDAP 信息，而是使用其他实用程序来实现这一目的，如nss_ldap、nss-pam-ldapd 或 SSSD 版本 1.8 或更早版本。运行以下版本

的 Red Hat Enterprise Linuxnbsp;Hat Enterprise Linuxnbsp;Linux 不使用 SSSD 1.9，因此被视为旧客户端：

- *RedRed Hat Enterprise Linuxnbsp;Hat EnterpriseRed Hat Enterprise Linuxnbsp;Linux 5.7 or later*
- *RedRed Hat Enterprise Linuxnbsp;Hat EnterpriseRed Hat Enterprise Linuxnbsp;Linux 6.0 – 6.3*



重要

不要将本节中描述的配置用于非传统客户端，即运行 SSSD 版本 1.9 或更高版本的客户端。SSSD 1.9 或更高版本为 IdM 与 AD 的跨林信任提供原生支持，这意味着 AD 用户可以在无需额外配置的情况下正确访问 IdM 客户端上的服务。

当一个传统客户端在与 AD 信任关系中加入 IdM 服务器的域时，compat LDAP 树会为 AD 用户提供所需的用户和组数据。但是，compat 树使 AD 用户只能访问有限数量的 IdM 服务。

旧客户端不提供以下服务的访问权限 ：

- *Kerberos 身份验证*
- *基于主机的访问控制(HBAC)*
- *SELinux 用户映射*
- *sudo 规则*

即使在存在旧客户端的情况下，也可以访问以下服务：

- *信息查找*

- 密码验证

5.7.1. AD 信任的服务器端配置

确保 IdM 服务器满足以下配置要求：

- 已安装 IdM 的 ipa-server 软件包以及 IdM 信任附加组件的 ipa-server-trust-ad 软件包。
- ipa-server-install 工具已运行来设置 IdM 服务器。
- ipa-adtrust-install --enable-compat 命令已运行，它会确保 IdM 服务器支持与 AD 域信任，以及兼容 LDAP 树可用。

  如果您在过去没有 --enable-compat 选项运行 ipa-adtrust-install，请再次运行它，这一次添加 --enable-compat。
- ipa trust-add ad.example.org 命令已运行来建立 AD 信任。

如果禁用了基于主机的访问控制(HBAC) allow_all 规则，请在 IdM 服务器上启用 system-auth 服务，该服务允许对 AD 用户进行身份验证。

您可以使用 ipa hbacrule-show 命令从命令行直接确定 allow_all 的当前状态。如果该规则被禁用，输出中会显示 Enabled: FALSE ：

```
[user@server ~]$ kinit admin
[user@server ~]$ ipa hbacrule-show allow_all
  Rule name: allow_all
  User category: all
  Host category: all
  Service category: all
  Description: Allow all users to access any host from any host
  Enabled: FALSE
```

注意

有关禁用和启用 HBAC 规则的信息，请参阅 Linux 域身份、身份验证和策略指南中的配置基于主机的访问控制。https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/linux_domain_identity_authentication_and_policy_guide/index#configuring-host-access

要在 IdM 服务器上启用 system-auth，请创建一个名为 system-auth 的 HBAC 服务，并使用这个服务添加 HBAC 规则来授予 IdM master 的访问权限。如需添加 HBAC 服务和规则，请参阅 Linux 域身份、身份验证和策略指南中的配置基于主机的访问控制 部分。https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/linux_domain_identity_authentication_and_policy_guide/index#configuring-host-access请注意，HBAC 服务是 PAM 服务名称；如果您添加新的 PAM 服务，请确保创建名称相同的 HBAC 服务，然后通过 HBAC 规则授予对此服务的访问权限。

5.7.2. 使用 ipa-advise 实用程序进行客户端配置

ipa-advise 程序提供配置指令，用于为 AD 信任设置旧的客户端。

要显示 ipa-advise 可以提供配置说明的完整场景列表，请在没有任何选项的情况下运行 ipa-advise。运行 ipa-advise 会打印所有可用配置指令集的名称，以及每个集合的作用以及建议使用它的描述。

```
[root@server ~]# ipa-advise
config-redhat-nss-ldap  : Instructions for configuring a system
    with nss-ldap as a IPA client.
    This set of instructions is targeted
    for platforms that include the
    authconfig utility, which are all
    Red Hat based platforms.
config-redhat-nss-pam-ldapd : Instructions for configuring a system
(...)
```

要显示一组指令，运行 ipa-advise 工具，并将指令设置为参数：

```
[root@server ~]# ipa-advise config-redhat-nss-ldap
#!/bin/sh
# ----------------------------------------------------------------------
# Instructions for configuring a system with nss-ldap as a IPA client.
# This set of instructions is targeted for platforms that include the
# authconfig utility, which are all Red Hat based platforms.
# ----------------------------------------------------------------------
# Schema Compatibility plugin has not been configured on this server. To
# configure it, run "ipa-adtrust-install --enable-compat"
# Install required packages via yum
```

```
yum install -y wget openssl nss_ldap authconfig

# NOTE: IPA certificate uses the SHA-256 hash function. SHA-256 was
# introduced in RHEL5.2. Therefore, clients older than RHEL5.2 will not
# be able to interoperate with IPA server 3.x.
# Please note that this script assumes /etc/openldap/cacerts as the
# default CA certificate location. If this value is different on your
# system the script needs to be modified accordingly.
# Download the CA certificate of the IPA server
mkdir -p -m 755 /etc/openldap/cacerts
wget http://idm.example.com/ipa/config/ca.crt -O /etc/openldap/cacerts/ca.crt
(...)
```

您可以使用 ipa-advise 实用程序配置 Linux 客户端，方法是将显示的说明作为 shell 脚本运行，或者手动执行说明。

以 shell 脚本的形式运行指令：

1. **创建 脚本文件。**

```
[root@server ~]# ipa-advise config-redhat-nss-ldap > setup_script.sh
```

2. **使用 chmod 实用程序向 文件添加执行权限。**

```
[root@server ~]# chmod +x setup_script.sh
```

3. **使用 scp 实用程序将 脚本复制到客户端。**

```
[root@server ~]# scp setup_script.sh root@client
```

4. **在客户端上运行 脚本。**

```
[root@client ~]# ./setup_script.sh
```

重要

在客户端上运行脚本文件之前，请务必仔细阅读和查看脚本文件。

要手动配置客户端，请从命令行执行 ipa-advise 显示的说明。

5.8. 跨林信任故障排除

本节介绍跨林信任环境中可能的问题以及解决问题的方法。

5.8.1. 对 ipa-extdom 插件进行故障排除

IdM 域中的 IdM 客户端，它信任的 ActiveActive Directorynbsp;Directory(AD)无法直接从 AD 接收用户和组的信息。另外，IdM 不会将 AD 用户的信息存储在 IdM master 上运行的目录服务器中。相反，IdM 服务器使用 ipa-extdom 接收 AD 用户和组的信息，并将它们转发到请求客户端。

设置 ipa-extdom 插件的 Config Timeout

ipa-extdom 插件针对 AD 用户的数据向 SSSD 发送请求。但是，并非所有请求的数据都可能已在 SSSD 缓存中。在本例中，SSSD 从 AD 域控制器(DC)请求数据。这对于某些操作可能非常耗时。配置超时值定义 ipa-extdom 插件在插件取消连接前等待 SSSD 回复的时间（以毫秒为单位），并为调用者返回超时错误。

默认情况下，配置超时为 10000 毫秒（10 秒）。

- 如果您设置了一个太小的值，如 500 毫秒，SSSD 可能没有足够的时间来响应，请求将始终返回超时。
- 如果该值太大，如30000 毫秒（30 秒），则单个请求可能会在这段时间内阻止与 SSSD 的连接。由于一次只能有一个线程连接到 SSSD，来自插件的所有其他请求都必须等待。
- 如果 IdM 客户端发送了大量请求，它们可能会阻止为目录服务器配置的所有可用工作程序，因此服务器可能在某些情况下无法响应任何类型的请求。

在以下情况下更改配置超时：

- 如果在请求 AD 用户和组信息时达到自己的搜索超时前，IdM 客户端经常收到超时错误，配置超时值太小。
- 如果 IdM 服务器上的 Directory 服务器经常被锁定，并且 pstack 实用程序报告很多或所有

worker 线程目前正在处理 ipa-extdom 请求，则该值太大。

例如，要将配置值设置为20000 毫秒（20 秒），请输入：

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config

changetype: modify
replace: ipaExtdomMaxNssTimeout
ipaExtdomMaxNssTimeout: 20000
```

为 NSS 调用设置 ipa-extdom 插件使用的 maximum Size

ipa-extdom 插件使用调用，这些调用使用与典型名称服务交换机(NSS)调用相同的 API 来请求 SSSD 中的数据。这些调用使用 SSSD 可以存储请求数据的缓冲。如果缓冲区太小，SSSD 会返回一个 ERANGE 错误，插件会使用更大的缓冲区重试请求。cn=ipa_extdom_extop,cn=plugins,cn=config 条目的 IdM master 中的 ipaExtdomMaxNssBufSize 属性定义缓冲区的最大大小，以字节为单位。

默认情况下，缓冲区为 134217728 字节(128 MB)。例如，如果组中包含如此多的成员，所有名称都不适合到缓冲区中，并且 IPA 客户端无法解析组，则仅增加该值。

例如，要将缓冲区设置为 268435456 字节(256 MB)，请输入：

```
# ldapmodify -D "cn=directory manager" -W

dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxNssBufSize
ipaExtdomMaxNssBufSize: 268435456
```

部分 III. 将 LINUX 域与 ACTIVE DIRECTORY 域集成：同步

这部分提供了有关如何同步 Active Directory 和 Identity Management 用户的说明，如何将现有环境从同步迁移到信任，以及如何在 Active Directory 环境中使用 ID Views。

第 6 章 同步 ACTIVEACTIVE DIRECTORYNBSP;DIRECTORY 和 IDENTITYIDENTITY MANAGEMENTNBSP;MANAGEMENT USERS

本章论述了 Active Directory 和 Red Hat Enterprise Linuxnbsp 之间同步;Hat Enterprise Linuxnbsp;Linux IdentityIdentity Managementnbsp;Management.同步是两个环境间接集成的两种方法之一。有关跨林信任的详细信息，这是另一种推荐的方法，请参阅 第 5 章 使用 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 创建 Cross-forest Trusts。如果您不确定要为您的环境选择哪一种方法，请参阅 第 1.3 节 “间接集成”。

身份管理使用同步来组合存储在 Active Directory 域中的用户数据和 IdM 域中存储的用户数据。服务之间复制和同步关键用户属性，包括密码。

条目同步通过类似于复制的过程执行，它使用 hook 从 Windows 服务器连接和检索目录数据。

密码同步通过 Windows 服务器上的 Windows 服务执行，然后与 IdentityIdentity Managementnbsp 通讯;Management 服务器。

6.1. 支持的 WINDOWS 平台

同步支持 ActiveActive Directorynbsp;Directory 林，它们使用以下林和域功能级别：

- 林功能级别范围：Windows Server 2008 - Windows Server 2012 R2
- 域功能级别范围：Windows Server 2008 - Windows Server 2012 R2

以下操作系统通过上述功能级别明确支持并测试以进行同步：

- Windows Server 2012 R2
- Windows Server 2016

PassSync 1.1.5 或更高版本与所有支持的 Windows Server 版本兼容。

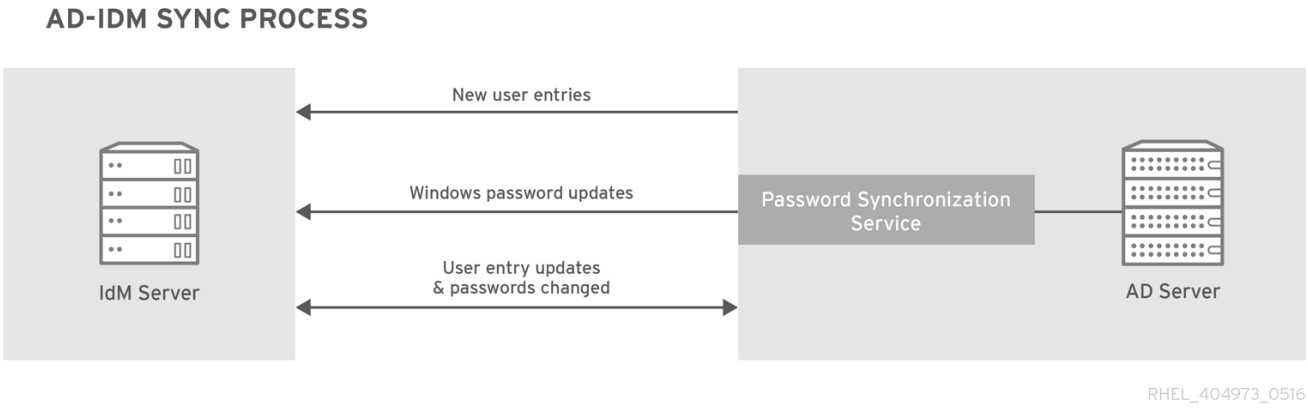
6.2. 关于 ACTIVE DIRECTORY 和 IDENTITYIDENTITY MANAGEMENTNBSP;MANAGEMENT

在 IdM 域中，通过在数据 master（服务器和副本）之间可靠地复制该信息，在服务器和副本之间共享信息。此过程是复制。

相似的过程可用于在 IdM 域和 Microsoft Active Directory 域之间共享数据。这是同步。

同步是指在 Active Directory 和 IdentityIdentity Managementnbsp 之间复制用户数据；Management。当用户在 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp 之间同步时，会使用目录同步(DirSync)LDAP 服务器扩展控制来搜索已更改对象的目录。

图 6.1. ActiveActive Directorynbsp;Directory and IdM Synchronization



同步在 aan IdMnbsp;IdM 服务器和 ActiveActive Directorynbsp;Directory 域控制器之间定义。协议定义识别可以同步的用户条目所需的所有信息，如要同步的子树，以及定义帐户属性的处理方式。使用默认值创建同步协议，这些默认值可以调整以满足特定域的需求。当两台服务器参与同步时，它们就称为同级服务器。

表 6.1. 同步协议中的信息

Windows 信息	IdM 信息

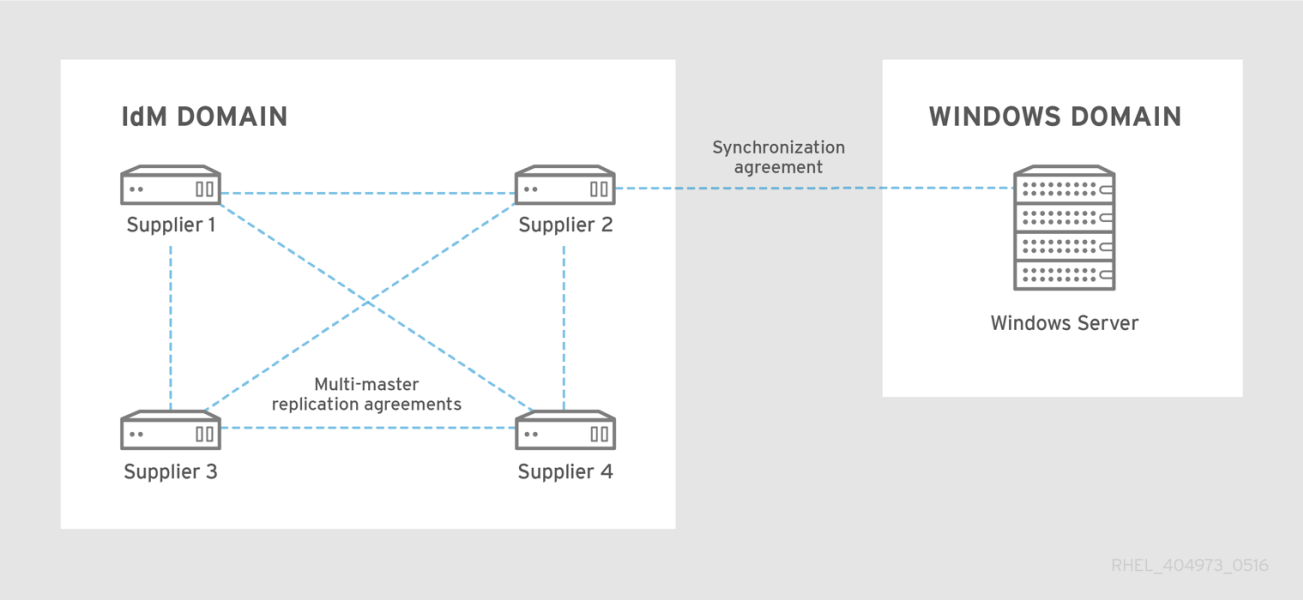
• 用户子树(**cn=Users,$SUFFIX**)
• 连接信息
  ○ Activeactive Directorynbsp;Directory 管理员用户名和密码
  ○ 密码同步服务密码
  ○ CA 证书
	• **用户子树（ou=People、$SUFFIX**）

同步通常是双向的。在一个与 IdM 服务器和副本共享信息非常相似的进程中，在 IdM 和 Windows 域之间来回发送信息。新用户条目除外，它们仅从 Windows 域添加到 IdM 域。可以将同步配置为仅同步一种方式。这是单向同步。

为防止数据冲突的风险，只有一个目录应源自或移除用户条目。这通常是 Windows 目录，它是 IT 环境中的主要身份存储，然后新帐户或帐户删除会同步到 IdentityIdentity Managementnbsp;Management peer。两个目录都可以修改条目。

然后，同步配置了一个 IdentityIdentity Managementnbsp;Management server 和一个 ActiveActive Directorynbsp;Directory 域控制器。IdentityIdentity Managementnbsp;Management 服务器在整个 Windows 域中传播至 IdM 域，而域控制器则在整个 Windows 域中传播更改。

图 6.2. 同步拓扑



IdM 同步有几个关键功能：

- 同步操作每五分钟运行一次。要修改频率，请在 Active Directory 对等 DN 中设置 winSyncInterval 属性：

  ```
  cn=meTowinserver.ad.example.com,cn=replica,cn=dc\3Didm\,dc\3Dexample\,dc\3Dcom,cn=
  mapping tree,cn=config
  ```

- 同步只能配置一个 ActiveActive Directorynbsp;Directory 域。

- 同步只能 配置一个 ActiveActive Directorynbsp;Directory 域控制器。

- 仅同步用户信息；组信息不.
- 用户属性和密码都可以同步。
- 虽然修改是双向的（从 ActiveActive Directorynbsp;Directory 到 IdM，从 IdM 到 ActiveActive Directorynbsp;Directory）时，创建帐户只能从 ActiveActive Directorynbsp;Directory 到 IdentityIdentity Managementnbsp;Management.在 ActiveActive Directorynbsp 中创建的新帐户；Directory 会自动同步到 IdM。但是，在 IdM 中创建的用户帐户还必须在 ActiveActive Directorynbsp;Directory 中创建，然后才能同步。在这种情况下，同步进程会尝试找到与 IdM 中 uid 属性相同的匹配帐户，而不是在 ActiveActive Directorynbsp;Directory 中找到 sAMAccountName 属性。如果找到匹配项，IdM ntUserDomainId 属性被设置为 ActiveActive Directorynbsp;Directory objectGUID 值。这些属性全局唯一且不可变，并且条目保持同步，即使它们被移动或重命名。
- 默认情况下，帐户锁定信息同步，因此一个域中禁用的用户帐户在另一个域中被禁用。
- 密码同步更改将立即生效。如果在一个对等上添加或更改了用户密码，该更改将立即传播到其他同级服务器。

  Password Synchronization 客户端会同步新密码或密码更新。

  现有密码以 IdM 和 ActiveActive Directorynbsp 的散列形式存储；Directory，当安装 Password Synchronization 客户端时，无法解密或同步现有密码。必须更改用户密码，以启动对等服务器之间的同步。
- 虽然只能有一个协议，但 PassSync 服务必须安装在每个 ActiveActive Directorynbsp;Directory 服务器上。

当 ActiveActive Directorynbsp;Directory 用户与 IdM 同步时，某些属性（包括 Kerberos 和 POSIX 属性）将自动添加到用户条目中。这些属性供 IdM 在其域中使用。它们不会在对应的 ActiveActive Directorynbsp;Directory 用户条目中同步。

同步中的一些数据可以在同步过程中修改。例如，某些属性可以自动添加到 ActiveActive Directorynbsp;Directory 用户帐户与 IdM 域同步时。这些属性更改定义为同步协议的一部分，如 第 6.5.2 节 “更改同步用户帐户属性的行为” 中所述。

6.3. 关于同步属性

IdentityIdentity Managementnbsp;Management 同步 IdM 和 ActiveActive Directorynbsp;Directory 用户条目之间的用户属性子集。条目中存在的任何其他属性（在 IdentityIdentity Managementnbsp;Management 或 ActiveActive Directorynbsp 中）都会被同步忽略。

注意

大多数 POSIX 属性都不会同步。

虽然 ActiveActive Directorynbsp;Directory LDAP 模式和 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Directory389 Directory Servernbsp;Server LDAP schema used by IdentityIdentity Managementnbsp;Management 有很多属性。这些属性只需在 ActiveActive Directorynbsp;Directory 和 IdM 用户条目之间同步，且不会影响属性名称或值格式。

用户架构，在 IdentityIdentity Managementnbsp 中是一样的 Same；管理和 Windows 服务器

- cn[2]
- physicalDeliveryOfficeName
- description
- postOfficeBox
- destinationIndicator
- postalAddress
- facsimileTelephoneNumber
- postalCode

- ***givenname***
- ***registeredAddress***
- ***homePhone***
- ***sn***
- ***homePostalAddress***
- ***st***
- ***Initials***
- ***街道***
- ***l***
- ***telephoneNumber***
- ***mail***
- ***teletexTerminalIdentifier***
- ***Mobile***
- ***telexNumber***

- *o*
- *title*
- *ou*
- *userCertificate*
- *寻呼机*
- *x121Address*

有些属性具有不同的名称，但在 IdM 间仍然有直接奇偶校验（使用 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server）和 ActiveActive Directorynbsp;Directory。这些属性由同步进程映射。

表 6.2. 用户架构在 IdentityIdentity Managementnbsp;Management 和 Active Directory 之间映射

IdentityIdentity Managementnbsp;Management	Active Directory
cn[a]	name
nsAccountLock	userAccountControl
ntUserDomainId	sAMAccountName
ntUserHomeDir	homeDirectory
ntUserScriptPath	scriptPath
ntUserLastLogon	lastLogon
ntUserLastLogoff	lastLogoff
ntUserAcctExpires	accountExpires
ntUserCodePage	codePage

IdentityIdentity Managementnbsp;Management	Active Directory
ntUserLogonHours	logonHours
ntUserMaxStorage	maxStorage
ntUserProfile	profilePath
ntUserParms	userParameters
ntUserWorkstations	userWorkstations

[a] 当从 IdentityIdentity Managementnbsp;Management to ActiveActive Directorynbsp;Directory）同步时，***cn*** 会直接映射到***cn***。***cn***从 ActiveActive Directorynbsp 同步;Directory ***cn*** 是从 ActiveActive Directorynbsp 中的 ***name*** 属性映射;Directory 到 IdentityIdentity Managementnbsp;Management 中的 ***cn*** 属性。

6.3.1. IdentityIdentity Managementnbsp;Management 和 Active Directory 之间的用户架构差异

虽然属性可以在 ActiveActive Directorynbsp;Directory 和 IdM 之间成功同步，但仍存在 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 定义底层 X.500 对象类的差异。这可能会导致在不同 LDAP 服务中处理数据的不同。

这部分论述了 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 处理在两个域间同步的一些属性的区别。

6.3.1.1. cn Attributes 的值

在 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server,Server, cn 属性可以是多值，而 Active Directory 此属性中必须只有一个值。当 IdentityIdentity Managementnbsp;Management cn 属性被同步时，只有一个值发送到 Active Directory peer。

对于同步，这意味着如果 cn 值添加到 Active Directory 条目，且该值不是 IdentityIdentity Managementnbsp 中的 cn 的值之一;Management，然后所有 IdentityIdentity Managementnbsp;Management cn 值都会被单个 Active Directory 值覆盖。

另一个重要的区别是，Active Directory 使用 cn 属性作为其命名属性，其中 IdentityIdentity Managementnbsp;Management 使用 uid。这意味着，如果在 IdentityIdentity Managementnbsp 中编辑 cn 属性，则可能完全命名条目（并意外）。

6.3.1.2. 街道和街道地址的值

Active Directory 将属性 streetAddress 用于用户的 postal 地址；这是 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server 使用 street 属性的方法。Active Directory 和 IdentityIdentity Managementnbsp 中有两个重要区别：Management 使用 streetAddress 和 street 属性：

- *在 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server, streetAddress 是 street 的别名。Active Directory 也具有 street 属性，但它是一个单独的属性，可以保存独立值，而不是 streetAddress 的别名。*
- *Active Directory 将 streetAddress 和 street 定义为单值属性，而 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server 将 street 定义为多值属性，如 RFC 4519 中指定的。*

由于 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server 和 Active Directory 处理 streetAddress 和 street 属性的不同方法，在 Active Directory 和 IdentityIdentity Managementnbsp 中设置地址属性时有两种：

- *同步过程将 ActiveActive Directorynbsp 中的 streetAddress 映射到 IdentityIdentity Managementnbsp;Management 中的 street 条目。为避免冲突，不应在 Active Directory 中使用 street 属性。*
- *只将一个 IdentityIdentity Managementnbsp;Management street 属性值同步到 Active Directory。如果 streetAddress 属性在 Active Directory 中被改变，且新值尚未存在于 IdentityIdentity Managementnbsp;Management 中，则 IdentityIdentity Managementnbsp;Management 中的所有 street 属性值替换为新的、单一 Active Directory 值。*

6.3.1.3. 初始属性限制

对于 initials 属性，Active Directory 会对六个字符的最大长度限制，但 389389 Directory Servernbsp;Directory389 Directory Servernbsp;Server 没有长度限制。如果在 IdentityIdentity Managementnbsp;Management 中添加大于 6 个字符的 initials 属性，则该值会在与 Active Directory 条目同步时进行修剪。

6.3.1.4. 要求姓氏(sn)属性

Activeactive Directorynbsp;Directory 允许在没有 surname 属性的情况下创建 人员 条目。但是，RFC 4519 将 人员 对象类定义为需要 surname 属性，这是 DirectoryDirectory Servernbsp;Server 中使用的定义。

如果在没有 surname 属性的情况下创建了 ActiveActive Directorynbsp;Directory 人员 条目，则该条目不会与 IdM 同步，因为它会失败并显示对象类违反情况。

6.3.2. Activeactive Directorynbsp;Directory Entries 和 POSIX Attributes

当 Windows 用户帐户包含 uidNumber 和 gidNumber 属性的值时， WinSync 不会将这些值同步到 Identity Management。相反， 它会在 Identity Management 中创建新的 UID 和 GID 值。

因此， uidNumber 和 gidNumber 的值在 Active Directory 和 Identity Management 中有所不同。

6.4. 设置 ACTIVEACTIVE DIRECTORYNBSP;DIRECTORY 用于同步

在 IdM 中启用了同步用户帐户。只需要设置同步协议(第 6.5.1 节 “创建同步协议”)。但是， ActiveActive Directorynbsp;Directory 确实需要配置为允许 IdentityIdentity Managementnbsp;Management server 连接到它。

6.4.1. 创建 ActiveActive Directorynbsp;Directory 用户进行同步

在 Windows 服务器上，需要创建 IdM 服务器将用于连接 Active Directory 域的用户。

在 Active Directory 中创建用户的流程涵盖在 Windows 服务器文档中， 该文档位于：新用户帐户必须具有正确的权限：

- 为同步用户帐户复制目录更改授予同步 Active Directory 子树的权限。同步用户需要副本权限才能执行同步操作。

  副本权利如下所述：

- 添加同步用户，作为帐户操作员 和企业只读域控制器组的成员。用户不需要从属于 Domain Admins 组。

6.4.2. 设置 ActiveActive Directorynbsp;Directory 证书颁发机构

IdentityIdentity Managementnbsp;Management server 使用安全连接连接到 ActiveActive Directorynbsp;Directory 服务器。这要求 ActiveActive Directorynbsp;Directory 服务器具有可用的

CA 证书或 CA 证书链，可导入到 IdentityIdentity Managementnbsp;Management 安全数据库，以便 Windows 服务器是一个信任的对等点。

虽然从技术上来说，这可以通过外部（到 ActiveActive Directorynbsp;Directory）CA 来完成，但大多数部署都应该使用 ActiveActive Directorynbsp;Directory 提供的证书服务。

在 ActiveActive Directorynbsp 中设置和配置证书服务的步骤包括在 Microsoft 文档中 http://technet.microsoft.com/en-us/library/cc772393(v=WS.10).aspx。

6.5. 管理同步协议

6.5.1. 创建同步协议

同步协议是使用 ipa-replica-manage connect 命令在 IdM 服务器上创建，因为它与 ActiveActive Directorynbsp;Directory 域创建连接。要建立到 ActiveActive Directorynbsp 的加密连接，IdM 必须信任 Windows CA 证书。

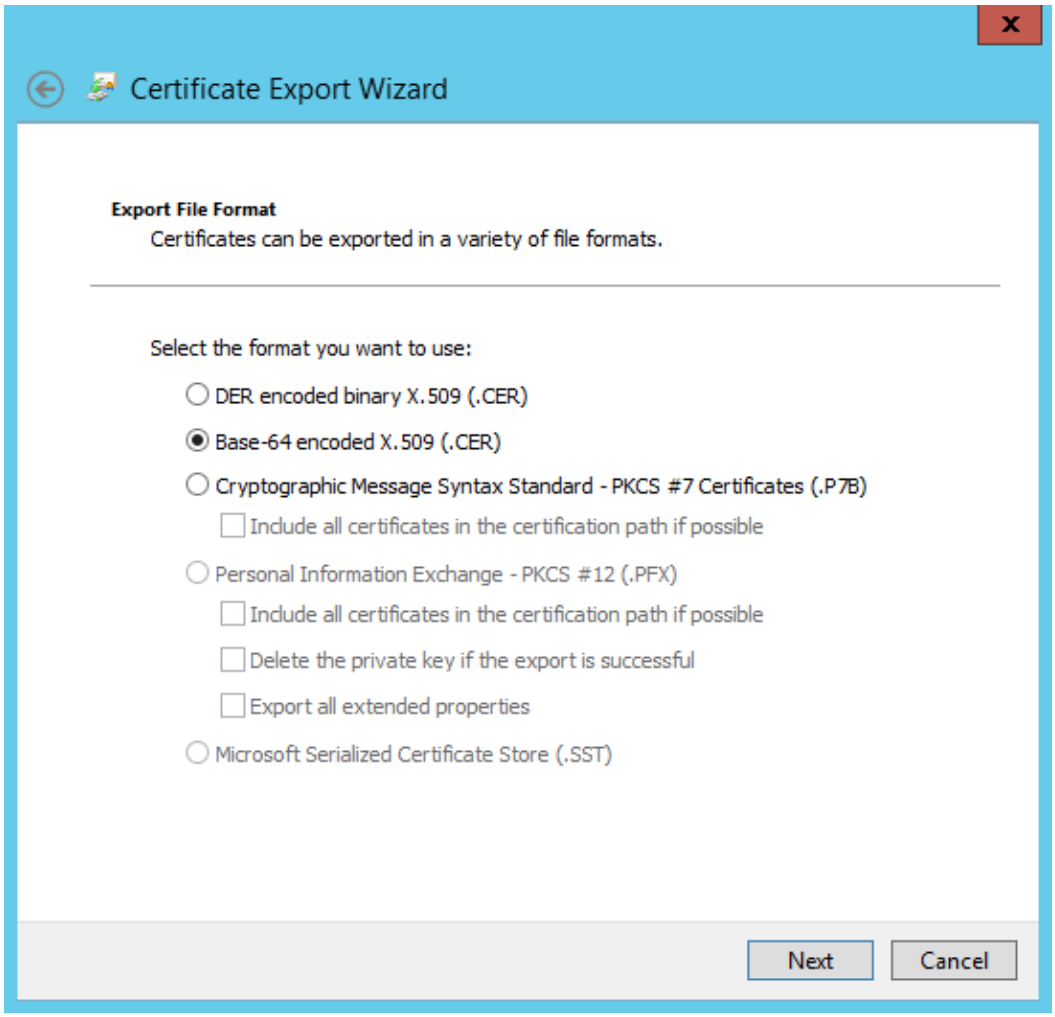
1. 将根证书颁发机构(CA)证书复制到 IdM 服务器中：
    a. 如果您的 ActiveActive Directorynbsp;Directory CA 证书是自签名的：
        i. 在 Windows 服务器上导出 ActiveActive Directorynbsp;Directory CA 证书。
            A. Super 键+R 组合键打开运行对话框。
            B. 输入 certsrv.msc 并单击"确定"。
            C. 右键单击本地证书颁发机构的名称，然后选择属性。
            D. 在 General 选项卡上，选择要在 CA 证书字段中导出的证书，然后单击查看证书。

E.

*在 **Details** 选项卡中，单击 **Copy to File** 以启动 证书导出向导。*

F.

*单击 **Next**，然后选择 **Base-64** 编码 **X.509(.CER)**。*



G.

*为导出的文件指定合适的目录和文件名。单击 **Next** 以导出证书，然后单击 **Finish**。*

H.

*将导出的证书复制到 **IdM** 服务器机器。*

b.

如果您的 ActiveActive Directorynbsp;Directory CA 证书由外部 CA 签名：

i.

***要找出 CA root** 证书是什么证书，显示证书链：*

```
# openssl s_client -connect adserver.example.com:636
CONNECTED(00000003)
```

```
depth=1 C = US, O = Demo Company, OU = IT, CN = Demo CA-28
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/O=Demo Company/OU=IT/CN=adserver.example.com
   i:/C=US/O=Demo Company/OU=IT/CN=Demo CA-1
 1 s:/C=US/O=Demo Company/OU=IT/CN=Demo CA-1
   i:/C=US/O=Demo Company/OU=IT/CN=Demo Root CA 2
```

上例显示 ActiveActive Directorynbsp;Directory 服务器的 CA 证书由 CN=Demo CA-1 签名，它由 CN=Demo Root CA 2 签名。这意味着 CN=Demo Root CA 2 是根 CA。

ii. 将 CA 证书复制到 IdM 服务器。

2. 删除 IdM 服务器中的任何现有 Kerberos 凭据。

```
$ kdestroy
```

3. 使用 ipa-replica-manage 命令创建 Windows 同步协议。这需要 --winsync 选项。如果密码与用户帐户同步，则也使用 --passsync 选项，并设置用于密码同步的密码。

--binddn 和--bindpw 选项在 ActiveActive Directorynbsp 上为系统帐户提供用户名和密码；Directory 服务器将用于连接到 ActiveActive Directorynbsp;Directory 服务器。

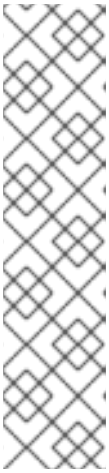
```
$ ipa-replica-manage connect --winsync \
 --binddn cn=administrator,cn=users,dc=example,dc=com \
 --bindpw Windows-secret \
 --passsync secretpwd \
 --cacert /etc/openldap/cacerts/windows.cer \
 adserver.example.com -v
```

- --WinSync ：将此识别为 Windows 同步协议。
- --bind DN : IdM 使用此 ActiveActive Directorynbsp 的 DN；Directory 帐户绑定到远程目录和同步属性。
- --bindpw ：同步帐户的密码。

- --cacert ：完整路径和文件名：
  - Activeactive Directorynbsp;Directory CA 证书（如果 CA 已被自签名）。
  - 外部 CA 证书，如果 ActiveActive Directorynbsp;Directory CA 由一个外部 CA 签名。
- --win-subtree ：包含要同步用户的 Windows 目录子树的 DN。默认值为 cn=Users,$SUFFIX。
- AD_server_name ： ActiveActive Directorynbsp 的全限定域名(FQDN)；Directory 域控制器。

4. 出现提示时，输入 Directory Manager 密码。

5. 可选。配置密码同步，如 第 6.6.2 节 “设置密码同步” 中所示。如果没有 Password Synchronization 客户端，用户属性会在对等服务器之间同步，但密码则不会。



注意

密码同步客户端捕获密码更改，然后在 ActiveActive Directorynbsp;Directory 和 IdM 之间同步它们。这意味着它将同步新密码或密码更新。

现有密码以 IdM 和 ActiveActive Directorynbsp 的散列形式存储；Directory，当安装 Password Synchronization 客户端时，无法解密或同步现有密码。必须更改用户密码，以启动对等服务器之间的同步。

6.5.2. 更改同步用户帐户属性的行为

创建同步协议时，它定义了同步进程在同步期间如何处理用户帐户属性的某些默认行为。这些类型的行为如如何处理锁定属性或如何处理不同的 DN 格式。可以通过编辑同步协议来更改此行为。

同步协议作为特殊的插件条目存在于 LDAP 服务器中，每一属性行为通过 LDAP 属性来设置。要更改同步行为，请使用 ldapmodify 命令直接修改 LDAP 服务器条目。

例如，帐户锁定属性在 IdM 和 ActiveActive Directorynbsp 之间同步。默认情况下，可以使用 ipaWinSyncAcctDisable 属性来禁用它。（更改意味着，如果在 ActiveActive Directorynbsp 中禁用了帐户，它仍然在 IdM 中活跃，反之亦然。）

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -w password

dn: cn=ipa-winsync,cn=plugins,cn=config
changetype: modify
replace: ipaWinSyncAcctDisable
ipaWinSyncAcctDisable: none

modifying entry "cn=ipa-winsync,cn=plugins,cn=config"
```

以下是同步设置属性的概述：

常规用户帐户参数

- ipaWinSyncNewEntryFilter ：设置搜索过滤器以查找包含要添加到新用户条目的对象类列表的条目。

  默认值为：(cn=ipaConfig)

- ipaWinSyncNewUserOCAttr ：在配置条目中设置 属性，该条目实际上包含要添加到新用户条目的对象类列表。

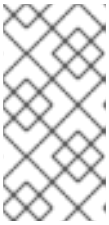
  默认值： ipauserobjectclasses

- ipaWinSyncHomeDirAttr ：识别条目中的哪个属性包含 POSIX 主目录的默认位置。

  默认值： ipaHomesRootDir

- ipaWinSyncUserAttr: 当它们从 ActiveActive Directorynbsp;Directory 域同步时，设置一个带有特定值的额外属性来添加到 ActiveActive Directorynbsp;Directory 域时。如果 属性为 multi-valued，则它可以设置多次，同步进程会将所有值添加到条目。

示例： ipaWinSyncUserAttr: attributeName attributeValue



注意

仅当条目尚未存在该属性时，这才会设置 属性值。如果存在 属性，则条目的值会在 ActiveActive Directorynbsp;Directory 条目被同步时使用。

- *ipaWinSyncForceSync ：设置匹配现有 AD 用户的现有 IdM 用户是否强制同步。当设置为 true 时，此类 IdM 用户会自动编辑，以便同步它们。*

  可能的值： true | false

  如果一个 IdMnbsp;IdM 用户帐户有一个 uid 参数，它与现有 ActiveActive Directorynbsp;Directory 用户相同，则该帐户 默认不会 同步。sAMAccountName此属性告知同步服务自动将 ntUser 和 ntUserDomainId 添加到 IdM 用户条目中，这允许它们同步。

用户帐户锁定参数

- *ipaWinSyncAcctDisable ：设置同步帐户锁定属性的方式。可以控制哪些帐户锁定设置生效。例如，to_ad 表示当在 IdM 中设置帐户锁定属性时，其值会同步到 ActiveActive Directorynbsp;Directory 并覆盖本地 ActiveActive Directorynbsp;Directory 值。默认情况下，帐户锁定属性从两个域同步。*

  可能的值：（默认 ）、to_ad、to_ds、none

- *ipaWinSyncInactivatedFilter ：设置搜索过滤器以查找用于存放已激活（禁用）用户的组的 DN。在大多数部署中不需要更改此设置。*

  默认值为： （&(cn=inactivated)(objectclass=groupOfNames)）

组参数

- *ipaWinSyncDefaultGroupAttr ：在新用户帐户中设置 属性，以引用该用户的默认组。然后，条目中的组名将用于查找用户帐户的 gidNumber。*

默认值： ipaDefaultPrimaryGroup

- ipaWinSyncDefaultGroupFilter ：设置新用户帐户中的 属性，以引用该用户的默认组。然后，条目中的组名将用于查找用户帐户的 gidNumber。

  默认值： ipaDefaultPrimaryGroup

域参数

- ipaWinSyncRealmAttr ：设置 realm 条目中包含 realm 名称的属性。

  默认值： cn

- ipaWinSyncRealmFilter ：设置搜索过滤器以查找包含 IdM 域名称的条目。

  默认值为：(objectclass=krbRealmContainer)

6.5.3. 更改 Synchronized Windows Subtree

创建同步协议会自动设置两个子树，以用作同步的用户数据库。在 IdM 中，默认值为 cn=users,cn=accounts,$SUFFIX, and for ActiveActive Directorynbsp;Directory，默认值为 CN=Users，$SUFFIX.

当使用 --win-subtree 选项创建同步协议时，ActiveActive Directorynbsp;Directory 子树的值可设为非默认值。在协议被创建后，可以使用 ldapmodify 命令编辑同步协议条目中的 nsds7WindowsReplicaSubtree 值来更改 ActiveActive Directorynbsp;Directory 子树。

1. 使用 ldapsearch 获取同步协议的名称。此搜索只会返回 dn 和 nsds7WindowsReplicaSubtree 属性的值，而不是整个条目。

```
[jsmith@ipaserver ~]$ ldapsearch -xLLL -D "cn=directory manager" -w password -p 389 -h
ipaserver.example.com -b cn=config objectclass=nsdswindowsreplicationagreement dn
nsds7WindowsReplicaSubtree

dn:
cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
```

```
tree,cn=config
nsds7WindowsReplicaSubtree: cn=users,dc=example,dc=com

... 8< ...
```

2. **修改同步协议**

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -W -p 389 -h
ipaserver.example.com <<EOF
 dn:
cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
 changetype: modify
 replace: nsds7WindowsReplicaSubtree
 nsds7WindowsReplicaSubtree: cn=alternateusers,dc=example,dc=com
 EOF

 modifying entry
"cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config"
```

新子树设置会立即生效。如果同步操作当前正在运行，则它将在当前操作完成后立即生效。

6.5.4. 配置 Uni-ward Synchronization

默认情况下，所有修改和删除都是双向的。ActiveActive Directorynbsp 的改变;Directory 被同步到 IdentityIdentity Managementnbsp;Management，以及对 IdentityIdentity Managementnbsp 中的条目更改;Management 同步到 ActiveActive Directorynbsp;Directory。这基本上是一个明显的、多主关系，其中 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 都是同步的对等点，且同时是数据 master。

但是，在某些数据结构或 IT 设计中，可能只有一个域应当是一个数据主域，另一个域应接受更新。这会将同步关系从多主关系（对等服务器等效）转变为主消费者关系。

这可以通过在同步协议中设置 oneWaySync 参数来完成。可能的值有 fromWindows （用于 ActiveActive Directorynbsp;Directory 到 IdentityIdentity Managementnbsp;Management 同步）和 toWindows （用于 IdentityIdentity Managementnbsp;Management to ActiveActive Directorynbsp;Directory 同步）。

例如，将 ActiveActive Directorynbsp 的更改同步;Directory 到 IdentityIdentity Managementnbsp;Management:

```
[jsmith@ipaserver ~]$ ldapmodify -x -D "cn=directory manager" -w password -p 389 -h
```

```
ipaserver.example.com

dn: cn=meToWindowsBox.example.com,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
changetype: modify
add: oneWaySync
oneWaySync: fromWindows
```

重要

启用单向同步不会自动阻止对未同步服务器上的更改，这可能会导致同步更新之间的同步对等点不一致。例如，单向同步配置为来自 ActiveActive Directorynbsp;Directory 到 IdentityIdentity Managementnbsp;Management, so ActiveActive Directorynbsp;Directory is(essence)data master.如果在 IdentityIdentity Managementnbsp;Management 上修改甚至删除了条目，则 IdentityIdentity Managementnbsp;Management 信息不同，这些更改永远不会被传递给 ActiveActive Directorynbsp;Directory。在下一次同步更新过程中，DirectoryDirectory 服务器nbsp 上将覆盖编辑；Server 和已删除的条目将被重新添加。

6.5.5. 删除同步协议

可以通过删除 断开 IdM 和 ActiveActive Directorynbsp;Directory 服务器的同步协议来停止同步。在创建同步协议中，删除同步协议使用 ipa-replica-manage disconnect 命令，然后是 ActiveActive Directorynbsp;Directory 服务器的主机名。

1. **删除同步协议。**

```
# ipa-replica-manage disconnect adserver.ad.example.com
```

2. **列出 IdM 目录证书数据库中的证书：**

```
# certutil -L -d /etc/dirsrv/slapd-IDM-EXAMPLE-COM/
Certificate Nickname                    Trust Attributes
                                        SSL,S/MIME,JAR/XPI

IDM.EXAMPLE.COM IPA CA                  CT,C,C
CN=adserver,DC=ad,DC=example,DC=com     C,,
Server-Cert                             u,u,u
```

3. **从 IdM 服务器数据库中删除 ActiveActive Directorynbsp;Directory CA 证书：**

```
# certutil -D -d /etc/dirsrv/slapd-IDM-EXAMPLE-COM/ -n
"CN=adserver,DC=ad,DC=example,DC=com"
```

6.5.6. WinSync Agreement 失败

创建同步协议会失败，因为它无法连接到 ActiveActive Directorynbsp;Directory 服务器。

一个最常见的同步协议失败是 IdM 服务器无法连接到 ActiveActive Directorynbsp;Directory 服务器：

```
"Update failed! Status: [81  - LDAP error: Can't contact LDAP server]
```

如果发生错误的 ActiveActive Directorynbsp;Directory CA 证书是在创建协议时指定的，则会出现这种情况。这会在 IdM LDAP 数据库（/etc/dirsrv/slapd-DOMAIN/ 目录中）中创建名为 Imported CA 的重复证书。这可使用 certutil 检查：

```
$ certutil -L -d /etc/dirsrv/slapd-DOMAIN/

Certificate Nickname                         Trust Attributes
SSL,S/MIME,JAR/XPI

CA certificate                               CTu,u,Cu
Imported CA                                  CT,,C
Server-Cert                                  u,u,u
Imported CA                                  CT,,C
```

要解决这个问题，从证书数据库中删除 CA 证书：

```
# certutil -d /etc/dirsrv/slapd-DOMAIN-NAME -D -n "Imported CA"
```

存在错误，指出密码未同步，因为它表示该条目存在

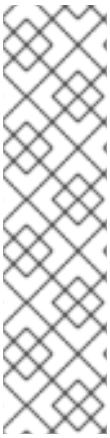
对于用户数据库中的一些条目，可能会有一条信息错误消息，指出没有重置密码，因为该条目已存在：

```
"Windows PassSync entry exists, not resetting password"
```

这不是错误。当没有更改 Password Synchronization 用户（Password Synchronization 用户）时，会发生此消息。Password Synchronization 用户是服务用来更改 IdM 中的密码的操作用户。

6.6. 管理密码同步

通过同步协议配置用户条目同步。但是，ActiveActive Directorynbsp 中的密码：Directory 和 IdentityIdentity Managementnbsp;Management 不是普通用户同步过程的一部分。必须在 ActiveActive Directorynbsp 上安装单独的客户端；Directory 服务器若要以用户帐户创建或密码捕获密码，然后使用同步更新转发该密码信息。



注意

密码同步客户端捕获密码更改，然后在 ActiveActive Directorynbsp;Directory 和 IdM 之间同步它们。这意味着它将同步新密码或密码更新。

现有密码以 IdM 和 ActiveActive Directorynbsp 的散列形式存储；Directory，当安装 Password Synchronization 客户端时，无法解密或同步现有密码。必须更改用户密码，以启动对等服务器之间的同步。

6.6.1. 设置 Windows Server for Password Synchronization

同步密码需要以下条件：

- Activeactive Directorynbsp;Directory 必须在 SSL 中运行。

  注意

  在企业根模式中安装 Microsoft 证书系统.Activeactive Directorynbsp;Directory 将自动注册来检索其 SSL 服务器证书。

- 密码同步服务必须安装到 每个 ActiveActive Directorynbsp;Directory 域控制器。要从 Windows 同步密码，PassSync 服务需要访问未加密的密码才能通过安全连接与 IdM 同步。由于用户可以在每个域控制器上更改密码，因此需要在每个域控制器上安装 PassSync 服务。

- 密码策略必须在 IdM 和 ActiveActive Directorynbsp;Directory 端设置相似。当同步目的地收到更新的密码时，它仅被验证为与源上的策略匹配。同步目的地上未重新验证它。

*要验证 **ActiveActive Directorynbsp;Directory** 密码复杂性策略是否已启用，请在 **ActiveActive Directorynbsp;Directory** 域控制器上运行：*

```
> dsquery * -scope base -attr pwdProperties
  pwdProperties
  1
```

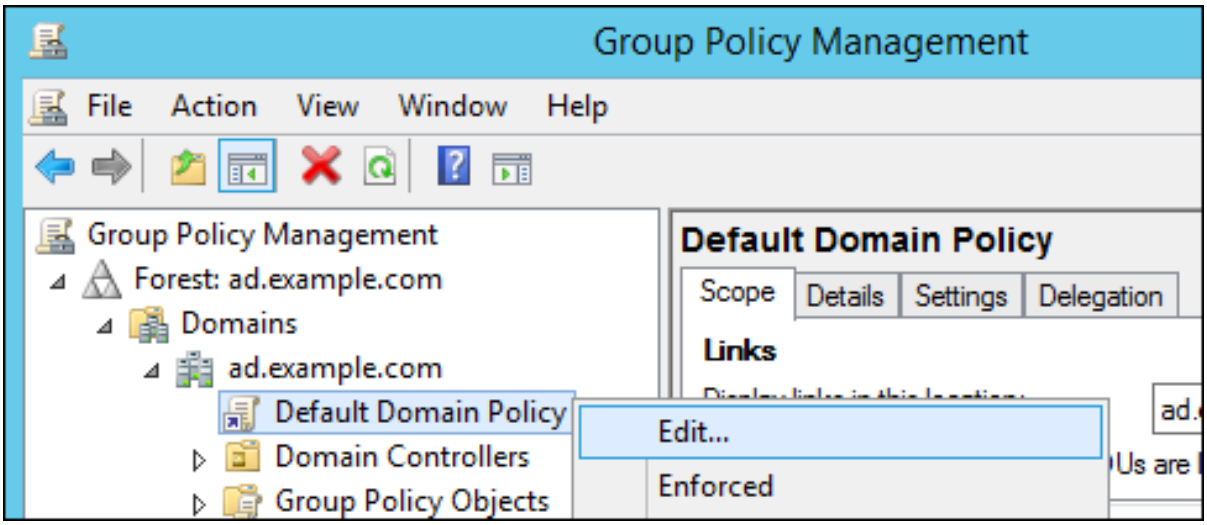
***如果将 attribute pwdProperties** 的值设为 **1**，则会为该域启用密码复杂性策略。*

注意

***如果您不确定**组策略是否为组织单元定义了开发密码设置（注意），请询问您的组策略管理员。*

*启用 **ActiveActive Directorynbsp;Directory** 密码复杂性设置：*

1. *从命令行运行 **gpmc.msc**。*
2. *选择 **Group Policy Management**。*
3. ***Forest： ad.example.com → 域ad.example.com.***
4. *右键单击 **Default Domain Policy** 条目，再选择 **Edit**。*



5.

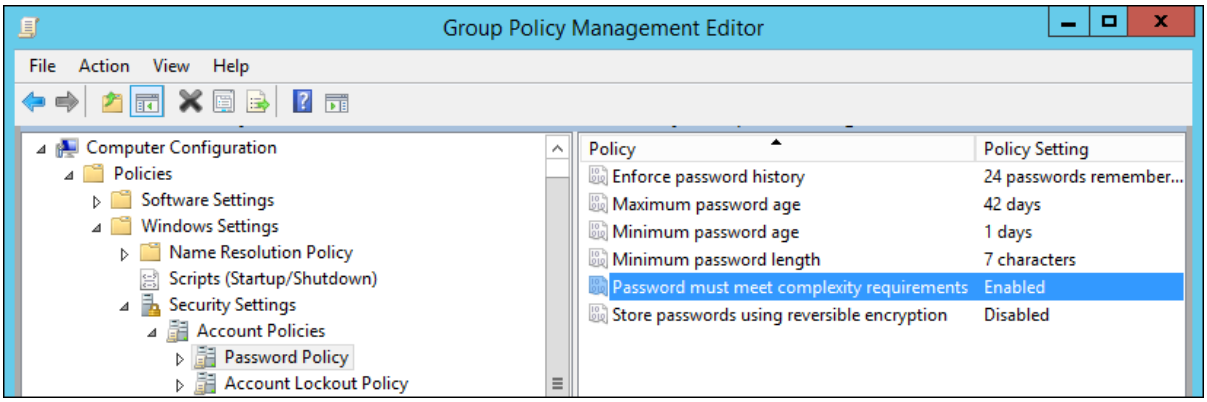
Group Policy Management Editor 会自动打开。

6.

打开"计算机配置策略"Windows → 设置安全设置帐户策略"密码"策略.

7.

启用密码必须满足复杂性要求选项并保存。



6.6.2. 设置密码同步

在 ActiveActive Directorynbsp;Directory 域中的每个域控制器上安装密码同步服务，以同步 Windows 密码。

1.

将 RedHat-PassSync-.msi 文件下载到 Active Directory 域控制器：*

a.

登录客户门户网站。

b.

单击页面顶部的 Downloads。

c.

选择 Red Hat Enterprise Linuxnbsp;Hat Enterprise Red Hat Enterprise Linuxnbsp;Linux from the product list.

d.

选择 Red Hat Enterprise Linuxnbsp 的最新版本;Hat Enterprise Linuxnbsp;Linux 6 或 Red Hat Enterprise Linuxnbsp;Hat Enterprise Linuxnbsp;Hat Enterprise Linuxnbsp;Linux 7 and architecture.

e.

在 ActiveActive Directorynbsp;Directory 域控制器架构中下载 WinSync Installer,

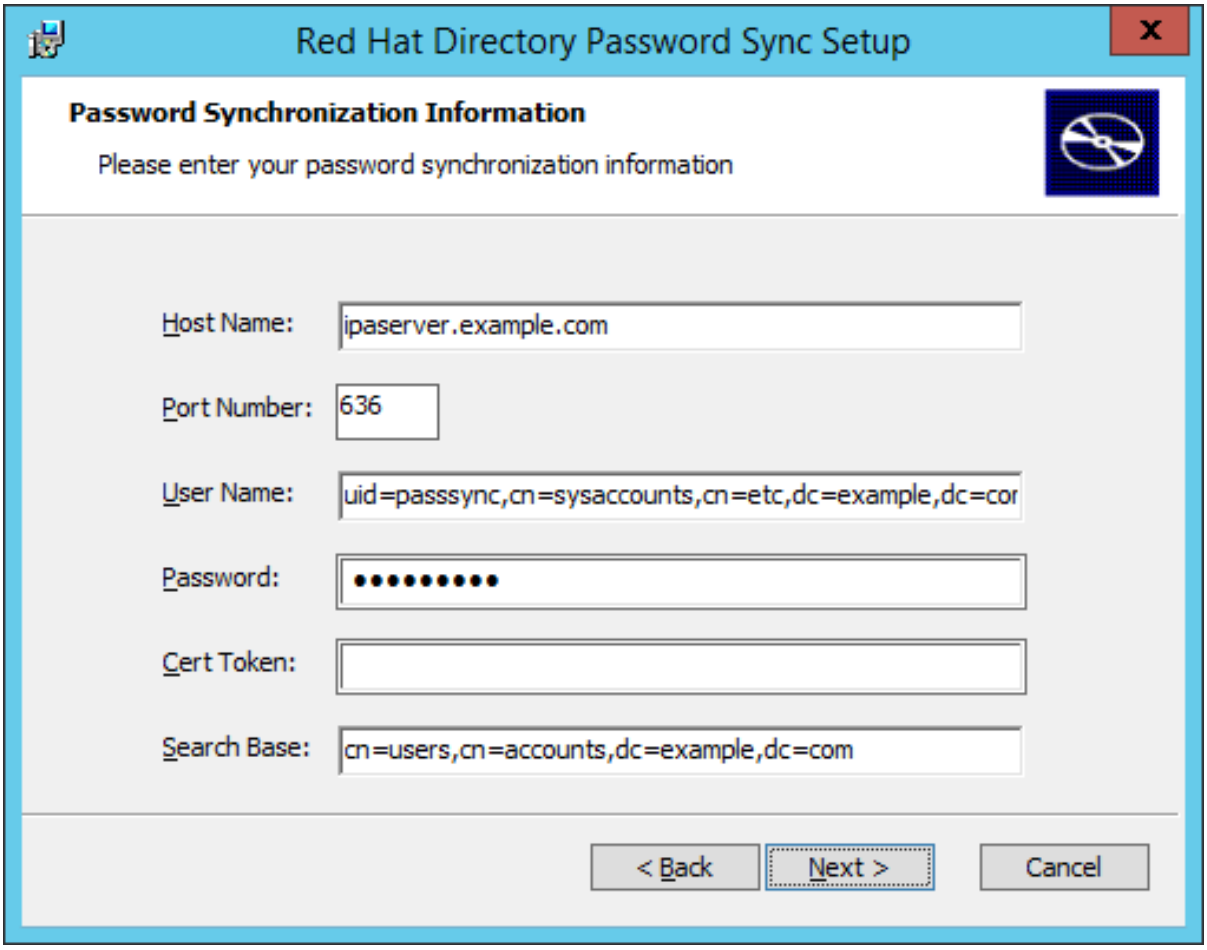
方法是点 Download Now 按钮。

2. 双击MSI 文件进行安装。

3. 此时将显示 Password Synchronrization Setup 窗口。按下一步开始安装。

4. 填写信息以建立与 IdM 服务器的连接。

- IdM 服务器连接信息，包括主机名和安全端口号。
- ActiveActive Directorynbsp;Directory 用来连接到 IdM 机器的系统用户的用户名。当 IdM 服务器上配置同步时，此帐户会自动配置。默认帐户为 uid=passsync,cn=sysaccounts,cn=etc,dc=example,dc=com.
- 同步协议创建时在 --passsync 选项中设置的密码。
- IdM 服务器上的 People 子树的搜索基础。ActiveActive Directorynbsp;Directory 服务器连接到与 ldapsearch 或 replication 操作类似的 IdM 服务器，因此它必须知道在 IdM 子树中查找用户帐户的位置。用户子树为 cn=users,cn=accounts,dc=example,dc=com。
- 此时不使用证书令牌，因此该字段应当留空。



按下一步，然后完成以安装密码同步。

5. *将 IdM 服务器的 CA 证书导入到 PassSync 证书存储中。*

   a. *从 http://ipa.example.com/ipa/config/ca.crt 下载 IdM 服务器的 CA 证书。*

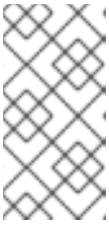
   b. *将 IdM CA 证书复制到 ActiveActive Directorynbsp;Directory 服务器。*

   c. *在 Password Synchronization 数据库中安装 IdM CA 证书。例如：*

```
cd "C:\Program Files\Red Hat Directory Password Synchronization"

certutil.exe -d . -A -n "IPASERVER.EXAMPLE.COM IPA CA" -t CT,, -a -i ipaca.crt
```

6. *重新启动 Windows 计算机以启动密码同步。*



注意

必须重新引导 Windows 机器。如果不重新启动，PasswordHook.dll 则未启用，密码同步将无法正常工作。

7. 如果应当同步现有帐户的密码，请重置用户密码。

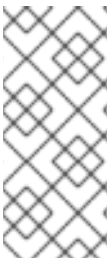
注意

密码同步客户端捕获密码更改，然后在 ActiveActive Directorynbsp;Directory 和 IdM 之间同步它们。这意味着它将同步新密码或密码更新。

现有密码以 IdM 和 ActiveActive Directorynbsp 的散列形式存储；Directory，当安装 Password Synchronization 客户端时，无法解密或同步现有密码。必须更改用户密码，以启动对等服务器之间的同步。

安装 Password Synchronization 应用时第一次尝试同步密码始终会失败，因为 DirectoryDirectory 服务器nbsp;Server 和 Active Directory 同步实体之间的 SSL 连接将始终失败。 创建证书和密钥数据库的工具与.msi 一起安装。

密码同步客户端无法同步 IdM admin 组的成员的密码。这种行为旨在防止密码同步代理或低级用户管理员更改顶级管理员的密码。



注意

仅在同步源上验证密码，以匹配密码策略。要验证并启用 ActiveActive Directorynbsp;Directory 密码复杂性策略，请参阅 第 6.6.1 节 “设置 Windows Server for Password Synchronization”。

---

[2] cn 的处理方式与其他同步属性不同。当从 IdentityIdentity Managementnbsp 同步;Management 到 ActiveActive Directorynbsp;Directory 时，它会被直接映射到cn。cn从 ActiveActive Directorynbsp 同步;Directory 到 IdentityIdentity Managementnbsp;Management 时，cn 从 Windows 上的 name 属性映射到 IdentityIdentity Managementnbsp;Management 中的 cn 属性。

第 7 章 将现有环境从同步迁移到信任

同步 和信任是间接集成两种可能的方法。通常不建议同步，红帽建议改为使用基于 Active Directory(AD)信任的方法。详情请查看 第 1.3 节 “间接集成”。

本章论述了如何将现有基于同步的设置迁移到 AD 信任。IdM 中提供以下迁移选项：

- 第 7.1 节 “使用 ipa-winsync-migrate自动从 Synchronization 迁移到 Trust”
- 第 7.2 节 “使用 ID 视图手动从同步迁移到 Trust”

7.1. 使用 IPA-WINSYNC-MIGRATE自动从 SYNCHRONIZATION 迁移到 TRUST

重要

ipa-winsync-migrate 实用程序仅在运行 Red Hat Enterprise Linux 7.2 或更高版本的系统上可用。

7.1.1. 如何使用 ipa-winsync-migrate Works 进行迁移

ipa-winsync-migrate 实用程序将所有同步的用户从 AD 林迁移，同时保留 Winsync 环境中的现有配置，并将其传送到 AD 信任中。对于 Winsync 协议创建的每个 AD 用户，ipa-winsync-migrate 在 Default Trust View 中创建了一个 ID 覆盖（请参阅 第 8.1 节 “Active Directory 默认信任视图”）。

迁移完成后：

- AD 用户的 ID 覆盖具有以下从 Winsync 中的原始条目复制的属性：
  - 登录名(uid)
  - UID号（uid 号）

- GID号(gid number)
- 主目录（主目录）
- GECOS条目(gecos)

- AD 信任中的用户帐户将其原始配置保留在 IdM 中，其中包括：
  - POSIX 属性
  - 用户组
  - 基于角色的访问控制规则
  - 基于主机的访问控制规则
  - SELinux 成员资格
  - sudo 规则

- 新 AD 用户添加为外部 IdM 组的成员。

- 删除原始 Winsync 复制协议、原始同步用户帐户和用户帐户的所有本地副本。

7.1.2. 如何使用 ipa-winsync-migrate 进行迁移

开始之前：

- 使用 ipa-backup 实用程序备份您的 IdM 设置。请参阅 Linux 域 身份、身份验证和策略指南中的备份和恢复 身份管理。

原因：迁移会影响 IdM 配置和许多用户帐户的重要部分。如有必要，创建备份可让您恢复原始设置。

迁移：

1. 使用同步的域创建信任关系。请参阅 第 5 章 使用 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 创建 Cross-forest Trusts。

2. 运行 ipa-winsync-migrate 并指定 AD 域和 AD 域控制器的主机名：

```
# ipa-winsync-migrate --realm example.com --server ad.example.com
```

如果在 ipa-winsync-migrate 创建的覆盖中发生冲突，则会显示有关冲突的信息，但迁移继续进行。

3. 从 AD 服务器卸载 Password Sync 服务。这会从 AD 域控制器移除同步协议。

有关该实用程序的详情，请查看 ipa-winsync-migrate(1) man page。

7.2. 使用 ID 视图手动从同步迁移到 TRUST

您可以使用 ID 视图手动更改 AD 用户生成的 POSIX 属性。

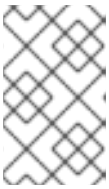
1. 为原始同步的用户和组条目创建备份。

2. 使用同步的域创建信任关系。有关创建信任的详情请参考 第 5 章 使用 ActiveActive Directorynbsp;Directory 和 IdentityIdentity Managementnbsp;Management 创建 Cross-forest Trusts。

3. 对于每个同步的用户和组，通过执行以下操作之一保留 IdM 生成的 UID 和 GID：

- 单独创建应用到特定主机的 ID 视图，并将用户 ID 覆盖添加到视图中。
- 在 Default Trust View 中创建用户 ID 覆盖。

详情请参阅在 不同主机上为用户帐户定义不同的属性值。



注意

只有 IdM 用户可以管理 ID 视图。AD 用户无法.

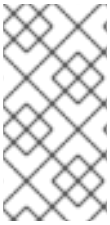
4. 删除原始同步的用户和组条目。

有关在 Active Directory 环境中使用 ID 视图的常规信息，请参考 第 8 章 在 Active Directory 环境中使用 ID 视图。

第 8 章 在 ACTIVE DIRECTORY 环境中使用 ID 视图

通过 ID 视图，您可以为 POSIX 用户或组属性指定新值，并定义要在其上应用新值的客户端或主机。

身份管理(IdM)以外的集成系统有时会根据与 IdM 中使用的算法不同的算法生成 UID 和 GID 值。通过覆盖之前生成的值使其与 IdM 中使用的值兼容，曾作为另一个集成系统的客户端可以完全与 IdM 集成。



注意

本章仅介绍与 Active Directory(AD)相关的 ID 视图功能。有关 ID 视图的常规信息，请参阅 Linux 域身份、身份验证和策略指南。

您可以在 AD 环境中使用 ID 视图来满足以下目的：

覆盖 AD 用户属性，如 POSIX 属性或 SSH 登录详情

详情请查看 第 8.3 节 “使用 ID 视图来定义 AD 用户属性”。

从同步迁移到基于信任的集成

详情请查看 第 7.2 节 “使用 ID 视图手动从同步迁移到 Trust”。

执行每个主机组覆盖 IdM 用户属性

详情请查看 第 8.4 节 “将 NIS 域迁移到 IdM”。

8.1. ACTIVE DIRECTORY 默认信任视图

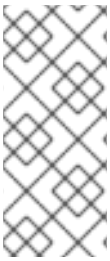
8.1.1. 默认信任视图

Default Trust View 是默认 ID 视图，始终应用到基于信任的设置中的 AD 用户和组。当您使用 ipa-adtrust-install 建立信任且无法删除时，它会自动创建。

使用 Default Trust View，您可以为 AD 用户和组定义自定义 POSIX 属性，从而覆盖 AD 中定义的值。

表 8.1. 应用默认信任视图

	AD 中的值	默认信任视图		结果
login	ad_user	ad_user	→	ad_user
UID	111	222	→	222
GID	111	（无值）	→	111



注意

Default Trust View 仅接受 AD 用户和组的覆盖，而不接受 IdM 用户和组的覆盖。它适用于 IdM 服务器和客户端，因此只需要为 ActiveActive Directorynbsp;Directory 用户和组提供覆盖。

8.1.2. 使用其他 ID 视图覆盖默认信任视图

如果另一个应用到主机的 ID 视图覆盖 Default Trust View 中的属性值，IdM 将在 Default Trust View 之上应用特定于主机的 ID 视图中的值。

- ***如果在特定于主机的 ID 视图中定义了属性，IdM 将应用此视图中的值。***
- ***如果在特定于主机的 ID 视图中未定义属性，IdM 将应用 Default Trust View 中的值。***

默认信任视图始终应用到 IdM 服务器和副本，以及 AD 用户和组。您无法为他们分配不同的 ID 视图：它们始终应用 Default Trust View 中的值。

表 8.2. 在默认信任视图上应用主机特定 ID 视图

	AD 中的值	默认信任视图	主机特定视图		结果
login	ad_user	ad_user	（无值）	→	ad_user
UID	111	222	333	→	333
GID	111	（无值）	333	→	333

8.1.3. 基于客户端版本的 ID 覆盖

IdM 主控机始终从 Default Trust View 应用 ID 覆盖，无论 IdM 客户端如何检索值：使用 SSSD 或使用 Schema 兼容性树请求。

但是，特定于主机的 ID 视图中的 ID 覆盖的可用性有限：

旧客户端：RHEL 6.3 及更早版本（SSSD 1.8 及更早版本）

客户端可以请求应用特定的 ID 视图。

要在传统客户端上使用特定于主机的 ID 视图，请将客户端上的基本 DN 更改为：cn=id_view_name,cn=views,cn=compat,dc=example,dc=com.

RHEL 6.4 到 7.0（SSSD 1.9 到 1.11）

不支持客户端上的特定于主机的 ID 视图。

RHEL 7.1 及更高版本（SSSD 1.12 及更高版本）

完全支持.

8.2. 修复 ID 冲突

IdM 使用 ID 范围来避免来自不同域的 POSIX ID 冲突。有关 ID 范围的详情，请查看 Linux 域身份、身份验证和策略指南中的 ID 范围。

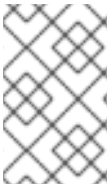
ID 视图中的 POSIX ID 不使用特殊范围类型，因为 IdM 必须允许与其他类型的 ID 范围重叠。例如，通过同步创建的 AD 用户具有与 IdM 用户相同的 ID 范围内的 POSIX ID。

POSIX ID 在 IdM 侧的 ID 视图中手动管理。因此，如果 ID 冲突发生，可以通过更改冲突 ID 来修复它。

8.3. 使用 ID 视图来定义 AD 用户属性

通过 ID 视图，您可以更改 AD 中定义的用户属性值。如需属性的完整列表，请参阅属性 View Can Override。

例如：如果您要管理混合的 Linux-Windows 环境，并希望手动为 AD 用户定义 POSIX 属性或 SSH 登录属性，但 AD 策略不允许它，您可以使用 ID 视图覆盖属性值。当 AD 用户对运行 SSSD 的客户端进行身份验证或使用兼容 LDAP 树进行身份验证时，身份验证过程中会使用新值。



注意

只有 IdM 用户可以管理 ID 视图。AD 用户无法.

覆盖属性值的过程遵循以下步骤：

1. 创建新的 ID 视图。
2. 在 ID 视图中添加用户 ID 覆盖，并指定 require 属性值。
3. 将 ID 视图应用到特定的主机。

有关如何执行这些步骤的详情，请参阅 Linux 域身份、身份验证和策略指南中的 在不同主机上 为用户帐户 定义不同的属性值。

8.4. 将 NIS 域迁移到 IDM

如果您要管理 Linux 环境，并想将具有不同 UID 和 GID 的不同 NIS 域迁移到现代身份管理解决方案中，您可以使用 ID 视图为现有主机设置主机特定 UID 和 GID，以防止更改现有文件和目录的权限。

迁移的过程遵循以下步骤：

1. 在 IdM 域中创建用户和组。详情请查看
   - 添加阶段或活动用户
   - 添加和删除用户组

2. 使用现有主机的 ID 视图覆盖用户创建过程中生成的 IdM ID：

    1. 创建单独的 ID 视图.

    2. 将用户和组的 ID 覆盖添加到 ID 视图。

    3. 将 ID 视图分配到特定的主机。

    详情请参阅在 不同主机上为用户帐户定义不同的属性值。

3. 在 Linux 域身份、身份验证和策略指南 中安装和卸载身份管理客户端.

4. 停用 NIS 域.

8.5. 使用 SHORT NAMES 进行解析和验证用户和组的配置选项

本节论述了配置选项，允许您使用简短的用户名或组名称，而不是 user_name@domain 或 domain\user_name 完全限定名称格式，以在 Active Directory(AD)环境中解析和验证用户和组。您可以配置它：

- 在信任 AD 的 Identity Management(IdM)中
- 在 Red Hat Enterprise Linux 中使用 SSSD 加入 AD

8.5.1. 域解析如何工作

您可以使用域解析顺序选项指定搜索域列表的顺序，以返回给定用户名的匹配项。您可以设置选项：

- 服务器上的.请参阅：
  - 第 8.5.2.1 节 “全局设置域解析顺序”
  - 第 8.5.2.2 节 “为 ID 视图设置域解析顺序”
- 在客户端上.请查看 第 8.5.3 节 “在 IdM 客户端中配置域解析顺序”

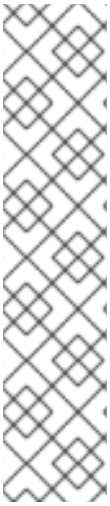
在具有 Active Directory 信任的环境中，建议应用一个或多个基于服务器的选项。

从特定客户端的角度来看，可以在以上三个位置中的多个位置中设置域解析顺序选项。客户端检查这三个位置的顺序是：

1. 本地 sssd.conf 配置
2. id 视图配置
3. 全局 IdM 配置

将仅使用首先找到的域解析顺序设置。

在 Red Hat Enterprise Linux 直接集成到 AD 的环境中，您只能在客户端上设置域解析顺序。



注意

如果出现以下情况，则必须使用限定名称：

- 用户名存在于多个域中
- SSSD 配置包括 default_domain_suffix 选项，您想要向未使用该选项指定的域发出请求

8.5.2. 在身份管理服务器上配置域解析顺序

如果域或子域中的大量客户端应使用相同的域解析顺序，请选择基于服务器的配置。

8.5.2.1. 全局设置域解析顺序

选择此选项将域解析顺序设置为信任中的所有客户端。要做到这一点，请使用 ipa config-mod 命令。例如，在 IdM 域中，它与多个子域信任 AD 林：

```
$ ipa config-mod --domain-resolution-order='idm.example.com:ad.example.com:subdomain1.ad.example.com:subdomain2.ad.example.com'
Maximum username length: 32
Home directory base: /home
...
Domain Resolution Order: idm.example.com:ad.example.com:subdomain1.ad.example.com:subdomain2.ad.example.com
...
```

通过以这种方式设置域解析顺序，来自 IdM 域和可信 AD 林的用户只能使用短名称登录。

8.5.2.2. 为 ID 视图设置域解析顺序

选择此选项以将设置应用到特定域中的客户端。

例如，在子域服务器上 server.idm.example.com，您会看到来自 subdomain2.ad.example.com 的子域比来自 subdomain1.ad.example.com 的更多登录。但是，全局解析顺序指出，在解析用户名时，subdomain1.ad.example.com 子域用户数据库在 subdomain2.ad.example.com 之前被尝试。要为特定服务器设置不同的顺序，为特定视图设置域解析顺序：

1. 使用域解析顺序选项集创建一个 ID 视图：

```
$ ipa idview-add example_view --desc "ID view for custom shortname resolution on
server.idm.example.com" --domain-resolution-order
subdomain2.ad.example.com:subdomain1.ad.example.com
-------------------------------
Added ID View "example_view"
-------------------------------
ID View Name: example_view
Description: ID view for custom shortname resolution on server.idm.example.com
Domain Resolution Order: subdomain2.ad.example.com:subdomain1.ad.example.com
```

2. 在客户端上应用视图。例如：

```
$ ipa idview-apply example_view --hosts server.idm.example.com
---------------------------------
Applied ID View "example_view"
---------------------------------
hosts: server.idm.example.com
-----------------------------------------
Number of hosts the ID View was applied to: 1
-----------------------------------------
```

有关 ID 视图的详情请参考 第 8 章 在 Active Directory 环境中使用 ID 视图。

8.5.3. 在 IdM 客户端中配置域解析顺序

如果要在较少数量的客户端上设置客户端的域解析顺序，或者客户端直接连接到 AD，请设置域解析顺序。

在 /etc/sssd/sssd.conf 文件的 [sssd] 部分中设置 domain_resolution_order 选项，例如：

```
domain_resolution_order = subdomain1.ad.example.com, subdomain2.ad.example.com
```

*有关配置 **domain_resolution_order** 选项的详情请参考 **sssd.conf(5)** 手册页。*

附录 A. 修订历史记录

请注意，修订号与本手册的版本相关，与 Red Hat Enterprise Linux 的版本号无关。

修订 7.0-51 Thu Mar 4 2021 Florian Delehaye
7.9 GA 版指南.添加了有关手动调整 DNA ID 范围的新部分。

修订 7.0-50 Wed May 27 2020 Florian Delehaye
多个修复和更新.

修订 7.0-49 Tue Aug 06 2019 Marc Muehlfeld
发布 7.7 GA 的文档版本.

修订 7.0-48 Wed Jun 05 2019 Marc Muehlfeld
更新了配置信任代理，添加了 AD 提供程序如何处理受信任域，以及更改 SSSD 显示的用户名格式.

修订 7.0-47 Tue Apr 08 2019 Marc Muehlfeld
几个小修复和更新。

修订 7.0-46 Mon Oct 29 2018 Filip Hanzelka
为 7.6 GA 发布准备文档.

修订 7.0-45 Mon Jun 25 2018 Filip Hanzelka
添加了 *SSSD 和 Winbind 之间的交换，用于 SMB 共享访问.*

修订 7.0-44 Thu Apr 5 2018 Filip Hanzelka
为 7.5 GA 发布准备文档.

修订 7.0-43 Wed Feb 28 2018 Filip Hanzelka
更新了 *SSSD 支持的 GPO 设置.*

修订 7.0-42 Mon Feb 12 2018 Aneta Šteflová Petrová
更新了使用共享机密创建双周信任.

修订 7.0-41 Mon Jan 29 2018 Aneta Šteflová Petrová
小修复.

修订 7.0-40 Fri Dec 15 2017 Aneta Šteflová Petrová
小修复.

修订 7.0-39 Mon Dec 6 2017 Aneta Šteflová Petrová
使用 Samba 进行 Active Directory 集成更新.

修订 7.0-38 Mon Dec 4 2017 Aneta Šteflová Petrová
更新了信任的 *DNS 和 Realm 设置.*

修订 7.0-37 Mon Nov 20 2017 Aneta Šteflová Petrová
更新了使用共享机密创建双周信任.

修订 7.0-36 Mon Nov 6 2017 Aneta Šteflová Petrová
小修复.

修订 7.0-35 Mon Oct 23 2017 Aneta Šteflová Petrová
更新了 *Active Directory 条目和 POSIX 属性，以及配置将 ID 映射作为 SSSD 提供程序的 AD 域.*

修订 7.0-34 Mon Oct 9 2017 Aneta Šteflová Petrová
添加用于使用短名称的配置选项.更新了信任控制器和信任代理.

修订 7.0-33 Tue Sep 26 2017 Aneta Šteflová Petrová
更新了 SSSD 章节中的自动发现部分。添加了有关配置可信域的两个部分。

修订 7.0-32 Tue Jul 18 2017 Aneta Šteflová Petrová
发布 7.4 GA 的文件版本.

修订 7.0-31 Tue May 23 2017 Aneta Šteflová Petrová
关于安全 ID 映射的小修复。

修订 7.0-30 Mon Apr 24 2017 Aneta Šteflová Petrová
定义 Windows 集成的小修补程序.

修订 7.0-29 Mon Apr 10 2017 Aneta Šteflová Petrová
更新了直接集成.

修订 7.0-28 Mon Mar 27 2017 Aneta Šteflová Petrová
迁移允许用户将其他用户的密码完全更改为 Linux 域身份指南，作为启用密码重置.更新了信任支持的 Windows 平台.修复了损坏的链接。其他次要更新.

修订 7.0-27 Mon Feb 27 2017 Aneta Šteflová Petrová
更新了信任的端口要求。轻微调整信任和同步.其他次要更新.

修订 7.0-26 Wed Nov 23 2016 Aneta Šteflová Petrová
添加了 ipa-winsync-migrate。信任、SSSD 和同步章节的小修复。

修订 7.0-25 Tue Oct 18 2016 Aneta Šteflová Petrová
7.3 GA 发布版本.

修订 7.0-24 Thu Jul 28 2016 Marc Muehlfeld
更新了图表，为服务和主机添加了 Kerberos 标志，以及其他次要修复.

修订 7.0-23 Thu Jun 09 2016 Marc Muehlfeld
更新了同步章节。删除了 Kerberos 章节。其他小修复.

修订 7.0-22 Tue Feb 09 2016 Aneta Petrová
更新了 realmd，删除索引，将 ID 视图的一部分移到 Linux 域身份指南和其他次要更新中。

修订 7.0-21 Fri Nov 13 2015 Aneta Petrová
带有小更新的 7.2 GA 版本。

修订 7.0-20 Thu Nov 12 2015 Aneta Petrová
7.2 GA 版本.

修订 7.0-19 Fri Sep 18 2015 Tomáš Čapek
更新了启动页面排序顺序。

修订 7.0-18 Thu Sep 10 2015 Aneta Petrová
更新了输出格式。

修订 7.0-17 Mon Jul 27 2015 Aneta Petrová
添加了基于 GPO 的访问控制，其他一些细微变化。

修订 7.0-16 Thu Apr 02 2015 Tomáš Čapek
添加了 ipa-advise，通过 SSSD 扩展扩展的 CIFS 共享，提醒 UNIX 扩展的身份管理。

修订 7.0-15 Fri Mar 13 2015 Tomáš Čapek
具有 7.1 最后编辑的异步更新.

修订 7.0-13 Wed Feb 25 2015 Tomáš Čapek
7.1 GA 版本.

修订 7.0-11 Fri Dec 05 2014 Tomáš Čapek
重新构建以更新初始页面上的排序顺序。

修订 7.0-7 Mon Sep 15 2014 Tomáš Čapek
第 5.3 节：为内容更新临时删除信任.

修订 7.0-5 June 27, 2014 Ella Deon Ballard
改进 Samba+Kerberos+Winbind 章节.

修订 7.0-4 June 13, 2014 Ella Deon Ballard
添加 Kerberos 域章节.

修订 7.0-3 June 11, 2014 Ella Deon Ballard
初始版本.