Red Hat Enterprise Linux 8

安装身份管理

安装 IdM 服务器和客户端的方法

Last Updated: 2024-07-23

Red Hat Enterprise Linux 8 安装身份管理

安装 IdM 服务器和客户端的方法

法律通告

摘要

根据您的环境，您可以安装 Red Hat Identity Management (IdM)来提供 DNS 和证书颁发机构(CA)服务，或者将 IdM 配置为使用现有的 DNS 和 CA 基础架构。 您可以手动或使用 Ansible Playbook 安装 IdM 服务器、副本和客户端。另外，您可以使用 Kickstart 文件在系统安装过程中自动将客户端加入到 IdM 域中。

目录

对红帽文档提供反馈 6

第 1 章 如何使用本指南 7

部分 I. 安装身份管理 8

第 2 章 为 IDM 服务器安装准备系统 9
2.1. 先决条件 9
2.2. 硬件建议 9
2.3. IDM 的自定义配置要求 9
2.4. FIPS 合规性 11
2.5. 支持启用了 FIPS 模式的跨林信任 12
2.6. IDM 的时间服务要求 12
2.7. IDM 的主机名和 DNS 要求 14
2.8. IDM 的端口要求 18
2.9. 打开 IDM 所需的端口 19
2.10. 安装 IDM 服务器所需的软件包 20
2.11. 为 IDM 安装设置正确的文件模式创建掩码 21
2.12. 确保 FAPOLICYD 规则不会阻止 IDM 安装和操作 22
2.13. IDM 安装命令的选项 22

第 3 章 安装 IDM 服务器：使用集成的 DNS，集成的 CA 作为 ROOT CA 25
3.1. 交互式安装 25
3.2. 非互动安装 27

第 4 章 安装 IDM 服务器：具有集成的 DNS，具有外部 CA 作为根CA 29
4.1. 交互式安装 29
4.2. 故障排除：外部 CA 安装失败 32

第 5 章 安装 IDM 服务器：使用集成的 DNS,没有 CA 34
5.1. 安装没有 CA 的 IDM 服务器所需的证书 34
5.2. 交互式安装 35

第 6 章 安装 IDM 服务器： 在不集成 DNS 的情况，将集成的 CA 作为 ROOT CA 38
6.1. 交互式安装 38
6.2. 非互动安装 39
6.3. 外部 DNS 系统的 IDM DNS 记录 40

第 7 章 安装 IDM 服务器： 在不集成 DNS 的情况下，使用外部 CA 作为 ROOT CA 42
7.1. 安装外部 CA 作为根 CA 的 IDM CA 时使用的选项 42
7.2. 交互式安装 43
7.3. 非互动安装 45
7.4. 外部 DNS 系统的 IDM DNS 记录 47

第 8 章 使用 LDIF 文件中的自定义数据库设置安装 IDM 服务器或副本 48

第 9 章 IDM 服务器安装故障排除 49
9.1. 查看 IDM 服务器安装错误日志 49
9.2. 检查 IDM CA 安装错误 50
9.3. 删除部分 IDM 服务器安装 51
9.4. 其他资源 52

第 10 章 卸载 IDM 服务器 53

第 11 章 重命名 IDM 服务器 56

第 12 章 更新和降级 IDM 57
12.1. 更新 IDM 软件包 57
12.2. 降级 IDM 软件包 57
12.3. 其他资源 57

第 13 章 为 IDM 客户端安装准备系统 58
13.1. 安装 IDM 客户端支持的 RHEL 版本 58
13.2. IDM 客户端的 DNS 要求 58
13.3. IDM 客户端的端口要求 58
13.4. IDM 客户端的 IPV6 要求 58
13.5. 从 IDM:CLIENT 流安装 IDM 客户端软件包 59
13.6. 从 IDM:DL1 流安装 IDM 客户端软件包 59

第 14 章 安装 IDM 客户端 61
14.1. 先决条件 61
14.2. 使用用户凭证安装客户端： 交互式安装 61
14.3. 使用一次性密码安装客户端：交互式安装 62
14.4. 安装客户端： 非互动安装 64
14.5. 安装客户端后删除前 IDM 配置 65
14.6. 测试 IDM 客户端 66
14.7. 在 IDM 客户端安装过程中执行的连接 66
14.8. IDM 客户端在安装后部署过程中与服务器的通信 66
14.9. SSSD 通信模式 67
14.10. CERTMONGER 通讯特征 68

第 15 章 使用 KICKSTART 安装 IDM 客户端 70
15.1. 使用 KICKSTART 安装客户端 70
15.2. 用于客户端安装的 KICKSTART 文件 70
15.3. 测试 IDM 客户端 71

第 16 章 IDM 客户端安装故障排除 72
16.1. 检查 IDM 客户端安装错误 72
16.2. 解决客户端安装无法更新 DNS 记录时的问题 72
16.3. 解决客户端安装无法加入 IDM KERBEROS 域时的问题 73
16.4. 其他资源 74

第 17 章 重新注册 IDM 客户端 75
17.1. IDM 中的客户端重新注册 75
17.2. 使用用户凭证重新注册客户端： 交互式重新注册 75
17.3. 使用 CLIENT KEYTAB: NON-INTERACTIVE REENROLLMENT 重新注册客户端 76
17.4. 测试 IDM 客户端 76

第 18 章 卸载 IDM 客户端 77
18.1. 卸载 IDM 客户端 77
18.2. 卸载 IDM 客户端：在以前的安装后执行额外的步骤 77

第 19 章 重命名 IDM 客户端系统 79
19.1. 准备 IDM 客户端以进行重命名 79
19.2. 卸载 IDM 客户端 79
19.3. 卸载 IDM 客户端：在以前的安装后执行额外的步骤 80
19.4. 重命名主机系统 81
19.5. 重新安装 IDM 客户端 81
19.6. 重新添加服务、重新生成证书和重新添加主机组 82

第 20 章 为 IDM 副本安装准备系统 83

20.1. 副本版本要求 83
20.2. 显示 IDM 软件版本的方法 83
20.3. 授权在 IDM 客户端上安装副本 84
20.4. 授权在未注册到 IDM 的系统上安装副本 85

第 21 章 安装 IDM 副本 87
21.1. 安装带有集成的 DNS 和 CA 的 IDM 副本 87
21.2. 安装带有集成 DNS 且没有 CA 的 IDM 副本 88
21.3. 安装没有集成 DNS 但有 CA 的 IDM 副本 89
21.4. 安装没有集成 DNS 且没有 CA 的 IDM 副本 90
21.5. 安装 IDM 隐藏的副本 91
21.6. 测试 IDM 副本 91
21.7. 在 IDM 副本安装过程中执行的连接 91

第 22 章 IDM 副本安装故障排除 93
22.1. IDM 副本安装错误日志文件 93
22.2. 查看 IDM 副本安装错误 93
22.3. IDM CA 安装错误日志文件 94
22.4. 检查 IDM CA 安装错误 95
22.5. 删除部分 IDM 副本安装 96
22.6. 解决无效凭证错误 97
22.7. 其他资源 98

第 23 章 卸载 IDM 副本 99

第 24 章 在现有 IDM 服务器上安装 DNS 100

第 25 章 从 IDM 服务器卸载集成的 IDM DNS 服务 102

第 26 章 在没有 CA 的部署中将 IDM CA 服务添加到 IDM 服务器 103
26.1. 将第一个 IDM CA 作为 ROOT CA 安装到现有 IDM 域中 103
26.2. 将第一个将外部 CA 作为 ROOT CA 的 IDM CA 安装到现有 IDM 域中 103

第 27 章 在带有 CA 的部署中将 IDM CA 服务添加到 IDM 服务器 105

第 28 章 从 IDM 服务器卸载 IDM CA 服务 106

第 29 章 管理复制拓扑 107
29.1. 解释复制协议、拓扑后缀和拓扑段 107
29.2. 使用拓扑图来管理复制拓扑 109
29.3. 使用 WEB UI 在两台服务器之间设置复制 112
29.4. 使用 WEB UI 停止两个服务器之间的复制 114
29.5. 使用 CLI 在两个服务器之间建立复制 115
29.6. 使用 CLI 停止两个服务器之间的复制 116
29.7. 使用 WEB UI 从拓扑中删除服务器 117
29.8. 使用 CLI 从拓扑中删除服务器 118
29.9. 使用 WEB UI 查看 IDM 服务器上的服务器角色 118
29.10. 使用 CLI 查看 IDM 服务器上的服务器角色 119
29.11. 将副本提升为 CA 续订服务器和 CRL 发布者服务器 120
29.12. 降级或提升隐藏的副本 120

第 30 章 安装并运行 IDM HEALTHCHECK 工具 122
30.1. IDM 中的 HEALTHCHECK 122
30.2. 安装 IDM HEALTHCHECK 123
30.3. 运行 IDM HEALTHCHECK 123
30.4. 其他资源 123

第 31 章 使用 ANSIBLE PLAYBOOK 来安装身份管理服务器 125
31.1. ANSIBLE 及其安装 IDM 的优点 125
31.2. 安装 ANSIBLE-FREEIPA 软件包 125
31.3. 在文件系统中的 ANSIBLE 角色位置 126
31.4. 为带有集成 DNS 和集成 CA 作为根 CA 的部署设置参数 126
31.5. 为带有外部 DNS 和集成 CA 作为根 CA 的部署设置参数 129
31.6. 使用 ANSIBLE PLAYBOOK 将集成 CA 的 IDM 服务器部署为 ROOT CA 131
31.7. 为带有集成 DNS 和外部 CA 作为根 CA 的部署设置参数 132
31.8. 为带有外部 DNS 和外部 CA 作为根 CA 的部署设置参数 135
31.9. 使用 ANSIBLE PLAYBOOK 将外部 CA 部署 IDM 服务器作为 ROOT CA 138
31.10. 使用 ANSIBLE PLAYBOOK 卸载 IDM 服务器 139
31.11. 如果这会导致断开连接的拓扑，请使用 ANSIBLE PLAYBOOK 卸载 IDM 服务器 140
31.12. 其他资源 141

第 32 章 使用 ANSIBLE PLAYBOOK 安装身份管理副本 143
32.1. 指定用于安装 IDM 副本的基础、服务器和客户端变量 143
32.2. 使用 ANSIBLE PLAYBOOK 指定用于安装 IDM 副本的凭证 146
32.3. 使用 ANSIBLE PLAYBOOK 部署 IDM 副本 148
32.4. 使用 ANSIBLE PLAYBOOK 卸载 IDM 副本 148

第 33 章 使用 ANSIBLE PLAYBOOK 安装身份管理客户端 149
33.1. 为自动发现客户端安装模式设置清单文件的参数 149
33.2. 当在客户端安装过程中无法自动发现时设置清单文件的参数 151
33.3. 使用 ANSIBLE PLAYBOOK 进行 IDM 客户端注册的授权选项 153
33.4. 使用 ANSIBLE PLAYBOOK 部署 IDM 客户端 155
33.5. 在 ANSIBLE 中使用一次性密码方法安装 IDM 客户端 155
33.6. ANSIBLE 安装后测试身份管理客户端 157
33.7. 使用 ANSIBLE PLAYBOOK 卸载 IDM 客户端 157

部分 II. 集成 IDM 和 AD 159

第 34 章 在 IDM 和 AD 间安装信任 160
34.1. WINDOWS 服务器支持的版本 160
34.2. 信任如何工作 161
34.3. AD 管理权利 161
34.4. 确保支持 AD 和 RHEL 中的通用加密类型 161
34.5. IDM 和 AD 间的通信所需的端口 163
34.6. 为信任配置 DNS 和域设置 166
34.7. 在活动目录 DNS 域中配置 IDM 客户端 173
34.8. 设置信任 175
34.9. 对设置跨林信任进行故障排除 190
34.10. 对客户端访问其他林中的服务进行故障排除 194
34.11. 使用命令行删除信任 197
34.12. 使用 IDM WEB UI 删除信任 198
34.13. 使用 ANSIBLE 删除信任 200
34.14. 删除对 AD 的信任后删除 ID 范围 201

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

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

第 1 章 如何使用本指南

身份管理(IdM)域包括 IdM 服务器，也称为副本和 IdM 客户端。虽然 安装 IdM 部署 总是以安装主 IdM 服务器开始，但下一个安装步骤的顺序取决于目标拓扑。例如，您可以在安装 IdM 客户端之前或之后安装 IdM 副本。另外，某些 IdM 部署需要 与活动目录的信任，而其他 IdM 部署则不需要。

其他资源

- 规划身份管理

部分 I. 安装身份管理

第 2 章 为 IDM 服务器安装准备系统

以下章节列出了安装身份管理(IdM)服务器的要求。在安装前，请验证您的系统满足这些要求。

2.1. 先决条件

- 您需要 **root** 特权才能在主机上安装身份管理(IdM)服务器。

2.2. 硬件建议

对于性能调整，RAM 是最重要的硬件。请确定您的系统有足够可用 RAM。典型的 RAM 要求是：

- 对于 10,000 个用户和 100 个组：至少 4 GB RAM 和 4 GB 交换（swap）空间
- 对于 100,000 个用户和 50,000 个组：至少 16 GB RAM 和 4 GB swap 空间

对于较大的部署，增加 RAM 比增加磁盘空间更为有效，因为许多数据都存储在缓存中。通常，对于大型部署，添加更多 RAM 会因为有更多的缓存使系统具有更好的性能。

注意

基本用户条目或带有证书的简单主机条目大约是 5-10 kB 大小。

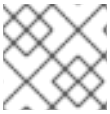
2.3. IDM 的自定义配置要求

在干净的系统上安装身份管理(IdM)服务器，无需为 DNS、Kerberos、Apache 或 Directory Server 等服务进行任何自定义配置。

IdM 服务器安装覆盖了系统文件来设置 IdM 域。IdM 将原始系统文件备份到 **/var/lib/ipa/sysrestore/**。当在生命周期结束时卸载 IdM 服务器时，会恢复这些文件。

IdM 中的 IPv6 要求

IdM 系统必须在内核中启用 IPv6 协议，并且 localhost (::1)能够使用它。如果禁用 IPv6，IdM 服务使用的 CLDAP 插件将无法初始化。



注意

不必在网络中启用 IPv6。如果需要，可以启用 IPv6 堆栈而不启用 IPv6 地址。

支持 IdM 中的加密类型

Red Hat Enterprise Linux (RHEL)使用 Kerberos 协议版本 5，它支持加密类型，如高级加密标准(AES)、Camellia 和数据加密标准(DES)。

支持的加密类型列表

虽然 IdM 服务器和客户端上的 Kerberos 库可能会支持更多的加密类型，但 IdM Kerberos 分发中心(KDC)只支持以下加密类型：

- **aes256-cts:normal**
- **aes256-cts:special** (默认)
- **aes128-cts:normal**

- **aes128-cts:special** （默认）
- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**
- **camellia128-cts-cmac:normal**
- **camellia128-cts-cmac:special**
- **camellia256-cts-cmac:normal**
- **camellia256-cts-cmac:special**

默认禁用 RC4 加密类型

RHEL 8 中已弃用并默认禁用以下 RC4 加密类型，因为它们被视为不如较新的 AES-128 和 AES-256 加密类型安全：

- **arcfour-hmac:normal**
- **arcfour-hmac:special**

有关手动启用 RC4 支持以与旧活动目录环境兼容的更多信息，请参阅 确保在 AD 和 RHEL 中对通用加密类型的支持。

删除了对 DES 和 3DES 加密的支持

由于安全考虑,在 RHEL 7 中弃用了对 DES 算法的支持。RHEL 8.3.0 中最近重新构建的 Kerberos 软件包从 RHEL 8 中删除了对 single-DES(DES)和 triple-DES(3DES)加密类型的支持。

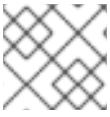
注意

标准 RHEL 8 IdM 安装默认不使用 DES 或 3DES 加密类型，且不受 Kerberos 升级的影响。

如果您手动配置任何服务或用户只使用**DES**或 3DES 加密（例如，对于遗留的客户端），您可能会在升级到最新的 Kerberos 软件包后遇到服务中断，例如：

- Kerberos 验证错误
- **unknown enctype** 加密错误
- 带有 DES 加密数据库主密钥 (**K/M**) 的 KDC 无法启动

红帽建议不要在您的环境中使用 DES 或者 3DES 加密。



注意

如果您将环境配置成了使用DES和3DES加密类型，则只需要禁用它们。

支持 IdM 中系统范围的加密策略

IdM 使用 **DEFAULT** 系统范围的加密策略。此政策为当前威胁模型提供安全设置。它允许 TLS 1.2 和 1.3 协议，以及 IKEv2 和 SSH2 协议。如果 RSA 密钥和 Diffie-Hellman 参数至少是 2048 位，则可以接受它们。此策略不允许 DES、3DES、RC4、DSA、TLS v1.0 和其他较弱的算法。

注意

您不能使用 **FUTURE** 系统范围的加密策略来安装 IdM 服务器。安装 IdM 服务器时，请确保您使用的是 **DEFAULT** 系统范围的加密策略。

其它资源

- 系统范围的加密策略
- man IPV6(7)

2.4. FIPS 合规性

有了 RHEL 8.3.0 或更高版本，您可以在启用了联邦信息处理标准(FIPS) 140 模式的系统上安装新的 IdM 服务器或副本。

要在 FIPS 模式下安装 IdM，首先在主机上启用 FIPS 模式，然后安装 IdM。IdM 安装脚本会检测是否启用了 FIPS，并将 IdM 配置为只使用符合 FIPS 140 标准的加密类型：

- **aes256-cts:normal**
- **aes256-cts:special**
- **aes128-cts:normal**
- **aes128-cts:special**
- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**

要使 IdM 环境符合 FIPS，**所有** IdM 副本都必须启用 FIPS 模式。

红帽建议您在 IdM 客户端中启用 FIPS 模式，特别是如果您可能将这些客户端提升到 IdM 副本。最终，由管理员来决定它们如何满足 FIPS 要求；红帽不强制执行 FIPS 标准。

迁移到符合 FIPS 的 IdM

您无法将现有 IdM 安装从非 FIPS 环境迁移到符合 FIPS 的安装。这不是技术问题，而是法律和监管限制。

要操作符合 FIPS 的系统，必须在 FIPS 模式下创建所有加密密钥资料。另外，加密密钥材料不得离开 FIPS 环境，除非它被安全包装，且永远不会在非 FIPS 环境中解封。

如果您的场景需要将非 FIPS IdM 领域迁移到符合 FIPS 的领域，您必须：

1. 在 FIPS 模式下创建一个新 IdM 领域
2. 使用阻止所有密钥材料的过滤器，从非 FIPS 领域执行到新 FIPS 模式领域的数据迁移

迁移过滤器必须阻止：

- KDC 主密钥、keytab 以及所有相关 Kerberos 密钥材料
- 用户密码
- 所有证书，包括 CA、服务和用户证书
- OTP 令牌
- SSH 密钥和指纹
- DNSSEC KSK 和 ZSK
- 所有 vault 条目
- 与 AD 信任相关的密钥材料

实际上，新的 FIPS 安装是一种不同的安装。即使具有严格的过滤，此类迁移可能无法通过 FIPS 140 认证。您的 FIPS 审核员可能会标记这个迁移。

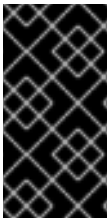
其它资源

- 有关 RHEL 操作系统中 FIPS 140 实现的更多信息，请参阅 *RHEL 安全强化* 文档中的 联邦信息处理标准 140 和 FIPS 模式。

2.5. 支持启用了 FIPS 模式的跨林信任

要在启用了 FIPS 模式的同时建立与 Active Directory(AD)域的跨林信任，您必须满足以下要求：

- IdM 服务器位于 RHEL 8.4.0 或更高版本中。
- 在设置信任时，您必须使用 AD 管理帐户验证。在启用 FIPS 模式时，您无法使用共享 secret 建立信任。



重要

RADIUS 身份验证不符合 FIPS，因为 RADIUS 协议使用 MD5 哈希函数来在客户端和服务器之间加密密码，在 FIPS 模式下，OpenSSL 禁用 MD5 摘要算法的使用。但是，如果 RADIUS 服务器与 IdM 服务器运行在同一台主机上，您可以临时解决这个问题，并通过执行 如何在 FIPS 模式中配置 FreeRADIUS 身份验证 中描述的步骤来启用 MD5 。

其它资源

- 有关在 RHEL 操作系统中 FIPS 模式的更多信息，请参阅 *安全强化* 文档中的 在 FIPS 模式下安装系统。
- 有关 FIPS 140-2 标准的详情，请查看国家标准与技术研究院(NIST)网站上的 加密模块的安全要求 。

2.6. IDM 的时间服务要求

以下章节讨论了使用 **chronyd** 来使 IdM 主机与中央时间源同步：

2.6.1. IdM 如何使用 chronyd 进行同步

您可以使用 **chronyd** 使 IdM 主机与中央时间源同步，如下所述。

Kerberos 是 IdM 中的底层验证机制，使用时间戳作为其协议的一部分。如果 IdM 客户端的系统时间与密钥发布中心(KDC)的系统时间相差超过 5 分钟，则 Kerberos 身份验证会失败。

为确保 IdM 服务器和客户端与中央时间源同步，IdM 安装脚本会自动配置 **chronyd** 网络时间协议(NTP)客户端软件。

如果您没有将任何 NTP 选项传给 IdM 安装命令，安装程序将搜索指向网络中 NTP 服务器的 **_ntp._udp** DNS 服务(SRV)记录，并使用该 IP 地址配置 **chrony**。如果您没有任何 **_ntp._udp** SRV 记录，**chronyd** 会使用 **chrony** 软件包提供的配置。

注意

因为 **ntpd** 在RHEL 8 中已被弃用，取而代之的是 **chronyd**，所以 IdM 服务器不再被配置为网络时间协议(NTP)服务器，只被配置为 NTP 客户端。RHEL 7 **NTP 服务器** IdM 服务器角色在 RHEL 8 中也已被弃用。

其他资源

- NTP 的实现
- 使用 Chrony 套件配置 NTP

2.6.2. IdM 安装命令的 NTP 配置选项列表

您可以使用 **chronyd** 使 IdM 主机与中央时间源同步。

您可以在任何 IdM 安装命令（**ipa-server-install**、**ipa-replica-install**、**ipa-client-install**）中指定以下选项来在设置过程中配置 **chronyd** 客户端软件。

表 2.1. IdM 安装命令的 NTP 配置选项列表

选项	行为
--ntp-server	使用它指定一个 NTP 服务器。您可以多次使用它来指定多个服务器。
--ntp-pool	使用它指定一个解析为主机名的多个 NTP 服务器池。
-N,--no-ntp	不要配置、启动或启用 **chronyd**。

其他资源

- NTP 的实现
- 使用 Chrony 套件配置 NTP

2.6.3. 确保 IdM 可以引用您的 NTP 时间服务器

此流程验证您是否具有必要的配置，以便 IdM 能够与您的网络时间协议(NTP)时间服务器同步。

先决条件

- 您已在环境中配置了 NTP 时间服务器。在本例中，之前配置的时间服务器的主机名为 **ntpserver.example.com**。

流程

1. 对您环境中的 NTP 服务器执行 DNS 服务(SRV)记录搜索。

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

2. 如果之前的 **dig** 搜索没有返回您的时间服务器，请添加一个指向时间服务器 **123** 端口的 **_ntp._udp** SRV 记录。这个过程取决于您的 DNS 解决方案。

验证步骤

- 在您执行搜索 **_ntp._udp** SRV 记录时，DNS 验证您的时间服务器的 **123** 端口是否返回一条记录。

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

其他资源

- NTP 的实现
- 使用 Chrony 套件配置 NTP

2.6.4. 其他资源

- NTP 的实现
- 使用 Chrony 套件配置 NTP

2.7. IDM 的主机名和 DNS 要求

以下概述了服务器和副本系统的主机名和 DNS 要求，以及如何验证系统是否满足要求。

这些要求适用于所有身份管理(IdM)服务器，以及那些带有集成 DNS 的服务器和没有集成 DNS 的服务器。

警告

DNS 记录对于几乎所有 IdM 域功能至关重要，包括运行 LDAP 目录服务、Kerberos 和 Active Directory 集成。请非常小心，并确保：

- 您有一个经过测试且可以正常工作的 DNS 服务
- 该服务已被正确配置

这个要求适用于带有**和**不带有集成 DNS 的 IdM 服务器。

验证服务器主机名

主机名必须是完全限定域名，如 ***server.idm.example.com***。

重要

不要使用单标签域名，例如 **.company**：IdM 域必须由一个或多个子域和一个顶级域组成，如 **example.com** 或 **company.example.com** 。

完全限定域名必须满足以下条件：

- 它是一个有效的 DNS 名称，即只允许数字、字母字符和连字符(-)。主机名中的其他字符（如下划线(_)）会导致 DNS 失败。
- 都是小写。不允许使用大写字母。
- 它无法解析回送地址。它必须解析系统的公共 IP 地址，而不是 **127.0.0.1**。

要验证主机名，在您要安装的系统中使用 **hostname** 工具：

```
# hostname
server.idm.example.com
```

hostname 的输出不能是 **localhost** 或 **localhost6**。

验证转发和反向 DNS 配置

1. 获取服务器的 IP 地址。

   a. **ip addr show** 命令显示 IPv4 和 IPv6 地址。在以下示例中，相关的 IPv6 地址为 **2001:DB8::1111**，因为其范围是全局的：

```
[root@server ~]# ip addr show
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
 link/ether 00:1a:4a:10:4e:33 brd ff:ff:ff:ff:ff:ff
 inet 192.0.2.1/24 brd 192.0.2.255 scope global dynamic eth0
  valid_lft 106694sec preferred_lft 106694sec
 inet6 2001:DB8::1111/32 scope global dynamic
```

```
    valid_lft 2591521sec preferred_lft 604321sec
 inet6 fe80::56ee:75ff:fe2b:def6/64 scope link
       valid_lft forever preferred_lft forever
...
```

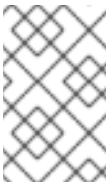
2. 使用 **dig** 工具证正向 DNS 配置。

   a. 运行 **dig +short *server.idm.example.com* A** 命令。返回的 IPv4 地址必须与 **ip addr show** 返回的 IP 地址匹配：

```
[root@server ~]# dig +short server.idm.example.com A
192.0.2.1
```

   b. 运行 **dig +short *server.idm.example.com* AAAA** 命令。如果返回一个地址，它必须与 **ip addr show** 返回的 IPv6 地址匹配：

```
[root@server ~]# dig +short server.idm.example.com AAAA
2001:DB8::1111
```



注意

如果 **dig** 没有返回 AAAA 记录的任何输出，那么这并不表示配置不正确。没有输出只表示系统在 DNS 中没有配置 IPv6 地址。如果您不打算在网络中使用 IPv6 协议，则可以继续进行安装。

3. 验证反向 DNS 配置（PTR 记录）。使用 **dig** 工具并添加 IP 地址。
   如果以下命令显示不同的主机名或没有主机名，则反向 DNS 配置不正确。

   a. 运行 **dig +short -x *IPv4_address*** 命令。输出必须显示服务器主机名。例如：

```
[root@server ~]# dig +short -x 192.0.2.1
server.idm.example.com
```

   b. 如果上一步中的 **dig +short -x *server.idm.example.com* AAAA** 命令返回 IPv6 地址，请使用 **dig** 查询 IPv6 地址。输出必须显示服务器主机名。例如：

```
[root@server ~]# dig +short -x 2001:DB8::1111
server.idm.example.com
```

注意

如果上一步中的 **dig +short *server.idm.example.com* AAAA** 没有显示任何 IPv6 地址，则查询 AAAA 记录不会输出任何内容。在这种情况下，这是正常的行为，不代表配置不正确。

警告

如果反向 DNS（PTR 记录）搜索返回多个主机名，那么 **httpd** 和其他与 IdM 关联的软件可能会显示无法预测的行为。红帽强烈建议每个 IP 只配置一个 PTR 记录。

验证 DNS 正向解析器的标准合规性（仅集成DNS需要）

确保您要与 IdM DNS 服务器一起使用的所有 DNS 正向解析器均符合 DNS(EDNS0)扩展机制和 DNS 安全扩展扩展(DNSSEC)标准。要做到这一点，请分别检查每个正向解析器的以下命令的输出：

```
$ dig +dnssec @IP_address_of_the_DNS_forwarder . SOA
```

命令显示的预期输出包含以下信息：

- 状态：**NOERROR**
- 标记：**ra**
- EDNS 标志：**do**
- **RRSIG** 记录必须在 **ANSWER** 部分中存在

如果输出中缺少任何这些项，请检查您的 DNS 正向解析器文档，验证是否支持并启用了 EDNS0 和 DNSSEC。在最新版本的 BIND 服务器中，**dnssec-enable yes；** 选项必须在 **/etc/named.conf** 文件中设置。

dig 生成的预期输出示例：

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48655
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; ANSWER SECTION:
. 31679 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2015100701 1800 900 604800 86400
. 31679 IN RRSIG SOA 8 0 86400 20151017170000 20151007160000 62530 . GNVz7SQs [...]
```

验证 /etc/hosts 文件

验证 **/etc/hosts** 文件是否满足以下条件之一：

- 该文件不包含主机的条目。它只列出主机的 IPv4 和 IPv6 localhost 条目。
- 该文件包含主机条目，并且文件满足以下所有条件：
  - 前两个条目是 IPv4 和 IPv6 localhost 条目。
  - 下一个条目指定 IdM 服务器 IPv4 地址和主机名。
  - IdM 服务器的 **FQDN** 位于 IdM 服务器的短名称之前。

- IdM 服务器主机名不是 localhost 条目的一部分。

以下是正确配置的 **/etc/hosts** 文件示例：

```
127.0.0.1   localhost localhost.localdomain \
localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain \
localhost6 localhost6.localdomain6
192.0.2.1 server.idm.example.com server
2001:DB8::1111 server.idm.example.com server
```

2.8. IDM 的端口要求

身份管理(IdM)使用多个端口 来与其服务进行通信。这些端口必须是开放的，并可用于 IdM 服务器的传入连接，这样 IdM 才能工作。。它们目前不被其他服务使用，或者被 防火墙 阻止。

表 2.2. IdM 端口

端口	端口	协议
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP 和 UDP
DNS	53	TCP 和 UDP（可选）

注意

IdM 使用端口 80 和 389。这是一种安全的做法，因为以下保障措施：

- IdM 通常将到达端口 80 的请求重定向到端口 443。端口 80(HTTP)仅用于提供在线证书状态协议(OCSP)响应和证书撤销列表(CRL)。两者均是数字签名的，因此可防止中间人攻击。
- 端口 389(LDAP)使用 STARTTLS 和通用安全服务 API(GSSAPI)进行加密。

此外，端口 8080、8443 和 749 必须是空闲的，因为它们在内部使用。不要打开这些端口，保持让防火墙阻止它们。

表 2.3. firewalld 服务

服务名称	详情请查看：
freeipa-ldap	**/usr/lib/firewalld/services/freeipa-ldap.xml**
freeipa-ldaps	**/usr/lib/firewalld/services/freeipa-ldaps.xml**

服务名称	详情请查看：
dns	**/usr/lib/firewalld/services/dns.xml**

2.9. 打开 IDM 所需的端口

流程

1. 验证 **firewalld** 服务是否正在运行。
   - 查看 **firewalld** 当前是否正在运行：

     ```
     # systemctl status firewalld.service
     ```

   - 启动 **firewalld** 并将其配置为在系统引导时自动启动：

     ```
     # systemctl start firewalld.service
     # systemctl enable firewalld.service
     ```

2. 使用 **firewall-cmd** 工具打开所需的端口。选择以下选项之一：
   a. 使用 **firewall-cmd --add-port** 命令在防火墙中添加各个端口。例如，要在默认区中打开端口：

      ```
      # firewall-cmd --permanent --add-port=
      {80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp}
      ```

   b. 使用 **firewall-cmd --add-service** 命令在防火墙中添加 **firewalld** 服务。例如，要在默认区中打开端口：

      ```
      # firewall-cmd --permanent --add-service={freeipa-4,dns}
      ```

      有关使用 **firewall-cmd** 开放系统上端口的详情，请参考 **firewall-cmd**(1)手册页。

3. 重新载入 **firewall-cmd** 配置以确保修改立即生效：

   ```
   # firewall-cmd --reload
   ```

   请注意，在生产环境的系统上重新载入 **firewalld** 可能会导致 DNS 连接超时。如果需要，为了避免超时的风险并在运行的系统上永久保留修改，请使用 **firewall-cmd** 命令的 **--runtime-to-permanent** 选项，例如：

   ```
   # firewall-cmd --runtime-to-permanent
   ```

验证

- 登录客户端子网上的主机，并使用 **nmap** 或 **nc** 实用程序连接到打开的端口或运行端口扫描。
  - 例如，要扫描 TCP 流量所需的端口：

    ```
    $ nmap -p 80,443,389,636,88,464,53 server.idm.example.com
    ```

```
[...]
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
88/tcp  open  kerberos-sec
389/tcp open  ldap
443/tcp open  https
464/tcp open  kpasswd5
636/tcp open  ldapssl
```

- 扫描 UDP 流量所需的端口：

```
# nmap -sU -p 88,464,53 server.idm.example.com
[...]
PORT    STATE         SERVICE
53/udp  open          domain
88/udp  open|filtered kerberos-sec
464/udp open|filtered kpasswd5
```

注意

您还必须为传入和传出流量打开基于网络的防火墙。

2.10. 安装 IDM 服务器所需的软件包

在 RHEL8 中，安装身份管理(IdM)服务器所需的软件包作为模块提供。IdM 服务器模块流称为 **DL1** 流，您需要先启用这个流，然后才能从此流下载软件包。以下流程演示了如何下载设置您选择的 IdM 环境所需的软件包。

先决条件

- 您有一个新安装的 RHEL 系统。
- 您已提供所需的软件仓库：
  - 如果您的 RHEL 系统不是在云中运行，您已将您的系统注册到 Red Hat Subscription Manager(RHSM)。详情请参阅 订阅管理器命令行中的注册、附加和删除订阅。您还可以启用 IdM 使用的 **BaseOS** 和 **AppStream** 软件仓库：

```
# subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms
# subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms
```

    有关如何使用 RHSM 启用和禁用特定存储库的详情，请参考 红帽订阅管理器中的配置选项。

  - 如果您的 RHEL 系统在云中运行请跳过注册。所需的软件仓库已通过 Red Hat Update Infrastructure(RHUI)提供。
- 您之前还没有启用 IdM 模块流。

流程

1. 启用 **idm:DL1** 流：

```
# yum module enable idm:DL1
```

2. 切换到通过 **idm:DL1** 流提供的 RPM：

```
# yum distro-sync
```

3. 根据您的 IdM 要求选择以下选项之一：

- 要下载在没有集成 DNS 的情况下安装 IdM 服务器所需的软件包：

```
# yum module install idm:DL1/server
```

- 要下载安装带有集成 DNS 的 IdM 服务器所需的软件包：

```
# yum module install idm:DL1/dns
```

- 要下载安装与 Active Directory 具有信任协议的 IdM 服务器所需的软件包：

```
# yum module install idm:DL1/adtrust
```

- 要从多个配置集下载软件包，如 **adtrust** 和 **dns** 配置集：

```
# yum module install idm:DL1/{dns,adtrust}
```

- 要下载安装 IdM 客户端所需的软件包：

```
# yum module install idm:DL1/client
```

重要

当您启用了其他流并从中下载软件包后，当切换到新的模块流时，需要首先明确删除所有安装的相关内容，并在启用新模块流前禁用当前模块流。在不禁用当前流的情况下尝试启用新流会导致错误。有关如何继续操作的详情，请参阅 切换到以后的流。

警告

虽然可以从模块单独安装软件包，但请注意，如果您安装的任何软件包来自于未列为该模块"API"的模块，则该软件包只能在该模块的上下文中被红帽所支持。例如，如果您直接从存储库安装 **bind-dyndb-ldap**，以用于自定义 389 目录服务器设置，则您遇到的任何问题都会被忽略，除非 IdM 也出现这些问题。

2.11. 为 IDM 安装设置正确的文件模式创建掩码

身份管理(IdM)安装过程要求将 **root** 帐户的文件模式创建掩码(**umask**)设为 **0022**。这允许除了 **root** 之外的用户可以读取在安装过程中创建的文件。如果设置了不同的 **umask**，IdM 服务器的安装会显示一个警告。如果继续安装，则服务器的一些功能将无法正常工作。例如，您无法从这个服务器安装 IdM 副本。安装后，您可以将 **umask** 设回其原始值。

先决条件

- 您有 **root** 特权。

流程

1. （可选）显示当前的 **umask** ：

```
# umask
0027
```

2. 将 **umask** 设为 **0022** ：

```
# umask 0022
```

3. （可选）在 IdM 安装完成后，将 **umask** 设回其原始值：

```
# umask 0027
```

2.12. 确保 FAPOLICYD 规则不会阻止 IDM 安装和操作

如果您在 RHEL 主机上使用 **fapolicyd** 软件框架来根据用户定义的策略控制应用程序的执行，则身份管理(IdM)服务器的安装会失败。由于安装和操作需要 Java 程序成功完成，因此，请确保 Java 和 Java 类没有被任何 **fapolicyd** 规则阻止。

如需更多信息，请参阅 导致 IdM 安装失败的 fapolicy 限制 KCS 解决方案。

2.13. IDM 安装命令的选项

ipa-server-install、**ipa-replica-install**、**ipa-dns-install** 和 **ipa-ca-install** 等命令有大量的选项，您可以用来为交互式安装提供额外的信息。您还可以使用这些选项来编写无人值守的安装脚本。

下表显示了不同组件的一些最常见的选项。特定组件的选项可在多个命令间共享。例如，您可以在 **ipa-ca-install** 和 **ipa-server-install** 命令中使用 **--ca-subject** 选项。

有关选项的详细列表，请查看 **ipa-server-install(1)**、**ipa-replica-install(1)**、**ipa-dns-install (1)** 和 **ipa-ca-install (1)** 手册页。

表 2.4. 常规选项：用于 ipa-server-install 和 ipa-replica-install

参数	描述
-d,--debug	启用 debug 日志记录来获得更详细的输出。
-u,--unattended	启用不提示用户输入的无人值守安装会话。
--hostname=*server.idm.example.com*	IdM 服务器机器的完全限定域名。只允许数字、小写字符和连字符(-)。
--ip-address *127.0.0.1*	指定服务器的 IP 地址。这个选项只接受与本地接口关联的 IP 地址。

参数	描述
--dirsrv-config-file *<LDIF_file_name>*	用于修改目录服务器实例配置的 LDIF 文件的路径。
-n *example.com*	用于 IdM 域的 LDAP 服务器域名。这通常基于 IdM 服务器的主机名。
-p *<directory_manager_password>*	LDAP 服务的超级用户 **cn=Directory Manager** 的密码。
-a *<ipa_admin_password>*	**admin** IdM 管理员帐户用于向 Kerberos 域进行身份验证的密码。对于 **ipa-replica-install**，改为使用 **-w**。
-r *<KERBEROS_REALM_NAME>*	为 IdM 域创建的 Kerberos 域的名称为大写，如 **EXAMPLE.COM**。对于 **ipa-replica-install**，这指定了现有 IdM 部署的 Kerberos 领域的名称。
--setup-dns	告知安装脚本在 IdM 域中设置 DNS 服务。
--setup-ca	在此副本上安装和配置 CA。如果没有配置 CA，证书操作将转发给安装了 CA 的另一个副本。对于 **ipa-server-install**，CA 被默认安装了，您不需要使用这个选项。

表 2.5. CA 选项：用于 **ipa-ca-install** 和 **ipa-server-install**

参数	描述
--ca-subject=*<SUBJECT>*	指定 CA 证书主题可辨识名称（默认为： CN=Certificate Authority,O=REALM.NAME）。相对可辨识名称(RDN)采用 LDAP 顺序，首先是最特定的 RDN。
--subject-base=*<SUBJECT>*	指定 IdM 发布的证书的主题基础（默认 O=REALM.NAME）。相对可辨识名称(RDN)采用 LDAP 顺序，首先是最特定的 RDN。
--external-ca	生成要由外部 CA 签名的证书签名请求。
--ca-signing-algorithm=*<ALGORITHM>*	指定 IdM CA 证书的签名算法。可能的值为 SHA1withRSA, SHA256withRSA, SHA512withRSA。默认值为 SHA256withRSA。如果外部 CA 不支持默认的签名算法，请将这个选项与 **--external-ca** 一起使用。

表 2.6. DNS 选项：在使用 **--setup-dns** 时，用于 **ipa-dns-install** 或 **ipa-server-install** 和 **ipa-replica-install**

参数	描述

参数	描述
--forwarder=*192.0.2.1*	指定要与 DNS 服务一起使用的 DNS 转发器。要指定多个转发器，请多次使用这个选项。
--no-forwarders	使用带有 DNS 服务而不是转发器的 root 服务器。
--no-reverse	设置 DNS 域时，不要创建反向 DNS 区域。如果已经配置了反向 DNS 区域，则使用现有的反向 DNS 区域。 如果没有使用这个选项，则默认值为 **true**。这指示安装脚本配置反向 DNS。

其他资源

- **ipa-server-install(1)** 手册页
- **ipa-replica-install(1)**手册页
- **ipa-dns-install(1)** 手册页
- **ipa-ca-install(1)** 手册页

第 3 章 安装 IDM 服务器：使用集成的 DNS，集成的 CA 作为 ROOT CA

安装带有集成 DNS 的新的身份管理(IdM)服务器有以下优点：

- 您可以使用原生 IdM 工具自动执行大多数维护和 DNS 记录管理。例如：在设置过程中自动创建 DNS SRV 记录，之后会自动更新。
- 您可以在安装 IdM 服务器过程中为稳定的外部互联网连接配置全局转发器。全局转发器对 Active Directory 的信任也很有用。
- 您可以设置 DNS 反向区域，以防止来自您的域的电子邮件被 IdM 域之外的电子邮件服务器视为垃圾邮件。

安装带有集成 DNS 的 IdM 有一定的限制：

- IdM DNS 并不意味着用作通用的 DNS 服务器。不支持某些高级 DNS 功能。如需更多信息，请参阅 IdM 服务器中提供的 DNS 服务。

本章描述了如何安装带有集成证书颁发机构(CA)作为根 CA的新 IdM 服务器。

注意

ipa-server-install 命令的默认配置是集成的 CA 作为根CA。如果没有 CA 选项，如指定了 **--external-ca** 或 **--ca-less**，则 IdM 服务器将安装为带有集成的 CA。

3.1. 交互式安装

在使用 **ipa-server-install** 工具进行交互式安装过程中，您需要提供系统的基本配置，如 realm、管理员的密码和目录管理器的密码。

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

流程

1. 运行 **ipa-server-install** 工具程序。

```
# ipa-server-install
```

2. 此脚本提示配置集成的 DNS 服务。输入 **yes**。

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

3. 该脚本提示输入一些必需的设置，并在括号中提供推荐的默认值。
   - 要接受默认值，请按 **Enter** 键。
   - 要提供自定义值，请输入所需的值。

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

警告

仔细规划这些名称。安装完成后您将无法更改它们。

4. 输入目录服务器超级用户(**cn=Directory Manager**)以及身份管理(IdM)管理系统用户帐户(**admin**)的密码。

```
Directory Manager password:
IPA admin password:
```

5. 脚本提示每台服务器的 DNS 转发器。

```
Do you want to configure DNS forwarders? [yes]:
```

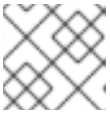
- 要配置每台服务器的 DNS 转发器，请输入 **yes**，然后按照命令行中的说明操作。安装过程会将转发器 IP 地址添加到 IdM LDAP。
  - 有关正向解析策略的默认设置，请查看 **ipa-dns-install**(1)手册页中的 **--forward-policy** 描述。
- 如果您不想使用 DNS 正向解析，请输入 **no**。
  如果没有 DNS 转发器，您 IdM 域中的主机将不能解析来自基础架构中其他的、内部的、DNS 域的名称。主机将只剩下公共 DNS 服务器来解析其 DNS 查询。

6. 脚本会提示检查是否需要配置与服务器关联的 IP 地址的任何 DNS 反向(PTR)记录。

```
Do you want to search for missing reverse zones? [yes]:
```

如果您运行搜索并发现丢失了反向区，脚本会询问您是否创建反向区以及 PTR 记录。

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```



注意

使用 IdM 管理反向区是可选的。您可以改为使用外部 DNS 服务来实现这一目的。

7. 输入 **yes** 以确认服务器配置。

```
Continue to configure the system with these values? [no]: yes
```

8. 安装脚本现在配置服务器。等待操作完成。

9. 安装脚本完成后，使用以下方法更新您的 DNS 记录：

   a. 将父域中的 DNS 委托程序添加到 IdM DNS 域。例如，如果 IdM DNS 域是 ***idm.example.com***，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

重要

每次安装 IdM DNS 服务器后都会重复这个步骤。

b. 将时间服务器的 **_ntp._udp** 服务(SRV)记录添加到您的 IdM DNS。IdM DNS 中新安装的 IdM 服务器的时间服务器的 SRV 记录可确保将来的副本和客户端安装会自动配置为与此主 IdM 服务器使用的时间服务器同步。

3.2. 非互动安装

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

流程

1. 使用选项运行 **ipa-server-install** 程序来提供所有所需信息。非互动安装的最低所需选项是：

   - **--realm** 提供 Kerberos 领域名
   - **--ds-password** 为目录管理者(DM)（目录服务器超级用户）提供密码
   - **--admin-password** 为 **admin**（身份管理(IdM)管理员）提供密码
   - **--unattended**，让安装进程为主机名和域名选择默认选项

   要安装使用集成 DNS 的服务器，还要添加以下选项：

   - **--setup-dns** 用于配置集成 DNS
   - **--forwarder** 或 **--no-forwarders**，取决于您是否要配置 DNS 正向解析器
   - **--auto-reverse** 或 **--no-reverse**，取决于您是否要配置在 IdM DNS 中创建的反向 DNS 区域的自动检测，或者不需要反向区域自动检测

   例如：

   ```
   # ipa-server-install --realm IDM.EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended --setup-dns --forwarder 192.0.2.1 --no-reverse
   ```

2. 安装脚本完成后，使用以下方法更新您的 DNS 记录：

   a. 将父域中的 DNS 委托程序添加到 IdM DNS 域。例如，如果 IdM DNS 域是 ***idm.example.com***，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

重要

每次安装 IdM DNS 服务器后都会重复这个步骤。

   b. 将时间服务器的 **_ntp._udp** 服务(SRV)记录添加到您的 IdM DNS。IdM DNS 中新安装的 IdM 服务器的时间服务器的 SRV 记录可确保将来的副本和客户端安装会自动配置为与此主 IdM 服务器使用的时间服务器同步。

其他资源

- 如需 ipa-server-install 接受的选项的完整列表，请运行 **ipa-server-install --help** 命令。

第 4 章 安装 IDM 服务器：具有集成的 DNS，具有外部 CA 作为根 CA

安装带有集成 DNS 的新的身份管理(IdM)服务器有以下优点：

- 您可以使用原生 IdM 工具自动执行大多数维护和 DNS 记录管理。例如：在设置过程中自动创建 DNS SRV 记录，之后会自动更新。
- 您可以在安装 IdM 服务器过程中为稳定的外部互联网连接配置全局转发器。全局转发器对 Active Directory 的信任也很有用。
- 您可以设置 DNS 反向区域，以防止来自您的域的电子邮件被 IdM 域之外的电子邮件服务器视为垃圾邮件。

安装带有集成 DNS 的 IdM 有一定的限制：

- IdM DNS 并不意味着用作通用的 DNS 服务器。不支持某些高级 DNS 功能。如需更多信息，请参阅 IdM 服务器中提供的 DNS 服务。

本章描述了如何安装具有外部证书颁发机构(CA)作为根CA的新 IdM 服务器。

4.1. 交互式安装

在使用 **ipa-server-install** 工具进行交互式安装过程中，您需要提供系统的基本配置，如 realm、管理员的密码和目录管理器的密码。

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

按照以下流程安装服务器：

- 带有集成的 DNS
- 使用外部证书颁发机构（CA）作为 root CA

先决条件

- 您已确定了要通过 **--external-ca-type** 选项指定的外部 CA 的类型。详情请查看 **ipa-server-install**(1)手册页。
- 如果您使用 Microsoft Certificate Services 证书颁发机构(MS CS CA)作为外部 CA：您已确定要通过 **--external-ca-profile** 选项指定的证书配置文件或模板。默认情况下使用 **SubCA** 模板。有关 **--external-ca-type** 和 **--external-ca-profile** 选项的更多信息，请参阅 在安装外部 CA 作为根 CA 的 IdM CA 时使用的选项。

流程

1. 使用 **--external-ca** 选项来运行 ipa-server-install 工具。

```
# ipa-server-install --external-ca
```

   - 如果您使用 Microsoft 证书服务(MS CS) CA，还使用 **--external-ca-type** 选项，并可选使用 **--external-ca-profile** 选项：

```
[root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --
external-ca-profile=<oid>/<name>/default
```

- 如果您没有使用 MS CS 为 IdM CA 生成签名证书，则不需要其他选项：

```
# ipa-server-install --external-ca
```

2. 此脚本提示配置集成的 DNS 服务。输入 **yes** 或 **no**。在此过程中，我们安装了带有集成 DNS 的服务器。

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

注意

如果您要安装没有集成 DNS 的服务器，安装脚本将不会提示您进行 DNS 配置，如下面步骤所述。如需了解安装没有 DNS 的服务器的步骤的详情，请参阅 *第 6 章 安装 IdM 服务器：在不集成 DNS 的情况，将集成的 CA 作为 root CA* 。

3. 该脚本提示输入一些必需的设置，并在括号中提供推荐的默认值。

- 要接受默认值，请按 **Enter** 键。
- 要提供自定义值，请输入所需的值。

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

警告

仔细规划这些名称。安装完成后您将无法更改它们。

4. 输入目录服务器超级用户(**cn=Directory Manager**)以及身份管理(IdM)管理系统用户帐户(**admin**)的密码。

```
Directory Manager password:
IPA admin password:
```

5. 脚本提示每台服务器的 DNS 转发器。

```
Do you want to configure DNS forwarders? [yes]:
```

- 要配置每台服务器的 DNS 转发器，请输入 **yes**，然后按照命令行中的说明操作。安装过程会将转发器 IP 地址添加到 IdM LDAP。
  - 有关正向解析策略的默认设置，请查看 **ipa-dns-install**(1)手册页中的 **--forward-policy** 描述。

- 如果您不想使用 DNS 正向解析，请输入 **no**。
  如果没有 DNS 转发器，您 IdM 域中的主机将不能解析来自基础架构中其他的、内部的、DNS 域的名称。主机将只剩下公共 DNS 服务器来解析其 DNS 查询。

6. 脚本会提示检查是否需要配置与服务器关联的 IP 地址的任何 DNS 反向(PTR)记录。

```
Do you want to search for missing reverse zones? [yes]:
```

如果您运行搜索并发现丢失了反向区，脚本会询问您是否创建反向区以及 PTR 记录。

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

注意

使用 IdM 管理反向区是可选的。您可以改为使用外部 DNS 服务来实现这一目的。

7. 输入 **yes** 以确认服务器配置。

```
Continue to configure the system with these values? [no]: yes
```

8. 在证书系统实例配置过程中，该工具会打印证书签名请求(CSR)的位置： **/root/ipa.csr**:

```
...

Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
  [1/8]: creating certificate server user
  [2/8]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-install as:
/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
```

当发生这种情况时：

a. 将位于 **/root/ipa.csr** 中的 CSR 提交给外部 CA。这个过程根据要用作外部 CA 的服务的不同而有所不同。

b. 在基础 64 编码 blob 中检索颁发的证书和颁发 CA 的 CA 证书链（Windows CA 的 PEM 文件或 Base_64 证书）。同样，不同的证书服务的进程会有所不同。通常，网页或通知电子邮件中的下载链接允许管理员下载所有需要的证书。

重要

确保获取 CA 的完整证书链，而不只是 CA 证书。

c. 再次运行 **ipa-server-install**，这次指定新发布的 CA 证书和 CA 链文件的位置和名称。例如：

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-
file=/tmp/cacert.pem
```

9. 安装脚本现在配置服务器。等待操作完成。

10. 安装脚本完成后，使用以下方法更新您的 DNS 记录：

    a. 将父域中的 DNS 委托程序添加到 IdM DNS 域。例如，如果 IdM DNS 域是 ***idm.example.com***，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

    重要

    每次安装 IdM DNS 服务器后都会重复这个步骤。

    b. 将时间服务器的 **_ntp._udp** 服务(SRV)记录添加到您的 IdM DNS。IdM DNS 中新安装的 IdM 服务器的时间服务器的 SRV 记录可确保将来的副本和客户端安装会自动配置为与此主 IdM 服务器使用的时间服务器同步。

注意

ipa-server-install --external-ca 命令有时可能会失败，并显示以下错误：

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s
CA -f /tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

当设置 ***_proxy** 环境变量时，会发生此失败。有关此问题的解决方案，请参阅 故障排除：外部 CA 安装失败。

4.2. 故障排除：外部 CA 安装失败

ipa-server-install --external-ca 命令失败并显示以下错误：

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f
/tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

env|grep proxy 命令显示如下变量：

```
# env|grep proxy
http_proxy=http://example.com:8080
ftp_proxy=http://example.com:8080
https_proxy=http://example.com:8080
```

这**意味着：**
***_proxy** 环境变量会阻止安装服务器。

解决此问题：

1. 使用以下 shell 脚本取消设置 ***_proxy** 环境变量：

```
# for i in ftp http https; do unset ${i}_proxy; done
```

2. 运行 **pkidestroy** 工具来删除失败的证书颁发机构(CA)子系统的安装：

```
# pkidestroy -s CA -i pki-tomcat; rm -rf /var/log/pki/pki-tomcat /etc/sysconfig/pki-
tomcat /etc/sysconfig/pki/tomcat/pki-tomcat /var/lib/pki/pki-tomcat /etc/pki/pki-tomcat
/root/ipa.csr
```

3. 删除失败的身份管理(IdM)服务器的安装：

```
# ipa-server-install --uninstall
```

4. 重新运行 **ipa-server-install --external-ca**。

第 5 章 安装 IDM 服务器：使用集成的 DNS,没有 CA

安装带有集成 DNS 的新的身份管理(IdM)服务器有以下优点：

- 您可以使用原生 IdM 工具自动执行大多数维护和 DNS 记录管理。例如：在设置过程中自动创建 DNS SRV 记录，之后会自动更新。
- 您可以在安装 IdM 服务器过程中为稳定的外部互联网连接配置全局转发器。全局转发器对 Active Directory 的信任也很有用。
- 您可以设置 DNS 反向区域，以防止来自您的域的电子邮件被 IdM 域之外的电子邮件服务器视为垃圾邮件。

安装带有集成 DNS 的 IdM 有一定的限制：

- IdM DNS 并不意味着用作通用的 DNS 服务器。不支持某些高级 DNS 功能。如需更多信息，请参阅 IdM 服务器中提供的 DNS 服务。

本章描述了如何安装没有证书颁发机构(CA)的新 IdM 服务器。

5.1. 安装没有 CA 的 IDM 服务器所需的证书

您需要提供安装没有证书颁发机构(CA)的身份管理(IdM)服务器所需的证书。通过使用描述的命令行选项，您可以将这些证书提供给 **ipa-server-install** 工具。

重要

您不能使用自签名的第三方服务器证书来安装服务器或副本，因为导入的证书文件必须包含签发 LDAP 和 Apache 服务器证书的 CA 的完整 CA 证书链。

LDAP 服务器证书和私钥

- **--dirsrv-cert-file** 用于 LDAP 服务器证书的证书和私钥文件
- **--dirsrv-pin** 用于访问 **--dirsrv-cert-file**中指定的文件中的私钥的密码

Apache 服务器证书和私钥

- **--http-cert-file** 用于 Apache 服务器证书的证书和私钥文件
- **--http-pin**，用于访问 **--http-cert-file**中指定的文件中的私钥的密码

发布 LDAP 和 Apache 服务器证书的 CA 完整 CA 证书链

- **--dirsrv-cert-file** 和 **--http-cert-file**用于具有完整 CA 证书链或部分证书链的证书文件

您可以提供在 **--dirsrv-cert-file** 和 **--http-cert-file** 选项中指定的以下格式的文件：

- Privacy-Enhanced Mail(PEM)编码的证书(RFC 7468)。请注意，身份管理安装程序接受串联的 PEM 编码的对象。
- 区分编码规则(DER)
- PKCS #7 证书链对象

- PKCS #8 私钥对象
- PKCS #12 归档

您可以多次指定 **--dirsrv-cert-file** 和 **--http-cert-file** 选项来指定多个文件。

完成完整 CA 证书链的证书文件（某些环境中不需要）

- **--ca-cert-file** 用于包含签发 LDAP、Apache 服务器和 Kerberos KDC 证书的 CA 证书的一个或多个文件。如果其他选项提供的证书文件中没有 CA 证书，请使用这个选项。

使用 **--dirsrv-cert-file** 和 **--http-cert-file** 以及 **--ca-cert-file** 提供的文件必须包含签发 LDAP 和 Apache 服务器证书的 CA 的完整 CA 证书链。

Kerberos 密钥分发中心(KDC) PKINIT 证书和私钥

- 如果您有 PKINIT 证书，请使用以下 2 个选项：
  - **--pkinit-cert-file** 用于 Kerberos KDC SSL 证书和私钥
  - **--pkinit-pin** 用于访问 **--pkinit-cert-file** 文件中指定的 Kerberos KDC 私钥的密码
- 如果您没有 PKINIT 证书，并希望使用带有自签名证书的本地 KDC 配置 IdM 服务器，请使用以下选项：
  - **--no-pkinit** 用于禁用 pkinit 设置步骤

其他资源

- 有关证书文件接受哪些选项的详情，请参见 **ipa-server-install**(1)手册页。
- 有关创建 RHEL IdM PKINIT 证书所需的 PKINIT 扩展的详情，请参阅 RHEL IdM PKINIT KDC 证书和扩展。

5.2. 交互式安装

在使用 **ipa-server-install** 工具进行交互式安装过程中，您需要提供系统的基本配置，如 realm、管理员的密码和目录管理器的密码。

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

流程

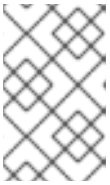
1. 运行 **ipa-server-install** 工具，并提供所有所需的证书。例如：

```
[root@server ~]# ipa-server-install \
    --http-cert-file /tmp/server.crt \
    --http-cert-file /tmp/server.key \
    --http-pin secret \
    --dirsrv-cert-file /tmp/server.crt \
    --dirsrv-cert-file /tmp/server.key \
    --dirsrv-pin secret \
    --ca-cert-file ca.crt
```

有关提供的证书的详情，请参阅 安装 IdM 服务器所需的不带 CA 的证书 。

2. 此脚本提示配置集成的 DNS 服务。输入 **yes** 或 **no**。在此过程中，我们安装了带有集成 DNS 的服务器。

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```



注意

如果您要安装没有集成 DNS 的服务器，安装脚本将不会提示您进行 DNS 配置，如下面步骤所述。如需了解安装不带 DNS 的服务器的详细步骤，请参阅 安装 IdM 服务器：没有集成的 DNS，集成的 CA 作为根 CA。

3. 该脚本提示输入一些必需的设置，并在括号中提供推荐的默认值。

- 要接受默认值，请按 **Enter** 键。
- 要提供自定义值，请输入所需的值。

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

警告

仔细规划这些名称。安装完成后您将无法更改它们。

4. 输入目录服务器超级用户(**cn=Directory Manager**)以及身份管理(IdM)管理系统用户帐户(**admin**)的密码。

```
Directory Manager password:
IPA admin password:
```

5. 脚本提示每台服务器的 DNS 转发器。

```
Do you want to configure DNS forwarders? [yes]:
```

- 要配置每台服务器的 DNS 转发器，请输入 **yes**，然后按照命令行中的说明操作。安装过程会将转发器 IP 地址添加到 IdM LDAP。
  - 有关正向解析策略的默认设置，请查看 **ipa-dns-install**(1)手册页中的 **--forward-policy** 描述。
- 如果您不想使用 DNS 正向解析，请输入 **no**。
  如果没有 DNS 转发器，您 IdM 域中的主机将不能解析来自基础架构中其他的、内部的、DNS 域的名称。主机将只剩下公共 DNS 服务器来解析其 DNS 查询。

6. 脚本会提示检查是否需要配置与服务器关联的 IP 地址的任何 DNS 反向(PTR)记录。

```
Do you want to search for missing reverse zones? [yes]:
```

如果您运行搜索并发现丢失了反向区，脚本会询问您是否创建反向区以及 PTR 记录。

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

注意

使用 IdM 管理反向区是可选的。您可以改为使用外部 DNS 服务来实现这一目的。

7. 输入 **yes** 以确认服务器配置。

```
Continue to configure the system with these values? [no]: yes
```

8. 安装脚本现在配置服务器。等待操作完成。

9. 安装脚本完成后，使用以下方法更新您的 DNS 记录：

   a. 将父域中的 DNS 委托程序添加到 IdM DNS 域。例如，如果 IdM DNS 域是 ***idm.example.com***，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

   重要

   每次安装 IdM DNS 服务器后都会重复这个步骤。

   b. 将时间服务器的 **_ntp._udp** 服务(SRV)记录添加到您的 IdM DNS。IdM DNS 中新安装的 IdM 服务器的时间服务器的 SRV 记录可确保将来的副本和客户端安装会自动配置为与此主 IdM 服务器使用的时间服务器同步。

第 6 章 安装 IDM 服务器：在不集成 DNS 的情况，将集成的 CA 作为 ROOT CA

本章描述了如何安装没有集成 DNS 的新的身份管理(IdM)服务器。

注意

红帽强烈建议在 IdM 部署中为基本用途安装集成 IdM 的 DNS：当 IdM 服务器也管理 DNS 时，DNS 和原生 IdM 工具之间存在紧密集成，从而实现一些 DNS 记录管理的自动化。

如需了解更多详细信息，请参阅 规划 DNS 服务和主机名。

6.1. 交互式安装

在使用 **ipa-server-install** 工具进行交互式安装过程中，您需要提供系统的基本配置，如 realm、管理员的密码和目录管理器的密码。

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

这个过程安装服务器：

- 没有集成的 DNS
- 集成身份管理(IdM)证书颁发机构(CA)作为根CA，这是默认的 CA 配置

流程

1. 运行 **ipa-server-install** 工具。

```
# ipa-server-install
```

2. 此脚本提示配置集成的 DNS 服务。按 **Enter** 键选择默认的 **no** 选项。

```
Do you want to configure integrated DNS (BIND)? [no]:
```

3. 该脚本提示输入一些必需的设置，并在括号中提供推荐的默认值。
   - 要接受默认值，请按 **Enter** 键。
   - 要提供自定义值，请输入所需的值。

```
Server host name [server.idm.example.com]:
Please confirm the domain name [idm.example.com]:
Please provide a realm name [IDM.EXAMPLE.COM]:
```

警告

仔细规划这些名称。安装完成后您将无法更改它们。

4. 输入目录服务器超级用户(**cn=Directory Manager**)和 IdM 管理系统用户帐户(**admin**)的密码。

```
Directory Manager password:
IPA admin password:
```

5. 该脚本提示输入一些必需的设置，并在括号中提供推荐的默认值。

- 要接受默认值，请按 **Enter** 键。
- 要提供自定义值，请输入所需的值。

```
NetBIOS domain name [EXAMPLE]:
Do you want to configure chrony with NTP server or pool address? [no]:
```

6. 输入 **yes** 以确认服务器配置。

```
Continue to configure the system with these values? [no]: yes
```

7. 安装脚本现在配置服务器。等待操作完成。

8. 安装脚本生成包含 DNS 资源记录的文件：下面示例输出中的 **/tmp/ipa.system.records.UFRPto.db** 文件。将这些记录添加到现有的外部 DNS 服务器中。更新 DNS 记录的过程因特定的 DNS 解决方案而异。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

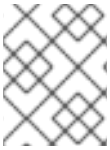
在将 DNS 记录添加到现有 DNS 服务器之前，服务器安装不会完成。

其他资源

- 有关您必须添加到 DNS 系统中的 DNS 资源记录的更多信息，请参阅 外部 DNS 系统的 IdM DNS 记录 。

6.2. 非互动安装

此流程安装没有集成的 DNS 的服务器，或者安装将集成的身份管理(IdM)证书颁发机构(CA)作为 root CA（这是默认的 CA 配置）的服务器。



注意

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

流程

1. 运行带有选项的 **ipa-server-install** 工具以提供所有必需的信息。非互动安装的最低所需选项是：

- **--realm** 提供 Kerberos 领域名
- **--ds-password** 为目录管理者(DM)（目录服务器超级用户）提供密码
- **--admin-password** 为 **admin** （IdM 管理员）提供密码
- **--unattended**，让安装进程为主机名和域名选择默认选项

例如：

```
# ipa-server-install --realm IDM.EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended
```

2. 安装脚本生成包含 DNS 资源记录的文件：下面示例输出中的 **/tmp/ipa.system.records.UFRPto.db** 文件。将这些记录添加到现有的外部 DNS 服务器中。更新 DNS 记录的过程因特定的 DNS 解决方案而异。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

在将 DNS 记录添加到现有 DNS 服务器之前，服务器安装不会完成。

其他资源

- 有关您必须添加到 DNS 系统中的 DNS 资源记录的更多信息，请参阅 外部 DNS 系统的 IdM DNS 记录 。
- 如需 ipa-server-install 接受的选项的完整列表，请运行 **ipa-server-install --help** 命令。

6.3. 外部 DNS 系统的 IDM DNS 记录

在安装了没有集成 DNS 的 IdM 服务器后，您必须将 IdM 服务器的 LDAP 和 Kerberos DNS 资源记录添加到外部 DNS 系统中。

ipa-server-install 安装脚本生成一个包含 DNS 资源记录列表的文件，其中文件名格式为 **/tmp/ipa.system.records.*<random_characters>*.db**，并打印添加这些记录的指令：

```
Please add records in this file to your DNS system: /tmp/ipa.system.records.6zdjqxh3.db
```

这是文件内容的示例：

```
_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"
```

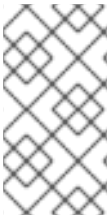
```
_kpasswd._tcp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_kpasswd._udp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_ldap._tcp.example.com. 86400 IN SRV 0 100 389 server.example.com.
```

注意

在将 IdM 服务器的 LDAP 和 Kerberos DNS 资源记录添加到 DNS 系统后，请确保 DNS 管理工具没有为 **ipa-ca** 添加 PTR 记录。DNS 中出现 **ipa-ca** 的 PTR 记录可能会导致后续的 IdM 副本安装失败。

第 7 章 安装 IDM 服务器： 在不集成 DNS 的情况下，使用外部 CA 作为 ROOT CA

本章描述了如何安装没有集成 DNS 的新的身份管理(IdM)服务器，该服务器使用外部证书颁发机构(CA)作为根CA。



注意

红帽强烈建议在 IdM 部署中为基本用途安装集成 IdM 的 DNS：当 IdM 服务器也管理 DNS 时，DNS 和原生 IdM 工具之间存在紧密集成，从而实现一些 DNS 记录管理的自动化。

如需了解更多详细信息，请参阅 规划 DNS 服务和主机名。

7.1. 安装外部 CA 作为根 CA 的 IDM CA 时使用的选项

如果适合以下条件之一，您可能希望安装外部 CA 作为 根 CA 的身份管理 IdM 证书颁发机构(CA)：

- 您正在使用 **ipa-server-install** 命令安装新的 IdM 服务器或副本。
- 您正在使用 **ipa-ca-install** 命令将 CA 组件安装到现有的 IdM 服务器中。

在安装外部 CA 作为根 CA 的 IdM CA 时，您可以对两个命令使用以下选项来创建证书签名请求(CSR)。

--external-ca-type=*TYPE*

外部 CA 的类型。可能的值是 ***generic*** 和 ***ms-cs***。默认值为 ***generic***。使用 ***ms-cs*** 来在生成的 CSR 中包含 Microsoft 证书服务(MS CS)所需的模板名称。要使用非默认配置文件，请将 **--external-ca-profile** 选项与 **--external-ca-type=ms-cs** 结合使用。

--external-ca-profile=*PROFILE_SPEC*

在为 IdM CA 发布证书时，请指定您希望 MS CS 应用的证书配置文件或模板。
请注意，如果 **--external-ca-type** 是 ms-cs，则只能使用 **--external-ca-profile** 选项。

您可以通过以下方法之一识别 MS CS 模板：

- ***<oid>:<majorVersion>[:<minorVersion>]***。您可以通过其对象标识符(OID)和主版本来指定证书模板。您还可以选择指定次版本。
- ***<name>***。您可以根据其名称指定证书模板。名称不能包含任何 : 字符，不能是 OID，否则基于 OID 的模板指定符语法优先。
- ***default***。如果您使用这个指定符，则会使用模板名称 ***SubCA***。

在某些情场景中，活动目录(AD)管理员可以使用 **下级证书机构** (SCA)模板（这是 AD CS 中的内置模板）来创建一个唯一的模板，来更好地满足组织的需求。例如，新模板可以具有自定义的有效期和自定义的扩展。关联的对象标识符(OID)可以在 AD **证书模板** 控制台中找到。

如果 AD 管理员禁用了原始的、内置的模板，则您在为 IdM CA 请求证书时，必须指定新模板的 OID 或名称。请您的 AD 管理员为您提供新模板的名称或 OID。

如果原始的 SCA AD CS 模板仍然被启用，则您可以通过指定 **--external-ca-type=ms-cs** 来使用它，而无需额外使用 **--external-ca-profile** 选项。在这种情况下，会使用 **subCA** 外部 CA 配置文件，它是与 SCA AD CS 模板对应的默认 IdM 模板。

7.2. 交互式安装

在使用 **ipa-server-install** 工具进行交互式安装过程中，您需要提供系统的基本配置，如 realm、管理员的密码和目录管理器的密码。

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

按照以下流程安装服务器：

- 没有集成的 DNS
- 使用外部证书颁发机构（CA）作为 root CA

先决条件

- 您已确定了要通过 **--external-ca-type** 选项指定的外部 CA 的类型。详情请查看 **ipa-server-install**(1)手册页。
- 如果您使用 Microsoft Certificate Services 证书颁发机构(MS CS CA)作为外部 CA：您已确定要通过 **--external-ca-profile** 选项指定的证书配置文件或模板。默认情况下使用 **SubCA** 模板。有关 **--external-ca-type** 和 **--external-ca-profile** 选项的更多信息，请参阅 在安装外部 CA 作为根 CA 的 IdM CA 时使用的选项。

流程

1. 使用 **--external-ca** 选项来运行 ipa-server-install 工具。
   - 如果您使用 Microsoft 证书服务(MS CS) CA，还使用 **--external-ca-type** 选项，并可选使用 **--external-ca-profile** 选项：

     ```
     [root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-profile=<oid>/<name>/default
     ```

   - 如果您没有使用 MS CS 为 IdM CA 生成签名证书，则不需要其他选项：

     ```
     # ipa-server-install --external-ca
     ```

2. 此脚本提示配置集成的 DNS 服务。按 **Enter** 键选择默认的 **no** 选项。

   ```
   Do you want to configure integrated DNS (BIND)? [no]:
   ```

3. 该脚本提示输入一些必需的设置，并在括号中提供推荐的默认值。
   - 要接受默认值，请按 **Enter** 键。
   - 要提供自定义值，请输入所需的值。

     ```
     Server host name [server.idm.example.com]:
     Please confirm the domain name [idm.example.com]:
     Please provide a realm name [IDM.EXAMPLE.COM]:
     ```

警告

仔细规划这些名称。安装完成后您将无法更改它们。

4. 输入目录服务器超级用户(**cn=Directory Manager**)和 IdM 管理系统用户帐户(**admin**)的密码。

```
Directory Manager password:
IPA admin password:
```

5. 输入 **yes** 以确认服务器配置。

```
Continue to configure the system with these values? [no]: yes
```

6. 在证书系统实例配置过程中，该工具会打印证书签名请求(CSR)的位置： **/root/ipa.csr**:

```
...

Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
  [1/8]: creating certificate server user
  [2/8]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-install as:
/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
```

当发生这种情况时：

a. 将位于 **/root/ipa.csr** 中的 CSR 提交给外部 CA。这个过程根据要用作外部 CA 的服务的不同而有所不同。

b. 在基础 64 编码 blob 中检索颁发的证书和颁发 CA 的 CA 证书链（Windows CA 的 PEM 文件或 Base_64 证书）。同样，不同的证书服务的进程会有所不同。通常，网页或通知电子邮件中的下载链接允许管理员下载所有需要的证书。

重要

确保获取 CA 的完整证书链，而不只是 CA 证书。

c. 再次运行 **ipa-server-install**，这次指定新发布的 CA 证书和 CA 链文件的位置和名称。例如：

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-
file=/tmp/cacert.pem
```

7. 安装脚本现在配置服务器。等待操作完成。

8. 安装脚本生成包含 DNS 资源记录的文件：下面示例输出中的 **/tmp/ipa.system.records.UFRPto.db** 文件。将这些记录添加到现有的外部 DNS 服务器中。更新 DNS 记录的过程因特定的 DNS 解决方案而异。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

在将 DNS 记录添加到现有 DNS 服务器之前，服务器安装不会完成。

其他资源

- 有关您必须添加到 DNS 系统中的 DNS 资源记录的更多信息，请参阅 外部 DNS 系统的 IdM DNS 记录 。
- **ipa-server-install --external-ca** 命令有时可能会失败，并显示以下错误：

```
ipa        : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f
/tmp/pass:quotes[configuration_file]' returned non-zero exit status 1
Configuration of CA failed
```

当设置 ***_proxy** 环境变量时，会发生此失败。有关此问题的解决方案，请参阅 故障排除：外部 CA 安装失败。

7.3. 非互动安装

这个过程安装服务器：

- 没有集成的 DNS
- 使用外部证书颁发机构（CA）作为 root CA

注意

ipa-server-install 安装脚本在 **/var/log/ipaserver-install.log** 中创建一个日志文件。如果安装失败，日志可帮助您辨别问题。

先决条件

- 您已确定了要通过 **--external-ca-type** 选项指定的外部 CA 的类型。详情请查看 **ipa-server-install**(1)手册页。
- 如果您使用 Microsoft Certificate Services 证书颁发机构(MS CS CA)作为外部 CA：您已确定要通过 **--external-ca-profile** 选项指定的证书配置文件或模板。默认情况下使用 **SubCA** 模板。
  有关 **--external-ca-type** 和 **--external-ca-profile** 选项的更多信息，请参阅 在安装外部 CA 作为根 CA 的 IdM CA 时使用的选项。

流程

1. 运行带有选项的 **ipa-server-install** 工具以提供所有必需的信息。使用外部 CA 的 IdM 服务器非互动安装的最低必需选项是：
   - **--external-ca** 用于指定外部 CA 是根CA

- **--realm** 提供 Kerberos 领域名
- **--ds-password** 为目录管理者(DM)（目录服务器超级用户）提供密码
- **--admin-password** 为 **admin** （IdM 管理员）提供密码
- **--unattended**，让安装进程为主机名和域名选择默认选项
  例如：

```
# ipa-server-install --external-ca --realm IDM.EXAMPLE.COM --ds-password
DM_password --admin-password admin_password --unattended
```

如果您使用 Microsoft 证书服务(MS CS) CA，也使用 **--external-ca-type** 选项，并选择使用 **--external-ca-profile** 选项。如需更多信息，请参阅 安装外部 CA 作为根 CA 的 IdM CA 时使用的选项。

2. 在证书系统实例配置过程中，该工具会打印证书签名请求(CSR)的位置： **/root/ipa.csr**:

```
...

Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes
  [1/11]: configuring certificate server instance
The next step is to get /root/ipa.csr signed by your CA and re-run /usr/sbin/ipa-server-install
as:
/usr/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
The ipa-server-install command was successful
```

当发生这种情况时：

a. 将位于 **/root/ipa.csr** 中的 CSR 提交给外部 CA。这个过程根据要用作外部 CA 的服务的不同而有所不同。

b. 在基础 64 编码 blob 中检索颁发的证书和颁发 CA 的 CA 证书链（Windows CA 的 PEM 文件或 Base_64 证书）。同样，不同的证书服务的进程会有所不同。通常，网页或通知电子邮件中的下载链接允许管理员下载所有需要的证书。

重要

确保获取 CA 的完整证书链，而不只是 CA 证书。

c. 再次运行 **ipa-server-install**，这次指定新发布的 CA 证书和 CA 链文件的位置和名称。例如：

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-
file=/tmp/cacert.pem --realm IDM.EXAMPLE.COM --ds-password DM_password --
admin-password admin_password --unattended
```

3. 安装脚本现在配置服务器。等待操作完成。

4. 安装脚本生成包含 DNS 资源记录的文件：下面示例输出中的 **/tmp/ipa.system.records.UFRPto.db** 文件。将这些记录添加到现有的外部 DNS 服务器中。更新 DNS 记录的过程因特定的 DNS 解决方案而异。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

在将 DNS 记录添加到现有 DNS 服务器之前，服务器安装不会完成。

其他资源

- 有关您必须添加到 DNS 系统中的 DNS 资源记录的更多信息，请参阅 外部 DNS 系统的 IdM DNS 记录 。

7.4. 外部 DNS 系统的 IDM DNS 记录

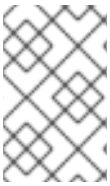
在安装了没有集成 DNS 的 IdM 服务器后，您必须将 IdM 服务器的 LDAP 和 Kerberos DNS 资源记录添加到外部 DNS 系统中。

ipa-server-install 安装脚本生成一个包含 DNS 资源记录列表的文件，其中文件名格式为 **/tmp/ipa.system.records.*<random_characters>*.db** ，并打印添加这些记录的指令：

```
Please add records in this file to your DNS system: /tmp/ipa.system.records.6zdjqxh3.db
```

这是文件内容的示例：

```
_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.
```



注意

在将 IdM 服务器的 LDAP 和 Kerberos DNS 资源记录添加到 DNS 系统后，请确保 DNS 管理工具没有为 **ipa-ca** 添加 PTR 记录。DNS 中出现 **ipa-ca** 的 PTR 记录可能会导致后续的 IdM 副本安装失败。

第 8 章 使用 LDIF 文件中的自定义数据库设置安装 IDM 服务器或副本

您可以使用活动目录数据库的自定义设置安装 IdM 服务器和 IdM 副本。以下流程演示了如何使用数据库设置创建 LDAP 数据交换格式(LDIF)文件，以及如何将这些设置传递给 IdM 服务器和副本安装命令。

先决条件

- 您已确定了可改进 IdM 环境性能的自定义目录服务器设置。请参阅 调整 IdM 目录服务器性能。

流程

1. 使用自定义数据库设置，创建一个 LDIF 格式的文本文件。使用短划线(-)分隔 LDAP 属性修改。这个示例为空闲超时和最大文件描述符设置了非默认值。

```
dn: cn=config
changetype: modify
replace: nsslapd-idletimeout
nsslapd-idletimeout=1800
-
replace: nsslapd-maxdescriptors
nsslapd-maxdescriptors=8192
```

2. 使用 **--dirsrv-config-file** 参数将 LDIF 文件传递给安装脚本。

   a. 要安装 IdM 服务器：

   ```
   # ipa-server-install --dirsrv-config-file filename.ldif
   ```

   b. 要安装 IdM 副本：

   ```
   # ipa-replica-install --dirsrv-config-file filename.ldif
   ```

其他资源

- **ipa-server-install** 和 **ipa-replica-install** 命令的选项

第 9 章 IDM 服务器安装故障排除

以下章节介绍了如何收集有关失败的 IdM 服务器安装的信息，以及如何解决常见的安装问题。

9.1. 查看 IDM 服务器安装错误日志

安装身份管理(IdM)服务器时，调试信息会附加到以下日志文件中：

- **/var/log/ipaserver-install.log**
- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/access**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**

日志文件的最后几行报告成功或失败，而 **ERROR** 和 **DEBUG** 条目则提供额外的上下文。

要解决 IdM 服务器安装失败的问题，请查看日志文件末尾的错误，并使用这些信息来解决任何相应的问题。

先决条件

- 您必须具有 **root** 特权才能显示 IdM 日志文件中的内容。

流程

1. 使用 **tail** 命令来显示日志文件的最后几行。以下示例显示了 **/var/log/ipaserver-install.log** 的最后 10 行。

```
[user@server ~]$ sudo tail -n 10 /var/log/ipaserver-install.log
[sudo] password for user:
value = gen.send(prev_value)
File "/usr/lib/python3.6/site-packages/ipapython/install/common.py", line 65, in _install
for unused in self._installer(self.parent):
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/init.py", line 564, in main
master_install(self)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/install.py", line 291, in decorated
raise ScriptError()

2020-05-27T22:59:41Z DEBUG The ipa-server-install command failed, exception:
ScriptError:
2020-05-27T22:59:41Z ERROR The ipa-server-install command failed. See
/var/log/ipaserver-install.log for more information
```

2. 要以交互方式查看日志文件，请使用 **less** 工具打开日志文件的末尾，然后使用↑ 和 ↓ 箭头键来导航。以下示例以交互方式打开 **/var/log/ipaserver-install.log** 文件。

```
[user@server ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

3. 通过使用剩余的日志文件重复此查看过程来收集额外的故障排除信息。

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log
```

```
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

其他资源

- 如果您无法解决失败的 IdM 服务器安装，且您有一个红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

9.2. 检查 IDM CA 安装错误

在身份管理(IdM)服务器上安装证书颁发机构(CA)服务时，调试信息会被附加到以下位置（按照推荐的优先级顺序）：

位置	描述
/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log	**pkispawn** 安装进程的高级别问题和 Python 跟踪
journalctl -u pki-tomcatd@pki-tomcat output	**pki-tomcatd@pki-tomcat** 服务中的错误
/var/log/pki/pki-tomcat/ca/debug.*$DATE*.log	公钥基础设施(PKI)产品核心中的大型 JAVA 堆栈跟踪活动
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit 日志文件	PKI 产品的审计日志
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.*$DATE*.log**	用于服务主体、主机和其它使用证书实体的证书操作的低级调试数据

注意

如果在安装可选 CA 组件时整个 IdM 服务器安装失败，则不会记录有关 CA 的详情；会在 **/var/log/ipaserver-install.log** 文件中记录一条信息，表示整个安装过程失败。红帽建议查看以上列出的日志文件以了解 CA 安装失败的详情。

唯一例外是您要安装 CA 服务，root CA 是外部 CA。如果来自外部 CA 的证书出现问题，则会在 **/var/log/ipaserver-install.log** 中记录错误。

要解决 IdM CA 安装失败的问题，请查看这些日志文件末尾的错误，并使用这些信息来解决任何相应的问题。

先决条件

- 您必须具有 **root** 特权才能显示 IdM 日志文件中的内容。

流程

1. 要以交互方式查看日志文件，请使用 **less** 程序打开日志文件的末尾，并在搜索 **ScriptError** 条目时，使用↑ 和 ↓箭头键来导航。以下示例将打开 **/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log**。

```
[user@server ~]$ sudo less -N +G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. 通过使用以上列出的所有日志文件重复此查看过程来收集额外的故障排除信息。

其他资源

- 如果您无法解决失败的 IdM 服务器安装，且您有一个红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

9.3. 删除部分 IDM 服务器安装

如果 IdM 服务器安装失败，可以保留一些配置文件。其他尝试安装 IdM 服务器会失败，安装脚本会报告 IPA 已配置。

带有现有部分 IdM 配置的系统示例

```
[root@server ~]# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-server-install command failed. See /var/log/ipaserver-install.log for more information
```

要解决这个问题，请卸载部分 IdM 服务器配置并重试安装过程。

先决条件

- 您必须有 **root** 权限。

流程

1. 从您要配置为 IdM 服务器的主机中卸载 IdM 服务器软件。

```
[root@server ~]# ipa-server-install --uninstall
```

2. 如果您因为重复安装失败而无法安装 IdM 服务器，请重新安装操作系统。
安装 IdM 服务器的要求之一是使用一个没有自定义的“干净”系统。失败的安装可能会因为意外修改系统文件而破坏主机的完整性。

其他资源

- 有关卸载 IdM 服务器的详情，请参考卸载 IdM 服务器。
- 如果重复卸载后尝试安装失败，且您有一个红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

9.4. 其他资源

- IdM 副本安装故障排除
- IdM 客户端安装故障排除
- 备份和恢复 IdM

第 10 章 卸载 IDM 服务器

按照以下流程卸载名为 **server123.idm.example.com** (server123)的身份管理(IdM)服务器。在流程中，您首先确保其他服务器运行关键服务，并且在执行卸载前拓扑将继续是冗余的。

先决条件

- 您有访问 server123 的 **root** 权限。
- 您有 IdM 管理员的凭证。

流程

1. 如果您的 IdM 环境使用集成的 DNS，请确保 server123 不是唯一 **启用的** DNS 服务器：

```
[root@server123 ~]# ipa server-role-find --role 'DNS server'
----------------------
2 server roles matched
----------------------
  Server name: server456.idm.example.com
  Role name: DNS server
  Role status: enabled
[...]
----------------------------
Number of entries returned 2
----------------------------
```

   如果 server123 是拓扑中唯一剩余的 DNS 服务器，请将 DNS 服务器角色添加到另一台 IdM 服务器。如需更多信息，请参阅 **ipa-dns-install(1)** 手册页。

2. 如果您的 IdM 环境使用集成证书颁发机构(CA)：

   a. 确保 server123 不是唯一 **启用的** CA 服务器：

```
[root@server123 ~]# ipa server-role-find --role 'CA server'
----------------------
2 server roles matched
----------------------
  Server name: server123.idm.example.com
  Role name: CA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: CA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

   如果 server123 是拓扑中唯一剩余的 CA 服务器，请将 CA 服务器角色添加到另一台 IdM 服务器。如需更多信息，请参阅 **ipa-ca-install(1)** 手册页。

   b. 如果您在 IdM 环境中已经启用了 vault，请确保 server123.idm.example.com 不是唯一 **启用的** 密钥恢复机构(KRA)服务器：

```
[root@server123 ~]# ipa server-role-find --role 'KRA server'
---------------------
2 server roles matched
---------------------
  Server name: server123.idm.example.com
  Role name: KRA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: KRA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

如果 server123 是拓扑中唯一剩余的 KRA 服务器，请将 KRA 服务器角色添加到另一台 IdM 服务器。如需更多信息，请参阅 **man ipa-kra-install(1)**。

c. 确保 server123.idm.example.com 不是 CA 续订服务器：

```
[root@server123 ~]# ipa config-show | grep 'CA renewal'
  IPA CA renewal master: r8server.idm.example.com
```

如果 server123 是 CA 续订服务器，请参阅 更改和重置 IdM CA 续订服务器，以了解有关如何将 CA 续订服务器角色移到另一台服务器的更多信息。

d. 确保 server123.idm.example.com 不是当前证书撤销列表(CRL)发布者：

```
[root@server123 ~]# ipa-crlgen-manage status
CRL generation: disabled
```

如果输出显示已在 server123 上启用了 CRL 生成，请参阅 在 IdM CA 服务器上生成 CRL ，以了解有关如何将 CRL 发布者角色移到另一台服务器的更多信息。

3. 连接到拓扑中的另一台 IdM 服务器：

```
$ ssh idm_user@server456
```

4. 在服务器上，获取 IdM 管理员的凭证：

```
[idm_user@server456 ~]$ kinit admin
```

5. 查看拓扑中分配给服务器的 DNA ID 范围：

```
[idm_user@server456 ~]$ ipa-replica-manage dnarange-show
server123.idm.example.com: 1001-1500
server456.idm.example.com: 1501-2000
[...]
```

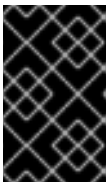
输出显示分配给 server123 和 server456 的一个 DNA ID 范围。

6. 如果 server123 是分配了 DNA ID 范围的拓扑中唯一的 IdM 服务器，请在 server456 上创建一个测试 IdM 用户，以确保服务器已分配了 DNA ID 范围：

```
[idm_user@server456 ~]$ ipa user-add test_idm_user
```

7. 从拓扑中删除 server123.idm.example.com：

```
[idm_user@server456 ~]$ ipa server-del server123.idm.example.com
```



重要

如果删除 server123 会导致断开连接的拓扑，则脚本会发出警告。有关如何在剩余的副本之间创建复制协议，以便删除可以继续的信息，请参阅 使用 CLI 在两个服务器之间设置复复制。

注意

运行 **ipa server-del** 命令会删除与 **domain** 和 **ca** 后缀的 server123 相关的所有复制数据和协议。这与域级别 0 IdM 拓扑正相反，其中您最初需要使用 **ipa-replica-manage del *server123*** 命令删除这些数据。域级别 0 IdM 拓扑是运行在 RHEL 7.2 及更早的版本中的拓扑。使用 **ipa domainlevel-get** 命令查看当前域级别。

8. 返回到 server123.idm.example.com ， 并卸载现有的 IdM 安装：

```
[root@server123 ~]# ipa-server-install --uninstall
...
Are you sure you want to continue with the uninstall procedure? [no]: true
```

9. 确定指向 server123.idm.example.com 的所有名称服务器(NS)DNS 记录已从您的 DNS 区域中删除。无论您使用由 IdM 还是外部 DNS 管理的集成 DNS，这个均适用。有关如何从 IdM 中删除 DNS 记录的更多信息，请参阅 在 IdM CLI 中删除 DNS 记录 。

其他资源

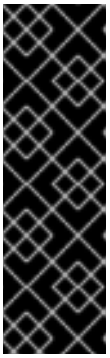
- RHEL 7 文档中的 显示和提升域级别
- 规划副本拓扑
- IdM CA 续订服务器说明
- 在 IdM CA 服务器上生成 CRL

第 11 章 重命名 IDM 服务器

您不能修改现有身份管理(IdM)服务器的主机名。但是，您可以将服务器替换为不同名称的副本。

流程

1. 安装将替换现有服务器的新副本，确保副本具有所需的主机名和 IP 地址。详情请参阅 安装 IdM 副本。



重要

如果您要卸载的服务器是证书撤销列表(CRL)发布者服务器，请在继续操作前，将另一台服务器作为 CRL 发布者服务器。

有关在迁移过程中如何进行此操作的详情，请查看以下部分：

- 在 RHEL 7 IdM CA 服务器中停止 CRL 生成
- 在新的 RHEL 8 IdM CA 服务器中启动 CRL 生成

2. 停止现有的 IdM 服务器实例。

```
[root@old_server ~]# ipactl stop
```

3. 卸载现有服务器，如 卸载 IdM 服务器 中所述。

第 12 章 更新和降级 IDM

12.1. 更新 IDM 软件包

您可以使用 **yum** 工具更新系统上的身份管理(IdM)软件包。

先决条件

- 确保您已应用了所有以前发布的与 RHEL 系统相关的勘误表。如需更多信息，请参阅 如何向我的 RHEL 系统应用软件包更新？KCS 文章。

流程

- 选择以下选项之一：
  - 更新所有与您的配置集相关且有可用更新的 IdM 软件包：

```
# yum upgrade ipa-*
```

  - 要安装或更新软件包以匹配任何启用的存储库中可用的配置文件的最新版本：

```
# yum distro-sync ipa-*
```

在至少一个服务器中更新 IdM 软件包后，拓扑中的所有其他服务器都会接收更新的模式，即使您没有更新它们的软件包。这将确保任何使用新模式的新条目都可以在其他服务器之间复制。

警告

当更新多个 IdM 服务器时，请在更新一个服务器后至少等待 10 分钟后再更新另一个服务器。但是，服务器成功更新所需的实际时间取决于部署的拓扑、连接的延迟以及更新所生成的修改数量。

当两个或更多个服务器同时更新，或在不同更新之间只能简短的间隔，则可能没有足够的时间来在整个拓扑间复制升级后的数据变化，从而会导致复制事件冲突。

重要

红帽建议仅升级到下一版本。例如，如果要升级到 RHEL 8.8 的 IdM，我们建议从 RHEL 8.7 的 IdM 升级。从早期版本升级可能会导致问题。

12.2. 降级 IDM 软件包

红帽不支持降级身份管理。

12.3. 其他资源

- **yum(8)** 手册页

第 13 章 为 IDM 客户端安装准备系统

本章描述了您的系统在安装身份管理(IdM)客户端时必须满足的条件。

13.1. 安装 IDM 客户端支持的 RHEL 版本

在 Red Hat Enterprise Linux 8 的最新次版本上运行的 IdM 服务器中的身份管理部署支持运行在最新次版本上的客户端：

- RHEL 7
- RHEL 8
- RHEL 9

注意

虽然其他客户端系统（如 Ubuntu）可以与 IdM 8 服务器一起使用，但红帽不提供对这些客户端的支持。

重要

如果您计划使 IdM 部署遵守 FIPS，红帽强烈建议将您的环境迁移到 RHEL 9。RHEL 9 是计划符合 FIPS 140-3 的第一个主要 RHEL 版本。

13.2. IDM 客户端的 DNS 要求

默认情况下，客户端安装程序会尝试为其主机名的父域搜索 **_ldap._tcp.DOMAIN** DNS SRV 记录。例如，如果客户端机器具有主机名 **client1.idm.example.com**，安装程序将尝试分别从 **_ldap._tcp.idm.example.com**、**_ldap._tcp.example.com** 和 **_ldap._tcp.com** DNS SRV 记录中检索 IdM 服务器主机名。然后，使用发现的域来在机器上配置客户端组件（如 SSSD 和 Kerberos 5 配置）。

但是，IdM 客户端的主机名不必是主 DNS 域的一部分。如果客户端机器主机名不在 IdM 服务器的子域中，请将 IdM 域作为 **ipa-client-install** 命令的 **--domain** 选项传递。在这种情况下，安装客户端后，SSSD 和 Kerberos 组件的配置文件中都会有域设置，并使用它来自动发现 IdM 服务器。

其他资源

- 有关 IdM 中 DNS 要求的详情，请参阅 IdM 的主机名和 DNS 要求。

13.3. IDM 客户端的端口要求

身份管理(IdM)客户端连接到 IdM 服务器上的多个端口，来与其服务进行通信。

在 IdM 客户端中，这些端口必须*在出站方向*被打开。如果您使用的防火墙不过滤传出数据包，如 **firewalld**，这些端口已在传出方向中可用。

其他资源

- 有关使用哪些特定端口的详情，请参阅 IdM 的端口要求。

13.4. IDM 客户端的 IPV6 要求

身份管理(IdM)不需要在您想要注册到 IdM 的主机的内核中启用 **IPv6** 协议。例如，如果您的内部网络只使用 **IPv4** 协议，那么您可以将系统安全服务守护进程(SSSD)配置为只使用 **IPv4** 来与 IdM 服务器进行通信。要做到这一点，您可以将以下行插入到 **/etc/sssd/sssd.conf** 文件的 **[domain/*NAME*]** 部分 ：

```
lookup_family_order = ipv4_only
```

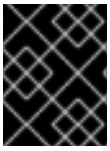
其他资源

- 有关 **lookup_family_order** 选项的详情，请查看 **sssd.conf (5)** 手册页。

13.5. 从 IDM:CLIENT 流安装 IDM 客户端软件包

在 RHEL8 中，安装身份管理(IdM)客户端所需的软件包作为模块提供。

idm:client 流是 **idm** 模块的默认流。如果您不需要在机器上安装服务器组件，请使用这个流来下载 IdM 客户端软件包。如果您需要持续使用长期支持的 IdM 客户端软件，则特别推荐使用 **idm:client** 流，前提是您不需要服务器组件。



重要

如果您计划在主机上安装 IdM 副本，请不要使用 **idm:client** 流。在这种情况下，使用 **idm:DL1** 流。

先决条件

- 在之前启用了 **idm:DL1** 流，并从中下载了软件包之后，切换到 **idm:client** 流时，您需要首先明确删除所有安装的相关内容，并在启用 **idm:client** 流之前禁用 **idm:DL1** 流。
  有关如何继续操作的详情，请参阅 切换到以后的流。

重要

在不禁用当前流的情况下尝试启用新流会导致错误。

流程

- 要下载安装 IdM 客户端所需的软件包：

```
# yum module install idm
```

13.6. 从 IDM:DL1 流安装 IDM 客户端软件包

在 RHEL8 中，安装身份管理(IdM)客户端所需的软件包作为模块提供。

您需要先启用 **idm:DL1** 流，然后才能从中下载软件包。如果您需要在机器上安装 IdM 服务器组件，请使用此流下载 IdM 客户端软件包。

先决条件

- 在之前启用了 **idm: client** 流，并从中下载了软件包之后，当切换到 **idm: DL1** 流时，您需要首先明确删除所有安装的相关内容，并在启用 **idm:DL1** 流前禁用 **idm: client** 流。
  有关如何继续操作的详情，请参阅 切换到以后的流。

重要

在不禁用当前流的情况下尝试启用新流会导致错误。

流程

1. 切换到通过 **idm:DL1** 流提供的 RPM：

```
# yum module enable idm:DL1
# yum distro-sync
```

2. 要下载安装 IdM 客户端所需的软件包：

```
# yum module install idm:DL1/client
```

第 14 章 安装 IDM 客户端

以下章节介绍了如何通过使用 **ipa-client-install** 工具将系统配置为身份管理(IdM)客户端。将系统配置为 IdM 客户端将其注册到 IdM 域中，并让系统在域中的 IdM 服务器中使用 IdM 服务。

要成功安装身份管理(IdM)客户端，您必须提供可用于注册客户端的凭证。

14.1. 先决条件

- 您已为 IdM 客户端安装准备了系统。详情请参阅 为 IdM 客户端安装准备系统。

14.2. 使用用户凭证安装客户端： 交互式安装

按照以下流程，使用授权用户的凭证以交互方式安装身份管理(IdM)客户端，来将系统注册到域中。

先决条件

- 确定您有用户授权将客户端注册到 IdM 域的凭证。例如，这可以是具有注册管理员角色的 **hostadmin** 用户。

流程

1. 在您要配置为 IdM 客户端的系统中运行 **ipa-client-install** 工具。

   ```
   # ipa-client-install --mkhomedir
   ```

   添加 **--enable-dns-updates** 选项，以便在以下任何一个条件适用时，使用客户端系统的 IP 地址更新 DNS 记录：

   - 已安装带有集成的 DNS 的 IdM 服务器
   - 网络中的 DNS 服务器接受使用 GSS-TSIG 协议的 DNS 条目更新

   ```
   # ipa-client-install --enable-dns-updates --mkhomedir
   ```

   启用 DNS 更新对以下客户端很有用：

   - 具有使用动态主机配置协议发布的动态 IP 地址
   - 有一个已分配的静态 IP 地址，但 IdM 服务器不知道它

2. 安装脚本尝试自动获取所有所需的设置，如 DNS 记录。

   - 如果在 IdM DNS 区域中正确设置了 SRV 记录，该脚本会自动发现所有其他必要的值并显示它们。输入 **yes** 以确认。

     ```
     Client hostname: client.example.com
     Realm: EXAMPLE.COM
     DNS Domain: example.com
     IPA Server: server.example.com
     BaseDN: dc=example,dc=com

     Continue to configure the system with these values? [no]: yes
     ```

- 要使用不同的值安装系统，请输入 **no**。然后再次运行 **ipa-client-install**，并通过在 **ipa-client-install** 中添加命令行选项来指定所需的值，例如：
  - **--hostname**
  - **--realm**
  - **--domain**
  - **--server**
  - **--mkhomedir**

重要

完全限定域名必须是有效的 DNS 名称：

- 仅允许数字、字母字符和连字符(**-**)。例如，不允许使用下划线，这可能导致 DNS 失败。
- 主机名必须都是小写。不允许使用大写字母。

- 如果脚本自动获取一些设置，它会提示您输入这些值。

3. 该脚本提示其身份用于注册客户端的用户。例如，这可能是具有注册管理员角色的 **hostadmin** 用户：

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

4. 安装脚本现在配置客户端。等待操作完成。

```
Client configuration complete.
```

其他资源

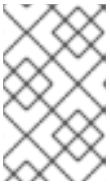
- 有关客户端安装脚本如何搜索 DNS 记录的详情，请查看 **ipa-client-install**(1)手册页中的 **DNS 自动发现** 部分。

14.3. 使用一次性密码安装客户端：交互式安装

按照以下流程，使用一次性密码以交互方式安装身份管理(IdM)客户端，来将系统注册到域中。

先决条件

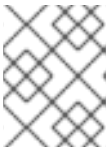
- 在域中的服务器上，将未来的客户端系统添加为 IdM 主机。在**ipa host-add** 命令中使用 **--random** 选项，来为注册生成一次性随机密码。



注意

ipa host-add <client_fqdn> 命令要求客户端 FQDN 可通过 DNS 解析。如果无法解析，请使用 **--ip address** 选项或其它选项提供 IdM 客户端系统的 IP 地址，并使用 **--force** 选项。

```
$ ipa host-add client.example.com --random
--------------------------------------------------
Added host "client.example.com"
--------------------------------------------------
  Host name: client.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```



注意

当使用生成的密码将机器注册到 IdM 域后，生成的密码将变为无效。注册完成后，它将被一个正确的主机 keytab 替换。

流程

1. 在您要配置为 IdM 客户端的系统中运行 **ipa-client-install** 工具。
使用 **--password** 选项来提供一次性随机密码。由于密码通常包含特殊字符，因此用单引号(')括起来。

```
# ipa-client-install --mkhomedir --password=password
```

添加 **--enable-dns-updates** 选项，以便在以下任何一个条件适用时，使用客户端系统的 IP 地址更新 DNS 记录：

- 已安装带有集成的 DNS 的 IdM 服务器
- 网络中的 DNS 服务器接受使用 GSS-TSIG 协议的 DNS 条目更新

```
# ipa-client-install --password 'W5YpARl=7M.n' --enable-dns-updates --mkhomedir
```

启用 DNS 更新对以下客户端很有用：

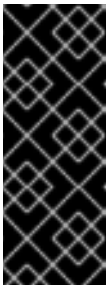
- 具有使用动态主机配置协议发布的动态 IP 地址
- 有一个已分配的静态 IP 地址，但 IdM 服务器不知道它

2. 安装脚本尝试自动获取所有所需的设置，如 DNS 记录。
   - 如果在 IdM DNS 区域中正确设置了 SRV 记录，该脚本会自动发现所有其他必要的值并显示它们。输入 **yes** 以确认。

```
Client hostname: client.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: server.example.com
BaseDN: dc=example,dc=com

Continue to configure the system with these values? [no]: yes
```

   - 要使用不同的值安装系统，请输入 **no**。然后再次运行 **ipa-client-install**，并通过在 **ipa-client-install** 中添加命令行选项来指定所需的值，例如：

- **--hostname**
- **--realm**
- **--domain**
- **--server**
- **--mkhomedir**



重要

完全限定域名必须是有效的 DNS 名称：

- 仅允许数字、字母字符和连字符(**-**)。例如，不允许使用下划线，这可能导致 DNS 失败。
- 主机名必须都是小写。不允许使用大写字母。

- 如果脚本自动获取一些设置，它会提示您输入这些值。

3. 安装脚本现在配置客户端。等待操作完成。

```
Client configuration complete.
```

其他资源

- 有关客户端安装脚本如何搜索 DNS 记录的详情，请查看 **ipa-client-install**(1)手册页中的 **DNS 自动发现** 部分。

14.4. 安装客户端： 非互动安装

对于非交互式安装，您必须使用命令行选项为 **ipa-client-install** 工具提供所有必需的信息。以下小节描述了非互动安装的最低所需选项。

客户端注册的预期验证方法选项

可用的选项有：

- **--principal** 和 **--password** 指定授权注册客户端的用户的凭证
- **--random** 指定为客户端生成的一次性随机密码
- **--keytab** 指定之前注册的 keytab

无人看守安装的选项

--unattended 选项允许在不需要用户确认的情况下运行安装。
如果在 IdM DNS 区域中正确设置了 SRV 记录，该脚本会自动发现所有其他必要的值。如果脚本无法自动发现这些值，请使用命令行选项提供它们，例如：

- **--hostname**，指定客户端机器的静态完全限定域名(FQDN)。

重要

FQDN 必须是一个有效的 DNS 名称：

- 只允许数字、字母字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
- 主机名必须都是小写。不允许使用大写字母。

- **--domain** 指定现有 IdM 部署的主 DNS 域，如 **example.com**。该名称是 IdM Kerberos 域名的小写版本。
- **--server** 指定要连接的 IdM 服务器的 FQDN。使用此选项时，会禁用 Kerberos 的 DNS 自动发现，并配置 KDC 和 Admin 服务器的固定列表。在正常情况下，不需要这个选项，因为服务器列表是从主 IdM DNS 域检索的。
- **--realm** 指定现有 IdM 部署的 Kerberos 域。通常，它是 IdM 安装所使用的主 DNS 域的大写版本。。在正常情况下，不需要这个选项，因为域名是从 IdM 服务器检索的。

非交互式安装的基本的 **ipa-client-install** 命令示例：

```
# ipa-client-install --password 'W5YpARl=7M.n' --mkhomedir --unattended
```

带有更多选项的用于非互动安装的 **ipa-client-install** 命令示例：

```
# ipa-client-install --password 'W5YpARl=7M.n' --domain idm.example.com --server
server.idm.example.com --realm IDM.EXAMPLE.COM --mkhomedir --unattended
```

其他资源

- 有关 **ipa-client-install** 可接受的选项的完整列表，请查看 **ipa-client-install**(1)手册页。

14.5. 安装客户端后删除前 IDM 配置

ipa-client-install 脚本不会从 **/etc/openldap/ldap.conf** 和 **/etc/sssd/sssd.conf** 文件中删除任何以前的 LDAP 和系统安全服务守护进程(SSSD)配置。如果在安装客户端前修改了这些文件中的配置，该脚本会添加新的客户端值，但会将它们注释掉。例如：

```
BASE   dc=example,dc=com
URI    ldap://ldap.example.com

#URI ldaps://server.example.com # modified by IPA
#BASE dc=ipa,dc=example,dc=com # modified by IPA
```

应用新的身份管理(IdM)} 配置值：

1. 打开 **/etc/openldap/ldap.conf** 和 **/etc/sssd/sssd.conf**。
2. 删除前面的配置。
3. 取消对新 IdM 配置的注释。

4. 依赖于系统范围的 LDAP 配置的服务器进程可能需要重启来应用更改。使用 **openldap** 库的应用程序通常会在启动时导入配置。

14.6. 测试 IDM 客户端

命令行界面告知您 **ipa-client-install** 已成功，但您也可以自行进行测试。

要测试身份管理(IdM)客户端是否可以获取服务器上定义的用户的信息，请检查您是否能够解析服务器上定义的用户。例如，检查默认的 **admin** 用户：

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

要测试身份验证是否正常工作，请从非 root 用户 **su** 到 root 用户：

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

14.7. 在 IDM 客户端安装过程中执行的连接

在 IdM 客户端安装过程中执行的请求 列出了身份管理(IdM)客户端安装工具 **ipa-client-install** 执行的操作。

表 14.1. 在 IdM 客户端安装过程中执行的请求

操作	使用的协议	目的
针对客户端系统中配置的 DNS 解析器的 DNS 解析	DNS	发现 IdM 服务器的 IP 地址；（可选）添加 A/AAAA 和 SSHFP 记录
对 IdM 副本上的端口 88（TCP/TCP6 和 UDP/UDP6）的请求	Kerberos	要获得 Kerberos ticket
JSON-RPC 在已发现或配置的 IdM 服务器中调用基于 IdM Apache 的 web-service	HTTPS	IdM 客户端注册；如果 LDAP 方法失败，检索 CA 证书链；根据需要请求证书验证
使用 SASL GSSAPI 身份验证、普通 LDAP 或两者,通过 TCP/TCP6 向 IdM 服务器上的 389 端口发请求。	LDAP	IdM 客户端注册；通过 SSSD 进程进行身份检索；对主机主体的 Kerberos 密钥进行检索
网络时间协议(NTP)发现和解析（可选）	NTP	将客户端系统和 NTP 服务器之间的时间同步

14.8. IDM 客户端在安装后部署过程中与服务器的通信

身份管理(IdM)框架的客户端通过两个不同的应用程序来实现：

- **ipa** 命令行界面(CLI)

- （*可选*）基于浏览器的 Web UI

CLI 安装后操作 显示了 IdM 客户端安装后部署过程中 CLI 执行的操作。 Web UI 安装后操作 显示了 IdM 客户端安装后部署过程中 Web UI 执行的操作。

表 14.2. CLI 安装后操作

操作	使用的协议	目的
针对客户端系统中配置的 DNS 解析器的 DNS 解析	DNS	发现 IdM 服务器的 IP 地址
对 IdM 副本上的端口 88（TCP/TCP6 和 UDP/UDP6）和 464（TCP/TCP6 和 UDP/UDP6）的请求	Kerberos	要获取 Kerberos 票据 ; 更改 Kerberos 密码 ; 与 IdM Web UI 进行身份验证
JSON-RPC 在已发现或配置的 IdM 服务器中调用基于 IdM Apache 的 web-service	HTTPS	任何 **ipa** 工具用法

表 14.3. Web UI 安装后操作

操作	使用的协议	目的
JSON-RPC 在已发现或配置的 IdM 服务器中调用基于 IdM Apache 的 web-service	HTTPS	检索 IdM Web UI 页面

其他资源

- 请参考 SSSD 通信模式 以了解有关 **SSSD** 守护进程如何与 IdM 和活动目录服务器上提供的服务进行通信的更多信息。
- 请参考 certmonger 通信模式 以了解有关 **certmonger** 守护进程如何与 IdM 和活动目录服务器上提供的服务进行通信的更多信息。

14.9. SSSD 通信模式

系统安全服务守护程序(SSSD)是一种用于访问远程目录和身份验证机制的系统服务。如果在身份管理 IdM 客户端上配置了，它将连接到 IdM 服务器，该服务器提供身份验证、授权和其他身份和策略信息。如果 IdM 服务器与 Active Directory(AD)是信任关系，SSSD 也会连接到 AD，使用 Kerberos 协议为 AD 用户执行身份验证。默认情况下，SSSD 使用 Kerberos 验证任何非本地用户。特殊情况下，SSSD 可能会被配置为使用 LDAP 协议。

SSSD 可以配置为与多个服务器通信。下表显示了 IdM 中 SSSD 的常见通信模式。

表 14.4. 与 IdM 服务器对话时在 IdM 客户端中的 SSSD 通信特征

操作	使用的协议	目的
针对客户端系统中配置的 DNS 解析器的 DNS 解析	DNS	发现 IdM 服务器的 IP 地址
向身份管理副本和 Active Directory 域控制器上的端口 88（TCP/TCP6 和 UDP/UDP6）、464（TCP/TCP6 和 UDP/UDP6）和 749(TCP/TCP6)发请求	Kerberos	获取 Kerberos 票据 ; 修改 Kerberos 密码
使用 SASL GSSAPI 身份验证、普通 LDAP 或两者,通过 TCP/TCP6 向 IdM 服务器上的 389 端口发请求。	LDAP	要获取有关 IdM 用户和主机的信息，请下载 HBAC 和 sudo 规则、自动挂载映射、SELinux 用户上下文、公共 SSH 密钥以及存储在 IdM LDAP 中的其他信息
（可选）如果是智能卡身份验证，则请求在线证书状态协议(OCSP)响应器（如果已配置）。这通常通过端口 80 完成，但它取决于客户端证书中的 OCSP 响应程序 URL 的实际值。	HTTP	获取在智能卡中安装的证书状态的信息

表 14.5. 与 Active Directory Domain Controller 对话时作为信任代理的 SSSD 服务器的通信模式

操作	使用的协议	目的
针对客户端系统中配置的 DNS 解析器的 DNS 解析	DNS	发现 IdM 服务器的 IP 地址
向身份管理副本和 Active Directory 域控制器上的端口 88（TCP/TCP6 和 UDP/UDP6）、464（TCP/TCP6 和 UDP/UDP6）和 749(TCP/TCP6)发请求	Kerberos	要获得 Kerberos 票据 ; 更改 Kerberos 密码 ; 远程管理 Kerberos
向端口 389（TCP/TCP6 和 UDP/UDP6）和 3268(TCP/TCP6)发请求.	LDAP	查询 Active Directory 用户和组群信息 ; 发现 Active Directory 域控制器
（可选）如果是智能卡身份验证，则请求在线证书状态协议(OCSP)响应器（如果已配置）。这通常通过端口 80 完成，但它取决于客户端证书中的 OCSP 响应程序 URL 的实际值。	HTTP	获取在智能卡中安装的证书状态的信息

其他资源

- IdM 客户端在安装后部署过程中与服务器的通信

14.10. CERTMONGER 通讯特征

Certmonger 是一个运行在身份管理(IdM)服务器和 IdM 客户端上的守护进程，允许及时续订与主机上的服务相关联的 SSL 证书。表 14.6 “certmonger 通讯特征” 显示 IdM 服务器上 **certmonger** 工具执行的操作。

表 14.6. certmonger 通讯特征

操作	使用的协议	目的
针对客户端系统中配置的 DNS 解析器的 DNS 解析	DNS	发现 IdM 服务器的 IP 地址
对 IdM 副本上的端口 88（TCP/TCP6 和 UDP/UDP6）和 464（TCP/TCP6 和 UDP/UDP6）的请求	Kerberos	要获得 Kerberos ticket
JSON-RPC 在已发现或配置的 IdM 服务器中调用基于 IdM Apache 的 web-service	HTTPS	请求新证书
通过 IdM 服务器的端口 8080(TCP/TCP6)进行访问	HTTP	为了获得在线证书状态协议(OCSP)响应器和证书状态
（在第一个安装的服务器或传输了证书跟踪的服务器上）通过 IdM 服务器的端口 8443(TCP/TCP6)进行访问	HTTPS	要在 IdM 服务器上管理证书颁发机构（只在 IdM 服务器和副本安装过程中）。服务器上的 **certmonger** 只与其本地服务器上的端口 8080 和 8443 联系，以进行 CA 相关的证书续订。

其他资源

- IdM 客户端在安装后部署过程中与服务器的通信

第 15 章 使用 KICKSTART 安装 IDM 客户端

在安装 Red Hat Enterprise Linux 时，Kickstart 注册会自动将新系统添加到身份管理(IdM)域。

15.1. 使用 KICKSTART 安装客户端

按照以下流程，使用 Kickstart 文件安装身份管理(IdM)客户端。

先决条件

- 在 kickstart 注册之前，请勿启动 **sshd** 服务。在注册客户端前启动 **sshd** 会自动生成 SSH 密钥，但 第 15.2 节 “用于客户端安装的 Kickstart 文件” 中的 Kickstart 文件会使用脚本来实现相同的目的，这是首选的解决方案。

流程

1. 在 IdM 服务器上预先创建主机条目，并为该条目设置临时密码：

   ```
   $ ipa host-add client.example.com --password=secret
   ```

   Kickstart 使用密码在客户端安装过程中进行验证，并在第一次验证尝试后过期。成功安装客户端后，它会使用它的 keytab 进行验证。

2. 创建一个包含 第 15.2 节 “用于客户端安装的 Kickstart 文件” 中描述的内容的 Kickstart 文件。使用 **network** 命令，确保在 Kickstart 文件中正确配置了网络。

3. 使用 Kickstart 文件安装 IdM 客户端。

15.2. 用于客户端安装的 KICKSTART 文件

您可以使用 Kickstart 文件安装身份管理(IdM)客户端。此处概述的 Kickstart 文件的内容必须满足某些要求。

要安装软件包列表中的 ipa-client 软件包

将 **ipa-client** 软件包添加到 Kickstart 文件的 %packages 部分。例如：

```
%packages
...
ipa-client
...
```

IdM 客户端的安装后说明

安装后的说明必须包括：

- 确保 SSH 密钥在注册前生成的说明
- 运行 **ipa-client-install** 工具的指令，同时指定：
  - 访问和配置 IdM 域服务所需的所有信息
  - 在 IdM 服务器中预创建客户端主机时设置的密码。在 第 15.1 节 “使用 Kickstart 安装客户端” 中。

例如：使用一次性密码的 Kickstart 安装后说明，以及从命令行而不是通过 DNS 检索所需的选项，如下所示：

```
%post --log=/root/ks-post.log

# Generate SSH keys; ipa-client-install uploads them to the IdM server by default
/usr/libexec/openssh/sshd-keygen rsa

# Run the client install script
/usr/sbin/ipa-client-install --hostname=client.example.com --domain=EXAMPLE.COM --enable-dns-updates --mkhomedir -w secret --realm=EXAMPLE.COM --server=server.example.com
```

另外，您还可以在 Kickstart 文件中包括其他选项，例如：

- 对于非交互式安装，将 **--unattended** 选项添加到 **ipa-client-install**。
- 要让客户端安装脚本为机器请求证书：
  - 将 **--request-cert** 选项添加到 **ipa-client-install**。
  - 将 Kickstart **chroot** 环境中的 **getcert** 和 **ipa-client-install** 工具的系统总线地址设为 **/dev/null**。要做到这一点，在 **ipa-client-install** 指令前将这些行添加到 Kickstart 文件中的安装后说明中：

    ```
    # env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null getcert list
    # env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null ipa-client-install
    ```

15.3. 测试 IDM 客户端

命令行界面告知您 **ipa-client-install** 已成功，但您也可以自行进行测试。

要测试身份管理(IdM)客户端是否可以获取服务器上定义的用户的信息，请检查您是否能够解析服务器上定义的用户。例如，检查默认的 **admin** 用户：

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

要测试身份验证是否正常工作，请从非 root 用户 **su** 到 root 用户：

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

第 16 章 IDM 客户端安装故障排除

以下小节论述了如何收集有关无法安装 IdM 客户端的信息,以及如何解决常见安装问题。

16.1. 检查 IDM 客户端安装错误

安装身份管理(IdM)客户端时，调试信息会附加到 **/var/log/ipaclient-install.log** 中。如果客户端安装失败，安装程序会记录失败并回滚更改以撤销对主机的任何修改。安装失败的原因可能不是在日志文件的末尾，因为安装程序也会记录回滚过程。

要解决 IdM 客户端安装失败的问题，请查看 **/var/log/ipaclient-install.log** 文件中标有 **ScriptError** 的行，并使用这些信息来解决任何相应的问题。

先决条件

- 您必须具有 **root** 特权才能显示 IdM 日志文件中的内容。

流程

1. 使用 **grep** 工具从 **/var/log/ipaserver-install.log** 文件中检索任何出现关键字 **ScriptError** 的内容。

```
[user@server ~]$ sudo grep ScriptError /var/log/ipaclient-install.log
[sudo] password for user:
2020-05-28T18:24:50Z DEBUG The ipa-client-install command failed, exception:
ScriptError: One of password / principal / keytab is required.
```

2. 要以交互方式查看日志文件，请使用 **less** 工具打开日志文件的末尾，然后使用↑ 和 ↓ 箭头键来导航。

```
[user@server ~]$ sudo less -N +G /var/log/ipaclient-install.log
```

其他资源

- 如果您无法解决失败的 IdM 客户端安装，且您有一个红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供客户端的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

16.2. 解决客户端安装无法更新 DNS 记录时的问题

IdM 客户端安装程序会使用 **nsupdate** 命令来创建 PTR、SSHFP 和其他 DNS 记录。但是，如果客户端在安装和配置了客户端软件后无法更新 DNS 记录，则安装过程会失败。

要解决这个问题，请验证配置，并查看 **/var/log/client-install.log 中的** DNS 错误。

先决条件

- 您使用 IdM DNS 作为 IdM 环境的 DNS 解决方案

流程

1. 确保客户端所在的 DNS 区的动态更新已被启用：

```
[user@server ~]$ ipa dnszone-mod idm.example.com. --dynamic-update=TRUE
```

2. 确保运行 DNS 服务的 IdM 服务器对 TCP 和 UDP 协议开放了端口 53。

```
[user@server ~]$ sudo firewall-cmd --permanent --add-port=53/tcp --add-port=53/udp
[sudo] password for user:
success
[user@server ~]$ firewall-cmd --runtime-to-permanent
success
```

3. 使用 **grep** 工具从 **/var/log/client-install.log** 中检索 **nsupdate** 命令的内容，以查看哪个 DNS 记录更新失败了。

```
[user@server ~]$ sudo grep nsupdate /var/log/ipaclient-install.log
```

其他资源

- 如果您无法解决失败的安装，且您有红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供客户端的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

16.3. 解决客户端安装无法加入 IDM KERBEROS 域时的问题

如果客户端无法加入 IdM Kerberos 域,IdM 客户端安装过程会失败。

```
Joining realm failed: Failed to add key to the keytab
child exited with 11

Installation failed. Rolling back changes.
```

这个失败可能是由空 Kerberos keytab 造成的。

先决条件

- 删除系统文件需要 **root** 特权。

流程

1. 删除 **/etc/krb5.keytab**。

```
[user@client ~]$ sudo rm /etc/krb5.keytab
[sudo] password for user:
[user@client ~]$ ls /etc/krb5.keytab
ls: cannot access '/etc/krb5.keytab': No such file or directory
```

2. 重试 IdM 客户端安装。

其他资源

- 如果您无法解决失败的安装，且您有红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供客户端的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

16.4. 其他资源

- 要解决安装第一个 IdM 服务器的问题，请参阅 IdM 服务器安装故障排除。
- 要排除安装 IdM 副本的问题，请参阅故障排除 IdM 副本安装。

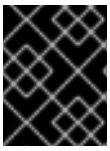
第 17 章 重新注册 IDM 客户端

如果客户端计算机因为客户端的硬件故障而被破坏并失去了与 IdM 服务器的连接，但您仍然拥有其 keytab，那么您可以重新注册客户端。在这种情况下，您希望使用相同的主机名将客户端恢复回 IdM 环境。

17.1. IDM 中的客户端重新注册

如果客户端计算机因为客户端的硬件故障而被破坏并失去了与 IdM 服务器的连接，但您仍然拥有其 keytab，那么您可以重新注册客户端。在这种情况下，您希望使用相同的主机名将客户端恢复回 IdM 环境。

在重新注册过程中，客户端会生成一个新的 Kerberos 密钥和 SSH 密钥，但 LDAP 数据库中客户端的身份保持不变。重新注册后，在机器与 IdM 服务器失去连接之前，主机像以前一样，其密钥和其他信息放在具有相同 **FQDN** 的同一 LDAP 对象中。



重要

您只能重新注册域条目仍然活跃的客户端。如果您卸载了客户端（使用 **ipa-client-install --uninstall**）或者禁用了其主机条目（使用 **ipa host-disable**），则无法重新注册它。

您不能在重命名客户端后重新注册客户端。这是因为在 IdM 中，LDAP 中客户端条目的关键属性是客户端的主机名，即其 **FQDN**。与重新注册客户端（在此期间客户端的 LDAP 对象保持不变）不同，重命名客户端的结果是，客户端的密钥和其他信息位于具有新 **FQDN** 的不同的 LDAP 对象中。因此，重命名客户端的唯一方法是从 IdM 卸载主机，更改主机的主机名，并使用新名称将其安装为 IdM 客户端。有关如何重命名客户端的详情，请参阅 重命名 IdM 客户端系统。

客户端重新注册过程中会发生什么

在重新启用过程中，IdM：

- 撤销原始主机证书
- 创建新 SSH 密钥
- 生成一个新的 keytab

17.2. 使用用户凭证重新注册客户端： 交互式重新注册

按照以下流程，使用授权用户的凭证以互动方式重新注册身份管理(IdM)客户端。

1. 重新创建具有相同主机名的客户端机器。
2. 在客户端机器上运行 **ipa-client-install --force-join** 命令：

```
# ipa-client-install --force-join
```

3. 该脚本提示其身份用于重新注册客户端的用户。例如，这可能是具有注册管理员角色的 **hostadmin** 用户：

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

其他资源

- 有关使用授权用户凭证注册客户端的详细流程，请参阅 使用用户凭证安装客户端：交互式安装。

17.3. 使用 CLIENT KEYTAB: NON-INTERACTIVE REENROLLMENT 重新注册客户端

先决条件

- 备份原始客户端 keytab 文件，例如在 **/tmp** 或 **/root** 目录中。

步骤

按照以下流程，使用客户端系统的 keytab 以非交互方式重新注册身份管理(IdM)客户端。例如，使用客户端 keytab 重新注册适用于自动安装。

1. 重新创建具有相同主机名的客户端机器。
2. 将 keytab 文件从备份位置复制到重新创建的客户端机器上的 **/etc/** 目录。
3. 使用 **ipa-client-install** 工具重新注册客户端，并使用 **--keytab** 选项指定 keytab 的位置：

```
# ipa-client-install --keytab /etc/krb5.keytab
```

注意

--keytab 选项中指定的 keytab只在进行身份验证以启动注册时才使用。在重新注册过程中，IdM 为客户端生成一个新的 keytab。

17.4. 测试 IDM 客户端

命令行界面告知您 **ipa-client-install** 已成功，但您也可以自行进行测试。

要测试身份管理(IdM)客户端是否可以获取服务器上定义的用户的信息，请检查您是否能够解析服务器上定义的用户。例如，检查默认的 **admin** 用户：

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

要测试身份验证是否正常工作，请从非 root 用户 **su** 到 root 用户：

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

第 18 章 卸载 IDM 客户端

作为管理员，您可以从环境中删除身份管理(IdM)客户端。

18.1. 卸载 IDM 客户端

卸载客户端会从身份管理(IdM)域中移除客户端，以及系统服务的所有特定的 IdM 配置，如系统安全服务守护进程(SSSD)。这会恢复客户端系统的以前的配置。

流程

1. 输入 **ipa-client-install --uninstall** 命令：

```
[root@client ~]# ipa-client-install --uninstall
```

2. 可选：检查您是否能为 IdM 用户获得 Kerberos 单据授予单(TGT)：

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@client ~]#
```

如果成功返回 Kerberos TGT 单，请遵循 卸载 IdM 客户端：多次安装后的其它步骤 中的其他卸载步骤。

3. 在客户端上，从每个已识别的 keytab，而不是 **/etc/krb5.keytab** 中删除旧的 Kerberos 主体：

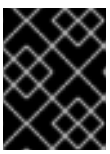
```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. 在 IdM 服务器中，从 IdM 中删除客户端主机的所有 DNS 条目：

```
[root@server ~]# ipa dnsrecord-del
Record name: old-client-name
Zone name: idm.example.com
No option to delete specific record provided.
Delete all? Yes/No (default No): true
----------------------
Deleted record "old-client-name"
```

5. 在 IdM 服务器中，从 IdM LDAP 服务器中删除客户端主机条目。这会删除所有服务并撤销为该主机发布的所有证书：

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



重要

如果您认为将来可能会使用不同的 IP 地址或不同的主机名来重新注册客户端，那么从 IdM LDAP 服务器中删除客户端主机条目至关重要。

18.2. 卸载 IDM 客户端：在以前的安装后执行额外的步骤

如果您多次将主机作为身份管理(IdM)客户端来安装和卸载，那么卸载过程可能无法恢复 IdM 之前的 Kerberos 配置。

在这种情况下，您必须手动删除 IdM Kerberos 配置。在某些情况下，您必须重新安装操作系统。

先决条件

- 您已使用 **ipa-client-install --uninstall** 命令来从主机中卸载 IdM 客户端配置。但是，您仍然可以从 IdM 服务器获得 IdM 用户的 Kerberos 单据授予单(TGT)。
- 您已检查了 **/var/lib/ipa-client/sysrestore** 目录是否为空，因此您不能使用目录中的文件来恢复系统的 IdM 客户端之前的配置。

流程

1. 检查 **/etc/krb5.conf.ipa** 文件：
   - 如果 **/etc/krb5.conf.conf.ipa** 文件的内容与安装 IdM 客户端之前的 **krb5.conf** 文件的内容相同，您可以：
     i. 删除 **/etc/krb5.conf** 文件：

     ```
     # rm /etc/krb5.conf
     ```

     ii. 将 **/etc/krb5.conf.ipa** 文件重命名为 **/etc/krb5.conf** ：

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - 如果 **/etc/krb5.conf.ipa** 文件的内容与安装 IdM 客户端之前的 **krb5.conf** 文件的内容不同，那么您可以至少将 Kerberos 配置直接恢复到安装操作系统之后的状态：

   i. 重新安装 **krb5-libs** 软件包：

   ```
   # yum reinstall krb5-libs
   ```

   作为依赖项，此命令还将重新安装 **krb5-workstation** 软件包和 **/etc/krb5.conf** 文件的原始版本。

2. 删除 **var/log/ipaclient-install.log** 文件（如果存在的话）。

验证步骤

- 尝试获取 IdM 用户凭证。这应该失败：

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@r8server ~]#
```

/etc/krb5.conf 文件现在恢复到其出厂状态。因此，您无法为主机上的 IdM 用户获取 Kerberos TGT。

第 19 章 重命名 IDM 客户端系统

以下章节描述了如何修改身份管理(IdM)客户端系统的主机名。

警告

重新命名客户端是一个手动过程。除非绝对需要修改主机名，否则请勿执行此操作。

重新命名 IdM 客户端涉及到：

1. 准备主机。详情请参阅 准备 IdM 客户端以进行重命名。
2. 从主机卸载 IdM 客户端。详情请查看 卸载客户端。
3. 重命名主机。详情请查看 重命名客户端。
4. 使用新名称在主机上安装 IdM 客户端。详情请查看 重新安装客户端。
5. 在 IdM 客户端安装后配置主机。详情请查看 重新添加服务、重新生成证书和重新添加主机组。

19.1. 准备 IDM 客户端以进行重命名

在卸载当前客户端之前，请记下客户端的某些设置。在使用新的主机名重新注册计算机后，您将应用此配置。

- 确定在机器上运行哪些服务：
  - 使用 **ipa service-find** 命令，并在输出中识别带有证书的服务：

    ```
    $ ipa service-find old-client-name.example.com
    ```

  - 此外，每个主机都有一个默认 *主机服务*，该服务不会出现在 **ipa service-find** 输出中。主机服务的服务主体（也称为 *主机主体*）是 **host/*old-client-name.example.com***。
- 对于 **ipa service-find *old-client-name.example.com*** 显示的所有服务主体，请确定 ***old-client-name.example.com*** 系统上相应的 keytab 的位置：

  ```
  # find / -name "*.keytab"
  ```

  客户端系统上的每个服务都有一个格式为 *service_name/host_name@REALM* 的 Kerberos 主体，例如 **ldap/*old-client-name.example.com@EXAMPLE.COM***.
- 识别机器所属的所有主机组。

  ```
  # ipa hostgroup-find old-client-name.example.com
  ```

19.2. 卸载 IDM 客户端

卸载客户端会从身份管理(IdM)域中移除客户端，以及系统服务的所有特定的 IdM 配置，如系统安全服务守护进程(SSSD)。这会恢复客户端系统的以前的配置。

流程

1. 输入 **ipa-client-install --uninstall** 命令：

```
[root@client ~]# ipa-client-install --uninstall
```

2. 可选：检查您是否能为 IdM 用户获得 Kerberos 单据授予单(TGT)：

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@client ~]#
```

如果成功返回 Kerberos TGT 票据，请遵循 卸载 IdM 客户端：多次安装后的其他步骤 中的其他卸载步骤。

3. 在客户端上，从每个已识别的 keytab，而不是 **/etc/krb5.keytab** 中删除旧的 Kerberos 主体：

```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. 在 IdM 服务器中，从 IdM 中删除客户端主机的所有 DNS 条目：

```
[root@server ~]# ipa dnsrecord-del
Record name: old-client-name
Zone name: idm.example.com
No option to delete specific record provided.
Delete all? Yes/No (default No): true
------------------------
Deleted record "old-client-name"
```

5. 在 IdM 服务器中，从 IdM LDAP 服务器中删除客户端主机条目。这会删除所有服务并撤销为该主机发布的所有证书：

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

重要

如果您认为将来可能会使用不同的 IP 地址或不同的主机名来重新注册客户端，那么从 IdM LDAP 服务器中删除客户端主机条目至关重要。

19.3. 卸载 IDM 客户端：在以前的安装后执行额外的步骤

如果您多次将主机作为身份管理(IdM)客户端来安装和卸载，那么卸载过程可能无法恢复 IdM 之前的 Kerberos 配置。

在这种情况下，您必须手动删除 IdM Kerberos 配置。在某些情况下，您必须重新安装操作系统。

先决条件

- 您已使用 **ipa-client-install --uninstall** 命令来从主机中卸载 IdM 客户端配置。但是，您仍然可以从 IdM 服务器获得 IdM 用户的 Kerberos 单据授予单(TGT)。
- 您已检查了 **/var/lib/ipa-client/sysrestore** 目录是否为空，因此您不能使用目录中的文件来恢复系统的 IdM 客户端之前的配置。

流程

1. 检查 **/etc/krb5.conf.ipa** 文件：
   - 如果 **/etc/krb5.conf.conf.ipa** 文件的内容与安装 IdM 客户端之前的 **krb5.conf** 文件的内容相同，您可以：
     i. 删除 **/etc/krb5.conf** 文件：

     ```
     # rm /etc/krb5.conf
     ```

     ii. 将 **/etc/krb5.conf.ipa** 文件重命名为 **/etc/krb5.conf** ：

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - 如果 **/etc/krb5.conf.ipa** 文件的内容与安装 IdM 客户端之前的 **krb5.conf** 文件的内容不同，那么您可以至少将 Kerberos 配置直接恢复到安装操作系统之后的状态：

   i. 重新安装 **krb5-libs** 软件包：

   ```
   # yum reinstall krb5-libs
   ```

   作为依赖项，此命令还将重新安装 **krb5-workstation** 软件包和 **/etc/krb5.conf** 文件的原始版本。
2. 删除 **var/log/ipaclient-install.log** 文件（如果存在的话）。

验证步骤

- 尝试获取 IdM 用户凭证。这应该失败：

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@r8server ~]#
```

/etc/krb5.conf 文件现在恢复到其出厂状态。因此，您无法为主机上的 IdM 用户获取 Kerberos TGT。

19.4. 重命名主机系统

根据需要重命名机器。例如：

```
# hostnamectl set-hostname new-client-name.example.com
```

现在，您可以使用新的主机名将身份验证(IdM)客户端重新安装到 IdM 域。

19.5. 重新安装 IDM 客户端

按照 安装客户端 中描述的流程在重命名的主机上安装客户端。

19.6. 重新添加服务、重新生成证书和重新添加主机组

流程

1. 在身份管理(IdM)服务器上，为 准备 IdM 客户端以进行重命名 中指定的每个服务添加新的 keytab 。

```
[root@server ~]# ipa service-add service_name/new-client-name
```

2. 为 准备 IdM 客户端以进行重命名 中分配了证书的服务生成证书。您可以做到这一点：
   - 使用 IdM 管理工具
   - 使用 **certmonger** 工具
3. 将客户端重新添加到 准备 IdM 客户端以进行重命名 中标识的主机组中。

第 20 章 为 IDM 副本安装准备系统

以下链接列出了安装身份验证(IdM)副本的要求。在安装前，请验证您的系统满足这些要求。

1. 确保 目标系统满足 IdM 服务器安装的一般要求。
2. 确保 目标系统满足 IdM 副本安装的额外的版本要求。
3. 授权目标系统注册到 IdM 域。如需更多信息，请参阅以下章节中最适合您需要的内容：
   - 授权在 IdM 客户端上安装副本
   - 授权在未注册到 IdM 的系统上安装副本

其他资源

- 规划副本拓扑

20.1. 副本版本要求

Red Hat Enterprise Linux(RHEL)8 副本只适用于运行在 RHEL 7.4 及更高版本上的身份验证(IdM)服务器。在将运行在 RHEL 8 上的 IdM 副本引入到现有的部署中之前，请将所有 IdM 服务器升级到 RHEL 7.4 或更高版本，并将域级别改为 1。

另外，副本必须运行相同的或更新的 IdM 版本。例如：

- 您已在 Red Hat Enterprise Linux 8 中安装了 IdM 服务器，并使用 IdM 4.x 软件包。
- 您必须在 Red Hat Enterprise Linux 8 或更高版本上安装副本，并使用 IdM 版本 4.x 或更高版本。

这样可确保把配置从服务器正确复制到副本。

有关如何显示 IdM 软件版本的详情，请参阅 显示 IdM 软件版本的方法 。

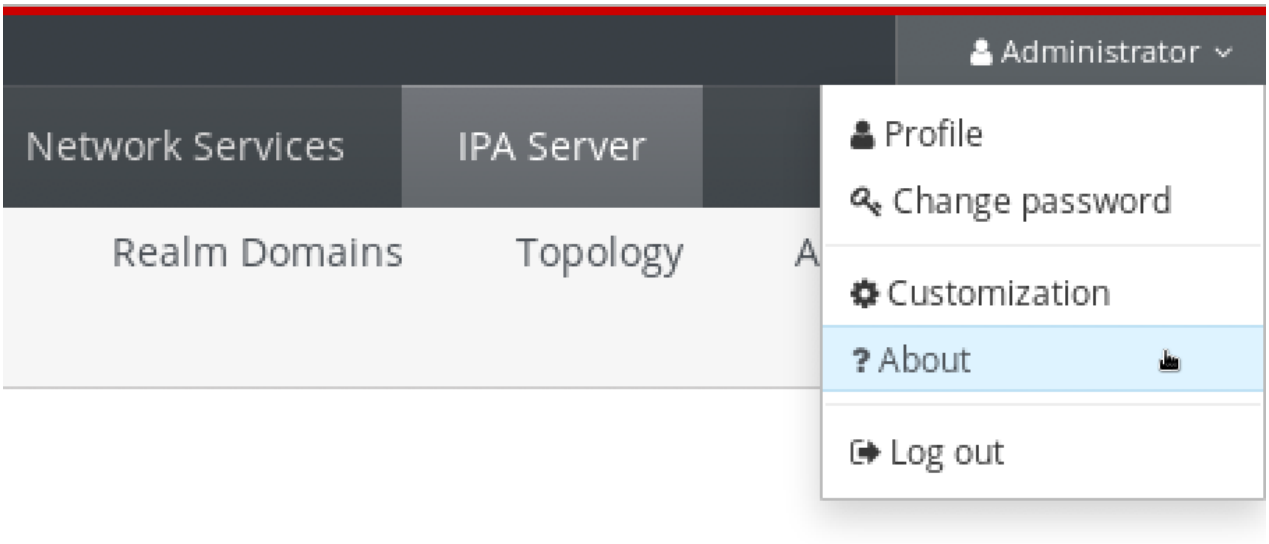
20.2. 显示 IDM 软件版本的方法

您可以使用以下命令显示 IdM 版本号：

- The IdM WebUI
- **ipa** 命令
- **rpm** 命令

通过 WebUI 显示版本

在 IdM Web UI 中，可以通过从右上角的用户名菜单中选择 **About** 来显示软件版本。



使用 ipa 命令显示版本

在命令行中使用 **ipa --version** 命令。

```
[root@server ~]# ipa --version
VERSION: 4.8.0, API_VERSION: 2.233
```

使用 rpm 命令显示版本

如果 IdM 服务工作不正常，您可以使用 **rpm** 工具来确定当前安装的 **ipa-server** 软件包的版本号。

```
[root@server ~]# rpm -q ipa-server
ipa-server-4.8.0-11.module+el8.1.0+4247+9f3fd721.x86_64
```

20.3. 授权在 IDM 客户端上安装副本

通过运行 **ipa-replica-install** 工具，在现有的身份管理(IdM)客户端上 安装副本 时，请选择下面的 **方法 1** 或 **方法 2** 来授权副本安装。如果以下任何一个适用，请选择 **方法 1**：

- 您希望高级系统管理员执行流程的初始部分，初级管理员执行其余部分。
- 您希望自动执行副本安装。

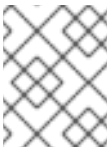
方法 1：ipaservers 主机组

1. 以 IdM admin 用户身份登录到任何一台 IdM 主机：

```
$ kinit admin
```

2. 将客户端机器添加到 **ipaservers** 主机组中：

```
$ ipa hostgroup-add-member ipaservers --hosts client.idm.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.idm.example.com, client.idm.example.com
-------------------------
Number of members added 1
-------------------------
```



注意

ipaservers 组中的成员授予机器类似于管理员凭证的提升特权。因此，在下一步中，初级系统管理员可以在主机上成功运行 **ipa-replica-install** 工具。

方法 2：特权用户的凭证

通过提供特权用户的凭证，选择以下任何一种方法来授权副本安装：

- 启动 **ipa-replica-install** 工具后，让身份管理(IdM)以交互方式提示您输入凭证。这是默认的行为。
- 在运行 **ipa-replica-install** 工具之前，立即以特权用户身份登录客户端。默认特权用户为 **admin** ：

```
$ kinit admin
```

其他资源

- 要启动安装过程，请参阅 安装 IdM 副本。
- 您可以使用 Ansible playbook 来安装 IdM 副本。如需更多信息，请参阅 使用 Ansible playbook 来安装身份管理副本。

20.4. 授权在未注册到 IDM 的系统上安装副本

当在没有在身份管理(IdM)域中注册的系统上 安装副本 时，**ipa-replica-install** 工具首先将系统注册为客户端，然后安装副本组件。在这种情况下，请选择下面的 **方法 1** 或 **方法 2** 来授权副本安装。如果以下任何一个适用，请选择 **方法 1**：

- 您希望高级系统管理员执行流程的初始部分，初级管理员执行其余部分。
- 您希望自动执行副本安装。

方法 1：在 IdM 服务器上生成的随机密码

在域中的任何服务器上输入以下命令：

1. 以管理员身份登录。

```
$ kinit admin
```

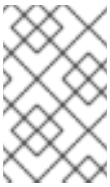
2. 将外部系统添加为 IdM 主机。使用 **ipa host-add** 命令的 **--random** 选项来生成用于后续副本安装的随机一次性密码。

```
$ ipa host-add replica.example.com --random
--------------------------------------------------
Added host "replica.example.com"
--------------------------------------------------
  Host name: replica.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```

当使用生成的密码将机器注册到 IdM 域后，生成的密码将变为无效。注册完成后，它将被一个正确的主机 keytab 替换。

3. 将系统添加到 **ipaservers** 主机组。

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.example.com, replica.example.com
-------------------------
Number of members added 1
-------------------------
```



注意

ipaservers 组中的成员授予机器类似于管理员凭证的提升特权。因此，在下一步中，**ipa-replica-install** 工具可以由提供生成的随机密码的初级系统管理员在主机上成功运行。

方法 2：特权用户的凭证

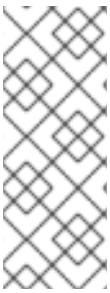
使用此方法，您可以通过提供特权用户的凭证来授权副本安装。默认特权用户为 **admin**。
在运行 IdM 副本安装工具之前不需要任何操作。在安装过程中，将主体名称和密码选项（**--principal *admin* --admin-password *password***）直接添加到 **ipa-replica-install** 命令中。

其他资源

- 要启动安装过程，请参阅 安装 IdM 副本。
- 您可以使用 Ansible playbook 来安装 IdM 副本。如需更多信息，请参阅 使用 Ansible playbook 来安装身份管理副本。

第 21 章 安装 IDM 副本

以下章节描述了如何使用命令行界面(CLI)以交互方式安装身份管理(IdM)副本。副本安装过程复制现有服务器的配置，并根据该配置安装副本。



注意

红帽建议 使用 Ansible 角色安装副本。通过使用 Ansible 角色，您可以一致地安装和自定义多个副本。

不使用 Ansible 的交互式和非交互式方法在拓扑中很有用，例如，其中副本准备被委派给用户或第三方。您还可以在地理上分散的拓扑中使用这些方法，其中您没有从 Ansible 控制器节点访问的权限。

先决条件

- 您一次安装一个 IdM 副本。不支持同时安装多个副本。
- 确保您的系统已为 IdM 副本安装做好了准备。

重要

如果没有执行此准备，安装 IdM 副本将失败。

有关个别类型的副本安装过程，请参阅：

- 第 21.1 节 “安装带有集成的 DNS 和 CA 的 IdM 副本”
- 第 21.2 节 “安装带有集成 DNS 且没有 CA 的 IdM 副本”
- 第 21.3 节 “安装没有集成 DNS 但有 CA 的 IdM 副本”
- 第 21.4 节 “安装没有集成 DNS 且没有 CA 的 IdM 副本”
- 第 21.5 节 “安装 IdM 隐藏的副本”

要解决副本安装过程的问题，请参阅：

- 第 22 章 *IdM 副本安装故障排除*

安装后，请参阅：

- 第 21.6 节 “测试 IdM 副本”
- 备份和恢复 IdM

21.1. 安装带有集成的 DNS 和 CA 的 IDM 副本

按照以下流程安装身份管理(IdM)副本：

- 带有集成的 DNS
- 带有证书颁发机构(CA)

例如，您可以在安装完带有集成 CA 的 IdM 服务器后复制 CA 服务以实现弹性。

重要

在使用 CA 配置副本时，副本的 CA 配置必须与其他服务器的 CA 配置一致。

例如，如果服务器包含集成的 IdM CA 作为根 CA，那么新副本也必须安装为将集成 CA 作为根 CA。本例中不提供其他 CA 配置。

在 **ipa-replica-install** 命令中包含**--setup-ca** 选项，可复制初始服务器的 CA 配置。

先决条件

- 确保您的系统已为 IdM 副本安装做好了准备。

流程

1. 在 **ipa-replica-install** 中输入以下选项：
   - **--setup-dns** 用来将副本配置为 DNS 服务器
   - 如果您不想使用任何每服务器转发器，请使用 **--forwarder** 来指定每服务器转发器或 **--no-forwarder**。要为故障转移的原因指定多个每服务器转发器，请多次使用 **--forwarder**。

     注意

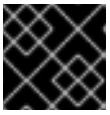
     ipa-replica-install 工具接受与 DNS 设置相关的许多其他选项，如 **--no-reverse** 或 **--no-host-dns**。有关它们的更多信息，请参阅 **ipa-replica-install**(1)手册页。

   - **--setup-ca** 用来在副本中包含一个 CA

   例如，要设置带有集成 DNS 服务器和 CA 的副本，其将不是由 IdM 服务器管理的所有 DNS 请求转发到运行在 IP 192.0.2.1 上的 DNS 服务器：

   ```
   # ipa-replica-install --setup-dns --forwarder 192.0.2.1 --setup-ca
   ```

2. 安装完成后，将父域的 DNS 委派添加到 IdM DNS 域。例如，如果 IdM DNS 域是 **idm.example.com**，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

   重要

   在每次安装完 IdM DNS 服务器后重复此步骤。

21.2. 安装带有集成 DNS 且没有 CA 的 IDM 副本

按照以下流程安装身份管理(IdM)副本：

- 带有集成的 DNS
- 在已安装 CA 的 IdM 环境中没有证书颁发机构(CA)。副本会将所有证书操作转发到安装了 CA 的 IdM 服务器。

先决条件

- 确保您的系统已为 IdM 副本安装做好了准备。

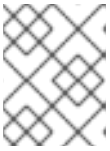
流程

1. 在 **ipa-replica-install** 中输入以下选项：

   - **--setup-dns** 用来将副本配置为 DNS 服务器
   - 如果您不想使用任何每服务器转发器，请使用 **--forwarder** 来指定每服务器转发器或 **--no-forwarder**。要为故障转移的原因指定多个每服务器转发器，请多次使用 **--forwarder**。

   例如，要设置一个带有集成 DNS 服务器的副本，其将不是由 IdM 服务器管理的所有 DNS 请求转发到运行在 IP 192.0.2.1 上的 DNS 服务器：

   ```
   # ipa-replica-install --setup-dns --forwarder 192.0.2.1
   ```

   注意

   ipa-replica-install 工具接受与 DNS 设置相关的许多其他选项，如 **--no-reverse** 或 **--no-host-dns**。有关它们的更多信息，请参阅 **ipa-replica-install**(1)手册页。

2. 安装完成后，将父域的 DNS 委派添加到 IdM DNS 域。例如，如果 IdM DNS 域是 **idm.example.com**，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

   重要

   在每次安装完 IdM DNS 服务器后重复此步骤。

21.3. 安装没有集成 DNS 但有 CA 的 IDM 副本

按照以下流程安装身份管理(IdM)副本：

- 没有集成的 DNS
- 带有证书颁发机构(CA)

重要

在使用 CA 配置副本时，副本的 CA 配置必须与其他服务器的 CA 配置一致。

例如，如果服务器包含集成的 IdM CA 作为根 CA，那么新副本也必须安装为将集成 CA 作为根 CA。本例中不提供其他 CA 配置。

在 **ipa-replica-install** 命令中包含**--setup-ca** 选项，可复制初始服务器的 CA 配置。

先决条件

- 确保您的系统已为 IdM 副本安装做好了准备。

流程

1. 在 **ipa-replica-install** 中输入 **--setup-ca** 选项。

   ```
   # ipa-replica-install --setup-ca
   ```

2. 在您的 DNS 服务器中添加新创建的 IdM DNS 服务记录：

   a. 以 **nsupdate** 格式将 IdM DNS 服务记录导出到文件中：

   ```
   $ ipa dns-update-system-records --dry-run --out dns_records_file.nsupdate
   ```

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

21.4. 安装没有集成 DNS 且没有 CA 的 IDM 副本

按照以下流程安装身份管理(IdM)副本：

- 没有集成的 DNS
- 在没有证书颁发机构(CA)的情况下，请手动提供所需的证书。这里的假设是安装第一个服务器时没有 CA。

重要

您不能使用自签名的第三方服务器证书来安装服务器或副本，因为导入的证书文件必须包含签发 LDAP 和 Apache 服务器证书的 CA 的完整 CA 证书链。

先决条件

- 确保您的系统已为 IdM 副本安装做好了准备。

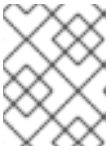
流程

- 输入 **ipa-replica-install**，并通过添加这些选项来提供所需的证书文件：
  - **--dirsrv-cert-file**
  - **--dirsrv-pin**
  - **--http-cert-file**
  - **--http-pin**

  有关使用这些选项提供的文件的详情，请参考 第 5.1 节 “安装没有 CA 的 IdM 服务器所需的证书”。

  例如：

  ```
  # ipa-replica-install \
      --dirsrv-cert-file /tmp/server.crt \
      --dirsrv-cert-file /tmp/server.key \
      --dirsrv-pin secret \
      --http-cert-file /tmp/server.crt \
      --http-cert-file /tmp/server.key \
      --http-pin secret
  ```



注意

不要添加 **--ca-cert-file** 选项。**ipa-replica-install** 工具从您安装的第一台服务器上自动获取这部分证书信息。

21.5. 安装 IDM 隐藏的副本

隐藏的（未公开的）副本是一台身份管理(IdM)服务器，其拥有所有正在运行且可用的服务。但是，它在 DNS 中没有 SRV 记录，并且不启用 LDAP 服务器角色。因此，客户端无法使用服务发现来检测这些隐藏的副本。

有关隐藏副本的详情，请参阅 隐藏副本模式。

先决条件

- 确保您的系统已为 IdM 副本安装做好了准备。

流程

- 要安装隐藏的副本，请使用以下命令：

```
ipa-replica-install --hidden-replica
```

请注意，命令安装一个不带 DNS SRV 记录，并且禁用了 LDAP 服务器角色的副本。

您还可以将现有副本的模式更改为隐藏。详情请参阅 隐藏的副本的降级和升级。

21.6. 测试 IDM 副本

创建副本后，检查副本是否按预期复制了数据。您可以使用以下步骤。

流程

1. 在新副本中创建用户：

```
[admin@new_replica ~]$ ipa user-add test_user
```

2. 确保用户在另一个副本中可见：

```
[admin@another_replica ~]$ ipa user-show test_user
```

21.7. 在 IDM 副本安装过程中执行的连接

IdM 副本安装期间执行的请求 列出了 **ipa-replica-install** （身份管理(IdM)副本安装工具）所执行的操作。

表 21.1. 在 IdM 副本安装过程中执行的请求

操作	使用的协议	目的
针对客户端系统中配置的 DNS 解析器的 DNS 解析	DNS	发现 IdM 服务器的 IP 地址

操作	使用的协议	目的
对发现的 IdM 服务器上的端口 88（TCP/TCP6 和 UDP/UDP6）的请求	Kerberos	要获得 Kerberos ticket
JSON-RPC 在已发现或配置的 IdM 服务器中调用基于 IdM Apache 的 web-service	HTTPS	IdM 客户端注册 ; 副本密钥检索和证书颁发（如果需要）
使用 SASL GSSAPI 验证、纯 LDAP 或两者都请求使用 TCP/TCP6 到 IdM 服务器上的端口 389	LDAP	IdM 客户端注册; CA 证书链检索; LDAP 数据复制
通过 TCP/TCP6 的请求到 IdM 服务器上的 22 端口	SSH	检查连接是否正常工作
（可选）访问 IdM 服务器上的端口 8443(TCP/TCP6)	HTTPS	在 IdM 服务器中管理证书颁发机构（只在 IdM 服务器和副本安装过程中）

第 22 章 IDM 副本安装故障排除

以下小节描述了收集有关失败的 IdM 副本安装信息的过程，以及如何解决一些常见安装问题。

22.1. IDM 副本安装错误日志文件

安装身份管理(IdM)副本时，调试信息会附加到 **副本** 上的以下日志文件中：

- **/var/log/ipareplica-install.log**
- **/var/log/ipareplica-conncheck.log**
- **/var/log/ipaclient-install.log**
- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/access**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**
- **/var/log/ipaserver-install.log**

副本安装进程还会将调试信息附加到副本所联系的 IdM **服务器** 上的以下日志文件中：

- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/access**
- **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**

每个日志文件的最后一行报告成功或失败，而 **ERROR** 和 **DEBUG** 条目则提供额外的上下文。

其他资源

- 查看 IdM 副本安装错误

22.2. 查看 IDM 副本安装错误

要解决 IdM 副本安装失败的问题，请查看新副本和服务器上安装错误日志文件的末尾，并使用这些信息解决任何相应的问题。

先决条件

- 您必须具有 **root** 特权才能显示 IdM 日志文件中的内容。

流程

1. 使用 **tail** 命令来显示主日志文件 **/var/log/ipareplica-install.log** 中的最新的错误。以下示例显示了最后 10 行。

```
[user@replica ~]$ sudo tail -n 10 /var/log/ipareplica-install.log
[sudo] password for user:
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 424, in
decorated
```

```
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 785, in
promote_check
  ensure_enrolled(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 740, in
ensure_enrolled
  raise ScriptError("Configuration of client side components failed!")

2020-05-28T18:24:51Z DEBUG The ipa-replica-install command failed, exception:
ScriptError: Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR The ipa-replica-install command failed. See
/var/log/ipareplica-install.log for more information
```

2. 要以交互方式查看日志文件，请使用 **less** 工具打开日志文件的末尾，然后使用 ↑ 和 ↓ 箭头键来导航。

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-install.log
```

3. （可选）当 **/var/log/ipareplica-install.log** 是副本安装的主日志文件时，您可以通过在副本和服务器上使用其他文件重复此查看过程来收集额外的故障排除信息。

   在副本中：

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-conncheck.log
[user@replica ~]$ sudo less -N +G /var/log/ipaclient-install.log
[user@replica ~]$ sudo less -N +G /var/log/httpd/error_log
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
[user@replica ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

   在服务器中：

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

其他资源

- IdM 副本安装错误日志文件
- 如果您无法解决失败的副本安装，且您有红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供副本的 **sosreport** 和服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

22.3. IDM CA 安装错误日志文件

在身份管理(IdM)副本上安装证书颁发机构(CA)服务会将调试信息附加到副本和与之通信的 IdM 服务器上的多个位置。

表 22.1. 在副本（按推荐的优先级顺序排列）：

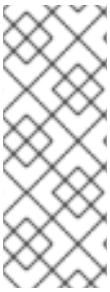
位置	描述
/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log	**pkispawn** 安装进程的高级别问题和 Python 跟踪
journalctl -u pki-tomcatd@pki-tomcat output	**pki-tomcatd@pki-tomcat** 服务中的错误
/var/log/pki/pki-tomcat/ca/debug.*$DATE*.log	公钥基础设施(PKI)产品核心中的大型 JAVA 堆栈跟踪活动
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit	PKI 产品的审计日志
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.*$DATE*.log**	用于服务主体、主机和其它使用证书实体的证书操作的低级调试数据

在由副本关联的服务器中：

- **/var/log/httpd/error_log** 日志文件

在现有 IdM 副本上安装 CA 服务也会将调试信息写入以下日志文件中：

- **/var/log/ipareplica-ca-install.log** 日志文件



注意

如果在安装可选 CA 组件时整个 IdM 副本安装失败，则不会记录有关 CA 的详情；会在 **/var/log/ipareplica-install.log** 文件中记录一条消息，表示整个安装过程失败。红帽建议查看以上列出的日志文件以了解 CA 安装失败的详情。

唯一例外是您要安装 CA 服务，root CA 是外部 CA。如果来自外部 CA 的证书出现问题，则会在 **/var/log/ipareplica-install.log** 中记录错误。

其他资源

- 检查 IdM CA 安装错误

22.4. 检查 IDM CA 安装错误

要解决 IdM CA 安装失败的问题，请查看 CA 安装错误日志文件末尾的错误，并使用这些信息来解决任何相应的问题。

先决条件

- 您必须具有 **root** 特权才能显示 IdM 日志文件中的内容。

流程

1. 要以交互方式查看日志文件，请使用 **less** 程序打开日志文件的末尾，并在搜索 **ScriptError** 条目时，使用↑ 和 ↓箭头键来导航。以下示例将打开 **/var/log/pki/pki-ca-spawn.*$TIME_OF_INSTALLATION*.log**。

```
[user@server ~]$ sudo less -N +G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. 通过重复这个对所有 CA 安装错误日志文件的查看过程来收集额外的故障排除信息。

其他资源

- IdM CA 安装错误日志文件
- 如果您无法解决失败的 IdM 服务器安装，且您有一个红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

22.5. 删除部分 IDM 副本安装

如果 IdM 副本安装失败，一些配置文件可能会留下来。安装 IdM 副本的额外尝试可能会失败，安装脚本会报告 IPA 已配置：

带有现有部分 IdM 配置的系统示例

```
[root@server ~]# ipa-replica-install
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

要解决这个问题，请从副本中卸载 IdM 软件，从 IdM 拓扑中删除副本，并重试安装过程。

先决条件

- 您必须有 **root** 权限。

流程

1. 在您要配置为 IdM 副本的主机上卸载 IdM 服务器软件。

```
[root@replica ~]# ipa-server-install --uninstall
```

2. 在拓扑中的所有其他服务器上，使用 **ipa server-del** 命令删除对未正确安装的副本的任何引用。

```
[root@other-replica ~]# ipa server-del replica.idm.example.com
```

3. 尝试安装副本。
4. 如果您因为重复安装失败而无法安装 IdM 副本，请重新安装操作系统。

安装 IdM 副本的要求之一是使用一个没有自定义的"干净"系统。失败的安装可能会因为意外修改系统文件而破坏主机的完整性。

其它资源

- 有关卸载 IdM 副本的详情，请参阅 卸载 IdM 副本。
- 如果重复卸载后尝试安装失败，且您有一个红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供副本的**sosreport** 和服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

22.6. 解决无效凭证错误

如果 IdM 副本安装失败并显示 **Invalid credentials** 错误，则主机上的系统时钟可能会彼此不同步：

```
[27/40]: setting up initial replication
Starting replication, please wait until this has completed.
Update in progress, 15 seconds elapsed
[ldap://server.example.com:389] reports: Update failed! Status: [49 - LDAP error: Invalid credentials]

[error] RuntimeError: Failed to start replication
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    Failed to start replication
ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

如果您使用 **--no-ntp** 或 **-N** 选项在时钟不同步时尝试进行副本安装，则安装会失败，因为服务无法使用 Kerberos 进行身份验证。

要解决这个问题，同步两个主机上的时钟并重试安装过程。

先决条件

- 您必须具有 **root** 权限才能修改系统时间。

流程

1. 手动或使用 **chronyd** 同步系统时钟。

   手动同步

   在服务器上显示系统时间，并设置副本的时间与之相匹配。

   ```
   [user@server ~]$ date
   Thu May 28 21:03:57 EDT 2020

   [user@replica ~]$ sudo timedatectl set-time '2020-05-28 21:04:00'
   ```

   - **与 chronyd 同步** ：
     请参阅 使用 Chrony 套件配置 NTP，以使用 **chrony** 工具配置和设置系统时间。

2. 再次尝试 IdM 副本安装。

其他资源

- 如果您无法解决失败的副本安装，且您有红帽技术支持订阅，请在 红帽客户门户网站 中创建一个技术支持问题单，并提供副本的 **sosreport** 和服务器的 **sosreport**。
- **sosreport** 工具从 RHEL 系统收集配置详情、日志和系统信息。有关 **sosreport** 工具的更多信息，请参阅 sosreport 是什么以及如何在 Red Hat Enterprise Linux 中创建它？ 。

22.7. 其他资源

- 对第一个 IdM 服务器安装进行故障排除
- IdM 客户端安装故障排除
- 备份和恢复 IdM

第 23 章 卸载 IDM 副本

作为 IdM 管理员，您可以从拓扑中删除身份管理(IdM)副本。如需更多信息，请参阅 卸载 IdM 服务器。

第 24 章 在现有 IDM 服务器上安装 DNS

按照以下流程，在最初没有安装它的身份管理(IdM)服务器上安装 DNS 服务。

先决条件

- 您了解使用带有集成 DNS 的 IdM 的优点和限制，如 安装 IdM 服务器：带有集成 DNS，带有集成 CA 作为根 CA 中所述。
- 您有到 IdM 服务器的 **root** 访问权限。

流程

1. [可选] 验证 DNS 尚未安装在 IdM 服务器上。

```
[root@r8server ~]# ipa server-role-show r8server.idm.example.com
Role name: DNS server
  Server name: r8server.idm.example.com
  Role name: DNS server
  Role status: absent
```

   输出确认服务器上没有 IdM DNS 。

2. 启用 **idm:DL1** 流：

```
[root@r8server ~]# yum module enable idm:DL1
```

3. 下载 **ipa-dns-server** 软件包及其依赖项：

```
[root@r8server ~]# yum module install idm:DL1/dns
```

4. 启动脚本来在服务器上安装 DNS：

```
[root@r8server ~]# ipa-dns-install
```

   a. 脚本提示每台服务器的 DNS 转发器。

```
Do you want to configure DNS forwarders? [yes]:
```

   - 要配置每台服务器的 DNS 转发器，请输入 **yes**，然后按照命令行中的说明操作。安装过程会将转发器 IP 地址添加到 IdM LDAP。
     - 有关正向解析策略的默认设置，请查看 **ipa-dns-install**(1)手册页中的 **--forward-policy** 描述。
   - 如果您不想使用 DNS 正向解析，请输入 **no**。
     如果没有 DNS 转发器，您 IdM 域中的主机将不能解析来自基础架构中其他的、内部的、DNS 域的名称。主机将只剩下公共 DNS 服务器来解析其 DNS 查询。

   b. 脚本会提示检查是否需要配置与服务器关联的 IP 地址的任何 DNS 反向(PTR)记录。

```
Do you want to search for missing reverse zones? [yes]:
```

   如果您运行搜索并发现丢失了反向区，脚本会询问您是否创建反向区以及 PTR 记录。

```
Do you want to create reverse zone for IP 192.0.2.1 [yes]:
Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
Using reverse zone(s) 2.0.192.in-addr.arpa.
```

注意

使用 IdM 管理反向区是可选的。您可以改为使用外部 DNS 服务来实现这一目的。

其他资源

- **man ipa-dns-install(1)**

第 25 章 从 IDM 服务器卸载集成的 IDM DNS 服务

如果您在身份管理(IdM)部署中有多个带有集成的 DNS 的服务器，您可能决定从其中一个服务器中删除集成的 DNS 服务。为此，您必须首先在其上重新安装 IdM 之前完全停用 IdM 服务器，这次没有集成的 DNS。

注意

虽然您可以将 DNS 角色添加到 IdM 服务器，但 IdM 不提供一种从 IdM 服务器中只删除 DNS 角色的方法：**ipa-dns-install** 命令没有 **--uninstall** 选项。

先决条件

- 您已在 IdM 服务器上安装了 DNS。
- 这不是您的 IdM 拓扑中最后一个集成的 DNS 服务。

流程

1. 识别冗余 DNS 服务，并按照在托管此服务的 IdM 副本上 卸载 IdM 服务器 中的流程操作。
2. 在同一个主机上，按照 没有集成的 DNS，有集成的 CA 作为 root CA 或 没有集成的 DNS，有外部 CA 作为 root CA 中的流程操作，具体取决于您的用例。

第 26 章 在没有 CA 的部署中将 IDM CA 服务添加到 IDM 服务器

如果您之前安装了没有证书颁发机构(CA)组件的身份管理(IdM)域，则您可以使用 **ipa-ca-install** 命令将 IdM CA 服务添加到域。根据您的要求，您可以选择以下选项之一：

- 将 IdM 证书服务器 CA 添加为 root CA。
- 将 IdM 证书服务器 CA 添加为从属 CA 添加，并将外部 CA 作为 root CA。

注意

有关支持的 CA 配置的详情，请参阅 规划您的 CA 服务。

26.1. 将第一个 IDM CA 作为 ROOT CA 安装到现有 IDM 域中

如果您之前安装了没有证书颁发机构(CA)组件的身份管理(IdM)，则您可以随后在 IdM 服务器上安装 CA。按照以下流程，在 *idmserver* 服务器上安装一个不隶属于任何外部 root CA 的 IdM CA。

先决条件

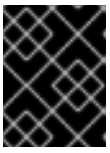
- 您在 *idmserver* 上具有 **root** 权限。
- IdM 服务器安装在 *idmserver* 上。
- 您的 IdM 部署没有安装 CA。
- 您知道 IdM **目录管理器** 的密码。

流程

1. 在 *idmserver* 上，安装 IdM 证书服务器 CA：

```
[root@idmserver ~] ipa-ca-install
```

2. 在拓扑中的每个 IdM 主机上，运行 **ipa-certupdate** 工具来使用 IdM LDAP 中的新证书的信息更新主机。



重要

如果在生成 IdM CA 证书后不运行 **ipa-certupdate**，则证书不会分发到其他 IdM 机器。

26.2. 将第一个将外部 CA 作为 ROOT CA 的 IDM CA 安装到现有 IDM 域中

如果您之前安装了没有证书颁发机构(CA)组件的身份管理(IdM)，则您可以随后在 IdM 服务器上安装 CA。按照以下流程，在 *idmserver* 服务器上安装一个 IdM CA，该 CA 隶属于外部 root CA，在 CA 之间有 0 个或多个中间 CA。

先决条件

- 您在 *idmserver* 上具有 **root** 权限。
- IdM 服务器安装在 *idmserver* 上。

- 您的 IdM 部署没有安装 CA。
- 您知道 IdM **目录管理器** 的密码。

流程

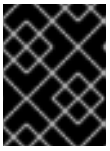
1. 开始安装：

```
[root@idmserver ~] ipa-ca-install --external-ca
```

2. 等待命令行界面通知您证书签名请求(CSR)已保存。
3. 将 CSR 提交到外部 CA。
4. 将发布的证书复制到 IdM 服务器。
5. 通过将证书和外部 CA 文件的路径添加到 **ipa-ca-install** 来继续安装：

```
[root@idmserver ~]# ipa-ca-install --external-cert-file=/root/master.crt --external-cert-file=/root/ca.crt
```

6. 在拓扑中的每个 IdM 主机上，运行 **ipa-certupdate** 工具来使用 IdM LDAP 中的新证书的信息更新主机。

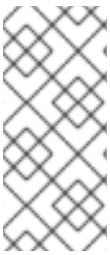


重要

在生成 IdM CA 证书后无法运行 **ipa-certupdate** 意味着证书不会被分发到其他 IdM 机器。

第 27 章 在带有 CA 的部署中将 IDM CA 服务添加到 IDM 服务器

如果您的身份管理(IdM)环境已经安装了 IdM 证书颁发机构(CA)服务，但特定的 IdM 服务器 *idmserver* 安装为没有 CA 的 IdM 副本，则您可以使用 **ipa-ca-install** 命令将 CA 服务添加到 *idmserver* 。



注意

对于以下场景，这个流程是相同的：

- IdM CA 是一个 root CA。
- IdM CA 隶属于一个外部 root CA。

先决条件

- 您在 *idmserver* 上具有 **root** 权限。
- IdM 服务器安装在 *idmserver* 上。
- 您的 IdM 部署已在另一个 IdM 服务器上安装了 CA。
- 您知道 IdM **目录管理器** 的密码。

流程

- 在 *idmserver* 上，安装 IdM 证书服务器 CA：

```
[root@idmserver ~] ipa-ca-install
```

第 28 章 从 IDM 服务器卸载 IDM CA 服务

如果您在拓扑中有超过四个带有 **CA 角色** 的身份管理(IdM)副本，并且您因为冗余的证书复制而遇到性能问题，则(RH)建议您从 IdM 副本中删除冗余的 CA 服务实例。为此，您必须首先在其上重新安装 IdM 之前完全停用受影响的 IdM 副本，这次没有 CA 服务。

注意

虽然您可以将 CA 角色 **添加** 到 IdM 副本中，但 IdM 没有提供一种从 IdM 副本中只 **删除** CA 角色的方法：**ipa-ca-install** 命令没有 **--uninstall** 选项。

先决条件

- 您已在拓扑中超过四个 IdM 服务器上安装了 IdM CA 服务。

流程

1. 识别冗余 CA 服务，并按照在托管此服务的 IdM 副本上 卸载 IdM 服务器 中的流程操作。
2. 在同一主机上，按照 安装 IdM 服务器：具有集成 DNS，没有 CA 中的流程操作。

第 29 章 管理复制拓扑

本章描述了如何管理身份管理(IdM)域中服务器之间的复制。

其他资源

- 规划副本拓扑

29.1. 解释复制协议、拓扑后缀和拓扑段

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

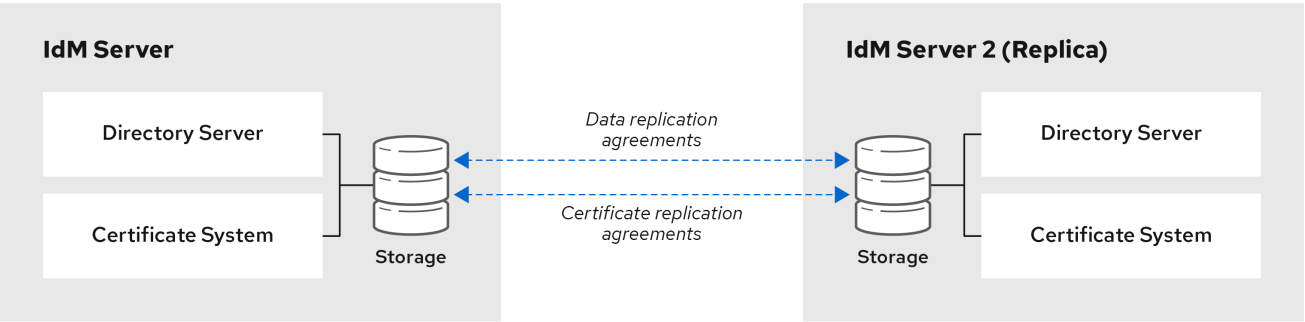
- 复制协议
- 拓扑后缀
- 拓扑段

29.1.1. IdM 副本之间的复制协议

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

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

图 29.1. 服务器和副本协议



IdM 使用两种复制协议：

域复制协议

这些协议复制身份信息。

证书复制协议

这些协议复制证书信息。

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

29.1.2. 拓扑后缀

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

配置复制协议时，它会在两个不同的服务器上加入同一类型的两个拓扑后缀。

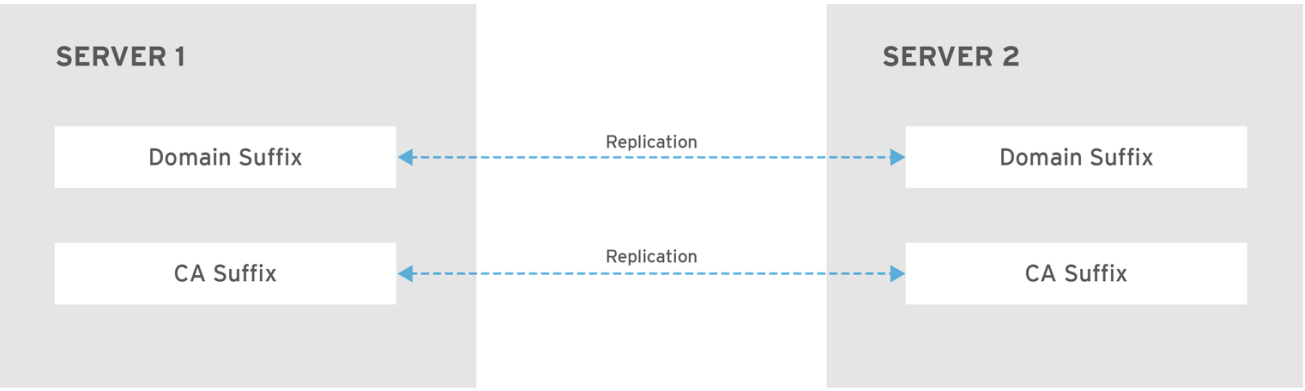
域 后缀：dc=*example*,dc=*com*

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

ca suffix: o=ipaca

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

图 29.2. **拓扑后缀**



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

例 29.1. 查看拓扑后缀

ipa topologysuffix-find 命令显示拓扑后缀列表：

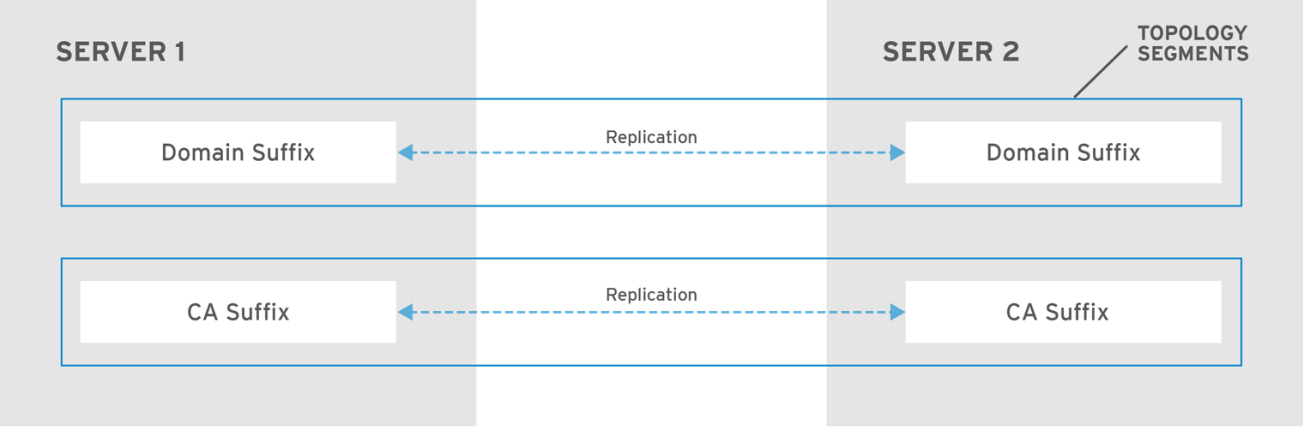
```
$ ipa topologysuffix-find
----------------------------
2 topology suffixes matched
----------------------------
  Suffix name: ca
  Managed LDAP suffix DN: o=ipaca

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

29.1.3. 拓扑段

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

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

图 29.3. 拓扑段



例 29.2. 查看拓扑段

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

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

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

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

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

29.2. 使用拓扑图来管理复制拓扑

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

访问拓扑图

要访问拓扑图：

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

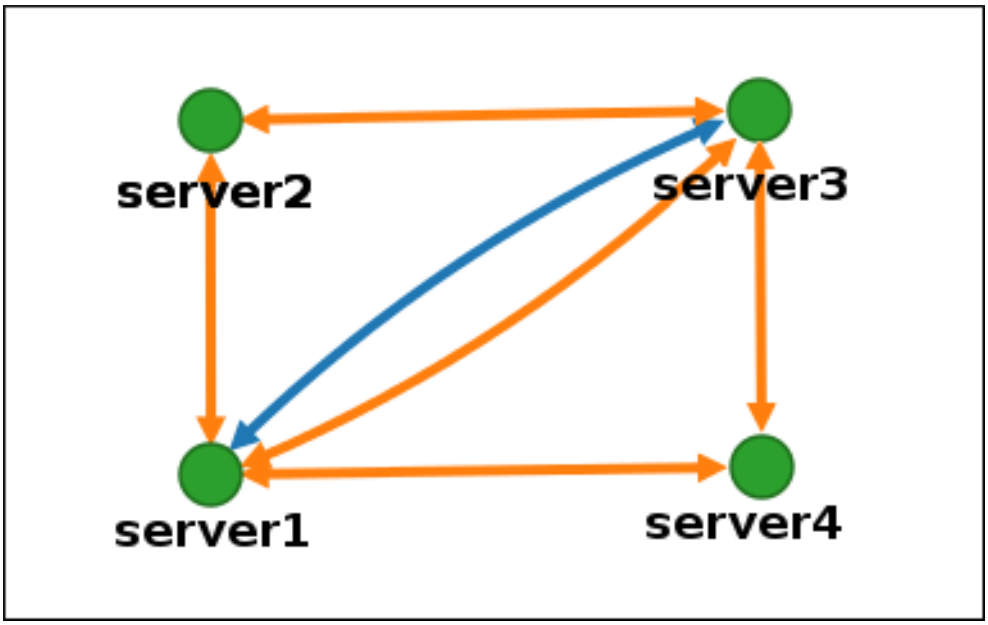
解释拓扑图

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

拓扑图示例：推荐的拓扑

以下推荐的拓扑示例显示了推荐的四个服务器的可能的拓扑之一：每个服务器至少连接到两个其他服务器，并且不止一台服务器是 CA 服务器。

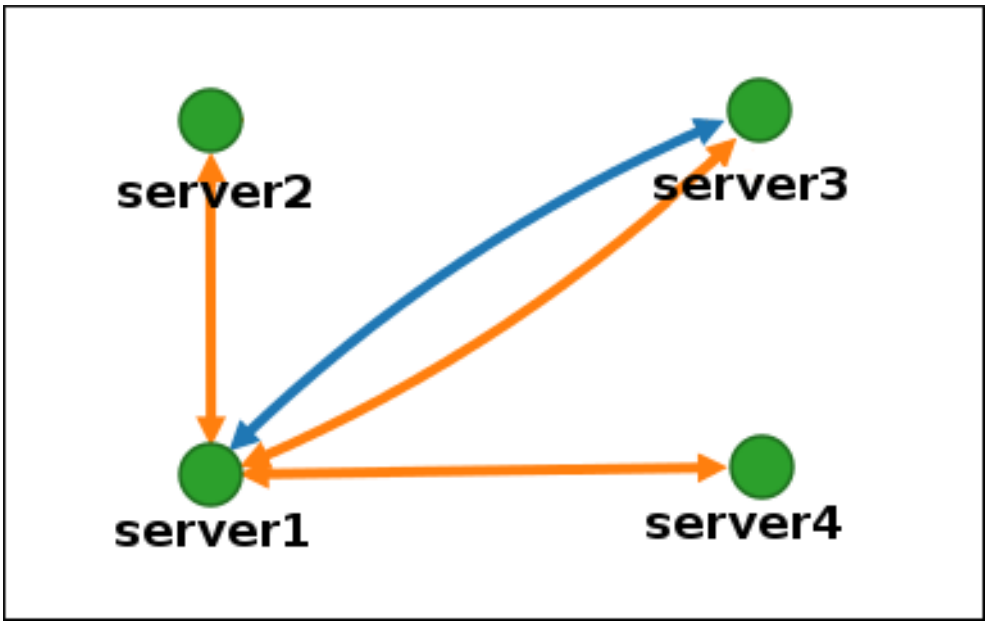
图 29.4. 建议的拓扑示例



拓扑图示例：不推荐的拓扑

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

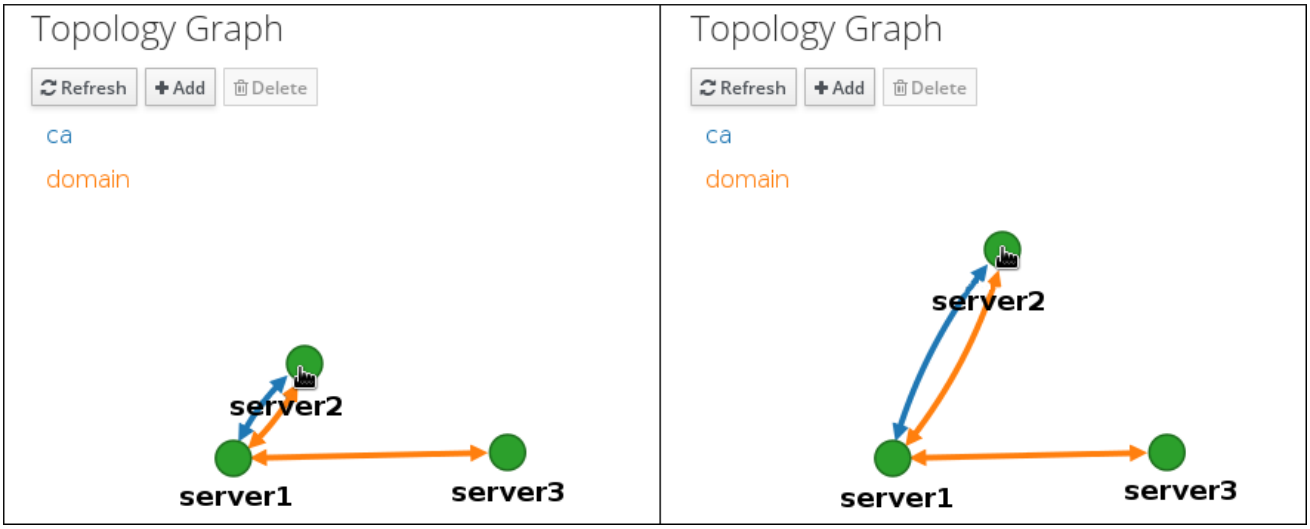
图 29.5. 不鼓励的拓扑示例：单点故障



自定义拓扑视图

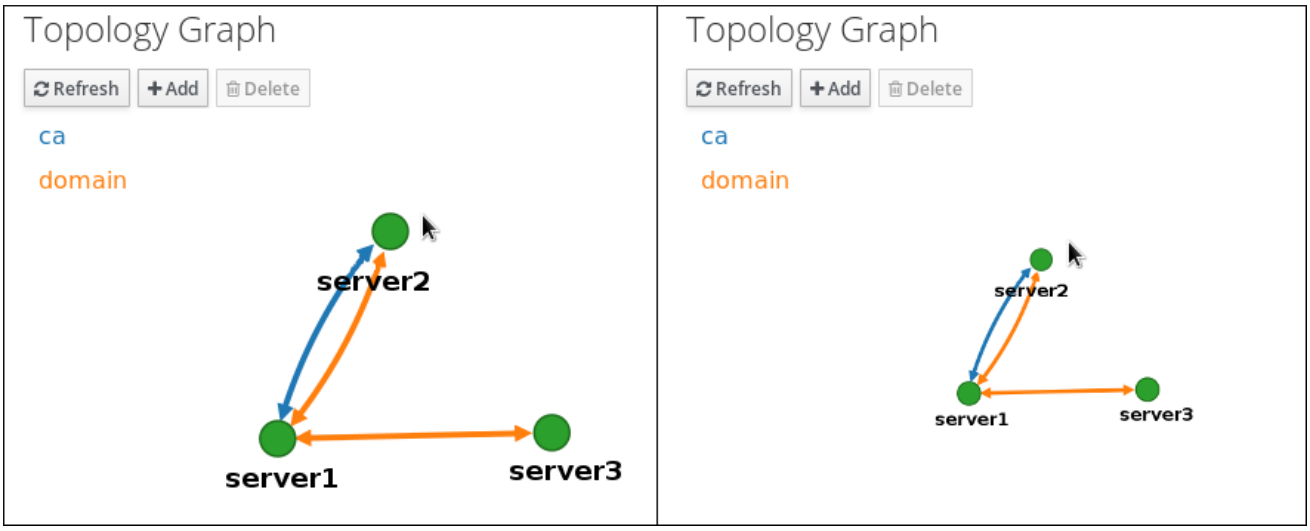
您可以通过拖动鼠标来移动单个拓扑节点：

图 29.6. 移动拓扑图节点



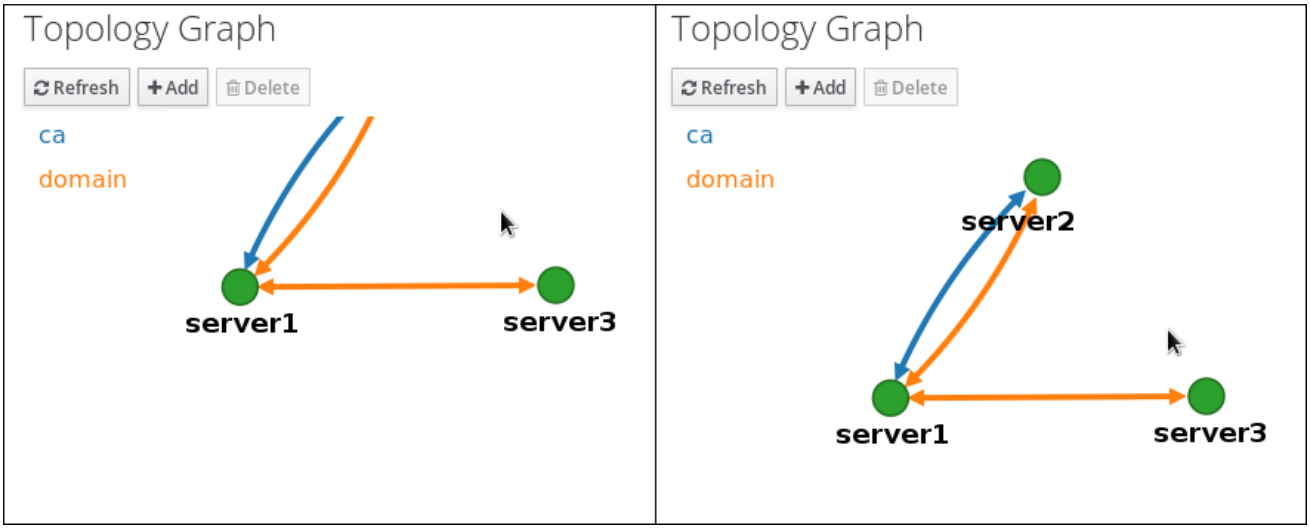
您可以使用鼠标滚轮放大和缩小拓扑图：

图 29.7. 缩放拓扑图



您可以通过按住鼠标左键来移动拓扑图的画布：

图 29.8. 移动拓扑图画布



29.3. 使用 WEB UI 在两台服务器之间设置复制

使用身份管理(IdM)的 Web 界面，您可选择两台服务器，并在它们之间创建新的复制协议。

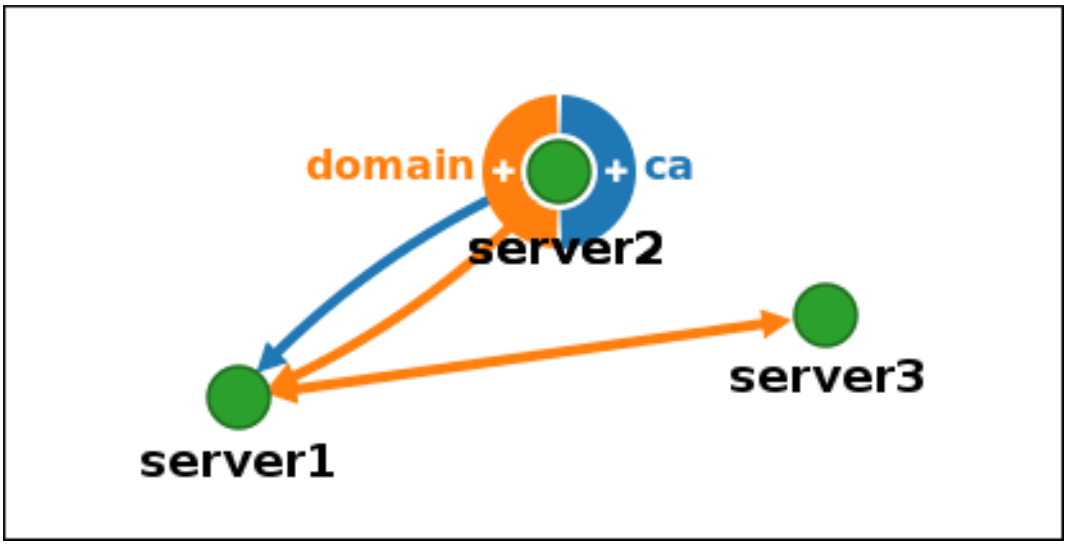
先决条件

- 您有 IdM 管理员凭证。

步骤

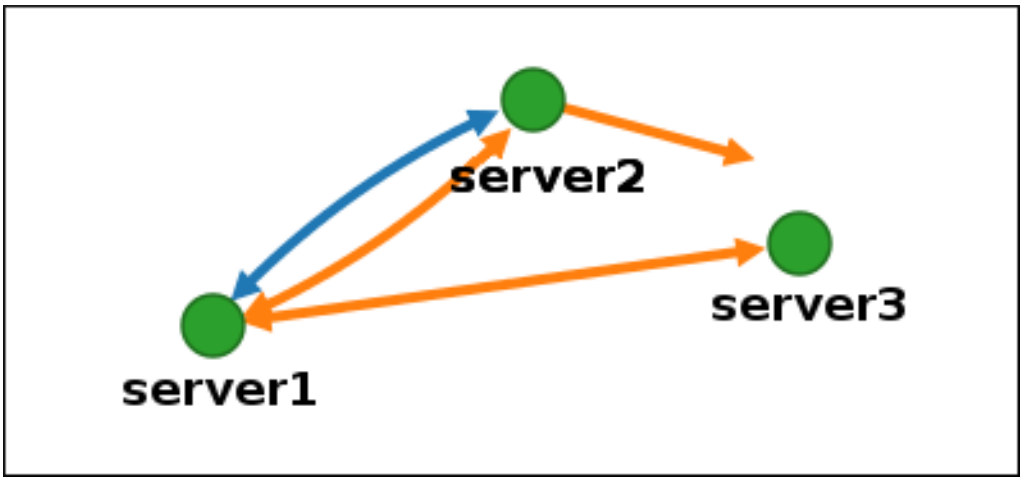
1. 在拓扑图中，将鼠标悬停在其中一台服务器节点上。

图 29.9. 域或 CA 选项



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

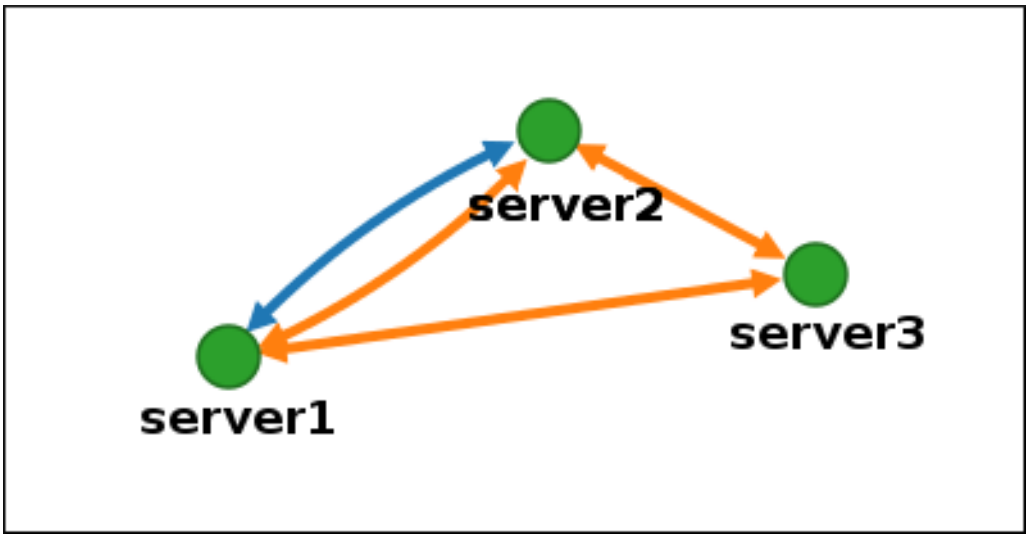
图 29.10. 创建新段



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

两个服务器之间的新拓扑段将它们加入复制协议。拓扑图现在显示更新的复制拓扑：

图 29.11. 新段创建好了



29.4. 使用 WEB UI 停止两个服务器之间的复制

使用身份管理(IdM)的 Web 界面，您可以删除服务器的复制协议。

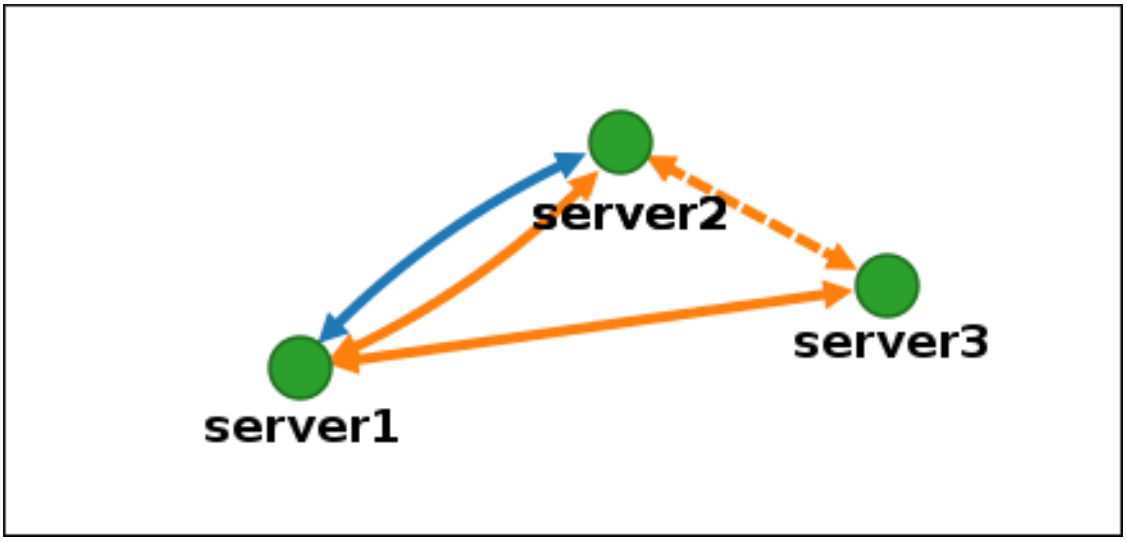
先决条件

- 您有 IdM 管理员凭证。

步骤

1. 单击代表您要删除的复制协议的箭头。这会高亮显示箭头。

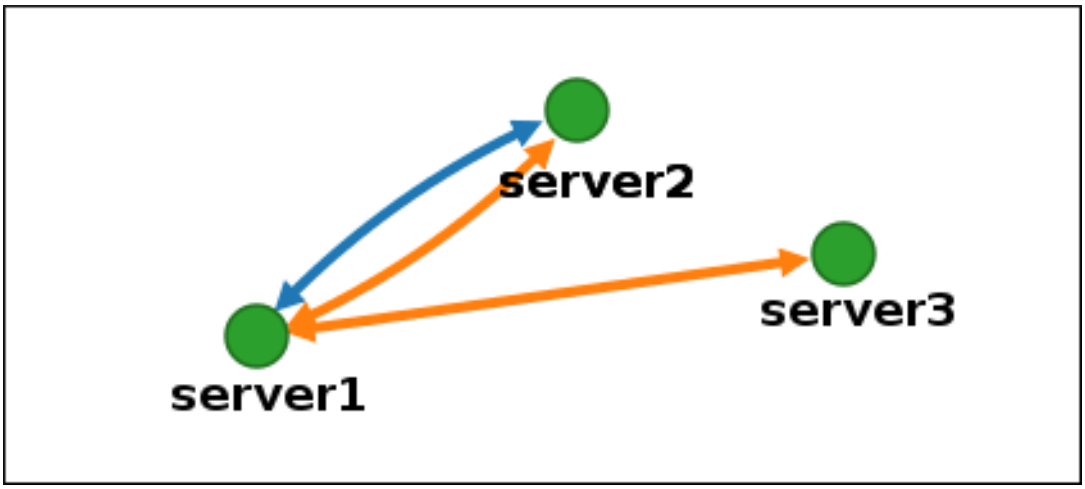
   图 29.12. 拓扑段高亮显示

2. 单击 **Delete**。
3. 在 **Confirmation** 窗口中，单击 **OK**。

IdM 删除两个服务器之间的拓扑段，这将删除它们的复制协议。拓扑图现在显示更新的复制拓扑：

图 29.13. 拓扑段删除了



29.5. 使用 CLI 在两个服务器之间建立复制

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

先决条件

- 您有 IdM 管理员凭证。

步骤

1. 使用 **ipa topologysegment-add** 命令为两台服务器创建一个拓扑段。出现提示时，请提供：
   - 所需的拓扑后缀：**domain** 或 **ca**
   - 代表两个服务器的左节点和右节点
   - （可选）段的自定义名称
     例如：

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

     添加新段来将服务器加入复制协议。

2. *可选。*使用 **ipa topologysegment-show** 命令验证是否已配置新段。

   ```
   $ ipa topologysegment-show
   Suffix name: domain
   Segment name: new_segment
   ```

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

29.6. 使用 CLI 停止两个服务器之间的复制

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

先决条件

- 您有 IdM 管理员凭证。

步骤

1. 要停止复制，您必须删除服务器之间相应的复制段。要做到这一点，您需要知道段的名称。如果您不知道名称，请使用 **ipa topologysegment-find** 命令来显示所有段，并在输出中找到所需的段。出现提示时，请提供所需的拓扑后缀： **domain** 或 **ca**。例如：

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

...

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

2. 使用 **ipa topologysegment-del** 命令删除来连接两个服务器的拓扑段。

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

删除段会删除复制协议。

3. *可选。*使用 **ipa topologysegment-find** 命令来验证段是否不再被列出。

```
$ ipa topologysegment-find
Suffix name: domain
------------------
7 segments matched
------------------
  Segment name: server2.example.com-to-server3.example.com
```

```
  Left node: server2.example.com
  Right node: server3.example.com
  Connectivity: both

...

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

29.7. 使用 WEB UI 从拓扑中删除服务器

您可以使用身份管理(IdM)Web 界面从拓扑中删除服务器。

先决条件

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

警告

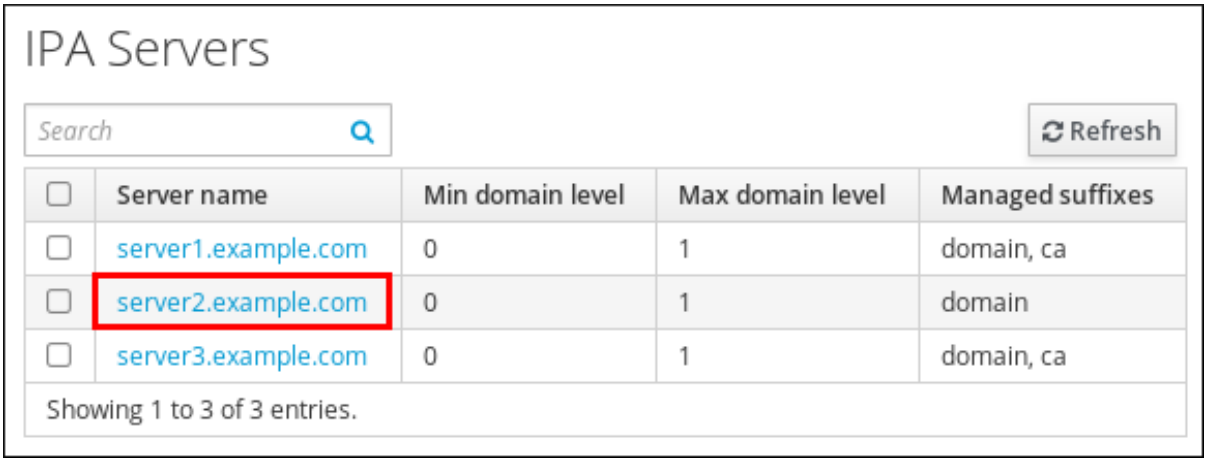
删除服务器是一个不可逆的操作。如果您删除了服务器，将其重新引入回拓扑的唯一方法是在机器上安装一个新副本。

步骤

要在不从机器卸载服务器组件的情况下从拓扑中删除服务器：

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

图 29.14. 选择服务器



3. 单击 **Delete Server**。

29.8. 使用 CLI 从拓扑中删除服务器

您可以使用命令行界面从拓扑中删除服务器。

先决条件

- 您有 IdM 管理员凭证。
- 您要删除的服务器 **不是** 连接其它服务器和拓扑其余部分的唯一服务器；这会导致其他服务器被隔离，这是不允许的。
- 您要删除的服务器 **不是** 您的最后一个 CA 或 DNS 服务器。

重要

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

步骤

要删除 **server1.example.com** ：

1. 在另一台服务器上，运行 **ipa server-del** 命令来删除 **server1.example.com**。该命令会删除指向服务器的所有拓扑段：

```
[user@server2 ~]$ ipa server-del
Server name: server1.example.com
Removing server1.example.com from replication topology, please wait...
-----------------------------------------------------------
Deleted IPA server "server1.example.com"
-----------------------------------------------------------
```

2. *可选* ：在 **server1.example.com** 上，运行 **ipa server-install --uninstall** 命令来从机器中卸载服务器组件。

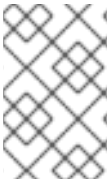
```
[root@server1 ~]# ipa server-install --uninstall
```

29.9. 使用 WEB UI 查看 IDM 服务器上的服务器角色

根据安装在 IdM 服务器上的服务，它可以执行各种 *服务器角色*。例如：

- CA 服务器
- DNS 服务器
- 密钥恢复授权(KRA)服务器。

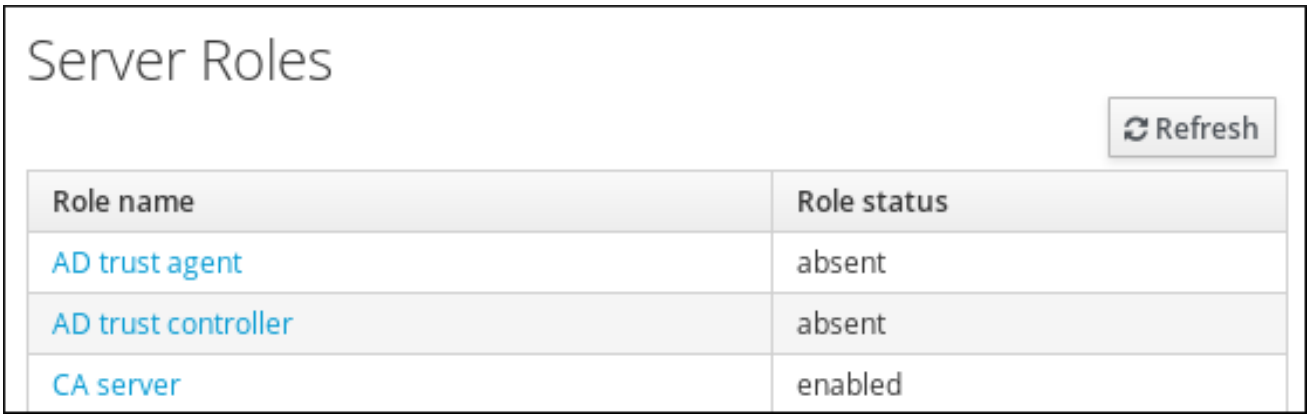
有关支持的服务器角色的完整列表，请参阅 **IPA 服务器 → 拓扑 → 服务器角色**。



注意

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

图 29.15. Web UI 中的服务器角色



29.10. 使用 CLI 查看 IDM 服务器上的服务器角色

根据安装在 IdM 服务器上的服务，它可以执行各种 *服务器角色*。例如：

- CA 服务器
- DNS 服务器
- 密钥恢复授权(KRA)服务器。

您可以使用以下命令来查看拓扑中哪些服务器执行哪些角色。

- **ipa config-show** 命令显示所有 CA 服务器以及当前 CA 续订服务器：

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

- **ipa server-show** 命令显示在特定服务器上启用的角色列表。例如，对于 *server.example.com* 上启用的角色列表：

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

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

```
$ ipa server-find --servrole "CA server"
---------------------
2 IPA servers matched
```

```
---------------------
  Server name: server1.example.com
  ...

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

29.11. 将副本提升为 CA 续订服务器和 CRL 发布者服务器

如果您的 IdM 部署使用嵌入式证书颁发机构(CA)，其中一个 IdM CA 服务器充当 CA 续订服务器（该服务器管理 CA 子系统证书的续订）。其中一个 IdM CA 服务器也充当 IdM CRL 发布者服务器（生成证书撤销列表的服务器）。默认情况下，CA 续订服务器和 CRL 发布者服务器角色安装在系统管理员使用 **ipa-server-install** 或 **ipa-ca-install** 命令在其上安装 CA 角色的第一个服务器上。

先决条件

- 您有 IdM 管理员凭证。

流程

- 更改当前的 CA 续订服务器。
- 配置副本来生成 CRL。

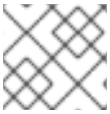
29.12. 降级或提升隐藏的副本

安装副本后，您可以配置副本是隐藏还是可见。

有关隐藏副本的详情，请参阅 隐藏副本模式。

如果副本是 CA 续订服务器，请在隐藏此副本前将服务移到另一个副本上。

详情请参阅 更改和重置 IdM CA 续订服务器。



注意

从 RHEL 8.2 开始，完全支持 RHEL 8.1 作为技术预览的隐藏副本功能。

流程

- 要隐藏副本，请输入：

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

或者，您可以使用以下命令使副本可见：

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

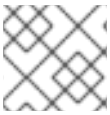
要查看拓扑中所有隐藏的副本的列表，请输入：

```
# ipa config-show
```

如果启用了所有副本，命令输出不会提到隐藏的副本

第 30 章 安装并运行 IDM HEALTHCHECK 工具

了解有关 IdM Healthcheck 工具以及如何安装和运行它的更多信息。



注意

- Healthcheck 工具只在 RHEL 8.1 或更高版本中提供。

30.1. IDM 中的 HEALTHCHECK

身份管理(IdM)中的 Healthcheck 工具可帮助发现可能影响 IdM 环境健康的问题。

注意

Healthcheck 工具是一个命令行工具，可在无需 Kerberos 身份验证的情况下使用。

模块是独立的

Healthcheck由独立模块组成，用于测试：

- 复制问题
- 证书有效期
- 证书颁发机构基础设施问题
- IdM 和 Active Directory 信任问题
- 正确的文件权限和所有权设置

两种输出格式

HealthCheck 生成以下输出，您可以使用 **output-type** 选项来设置：

- **JSON** ：JSON 格式的机器可读输出（默认）
- **human**：人类可读的输出

您可以使用 **--output-file** 选项来指定不同的文件目标。

结果

每个 Healthcheck 模块返回以下结果之一：

SUCCESS
: 配置为预期

WARNING
: 不是错误，但需要对其进行检查和评估

ERROR
: 未按预期配置

CRITICAL
: 未按预期配置，可能会有非常大的影响

30.2. 安装 IDM HEALTHCHECK

按照以下流程安装 IdM Healthcheck 工具。

流程

- 安装 **ipa-healthcheck** 软件包：

```
[root@server ~]# yum install ipa-healthcheck
```

注意

在 RHEL 8.1 和 8.2 系统上，使用 **yum install /usr/bin/ipa-healthcheck** 命令。

验证步骤

- 使用 **--failures-only** 选项使 **ipa-healthcheck** 只报告错误。功能齐全的 IdM 安装返回一个空结果 **[]**。

```
[root@server ~]# ipa-healthcheck --failures-only
[]
```

其他资源

- 使用 **ipa-healthcheck --help** 查看所有支持的参数。

30.3. 运行 IDM HEALTHCHECK

Healthcheck 可以手动运行，也可以使用 日志循环 自动运行。

先决条件

- 必须安装 Healthcheck 工具。请参阅 安装 IdM Healthcheck。

流程

- 要手动运行healthcheck，请输入 **ipa-healthcheck** 命令。

```
[root@server ~]# ipa-healthcheck
```

其他资源

有关所有选项，请查看手册页: **man ipa-healthcheck**。

30.4. 其他资源

- 有关使用 IdM 健康检查的示例，请参阅 配置和管理身份管理 指南中的以下章节。
  - 检查服务
  - 验证您的 IdM 和 AD 信任配置

- 验证证书
- 验证系统证书
- 检查磁盘空间
- 验证 IdM 配置文件的权限
- 检查复制

- 您还可以看到这些章节被组织到一个指南中：使用 IdM 健康检查来监控 IdM 环境

第 31 章 使用 ANSIBLE PLAYBOOK 来安装身份管理服务器

了解如何使用 Ansible 将系统配置为 IdM 服务器。将系统配置为 IdM 服务器建立 IdM 域并让系统向 IdM 客户端提供 IdM 服务。您可以使用 **ipaserver** Ansible 角色来管理部署。

先决条件

- 您了解了一般的 Ansible 和 IdM 概念。

31.1. ANSIBLE 及其安装 IDM 的优点

Ansible 是一个自动化工具，用于配置系统、部署软件和执行滚动更新。Ansible 包含对身份验证(IdM)的支持，您可以使用 Ansible 模块来自动执行安装任务，如 IdM 服务器、副本、客户端或整个 IdM 拓扑的设置。

使用 Ansible 安装 IdM 的优点
以下列表提供了使用 Ansible 安装身份管理与手动安装的优点。

- 您不需要登录受管节点。
- 您不需要配置每个主机上的设置来单独部署。反之，您可以有一个清单文件来部署完整的集群。
- 您可以稍后重复将清单文件用于管理任务，例如添加用户和主机。即使与 IdM 相关的任务，也可以重复使用清单文件。

其他资源

- 自动化 Red Hat Identity Management 安装
- 规划身份管理
- 为 IdM 服务器安装准备系统

31.2. 安装 ANSIBLE-FREEIPA 软件包

按照以下流程安装 **ansible-freeipa** 软件包，该软件包为安装和管理身份管理(IdM)提供 Ansible 角色和模块。

先决条件

- 确定控制器是一个带有有效订阅的 Red Hat Enterprise Linux 系统。否则，请参阅官方 Ansible 文档 安装指南 来获取替代安装说明。
- 确保您可以通过 **SSH** 协议，从控制器访问受管节点。检查该受管节点是否已列在控制器的 **/root/.ssh/known_hosts** 文件中。

流程

在 Ansible 控制器上使用以下步骤。

1. 如果您的系统在 RHEL 8.5 及更早版本中运行，请启用所需的软件仓库：

```
# subscription-manager repos --enable ansible-2.8-for-rhel-8-x86_64-rpms
```

2. 如果您的系统在 RHEL 8.5 及更早版本中运行，请安装 **ansible** 软件包：

```
# yum install ansible
```

3. 安装 **ansible-freeipa** 软件包：

```
# yum install ansible-freeipa
```

角色和模块安装到 **/usr/share/ansible/roles/** 和 **/usr/share/ansible/plugins/modules** 目录中。

31.3. 在文件系统中的 ANSIBLE 角色位置

默认情况下，**ansible-freeipa** 角色安装到 **/usr/share/ansible/roles/** 目录。**ansible-freeipa** 软件包的结构如下：

- **/usr/share/ansible/roles/** 目录将 **ipaserver**、**ipareplica** 和 **ipaclient** 角色存储在 Ansible 控制器上。每个角色目录都会在 **README.md** Markdown 文件中保存示例、基本概述、有关角色的许可证和文档。

```
[root@server]# ls -1 /usr/share/ansible/roles/
ipaclient
ipareplica
ipaserver
```

- **/usr/share/doc/ansible-freeipa/** 目录将有关各个角色和拓扑的文档存储在 **README.md** Markdown 文件中。它还存储了 **playbooks/** 子目录。

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/
playbooks
README-client.md
README.md
README-replica.md
README-server.md
README-topology.md
```

- **/usr/share/doc/ansible-freeipa/playbooks/** 目录存储示例 playbook:

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/playbooks/
install-client.yml
install-cluster.yml
install-replica.yml
install-server.yml
uninstall-client.yml
uninstall-cluster.yml
uninstall-replica.yml
uninstall-server.yml
```

31.4. 为带有集成 DNS 和集成 CA 作为根 CA 的部署设置参数

完成这个流程，来在使用 IdM 集成 DNS 解决方案的环境中为安装带有集成 CA 作为根 CA 的 IdM 服务器配置清单文件。

注意

此流程中的清单使用 **INI** 格式。或者，也可以使用 **YAML** 或 **JSON** 格式。

流程

1. 创建 **~/MyPlaybooks/** 目录：

```
$ mkdir MyPlaybooks
```

2. 创建一个 **~/MyPlaybooks/inventory** 文件。

3. 打开清单文件进行编辑。指定您要用作 IdM 服务器的主机的完全限定域名(**FQDN**)。确保 **FQDN** 满足以下条件：

   - 只允许字母数字字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。

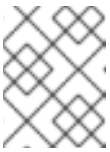
4. 指定 IdM 域和域信息。

5. 通过添加以下选项来指定您要使用集成的 DNS：

```
ipaserver_setup_dns=true
```

6. 指定 DNS 转发设置。选择以下选项之一：

   - 如果您希望安装程序使用 **/etc/resolv.conf** 文件中的正向解析器，请使用 **ipaserver_auto_forwarders=true** 选项。如果在 **/etc/resolv.conf** 文件中指定的名称服务器是 localhost 127.0.0.1 地址，或者位于虚拟私有网络中，并且您使用的 DNS 服务器通常无法从公共互联网访问，则不要使用这个选项。
   - 使用 **ipaserver_forwarders** 选项手动指定您的转发器。安装过程将转发器 IP 地址添加到安装的 IdM 服务器上的 **/etc/named.conf** 文件中。
   - 使用 **ipaserver_no_forwarders=true** 选项配置要使用的根 DNS 服务器。



注意

如果没有 DNS 转发器，您的环境会被隔离，且基础架构中的其他 DNS 域的名称不会被解析。

7. 指定 DNS 反向记录和区域设置。从以下选项中选择：

   - 使用 **ipaserver_allow_zone_overlap=true** 选项来允许创建（反向）区域，即使区已经可解析。
   - 使用 **ipaserver_reverse_zones** 选项来手动指定反向区域。
   - 如果您不希望安装程序创建反向 DNS 区域，请使用 **ipaserver_no_reverse=true** 选项。

注意

使用 IdM 管理反向区是可选的。您可以改为使用外部 DNS 服务来实现这一目的。

8. 指定 **admin** 和 **Directory Manager** 的密码。使用 Ansible Vault 来存储密码，并从 playbook 文件中引用 Vault 文件。另外，也可以更安全地指定清单文件中直接的密码。

9. （可选）指定要由 IdM 服务器使用的自定义 **firewalld** 区域。如果您没有设置自定义区，IdM 会将其服务添加到默认的 **firewalld** 区域中。预定义的默认区域是 **public**。

重要

指定的 **firewalld** 区域必须存在，并且是永久的。

包含所需服务器信息的清单文件示例（密码除外）

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
[...]
```

包含所需服务器信息（包括密码）的清单文件示例

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

带有自定义 firewalld 区的清单文件示例

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

使用存储在 Ansible Vault 文件中的 admin 和 Directory Manager 密码设置 IdM 服务器的 playbook 示例

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

使用清单文件中的 admin 和 Directory Manager 密码来设置 IdM 服务器的 playbook 示例

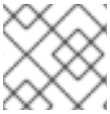
```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    state: present
```

其他资源

- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.5. 为带有外部 DNS 和集成 CA 作为根 CA 的部署设置参数

完成这个流程，来为在使用外部 DNS 解决方案的环境中安装带有集成 CA 作为根 CA 的 IdM 服务器配置清单文件。



注意

此流程中的清单文件使用 **INI** 格式。或者，也可以使用 **YAML** 或 **JSON** 格式。

流程

1. 创建 **~/MyPlaybooks/** 目录：

```
$ mkdir MyPlaybooks
```

2. 创建一个 **~/MyPlaybooks/inventory** 文件。
3. 打开清单文件进行编辑。指定您要用作 IdM 服务器的主机的完全限定域名(**FQDN**)。确保 **FQDN** 满足以下条件：
   - 只允许字母数字字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。

4. 指定 IdM 域和域信息。

5. 确保 **ipaserver_setup_dns** 选项被设为 **no** 或空缺。

6. 指定 **admin** 和 **Directory Manager** 的密码。使用 Ansible Vault 来存储密码，并从 playbook 文件中引用 Vault 文件。另外，也可以更安全地指定清单文件中直接的密码。

7. （可选）指定要由 IdM 服务器使用的自定义 **firewalld** 区域。如果您没有设置自定义区，IdM 会将其服务添加到默认的 **firewalld** 区域中。预定义的默认区域是 **public**。

重要

指定的 **firewalld** 区域必须存在，并且是永久的。

包含所需服务器信息的清单文件示例（密码除外）

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

包含所需服务器信息（包括密码）的清单文件示例

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

带**有自定义 firewalld 区的清单文件示例**

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

使用存储在 Ansible Vault 文件中的 admin 和 Directory Manager 密码设置 IdM 服务器的 playbook 示例

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

使用清单文件中的 admin 和 Directory Manager 密码来设置 IdM 服务器的 playbook 示例

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

  roles:
  - role: ipaserver
    state: present
```

其他资源

- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.6. 使用 ANSIBLE PLAYBOOK 将集成 CA 的 IDM 服务器部署为 ROOT CA

完成此流程，来使用 Ansible playbook 部署带有集成证书颁发机构(CA)作为根 CA 的 IdM 服务器。

先决条件

- 受管节点是一个具有静态 IP 地址和可正常工作的软件包管理器的 Red Hat Enterprise Linux 8 系统。
- 您已通过选择以下流程之一设置了与您的场景相应的参数：
  - 带有集成 DNS 的流程
  - 带有外部 DNS 的流程

流程

1. 运行 Ansible playbook:

```
$ ansible-playbook -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-server.yml
```

2. 选择以下选项之一：

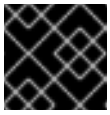
- 如果您的 IdM 部署使用外部 DNS：将包含在 **/tmp/ipa.system.records.UFRPto.db** 文件中的 DNS 资源记录添加到现有的外部 DNS 服务器中。更新 DNS 记录的过程因特定的 DNS 解决方案而异。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

在将 DNS 记录添加到现有 DNS 服务器之前，服务器安装不会完成。

- 如果您的 IdM 部署使用集成的 DNS:
  - 将父域中的 DNS 委托程序添加到 IdM DNS 域。例如，如果 IdM DNS 域是 ***idm.example.com***，请在 **example.com** 父域中添加一个名字服务器(NS)记录。



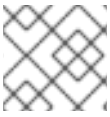
重要

每次安装 IdM DNS 服务器后都会重复这个步骤。

  - 将时间服务器的 **_ntp._udp** 服务(SRV)记录添加到您的 IdM DNS。IdM DNS 中新安装的 IdM 服务器的时间服务器的 SRV 记录可确保将来的副本和客户端安装会自动配置为与此主 IdM 服务器使用的时间服务器同步。

31.7. 为带有集成 DNS 和外部 CA 作为根 CA 的部署设置参数

完成这个流程，来为在使用 IdM 集成 DNS 解决方案的环境中安装带有外部 CA 作为根 CA 的 IdM 服务器配置清单文件。



注意

此流程中的清单文件使用 **INI** 格式。或者，也可以使用 **YAML** 或 **JSON** 格式。

流程

1. 创建 **~/MyPlaybooks/** 目录：

```
$ mkdir MyPlaybooks
```

2. 创建一个 **~/MyPlaybooks/inventory** 文件。
3. 打开清单文件进行编辑。指定您要用作 IdM 服务器的主机的完全限定域名(**FQDN**)。确保 **FQDN** 满足以下条件：
   - 只允许字母数字字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。
4. 指定 IdM 域和域信息。

5. 通过添加以下选项来指定您要使用集成的 DNS：

```
ipaserver_setup_dns=true
```

6. 指定 DNS 转发设置。选择以下选项之一：

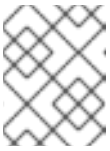
- 如果您希望安装过程使用 **/etc/resolv.conf** 文件中的正向解析器，请使用 **ipaserver_auto_forwarders=true** 选项。如果 **/etc/resolv.conf** 文件中指定的名字服务器是 localhost 127.0.0.1 地址，或者如果您在虚拟私有网络中，并且您使用的 DNS 服务器通常无法从公共互联网访问，则不建议使用此选项。
- 使用 **ipaserver_forwarders** 选项手动指定您的转发器。安装过程将转发器 IP 地址添加到安装的 IdM 服务器上的 **/etc/named.conf** 文件中。
- 使用 **ipaserver_no_forwarders=true** 选项配置要使用的根 DNS 服务器。

注意

如果没有 DNS 转发器，您的环境会被隔离，且基础架构中的其他 DNS 域的名称不会被解析。

7. 指定 DNS 反向记录和区域设置。从以下选项中选择：

- 使用 **ipaserver_allow_zone_overlap=true** 选项来允许创建（反向）区域，即使区已经可解析。
- 使用 **ipaserver_reverse_zones** 选项来手动指定反向区域。
- 如果您不希望安装过程创建反向 DNS 区域，请使用 **ipaserver_no_reverse=true** 选项。



注意

使用 IdM 管理反向区是可选的。您可以改为使用外部 DNS 服务来实现这一目的。

8. 指定 **admin** 和 **Directory Manager** 的密码。使用 Ansible Vault 来存储密码，并从 playbook 文件中引用 Vault 文件。另外，也可以更安全地指定清单文件中直接的密码。

9. （可选）指定要由 IdM 服务器使用的自定义 **firewalld** 区域。如果您没有设置自定义区，IdM 会将其服务添加到默认的 **firewalld** 区中。预定义的默认区域是 **public**。

重要

指定的 **firewalld** 区域必须存在，并且是永久的。

包含所需服务器信息的清单文件示例（密码除外）

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
```

```
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
[...]
```

包含所需服务器信息（包括密码）的清单文件示例

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

带**有自定义 firewalld 区的清单文件示例**

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

10. 为安装的第一个步骤创建一个 playbook。输入有关生成证书签名请求(CSR)，并将其从控制器复制到受管节点的说明。

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: true

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
```

```
    src: /root/ipa.csr
    dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    flat: true
```

11. 为安装的最后步骤创建另一个 playbook。

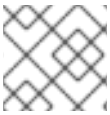
```
---
- name: Playbook to configure IPA server Step 2
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files:
      - "/root/servercert20240601.pem"
      - "/root/cacert.pem"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] }}-{{ item }}" to "/root/{{ item }}" on node
    ansible.builtin.copy:
      src: "{{ groups.ipaserver[0] }}-{{ item }}"
      dest: "/root/{{ item }}"
      force: true
    with_items:
    - servercert20240601.pem
    - cacert.pem

  roles:
  - role: ipaserver
    state: present
```

其他资源

- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.8. 为带有外部 DNS 和外部 CA 作为根 CA 的部署设置参数

完成这个流程，来为在使用外部 DNS 解决方案的环境中安装带有外部 CA 作为根 CA 的 IdM 服务器配置清单文件。



注意

此流程中的清单文件使用 **INI** 格式。或者，也可以使用 **YAML** 或 **JSON** 格式。

流程

1. 创建 **~/MyPlaybooks/** 目录：

```
$ mkdir MyPlaybooks
```

2. 创建一个 **~/MyPlaybooks/inventory** 文件。

3. 打开清单文件进行编辑。指定您要用作 IdM 服务器的主机的完全限定域名(**FQDN**)。确保 **FQDN** 满足以下条件：

   - 只允许字母数字字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。

4. 指定 IdM 域和域信息。

5. 确保 **ipaserver_setup_dns** 选项被设为 **no** 或空缺。

6. 指定 **admin** 和 **Directory Manager** 的密码。使用 Ansible Vault 来存储密码，并从 playbook 文件中引用 Vault 文件。另外，也可以更安全地指定清单文件中直接的密码。

7. （可选）指定要由 IdM 服务器使用的自定义 **firewalld** 区域。如果您没有设置自定义区，IdM 会将其服务添加到默认的 **firewalld** 区域中。预定义的默认区域是 **public**。

重要

指定的 **firewalld** 区域必须存在，并且是永久的。

包含所需服务器信息的清单文件示例（密码除外）

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

包含所需服务器信息（包括密码）的清单文件示例

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

带有自定义 firewalld 区的清单文件示例

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

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
```

```
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

8. 为安装的第一个步骤创建一个 playbook。输入有关生成证书签名请求(CSR)，并将其从控制器复制到受管节点的说明。

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: true

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: true
```

9. 为安装的最后步骤创建另一个 playbook。

```
---
- name: Playbook to configure IPA server Step 2
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files:
      - "/root/servercert20240601.pem"
      - "/root/cacert.pem"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] }}-{{ item }}" to "/root/{{ item }}" on node
    ansible.builtin.copy:
      src: "{{ groups.ipaserver[0] }}-{{ item }}"
      dest: "/root/{{ item }}"
      force: true
    with_items:
    - servercert20240601.pem
    - cacert.pem
```

```
roles:
- role: ipaserver
  state: present
```

其他资源

- 安装 IdM 服务器： 在不集成 DNS 的情况下，使用外部 CA 作为 root CA
- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.9. 使用 ANSIBLE PLAYBOOK 将外部 CA 部署 IDM 服务器作为 ROOT CA

完成此流程，来使用 Ansible playbook 部署具有外部证书颁发机构(CA)作为根 CA 的 IdM 服务器。

先决条件

- 受管节点是一个具有静态 IP 地址和可正常工作的软件包管理器的 Red Hat Enterprise Linux 8 系统。
- 您已通过选择以下流程之一设置了与您的场景相应的参数：
  - 带有集成 DNS 的流程
  - 带有外部 DNS 的流程

流程

1. 使用安装第一步的说明运行 Ansible playbook，如 **install-server-step1.yml** ：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
~/MyPlaybooks/install-server-step1.yml
```

2. 在控制器上找到 **ipa.csr** 证书签名请求文件，并提交给外部的 CA。
3. 将外部 CA 签名的 IdM CA 证书放在控制器文件系统中，以便下一步中的 playbook 可以找到它。
4. 使用安装最后一步的说明运行 Ansible playbook，如 **install-server-step2.yml** ：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-server-
step2.yml
```

5. 选择以下选项之一：
   - 如果您的 IdM 部署使用外部 DNS：将包含在 **/tmp/ipa.system.records.UFRPto.db** 文件中的 DNS 资源记录添加到现有的外部 DNS 服务器中。更新 DNS 记录的过程因特定的 DNS 解决方案而异。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
```

```
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

在将 DNS 记录添加到现有 DNS 服务器之前，服务器安装不会完成。

- 如果您的 IdM 部署使用集成的 DNS:
  - 将父域中的 DNS 委托程序添加到 IdM DNS 域。例如，如果 IdM DNS 域是 ***idm.example.com***，请在 **example.com** 父域中添加一个名字服务器(NS)记录。

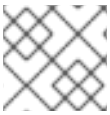
    

    重要

    每次安装 IdM DNS 服务器后都会重复这个步骤。

  - 将时间服务器的 **_ntp._udp** 服务(SRV)记录添加到您的 IdM DNS。IdM DNS 中新安装的 IdM 服务器的时间服务器的 SRV 记录可确保将来的副本和客户端安装会自动配置为与此主 IdM 服务器使用的时间服务器同步。

31.10. 使用 ANSIBLE PLAYBOOK 卸载 IDM 服务器



注意

在现有的身份管理(IdM)部署中，**副本** 和 **服务器** 是可交换的术语。

完成此流程，使用 Ansible playbook 来卸载 IdM 副本。在本例中：

- 从 **server123.idm.example.com** 卸载 IdM 配置。
- **server123.idm.example.com** 和关联的主机条目从 IdM 拓扑中删除。

先决条件

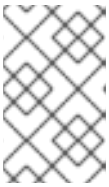
- 在控制节点上：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已在 ***~/MyPlaybooks/*** 目录中创建了一个带有 IdM 服务器的完全限定域名(FQDN)的 Ansible 清单文件。在本例中，FQDN 是 **server123.idm.example.com**。
  - 您已将 **ipaadmin_password** 存储在 **secret.yml** Ansible vault 中。
  - 要使 **ipaserver_remove_from_topology** 选项正常工作，系统必须运行在 RHEL 8.9 或更高版本上。
- 在受管节点上：
  - 系统在 RHEL 8 上运行。

流程

1. 使用以下内容创建 Ansible playbook 文件 **uninstall-server.yml** ：

```
---
- name: Playbook to uninstall an IdM replica
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    ipaserver_remove_from_domain: true
    state: absent
```

ipaserver_remove_from_domain 选项从 IdM 拓扑中取消主机注册。



注意

如果 server123.idm.example.com 的删除导致断开连接的拓扑，则删除操作将被中止。如需更多信息，请参阅 如果这会导致断开连接的拓扑，请使用 Ansible playbook 卸载 IdM 服务器。

2. 卸载副本：

```
$ ansible-playbook --vault-password-file=password_file -v -i
<path_to_inventory_directory>/inventory <path_to_playbooks_directory>/uninstall-
server.yml
```

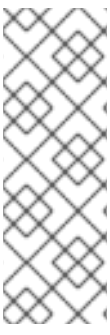
3. 确保指向 **server123.idm.example.com** 的所有名称服务器(NS) DNS 记录都从 DNS 区域中删除。无论您使用由 IdM 还是外部 DNS 管理的集成 DNS，这个均适用。有关如何从 IdM 中删除 DNS 记录的更多信息，请参阅 在 IdM CLI 中删除 DNS 记录 。

31.11. 如果这会导致断开连接的拓扑，请使用 ANSIBLE PLAYBOOK 卸载 IDM 服务器

注意

在现有的身份管理(IdM)部署中，**副本** 和 **服务器** 是可交换的术语。

完成此流程，使用 Ansible playbook 卸载 IdM 副本，即使这会导致断开连接的 IdM 拓扑。在示例中，**server456.idm.example.com** 用于从拓扑中删除副本和 FQDN 为 server123.idm.example.com **server123.idm.example.com** 的相关的主机条目，使某些副本与 **server456.idm.example.com** 以及拓扑的其余部分断开连接。



注意

如果只使用 **remove_server_from_domain** 从拓扑中删除副本不会导致断开连接的拓扑，则不需要其他选项。如果结果是断开连接的拓扑，您必须指定您要保留域的哪一部分。在这种情况下，您必须执行以下操作：

- 指定 **ipaserver_remove_on_server** 值。
- 将 **ipaserver_ignore_topology_disconnect** 设置为 True。

先决条件

- 在控制节点上：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 系统运行在 RHEL 8.9 或更高版本上。
  - 您已安装 **ansible-freeipa** 软件包。
  - 您已在 ***~/MyPlaybooks/*** 目录中创建了一个带有 IdM 服务器的完全限定域名(FQDN)的 Ansible 清单文件。在本例中，FQDN 是 **server123.idm.example.com**。
  - 您已将 **ipaadmin_password** 存储在 **secret.yml** Ansible vault 中。
- 在受管节点上：
  - 系统在 8 或更高版本中运行。

流程

1. 使用以下内容创建 Ansible playbook 文件 **uninstall-server.yml** ：

```
---
- name: Playbook to uninstall an IdM replica
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    ipaserver_remove_from_domain: true
    ipaserver_remove_on_server: server456.idm.example.com
    ipaserver_ignore_topology_disconnect: true
    state: absent
```

注意

正常情况下，如果删除 server123 不会造成断开连接的拓扑：如果 **ipaserver_remove_on_server** 的值没有设置，则 server123 上的副本会使用 server123 的复制协议自动删除。

2. 卸载副本：

```
$ ansible-playbook --vault-password-file=password_file -v -i
<path_to_inventory_directory>/hosts <path_to_playbooks_directory>/uninstall-
server.yml
```

3. 确保指向 **server123.idm.example.com** 的所有名称服务器(NS) DNS 记录都从 DNS 区域中删除。无论您使用由 IdM 还是外部 DNS 管理的集成 DNS，这个均适用。有关如何从 IdM 中删除 DNS 记录的更多信息，请参阅 在 IdM CLI 中删除 DNS 记录 。

31.12. 其他资源

- 规划副本拓扑

- 使用 Ansible playbook 备份和恢复 IdM 服务器
- 清单基础知识：格式、主机和组

第 32 章 使用 ANSIBLE PLAYBOOK 安装身份管理副本

使用 Ansible 将其注册到 IdM 域来将系统配置为 IdM 副本，并让系统在域中的 IdM 服务器上使用 IdM 服务。

部署是由 **ipareplica** Ansible 角色来管理的。该角色可以使用自动发现模式来识别 IdM 服务器、域和其他设置。但是，如果您在类似层的模式中部署多个副本，在不同时间部署不同的副本组，则必须为每个组定义特定的服务器或副本。

先决条件

- 您已在 Ansible 控制节点上安装了 ansible-freeipa 软件包。
- 您了解了一般的 Ansible 和 IdM 概念。
- 您已 计划部署中的副本拓扑。

32.1. 指定用于安装 IDM 副本的基础、服务器和客户端变量

完成这个步骤来配置用于安装 IdM 副本的清单文件。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。

流程

1. 打开清单文件进行编辑。指定主机的完全限定域名(FQDN)来成为 IdM 副本。FQDN 必须是有效的 DNS 名称：
   - 仅允许数字、字母字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。

   仅定义副本 FQDN 的简单清单主机文件示例

   ```
   [ipareplicas]
   replica1.idm.example.com
   replica2.idm.example.com
   replica3.idm.example.com
   [...]
   ```

   如果 IdM 服务器已经部署，且在 IdM DNS 区中正确设置了 SRV 记录，那么脚本会自动发现所有其他必需的值。

2. [可选] 根据您的拓扑设计方式在清单文件中提供额外的信息：

   场景 1

   如果要避免自动发现，并且使 **[ipareplicas]** 部分中列出的所有副本都使用特定的 IdM 服务器，请在清单文件的 **[ipaservers]** 部分中设置服务器。

带有 IdM 服务器 FQDN 和定义的副本的清单主机文件示例

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

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]
```

场景 2

或者，如果您想避免自动发现，但希望使用特定的服务器来部署特定副本，请分别在清单文件的 **[ipareplicas]** 部分中为特定副本设置服务器。

为特定副本定义了特定 IdM 服务器的清单文件示例

```
[ipaservers]
server.idm.example.com
replica1.idm.example.com

[ipareplicas]
replica2.idm.example.com
replica3.idm.example.com ipareplica_servers=replica1.idm.example.com
```

在上例中，**replica3.idm.example.com** 使用已部署的 **replica1.idm.example.com** 作为其复制源。

场景 3

如果您在一个批处理中部署多个副本，并且时间是您关心的问题，那么多层副本部署可能对您很有用。在清单文件中定义特定的副本组，如 **[ipareplicas_tier1]** 和 **[ipareplicas_tier2]**，并在 **install-replica.yml** playbook 中为每个组设计单独的 play。

定义了副本层的清单文件示例

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

[ipareplicas_tier1]
replica1.idm.example.com

[ipareplicas_tier2]
replica2.idm.example.com \
ipareplica_servers=replica1.idm.example.com,server.idm.example.com
```

将使用 **ipareplica_servers** 中的第一个条目。第二个条目将用作回退选项。在使用多个层来部署 IdM 副本时，您必须在 playbook 中有单独的任务来首先从 tier1 部署副本，然后从 tier2 部署副本。

为不同副本组使用不同 play 的 playbook 文件示例

```
---
- name: Playbook to configure IPA replicas (tier1)
```

```
  hosts: ipareplicas_tier1
  become: true

  roles:
  - role: ipareplica
    state: present

- name: Playbook to configure IPA replicas (tier2)
  hosts: ipareplicas_tier2
  become: true

  roles:
  - role: ipareplica
    state: present
```

3. [可选] 提供有关 **firewalld** 和 DNS 的更多信息：

场景 1

如果您希望副本使用指定的 **firewalld** 区，如内部区，您可以在清单文件中指定它。如果您没有设置自定义区，IdM 会将其服务添加到默认的 **firewalld** 区域中。预定义的默认区域是 **public**。

重要

指定的 **firewalld** 区域必须存在，并且是永久的。

带有自定义 firewalld 区域的简单清单主机文件示例

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

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_firewalld_zone=custom zone
```

场景 2

如果您希望副本托管 IdM DNS 服务，请将 **ipareplica_setup_dns=true** 行添加到 **[ipareplicas:vars]** 部分。另外，请指定您是否要使用每服务器 DNS 转发器：

- 要配置每服务器转发器，请将 **ipareplica_forwarders** 变量和字符串列表添加到 **[ipareplicas:vars]** 部分，例如：**ipareplica_forwarders=192.0.2.1,192.0.2.2**
- 若要配置无每服务器转发器，请将以下行添加到 **[ipareplicas:vars]** 部分：**ipareplica_no_forwarders=true**。
- 要根据副本的 **/etc/resolv.conf** 文件中列出的转发器配置每服务器转发器，请将 **ipareplica_auto_forwarders** 变量添加到 **[ipareplicas:vars]** 部分。

带有在副本上设置 DNS 和每个服务器转发器的指令的清单文件示例

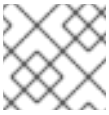
```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_setup_dns=true
ipareplica_forwarders=192.0.2.1,192.0.2.2
```

场景 3

使用 **ipaclient_configure_dns_resolve** 和 **ipaclient_dns_servers** 选项（如果可用的话）指定 DNS 解析器，来简化集群部署。这在您的 IdM 部署使用集成的 DNS 时特别有用：

指定 DNS 解析器的清单文件片段：

```
[...]
[ipaclient:vars]
ipaclient_configure_dns_resolver=true
ipaclient_dns_servers=192.168.100.1
```



注意

ipaclient_dns_servers 列表必须仅包含 IP 地址。主机名不允许。

其他资源

- **/usr/share/ansible/roles/ipareplica/README.md**

32.2. 使用 ANSIBLE PLAYBOOK 指定用于安装 IDM 副本的凭证

完成这个步骤来配置安装 IdM 副本的授权。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。

流程

1. 指定 **授权部署副本的用户的密码**，如 IdM **admin**。
   - 红帽建议使用 Ansible Vault 来存储密码，并从 playbook 文件引用 Vault 文件，如 **install-replica.yml** ：

使用来自清单文件和 Ansible Vault 文件中的密码的主体的 playbook 文件示例

```
- name: Playbook to configure IPA replicas
  hosts: ipareplicas
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipareplica
    state: present
```

有关如何使用 Ansible Vault 的详细信息，请参阅官方 Ansible Vault 文档。

- 直接在清单文件中提供 **admin** 的凭证不太安全。请在清单文件的 **[ipareplicas:vars]** 部分中使用 **ipaadmin_password** 选项。然后，清单文件和 **install-replica.yml** playbook 文件类似如下：

  清单 hosts.replica 文件示例

  ```
  [...]
  [ipareplicas:vars]
  ipaadmin_password=Secret123
  ```

  使用清单文件中的主体和密码的 playbook 示例

  ```
  - name: Playbook to configure IPA replicas
    hosts: ipareplicas
    become: true

    roles:
    - role: ipareplica
      state: present
  ```

- 或者，在清单文件中提供授权直接部署副本的另一个用户的凭证也不太安全。要指定不同的授权用户，请使用 **ipaadmin_principal** 选项作为用户名，使用 **ipaadmin_password** 选项作为密码。然后，清单文件和 **install-replica.yml** playbook 文件类似如下：

  清单 hosts.replica 文件示例

  ```
  [...]
  [ipareplicas:vars]
  ipaadmin_principal=my_admin
  ipaadmin_password=my_admin_secret123
  ```

  使用清单文件中的主体和密码的 playbook 示例

  ```
  - name: Playbook to configure IPA replicas
    hosts: ipareplicas
    become: true
  ```

```
roles:
- role: ipareplica
  state: present
```

其他资源

- **/usr/share/ansible/roles/ipareplica/README.md**

32.3. 使用 ANSIBLE PLAYBOOK 部署 IDM 副本

完成此流程，使用 Ansible playbook 来部署 IdM 副本。

先决条件

- 受管节点是一个具有静态 IP 地址和可正常工作的软件包管理器的 Red Hat Enterprise Linux 8 系统。
- 您已经配置了 用于安装 IdM 副本的清单文件。
- 您已经配置了 用于安装 IdM 副本的授权。

流程

- 运行 Ansible playbook:

```
$ ansible-playbook -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-replica.yml
```

32.4. 使用 ANSIBLE PLAYBOOK 卸载 IDM 副本

注意

在现有的身份管理(IdM)部署中，**副本** 和 **服务器** 是可交换的术语。有关如何卸载 IdM 服务器的详情，请参考 使用 Ansible playbook 卸载 IdM 服务器 或使用 Ansible playbook 卸载 IdM 服务器，即使这会导致断开连接的拓扑。

其他资源

- IdM 服务器和客户端简介

第 33 章 使用 ANSIBLE PLAYBOOK 安装身份管理客户端

了解如何使用 Ansible 将系统配置为身份管理(IdM)客户端。将系统配置为 IdM 客户端将其注册到 IdM 域中，并让系统在域中的 IdM 服务器中使用 IdM 服务。

部署是由 **ipaclient** Ansible 角色来管理的。默认情况下，该角色使用 autodiscovery 模式来识别 IdM 服务器、域和其他设置。角色可以被修改为使用 Ansible playbook 使用指定的设置，例如在清单文件中。

先决条件

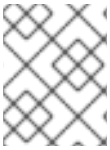
- 您已在 Ansible 控制节点上安装了 ansible-freeipa 软件包。
- 您使用 Ansible 版本 2.14 或更高版本。
- 您了解了一般的 Ansible 和 IdM 概念。

33.1. 为自动发现客户端安装模式设置清单文件的参数

要使用 Ansible playbook 安装身份管理(IdM)客户端，请在清单文件中配置目标主机参数，如 **inventory**：

- 有关主机的信息
- 对任务的授权

根据您拥有的清单插件，清单文件可以采用多种格式。**INI** 格式是 Ansible 的默认值之一，如下例中使用。



注意

要在 RHEL 中将智能卡与图形用户界面搭配使用，请确保在 Ansible playbook 中包含 **ipaclient_mkhomedir** 变量。

流程

1. **打开清单文件** 进行编辑。
2. 指定主机的完全限定主机名(FQDN)，使其成为 IdM 客户端。完全限定域名必须是有效的 DNS 名称：
   - 仅允许数字、字母字符和连字符(-)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。不允许使用大写字母。

   如果在 IdM DNS 区域中正确设置了 SRV 记录，该脚本会自动发现所有其他必要的值。

   只带有客户端 FQDN 定义的简单的清单主机文件示例

   ```
   [ipaclients]
   client.idm.example.com
   [...]
   ```

3. 指定注册客户端的凭证。可用的验证方法如下：
   - 注册 **客户端的用户权限的密码。**这是默认选项。
     - 红帽建议使用 Ansible Vault 来存储密码，并从 playbook 文件引用 Vault 文件，如

- 还指定以使用 Ansible Vault 来存储密码，并从 playbook 文件引用 vault 文件，如 **install-client.yml** ：

  使用来自清单文件和 Ansible Vault 文件中的密码的主体的 playbook 文件示例

  ```
  - name: Playbook to configure IPA clients with username/password
    hosts: ipaclients
    become: true
    vars_files:
    - playbook_sensitive_data.yml

    roles:
    - role: ipaclient
      state: present
  ```

- 在 **inventory/hosts** 文件的 **[ipaclients:vars]** 部分中使用 **ipaadmin_password** 选项来提供 **admin** 的凭证不太安全。或者，指定不同的授权用户，请使用 **ipaadmin_principal** 选项作为用户名，使用 **ipaadmin_password** 选项作为密码。然后，**inventory/hosts** 清单文件和 **install-client.yml** playbook 文件类似如下：

  清单主机文件示例

  ```
  [...]
  [ipaclients:vars]
  ipaadmin_principal=my_admin
  ipaadmin_password=Secret123
  ```

  使用清单文件中的主体和密码的 Playbook 示例

  ```
  - name: Playbook to unconfigure IPA clients
    hosts: ipaclients
    become: true

    roles:
    - role: ipaclient
      state: true
  ```

- 之前注册的**客户端 keytab**，（如果其仍然可用）：
  如果系统之前作为身份管理客户端注册，则可以使用这个选项。要使用此身份验证方法，请取消 **#ipaclient_keytab** 选项的注释，指定存储 keytab 的文件的路径，例如在 **inventory/hosts** 的 **[ipaclient:vars]** 部分。

- **在注册过程中生成的随机一次性密码** (OTP)。要使用此身份验证方法，请在清单文件中使用 **ipaclient_use_otp=true** 选项。例如，您可以取消 **inventory/hosts** 文件的 **[ipaclients:vars]** 部分中的 **ipaclient_use_otp=true** 选项的注释。请注意，对于 OTP，还必须指定以下选项之一：

  - **授权注册客户端的用户的密码** ，例如，为 **inventory/hosts** 文件的 **[ipaclients:vars]** 部分的 **ipaadmin_password** 提供值。

  - admin keytab，例如，为 **inventory/hosts** 的 **[ipaclients:vars]** 部分中的 **ipaadmin_keytab** 提供值。

4. [可选] 使用 **ipaclient_configure_dns_resolve** 和 **ipaclient_dns_servers** 选项（如果可用的话）指定 DNS 解析器，以简化集群部署。这在您的 IdM 部署使用集成的 DNS 时特别有用：

指定 DNS 解析器的清单文件片段：

```
[...]
[ipaclients:vars]
ipaadmin_password: "{{ ipaadmin_password }}"
ipaclient_domain=idm.example.com
ipaclient_configure_dns_resolver=true
ipaclient_dns_servers=192.168.100.1
```

注意

ipaclient_dns_servers 列表必须仅包含 IP 地址。主机名不允许。

5. 从 RHEL 8.9 开始，您还可以指定 **ipaclient_subid: true** 选项，以便为 IdM 级别上的 IdM 用户 subid 范围。

其他资源

- **/usr/share/ansible/roles/ipaclient/README.md**
- 手动管理 subID 范围

33.2. 当在客户端安装过程中无法自动发现时设置清单文件的参数

要使用 Ansible playbook 安装身份管理客户端，请在清单文件,如 **inventory/hosts** 中配置目标主机参数：

- 有关主机、IdM 服务器和 IdM 域或 IdM 领域的信息
- 对任务的授权

根据您拥有的清单插件，清单文件可以采用多种格式。**INI** 格式是 Ansible 的默认值之一，如下例中使用。

注意

要在 RHEL 中将智能卡与图形用户界面搭配使用，请确保在 Ansible playbook 中包含 **ipaclient_mkhomedir** 变量。

流程

1. 指定主机的完全限定主机名(FQDN)，使其成为 IdM 客户端。完全限定域名必须是有效的 DNS 名称：
   - 仅允许数字、字母字符和连字符(**-**)。例如，不允许使用下划线，这可能导致 DNS 失败。
   - 主机名必须都是小写。不允许使用大写字母。
2. 在 **inventory/hosts** 文件的相关部分中指定其他选项：
   - **[ipaservers]** 部分中服务器的 FQDN，用于指示客户端将注册到哪个 IdM 服务器
   - 以下两个选项之一：
     - **[ipaclients:vars]** 部分中的 **ipaclient_domain** 选项，用来指示客户端将注册到的 IdM 服务器的 DNS 域名

- **[ipaclients:vars]** 部分中的 **ipaclient_realm** 选项，用于指示 IdM 服务器控制的 Kerberos 域的名称

带有客户端 FQDN、服务器 FQDN 和定义的域的清单主机文件示例

```
[ipaclients]
client.idm.example.com

[ipaservers]
server.idm.example.com

[ipaclients:vars]
ipaclient_domain=idm.example.com
[...]
```

3. 指定注册客户端的凭证。可用的验证方法如下：

- 注册 **客户端的用户权限的密码。**这是默认选项。
  - 红帽建议使用 Ansible Vault 来存储密码，并从 playbook 文件引用 Vault 文件，如 **install-client.yml** ：

使用来自清单文件和 Ansible Vault 文件中的密码的主体的 playbook 文件示例

```
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaclient
    state: present
```

- 不太安全的是，使用 **inventory/hosts** 文件的 **[ipaclients:vars]** 部分中的 **ipaadmin_password** 选项提供的 **admin** 的凭证。或者，指定不同的授权用户，请使用 **ipaadmin_principal** 选项作为用户名，使用 **ipaadmin_password** 选项作为密码。**install-client.yml** playbook 文件类似如下：

清单主机文件示例

```
[...]
[ipaclients:vars]
ipaadmin_principal=my_admin
ipaadmin_password=Secret123
```

使用清单文件中的主体和密码的 Playbook 示例

```
- name: Playbook to unconfigure IPA clients
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: true
```

- 之前注册的**客户端 keytab**，如果仍然可用：
  如果系统之前作为身份管理客户端注册，则可以使用这个选项。要使用此身份验证方法，请取消 **ipaclient_keytab** 选项的注释，指定存储 keytab 的文件的路径，例如在 **inventory/hosts** 的 **[ipaclient:vars]** 部分。

- **在注册过程中生成的随机一次性密码** (OTP)。要使用此身份验证方法，请在清单文件中使用 **ipaclient_use_otp=true** 选项。例如，您可以取消 **inventory/hosts** 文件的 **[ipaclients:vars]** 部分中的 **#ipaclient_use_otp=true** 选项的注释。请注意，对于 OTP，还必须指定以下选项之一：

  - **授权注册客户端的用户的密码**，例如，为 **inventory/hosts** 文件的 **[ipaclients:vars]** 部分的 **ipaadmin_password** 提供值。

  - admin keytab，例如，为 **inventory/hosts** 的 **[ipaclients:vars]** 部分中的 **ipaadmin_keytab** 提供值。

4. 从 RHEL 8.9 开始，您还可以指定 **ipaclient_subid: true** 选项，以便为 IdM 级别上的 IdM 用户 subid 范围。

其他资源

- **/usr/share/ansible/roles/ipaclient/README.md**
- 手动管理 subID 范围

33.3. 使用 ANSIBLE PLAYBOOK 进行 IDM 客户端注册的授权选项

您可以使用以下任一方法授权 IdM 客户端注册：

- 一个随机的一次性密码(OTP)+ 管理员密码
- 一个随机的一次性密码(OTP)+ admin keytab
- 之前注册中的客户端 keytab
- 授权注册清单文件中的客户端(**管理员**)的用户密码
- 授权注册存储在 Ansible vault 中的客户端(**管理员**)的用户密码

在 IdM 客户端安装前，可以让 IdM 管理员生成的 OTP。在这种情况下，您不需要在 OTP 本身以外的安装的任何凭证。

以下是这些方法的清单文件示例：

表 33.1. 清单文件示例

授权选项	清单文件
一个随机的一次性密码(OTP)+ 管理员密码	[ipaclients:vars] ipaadmin_password=Secret123 ipaclient_use_otp=true

授权选项	清单文件
一个随机的一次性密码(OTP)	[ipaclients:vars] ipaclient_otp=<W5YpARl=7M.> 这个场景假定 OTP 已在安装前由 IdM **admin** 生成。
一个随机的一次性密码(OTP)+ admin keytab	[ipaclients:vars] ipaadmin_keytab=/root/admin.keytab ipaclient_use_otp=true
之前注册中的客户端 keytab	[ipaclients:vars] ipaclient_keytab=/root/krb5.keytab
存储在清单文件中的 **admin** 用户的密码	[ipaclients:vars] ipaadmin_password=Secret123
存储在 Ansible vault 文件中的 **admin** 用户的密码	[ipaclients:vars] [...]

如果您使用存储在 Ansible vault 文件中的 **admin** 用户的密码，则对应的 playbook 文件必须具有额外的 **vars_files** 指令：

表 33.2. 存储在 Ansible vault 中的用户密码

清单文件	Playbook 文件

[ipaclients:vars]
[...]
	- name: Playbook to configure IPA clients
	  hosts: ipaclients
	  become: true
	  vars_files:
	  - ansible_vault_file.yml
	
	  roles:
	  - role: ipaclient
	  state: present

在上述所有其他授权场景中，基本的 playbook 文件可能如下所示：

```
- name: Playbook to configure IPA clients
  hosts: ipaclients
```

```
become: true

roles:
- role: ipaclient
  state: true
```

注意

从 RHEL 8.8 开始，在上述两个 OTP 授权场景中，使用 **kinit** 命令请求管理员的 TGT 发生在第一个指定或发现的 IdM 服务器上。因此，不需要对 Ansible 控制节点进行额外的修改。在 RHEL 8.8 之前，控制节点上需要 **krb5-workstation** 软件包。

33.4. 使用 ANSIBLE PLAYBOOK 部署 IDM 客户端

完成此流程，使用 Ansible playbook 在 IdM 环境中部署 IdM 客户端。

先决条件

- 受管节点是一个具有静态 IP 地址和可正常工作的软件包管理器的 Red Hat Enterprise Linux 8 系统。
- 您已将 IdM 客户端部署的参数设置为与您的部署场景相对应：
  - 为自动发现客户端安装模式设置清单文件的参数
  - 当在客户端安装过程中无法自动发现时设置清单文件的参数

流程

- 运行 Ansible playbook:

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-client.yml
```

33.5. 在 ANSIBLE 中使用一次性密码方法安装 IDM 客户端

您可以为身份管理(IdM)中的新主机生成一次性密码(OTP)，并使用它来将系统注册到 IdM 域中。此流程描述了如何在为另一个 IdM 主机生成 OTP 后使用 Ansible 安装 IdM 客户端。

如果机构中存在具有不同权限的两个系统管理员，则安装 IdM 客户端的这个方法非常方便：

- 一个具有 IdM 管理员凭证。
- 另一个具有所需的 Ansible 凭据，包括主机 **root** 访问权限，成为 IdM 客户端。

IdM 管理员执行生成 OTP 密码的步骤的第一个部分。Ansible 管理员执行流程的剩余部分，其中 OTP 用于安装 IdM 客户端。

先决条件

- 您有 IdM **admin** 凭证或至少具有 **Host Enrollment** 特权以及在 IdM 中添加 DNS 记录的权限。
- 您已在 Ansible 受管节点上配置了用户升级方法，以便您安装 IdM 客户端。

- 如果您的 Ansible 控制节点在 RHEL 8.7 或更早版本上运行，则必须能够在 Ansible 控制节点上安装软件包。
- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 您已创建了带有 IdM 服务器的完全限定域名(FQDN)的 Ansible 清单文件。
- 受管节点是一个具有静态 IP 地址和可正常工作的软件包管理器的 Red Hat Enterprise Linux 8 系统。

流程

1. 以具有 **Host Enrollment** 权限和添加 DNS 记录权限的 IdM 用户身份 **SSH** 到 IdM 主机：

```
$ ssh admin@server.idm.example.com
```

2. 为新客户端生成 OTP：

```
[admin@server ~]$ ipa host-add client.idm.example.com --ip-address=172.25.250.11 --random
 ----------------------------------------------------
 Added host "client.idm.example.com"
 ----------------------------------------------------
  Host name: client.idm.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.idm.example.com
```

--ip-address= &*lt;your_host_ip_address* > 选项将主机添加到带有指定 IP 地址的 IdM DNS 中。

3. 退出 IdM 主机：

```
$ exit
logout
Connection to server.idm.example.com closed.
```

4. 在 ansible 控制器上，更新清单文件使其包含随机密码：

```
[...]
[ipaclients]
client.idm.example.com

[ipaclients:vars]
ipaclient_domain=idm.example.com
ipaclient_otp=W5YpARl=7M.n
[...]
```

5. 如果您的 ansible 控制器正在运行 RHEL 8.7 或更早版本，请安装 **krb5-workstation** 软件包提供的 **kinit** 工具：

```
$ sudo dnf install krb5-workstation
```

6. 运行 playbook 来安装客户端：

```
$ ansible-playbook -i inventory install-client.yml
```

33.6. ANSIBLE 安装后测试身份管理客户端

命令行界面(CLI)告知您 **ansible-playbook** 命令已成功完成，但您也可以自行进行测试。

要测试身份管理客户端是否可以获取服务器上定义的用户的信息，请检查您是否能够解析服务器上定义的用户。例如，检查默认的 **admin** 用户：

```
[user@client1 ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

要测试身份验证是否正常工作，请**su -** 为另一个已存在的 IdM 用户：

```
[user@client1 ~]$ su - idm_user
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[idm_user@client1 ~]$
```

33.7. 使用 ANSIBLE PLAYBOOK 卸载 IDM 客户端

完成此流程，使用 Ansible playbook 将主机卸载为 IdM 客户端。

先决条件

- IdM 管理员凭证。
- 受管节点是一个具有静态 IP 地址的 Red Hat Enterprise Linux 8 系统。

流程

- 使用说明运行 Ansible playbook 来卸载客户端，如 **uninstall-client.yml** ：

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory ~/MyPlaybooks/uninstall-client.yml
```

重要

卸载客户端只从主机中删除基本的 IdM 配置，但会在主机上保留配置文件，以防您决定重新安装客户端。另外，卸载有以下限制：

- 它不会从 IdM LDAP 服务器中删除客户端主机条目。卸载仅是将主机取消注册。
- 它不会从 IdM 中删除任何位于客户端的服务。
- 它不会从 IdM 服务器中删除客户端的 DNS 条目。
- 它不会删除 **/etc/krb5.keytab** 之外的 keytab 的旧主体。

请注意，卸载会删除 IdM CA 为主机发布的所有证书。

其他资源

- 卸载 IdM 客户端

部分 II. 集成 IDM 和 AD

第 34 章 在 IDM 和 AD 间安装信任

了解更多有关如何在身份管理 IdM 服务器和活动目录(AD)之间创建信任，其中两个服务器都位于同一林中。

注意

在 RHEL 7 中，*synchronization* 和 *trust* 是把 RHEL 系统间接集成到活动目录(AD)的两种方法。在 RHEL 8 中，同步已弃用。要集成 IdM 和 AD，请使用信任方法。要从同步迁移到信任，请参阅 在 Linux 域与活动目录域集成的上下文中，将现有环境从同步迁移到信任。

先决条件

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

34.1. WINDOWS 服务器支持的版本

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

- 林功能级别范围：Windows Server 2012 SAS- SASWindows Server 2016
- 域功能级别范围：Windows Server 2012 SAS-66Windows Server 2016

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

- Windows Server 2022 (RHEL 8.7 及更高版本)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

重要

在 RHEL 8.4 中，身份管理 (IdM) 不支持使用运行 Windows Server 2008 R2 或更早版本的 Active Directory 域控制器建立对 Active Directory 的信任。现在，RHEL IdM 在建立信任关系时需要 SMB 加密，这只在 Windows Server 2012 或更高版本中被支持。

34.2. 信任如何工作

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

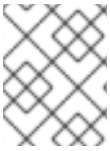
- 登录访问 Linux 系统和资源。
- 使用单点登录（SSO）。

所有 IdM 对象都在 IdM 中的信任中管理。

所有 AD 对象都在信任的 AD 中管理。

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

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



注意

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

34.3. AD 管理权利

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

这样 AD 管理员必须是以下组之一的成员：

- AD 林中的企业管理员组
- AD 林的林根域中的域管理员组

其他资源

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

34.4. 确保支持 AD 和 RHEL 中的通用加密类型

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

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

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

重要

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

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

34.4.1. 在 AD 中启用 AES 加密（推荐）

要确保 AD 林中活动目录(AD)域间的信任支持强 AES 加密类型，请参阅以下 Microsoft 文章: AD DS: 安全性: 当访问信任域中的资源时，出现 Kerberos "Unsupported etype" 错误

34.4.2. 使用 GPO 在 Active Directory 中启用 AES 加密类型

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

请注意，RHEL 不再支持弱 DES 和 RC4 加密类型。

先决条件

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

流程

1. 打开组**策略管理控制台**。
2. 右键单击**默认域策略**，然后选择**编辑**。打开组**策略管理编辑器**。
3. 导航到 **计算机配置 → 策略 → Windows 设置 → 安全设置 → 本地策略 → 安全选项**。
4. 双击 **网络安全：配置 Kerberos 策略允许的加密类型**。
5. 选择**AES256_HMAC_SHA1**和可选的**未来加密类型**。
6. 点**确定**。
7. 关闭组**策略管理编辑器**。
8. 对**默认域控制器策略**重复上述步骤。
9. 等待 Windows 域控制器(DC)自动应用组策略。或者，如果要在 DC 上手动应用 GPO，请使用具有管理员权限的帐户输入以下命令：

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

34.4.3. 在 RHEL 中启用 RC4 支持

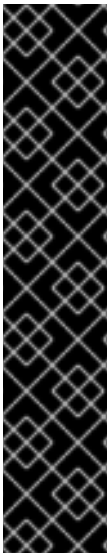
在针对 AD 域控制器发生身份验证的每个 RHEL 主机上，完成以下概述的步骤。

流程

1. 除了 **DEFAULT** 加密策略之外，使用 **update-crypto-policies** 命令来启用 **AD-SUPPORT** 加密子策略。

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

2. 重启主机。



重要

AD-SUPPORT 加密子策略只在 RHEL 8.3 及更新版本中提供。

- 要在 RHEL 8.2 中启用对 RC4 的支持，请使用 **cipher = RC4-128+** 创建并启用自定义加密模块策略。如需了解更多详细信息，请参阅 使用子策略自定义系统范围的加密策略。
- 要在 RHEL 8.0 和 RHEL 8.1 中启用对 RC4 的支持，请将 **+rc4** 添加到 **/etc/crypto-policies/back-ends/krb5.config** 文件中的 **permitted_enctypes** 选项中：

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
```

34.4.4. 其他资源

- 请参阅 使用系统范围的加密策略。
- 请参阅 信任控制器和信任代理。

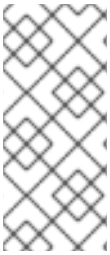
34.5. IDM 和 AD 间的通信所需的端口

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

表 34.1. AD 信任所需的端口

服务	端口	协议
端点解析端口映射器	135	TCP
NetBIOS-DGM	138	TCP 和 UDP

服务	端口	协议
NetBIOS-SSN	139	TCP 和 UDP
Microsoft-DS	445	TCP 和 UDP
Dynamic RPC	49152-65535	TCP
AD Global Catalog	3268	TCP
LDAP	389	TCP 和 UDP



注意

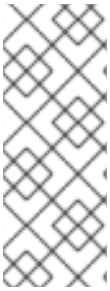
在 IdM 服务器中不需要为信任打开 TCP 端口 389，但与 IdM 服务器通信的客户端需要这样端口。

要使 DCE RPC 端点映射程序正常工作，并在 IdM-AD 信任创建过程中被使用，需要 TCP 端口 135。

要打开端口，您可以使用以下方法：

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

  详情请查看 **firewall-cmd** 手册页。

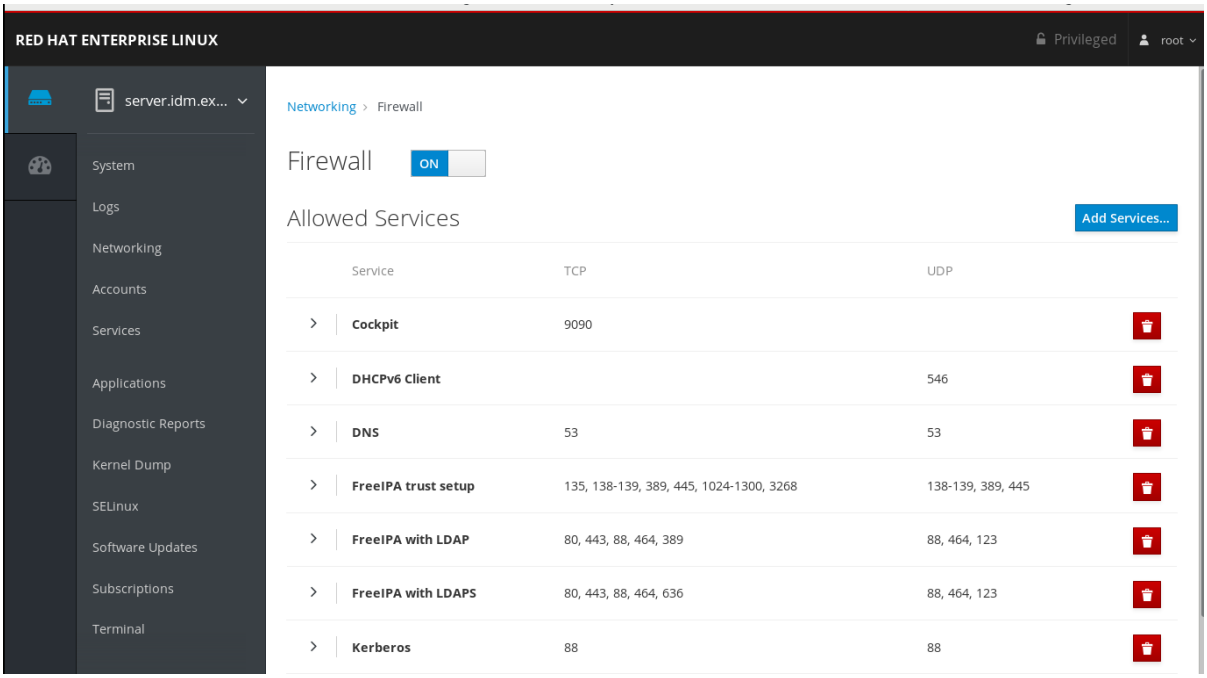


注意

如果您使用 RHEL 8.2 及更早版本，**freeipa-trust** firewalld 服务包含一个 **1024-1300** RPC 端口范围，这是不正确的。在 RHEL 8.2 及更早版本中，除了启用 **freeipa-trust** firewalld 服务外，您必须手动打开 TCP 端口范围 **49152-65535**。

这个问题已在 Bug 1850418 - 更新 freeipa-trust.xml 定义以使其包含正确的动态 RPC 范围中针对 RHEL 8.3 及之后的版本修复了。

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



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

注意

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

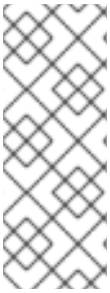
这个问题已在 Bug 1850418 - 更新 freeipa-trust.xml 定义以使其包含正确的动态 RPC 范围 中针对 RHEL 8.3 及之后的版本修复了。

表 34.2. 信任中的 IdM 服务器所需的端口

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

表 34.3. AD 信任中 IdM 客户端所需的端口

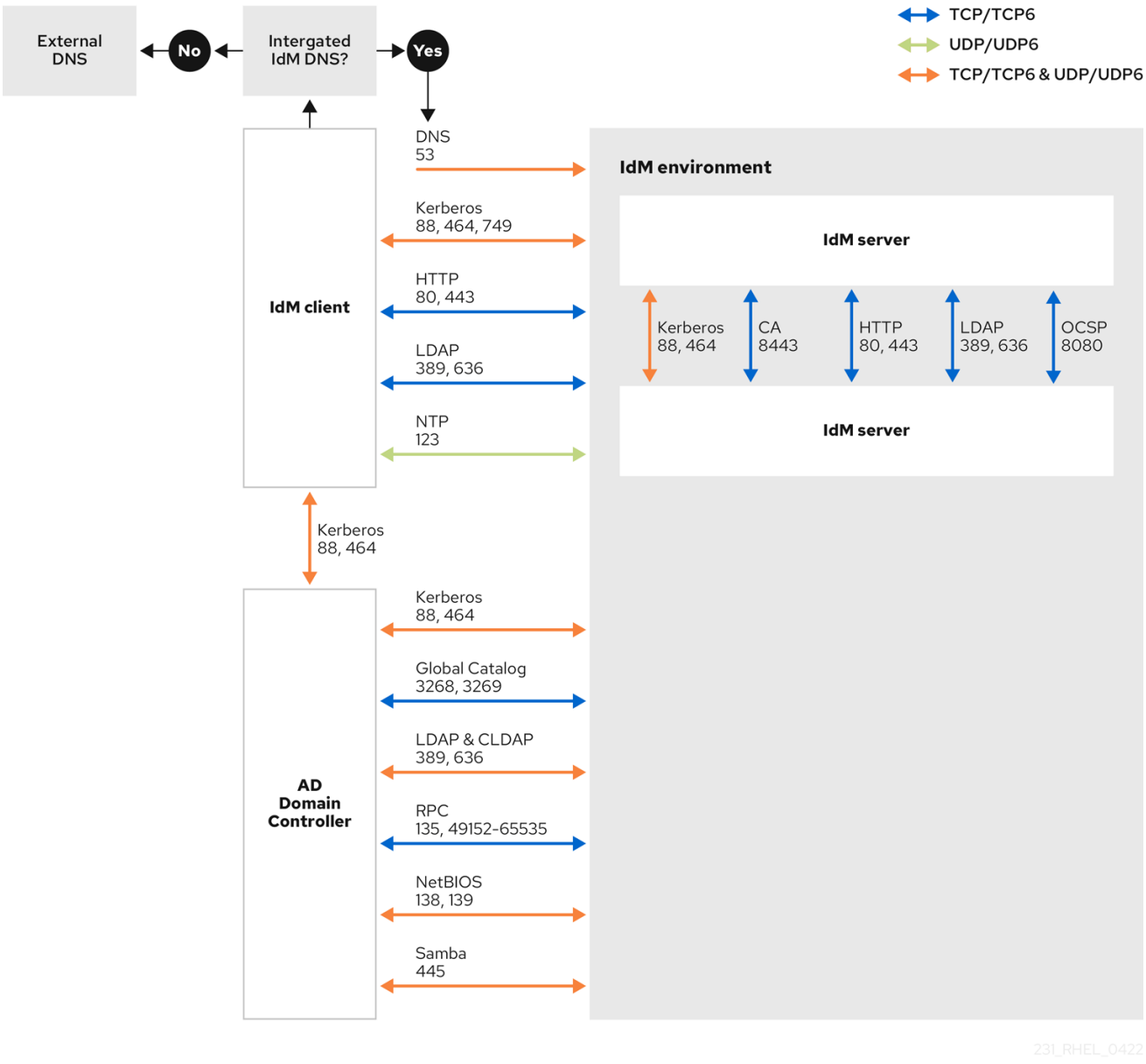
服务	端口	协议
Kerberos	88	UDP 和 TCP



注意

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

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



其他资源

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

34.6. 为信任配置 DNS 和域设置

在您连接信任中的身份管理(IdM)和 Active Directory(AD)之前，您需要确保服务器可以互相看到，并能够正确解析域名。将 DNS 配置为允许在以下服务器之间使用域名：

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

DNS 设置需要：

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

34.6.1. 唯一的主 DNS 域

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

每个系统都必须配置自己的唯一的主 DNS 域。例如：

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

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

Kerberos realm 名称作为主 DNS 域名的大写版本

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

DNS 记录可从信任中的所有 DNS 域解析

所有机器都必须能够从所有涉及信任关系的 DNS 域解析 DNS 记录。

IdM 和 AD DNS 域

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

注意

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

您可以运行以下命令来获取特定于您的系统设置所需的 SRV 记录列表：

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

生成的列表可以类似如下：

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

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

34.6.2. 在 IdM Web UI 中配置 DNS 转发区域

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

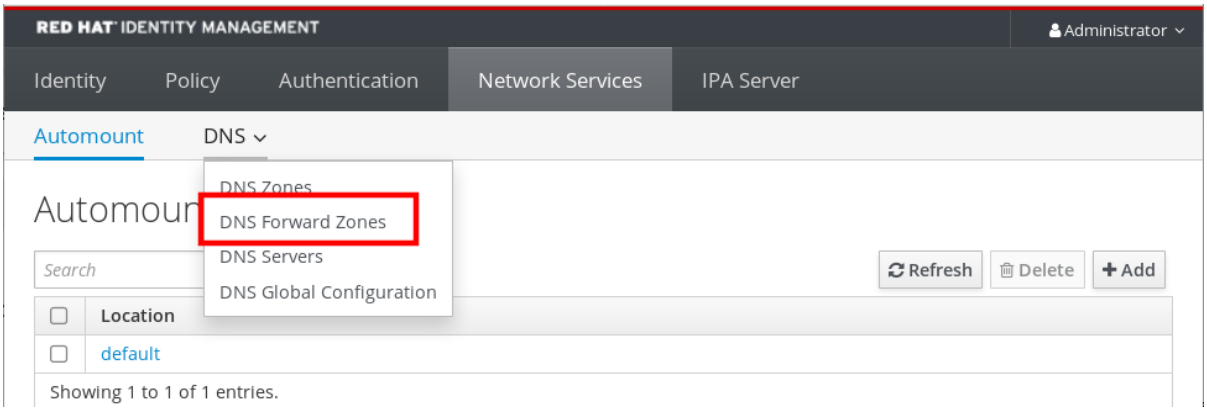
使用 DNS 转发区域，您可以将对特定区域的 DNS 查询转发到不同的 DNS 服务器。例如，您可以将活动目录(AD)域的 DNS 查询转发到 AD DNS 服务器。

先决条件

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

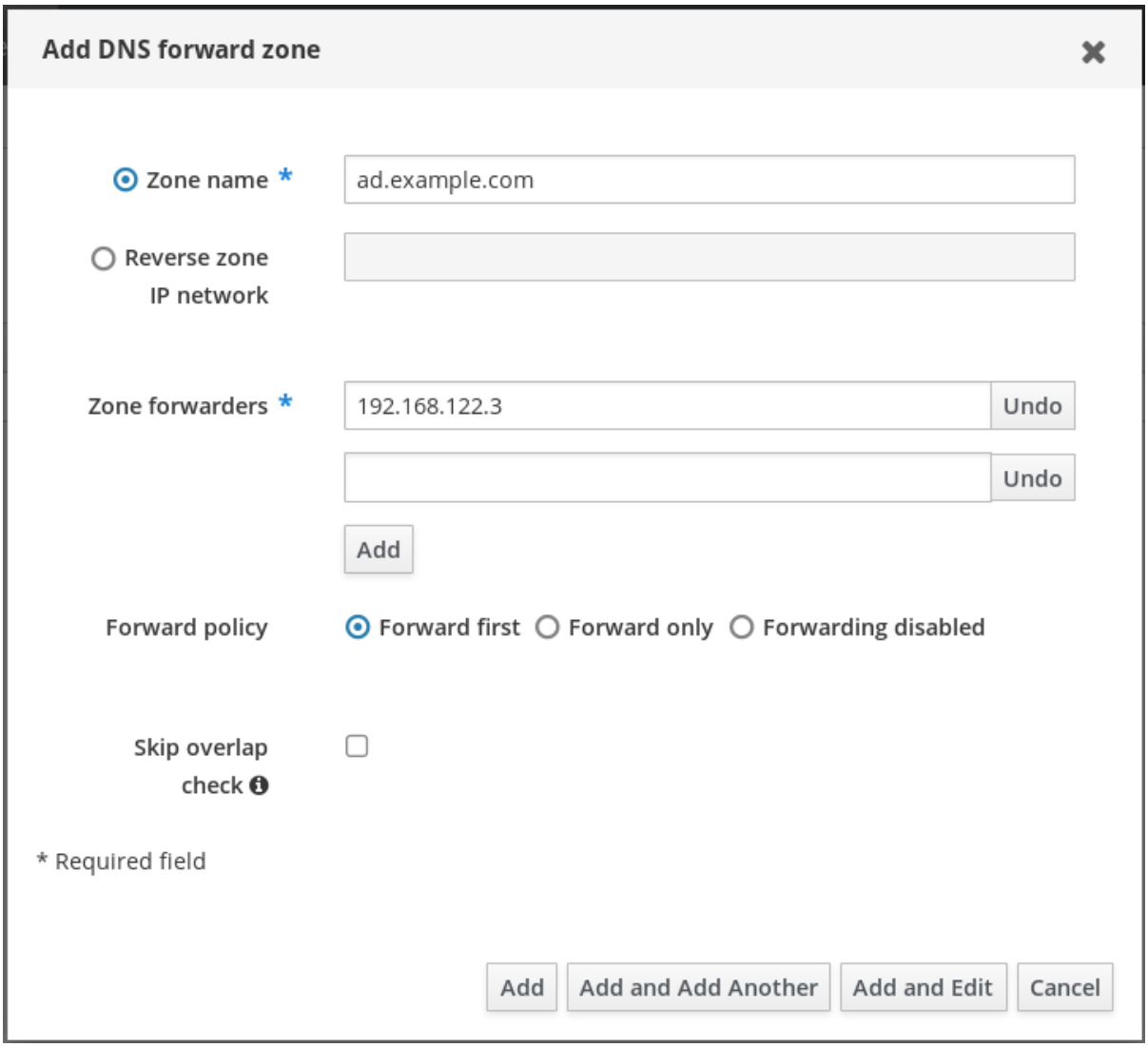
流程

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



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

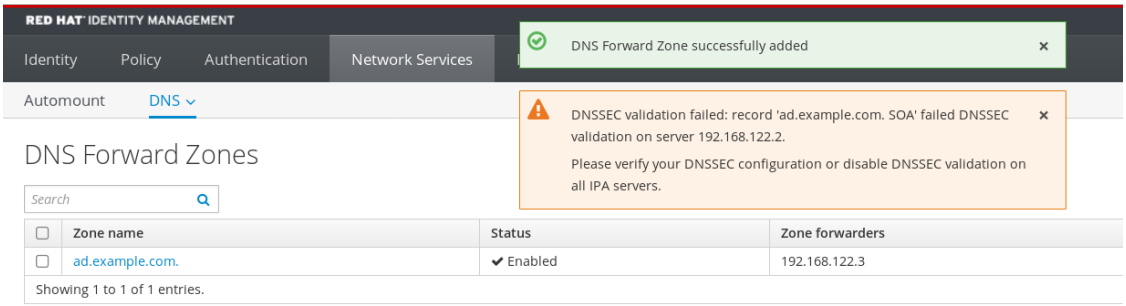
9. 点击 **Add** 按钮。



正向区已添加到 DNS 设置中，您可以在 DNS Forward Zones 设置中进行验证。Web UI 会用以下弹出消息告诉您是否成功：**DNS Forward Zone successfully added.**

注意

在向配置中添加转发区域后，Web UI 可能会显示有关 DNSSEC 验证失败的警告。



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

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

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

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

3. 保存并关闭配置文件。
4. 重启 DNS 服务：

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

验证步骤

- 将 **nslookup** 命令与远程 DNS 服务器名称一起使用：

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

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

如果您正确配置了域转发，则会显示远程 DNS 服务器的 IP 地址。

34.6.3. 在 CLI 中配置 DNS 转发区域

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

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

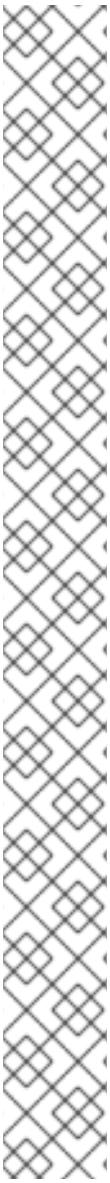
先决条件

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

流程

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

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



注意

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

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

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

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

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

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

3. 保存并关闭配置文件。
4. 重启 DNS 服务：

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

验证步骤

- 将 **nslookup** 命令与远程 DNS 服务器名称一起使用：

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

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

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

34.6.4. 在 AD 中配置 DNS 转发

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

先决条件

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

流程

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

34.6.5. 验证 DNS 配置

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

先决条件

- 您需要以 sudo 权限登录。

流程

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

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

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

这些命令应该列出所有 IdM 服务器。

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

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

如果前面的步骤没有返回所有预期的记录，请使用缺失的记录更新 DNS 配置：

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

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

- 如果您的 IdM 环境没有使用集成的 DNS 服务器：

  1. 在 IdM 服务器中，将 IdM DNS 记录导出到文件中：

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

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

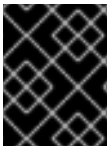
  2. 使用 **nsupdate** 工具和 **dns_records_file.nsupdate** 文件向 DNS 服务器提交 DNS 更新请求。如需更多信息，请参阅 RHEL 7 文档中的 使用 nsupdate 更新外部 DNS 记录。或者，请参阅 DNS 服务器文档来添加 DNS 记录。

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

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

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

34.7. 在活动目录 DNS 域中配置 IDM 客户端

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



重要

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

您的 IdM 客户端配置取决于您是否需要使用 Kerberos 单点登录。

34.7.1. 配置没有 Kerberos 单点登录的 IdM 客户端

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

流程

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

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

这个选项禁用了活动目录 DNS 域的 SRV 记录自动检测。

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

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

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

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

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

34.7.2. 请求没有单点登录的 SSL 证书

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

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

先决条件

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

流程

- 使用 **certmonger** 来请求使用 FQDN 的证书：

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

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

34.7.3. 配置带有 Kerberos 单点登录的 IdM 客户端

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

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

流程

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

```
ignore_acceptor_hostname = true
```

34.7.4. 请求带有单点登录的 SSL 证书

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

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

先决条件

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

流程

1. 在 IdM 服务器上创建一个新的主机对象：

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

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

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

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

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

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

34.8. 设置信任

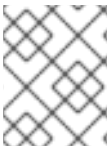
本节描述了如何使用命令行在 IdM 端上配置身份管理(IdM)/Active Directory(AD)信任。

先决条件

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

34.8.1. 为信任准备 IdM 服务器

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



注意

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

先决条件

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

步骤

1. 安装所需的软件包：

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

2. 以 IdM 管理用户身份进行身份验证：

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

3. 运行 **ipa-adtrust-install** 工具：

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

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

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

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

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

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

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

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
```

```
This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted users.

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

6. 提示时，输入 IdM 域的 NetBIOS 名称，或者按 **Enter** 接受推荐的名称：

```
Trust is configured but no NetBIOS domain name found, setting it now.
Enter the NetBIOS name for the IPA domain.
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
Example: EXAMPLE.

NetBIOS domain name [IDM]:
```

7. 系统会提示您运行 SID 生成任务，以便为任何现有用户创建 SID：

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

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

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

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

9. 确保正确配置了DNS，如 验证信任的 DNS 配置 中所述。

重要

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

10. 重启 **ipa** 服务：

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

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

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

34.8.2. 使用命令行设置信任协议

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

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

- **Two-way trust（双向信任）** – Two-way trust 可让 AD 用户和组访问 IdM 中的资源。
  您必须为像 Microsoft SQL Server 这样的解决方案配置双向信任，该解决方案希望 Kerberos 协议的 **S4U2Self** 和 **S4U2Proxy** Microsoft 扩展能够跨信任边界工作。RHEL IdM 主机上的应用可能会向 Active Directory 域控制器请求有关 AD 用户的 **S4U2Self** 或 **S4U2Proxy** 信息，双向信任提供了这一特性。

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

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

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

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

以下步骤演示了如何创建单向信任协议。

先决条件

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

流程

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

  - 要使 SSSD 为基于其 SID 的 AD 用户自动生成 UID 和 GID，请创建与 **活动目录域** ID 范围类型的信任协议。这是最常见的配置。

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

  - 如果您已经为活动目录中的用户配置了 POSIX 属性（如 **uidNumber** 和 **gidNumber**），并且希望 SSSD 处理此信息，请使用 **带有 POSIX 属性的活动目录域** ID range 类型创建信任协议：

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

警告

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

如果 IdM 在林根域中检测到任何 POSIX 属性，则信任安装脚本会选择 **带有 POSIX 属性的活动目录域** ID range，并假定已在 AD 中正确定义了 UID 和 GID。如果没有在 AD 中正确设置了 POSIX 属性，则您将无法解析 AD 用户。

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

34.8.3. 在 IdM Web UI 中设置信任协议

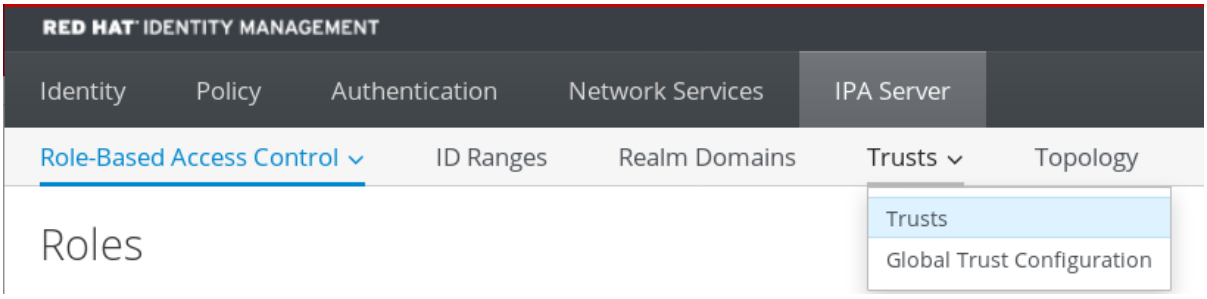
按照以下流程，使用 IdM Web UI 在 IdM 端配置身份管理(IdM)/活动目录(AD)信任协议。

先决条件

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

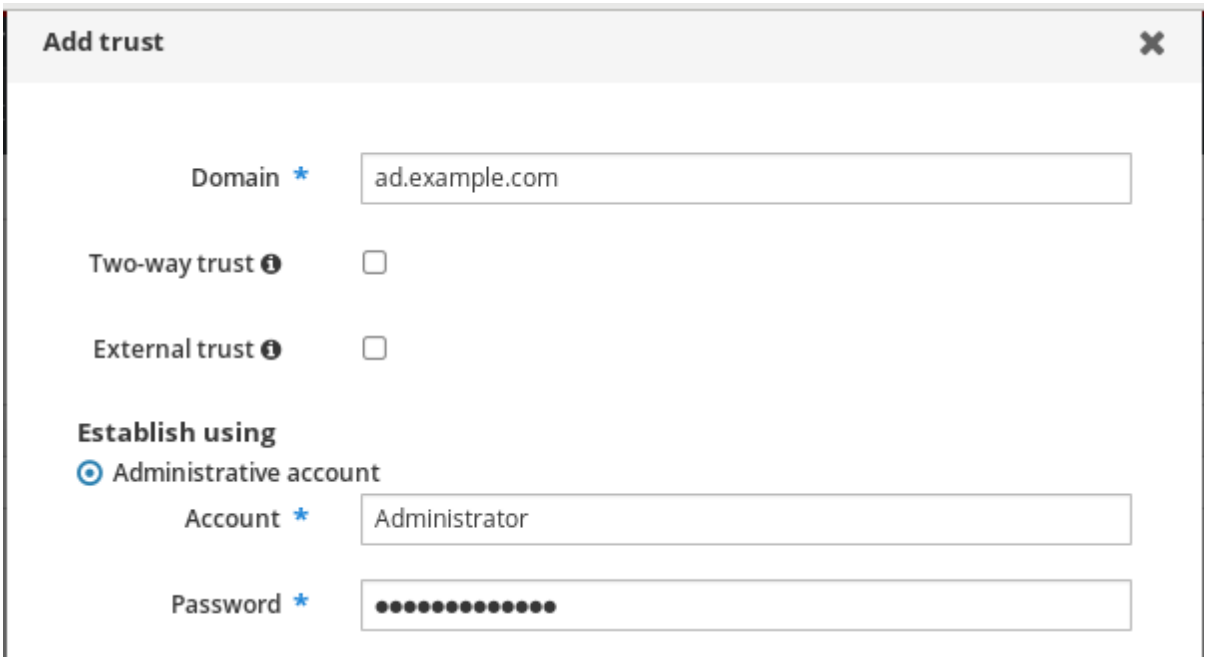
流程

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



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

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



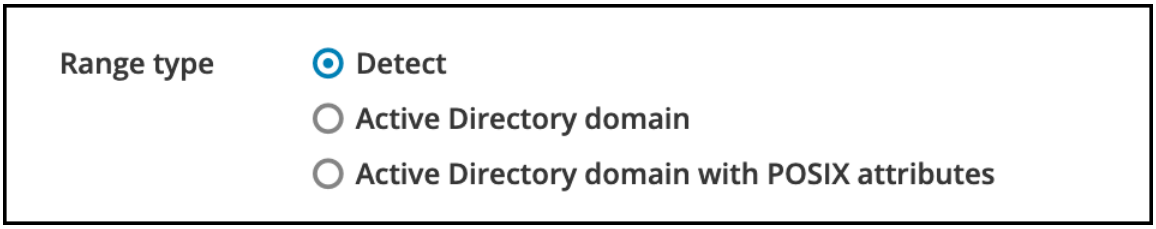
8. 如果要使 AD 用户和组能够访问 IdM 中的资源，请 *(可选)*选择 **Two-way trust**。但是，IdM 中的双向信任并不为用户授予与 AD 中的单向信任解决方案相比的额外权利。由于默认的跨林信任 SID 过滤设置，这两个解决方案被视为同等安全。

9. 如果您要为不是 AD 林根域的 AD 域配置信任，请 *（可选）*选择 **External trust**。虽然林信任总是需要在 IdM 和活动目录林的根域之间建立信任，但您可以建立从 IDM 到 AD 林中任何一个域的外部信任。

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

    a. 要使 SSSD 为基于其 SID 的 AD 用户自动生成 UID 和 GID，请选择 **活动目录域** ID range 类型。这是最常见的配置。

    b. 如果您已经为活动目录中的用户配置了 POSIX 属性（如 **uidNumber** 和 **gidNumber**），并且希望 SSSD 处理此信息，请选择 **带有 POSIX 属性的活动目录域** ID range 类型。



警告

如果您在默认 **Detect** 选项上保留 **Range 类型** 设置，IdM 会尝试通过请求林根域中 AD 域控制器的详情来自动选择合适的 range 类型。如果 IdM 没有检测到任何 POSIX 属性，则信任安装脚本会选择 **活动目录域** ID range。

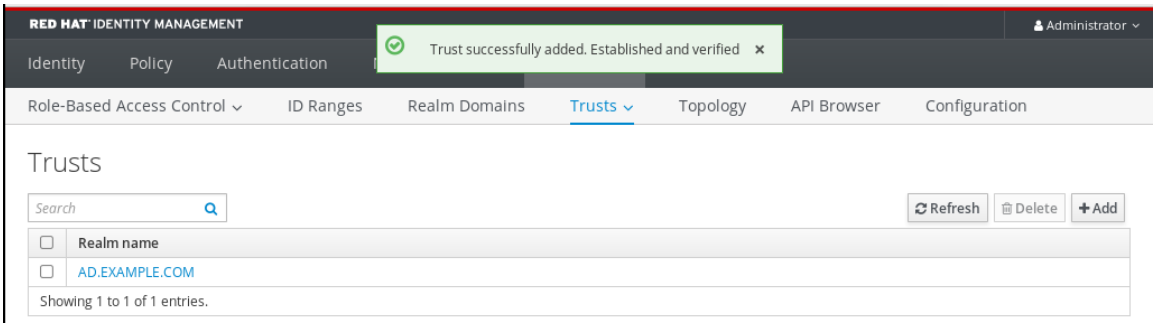
如果 IdM 在林根域中检测到任何 POSIX 属性，则信任安装脚本会选择 **带有 POSIX 属性的活动目录域** ID range，并假定已在 AD 中正确定义了 UID 和 GID。如果没有在 AD 中正确设置了 POSIX 属性，则您将无法解析 AD 用户。

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

11. 点击 **Add**。

验证步骤

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



现在，可以继续测试信任连接和 Kerberos 身份验证。

34.8.4. 使用 Ansible 建立信任协议

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

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

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

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

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

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

先决条件

- Windows 管理员的用户名和密码。
- IdM **admin** 密码。
- 您已为信任准备了 IdM 服务器。
- 您可以使用 IdM 的 4.8.7 版本或更高版本。要查看您在服务器上已安装的 IdM 版本，请运行 **ipa --version**。
- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（也就是在其上执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，来作为 IdM 客户端、服务器或副本。

流程

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

2. 根据您的用例选择以下场景之一：

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

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

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

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

在示例中：

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

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

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

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

- 要创建信任协议，其中 IdM 试图自动选择合适的范围类型、**ipa-ad-trust** 或 **ipa-ad-trust-posix**，通过请求林根域中 AD 域控制器的详情，创建一个具有以下内容的 **add-trust.yml** playbook：

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

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

警告

如果您在创建信任时没有指定 ID 范围类型，且 IdM 没有检测到 AD 林根域中的任何 POSIX 属性，则信任安装脚本会选择 **活动目录域** ID 范围。

如果 IdM 在林根域中检测到任何 POSIX 属性，则信任安装脚本会选择 **带有 POSIX 属性的活动目录域** ID range，并假定已在 AD 中正确定义了 UID 和 GID。

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

3. 保存该文件。
4. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

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

其他资源

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

34.8.5. 验证 Kerberos 配置

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

流程

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

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

2. 为 IdM 域中的服务请求 ticket：

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

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

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

Valid starting       Expires              Service principal
```

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

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

34.8.6. 验证 IdM 上的信任配置

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

先决条件

- 您需要使用管理员权限登录。

流程

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

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

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

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

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

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

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

.

34.8.7. 验证 AD 上的信任配置

配置信任后，验证：

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

先决条件

- 您需要使用管理员权限登录。

流程

流程

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

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

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

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

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

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

    "IDM.EXAMPLE.COM"
```

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

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

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

5. 验证 AD 服务是否可以从 AD 服务器解析。

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

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

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

34.8.8. 创建信任代理

信任代理是一个可以对 AD 域控制器执行身份查找的IdM 服务器。

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

先决条件

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

流程

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

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

该命令启动一个交互式配置会话，并提示您设置代理所需的信息。

2. 重启信任代理上的 IdM 服务。

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

3. 从信任代理上的 SSSD 缓存中删除所有条目：

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

4. 验证副本是否安装了 AD 信任代理角色：

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

其他资源

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

34.8.9. 在 CLI 上为 POSIX ID range 启用自动私有组映射

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

此流程解释了如何在命令行上为 **auto_private_groups** SSSD 参数设置 **hybrid** 选项来为 ID range 启用自动私有组映射。因此，IdM 可以解析在 AD 中没有配置主组的 AD 用户。

先决条件

- 您已成功在 IdM 和 AD 环境之间成功建立了 POSIX 跨林信任。

流程

1. 显示所有 ID range，并记录您要修改的 AD ID range。

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

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

2. 使用 **ipa idrange-mod** 命令调整 AD ID range 的自动私有组行为。

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

3. 重置 SSSD 缓存以启用新的设置。

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

其他资源

- 为 AD 用户自动映射私有组的选项

34.8.10. 在 IdM WebUI 中为 POSIX ID range 启用自动私有组映射

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

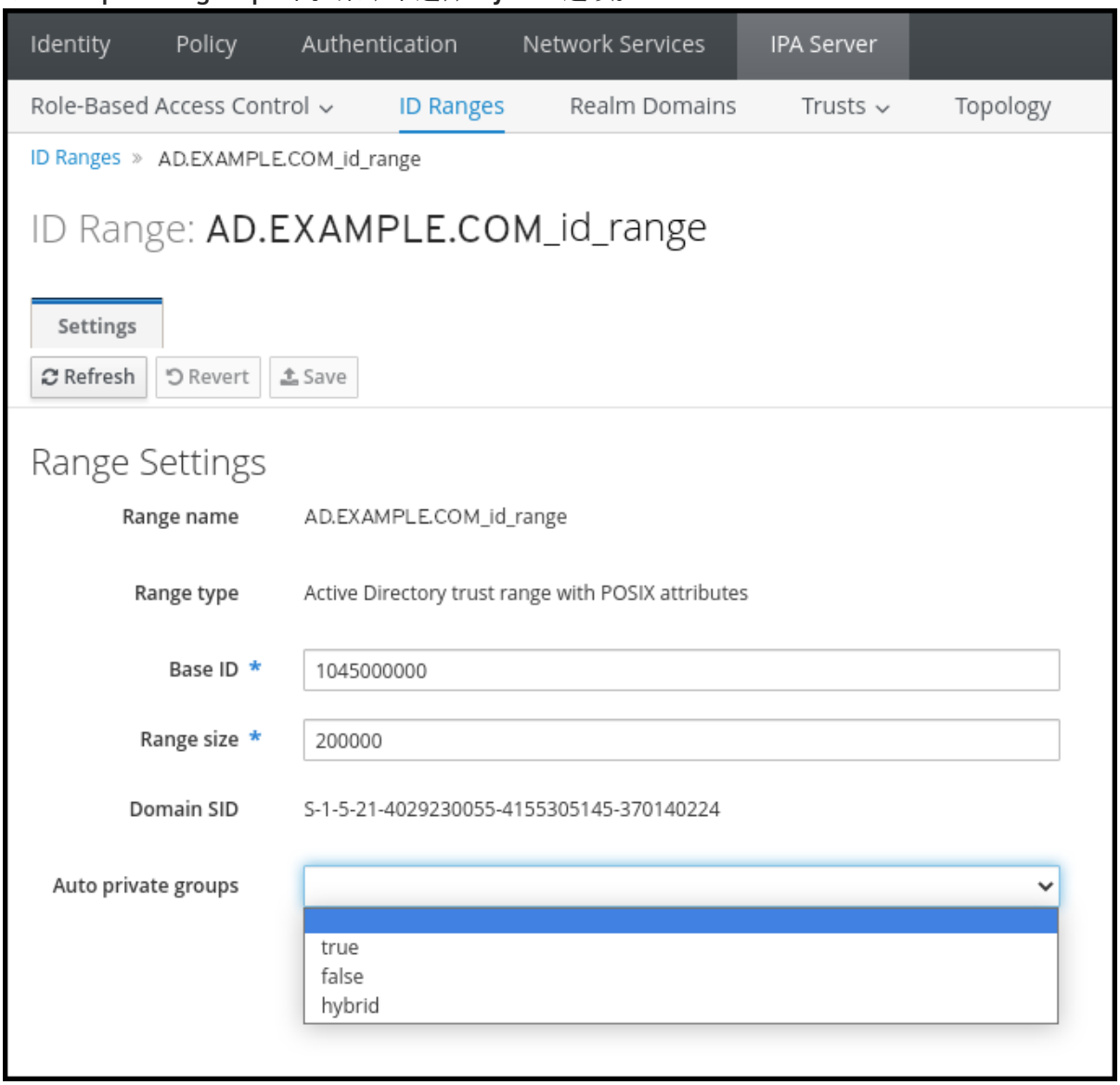
此流程解释了如何在身份管理(IdM)WebUI 中为 **auto_private_groups** SSSD 参数设置 **hybrid** 选项来为 ID range 启用自动私有组映射。因此，IdM 可以解析在 AD 中没有配置主组的 AD 用户。

先决条件

- 您已成功在 IdM 和 AD 环境之间成功建立了 POSIX 跨林信任。

流程

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



5. 点击 **Save** 按钮来保存您的更改。

其他资源

- 为 AD 用户自动映射私有组的选项

34.9. 对设置跨林信任进行故障排除

了解更多有关对在身份管理(IdM)环境和活动目录(AD)林之间配置跨林信任的过程进行故障排除的信息。

34.9.1. 建立与 AD 的跨林信任时的事件序列

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

第 1 部分：命令验证设置和输入

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

第 2 部分：命令尝试建立到活动目录域的信任

4. 为每个信任方向创建单独的信任对象。在两端（IdM 和 AD）都会创建每个对象。如果您要建立单向信任，只在每一端上创建一个对象。
5. IdM 服务器使用 Samba 套件为活动目录处理域控制器功能，并在目标 AD PDC 上创建信任对象：
   a. IdM 服务器建立到目标 DC 上 **IPC$** 共享的安全连接。从 RHEL 8.4 开始，连接至少需要 Windows Server 2012 及以上版本的 SMB3 协议，以确保会话使用的基于AES 加密的连接足够安全。
   b. IdM 服务器使用 **LSA QueryTrustedDomainInfoByName** 调用来查询是否存在可信域对象(TDO)。
   c. 如果 TDO 已存在，则使用 **LSA DeleteTrustedDomain** 调用删除它。

注意

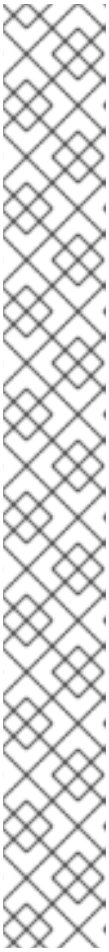
如果用来建立信任的 AD 用户帐户没有林根的全部 **Enterprise Admin(EA)** 或 **Domain Admin(DA)** 权限，如 **Incoming Forest Trust Builders** 组的成员，这个调用会失败。如果旧的 TDO 没有被自动删除，则 AD 管理员必须手动将其从 AD 中删除。

   d. IdM 服务器使用 **LSA CreateTrustedDomainEx2** 调用创建一个新的 TDO。TDO 凭证是使用 Samba 提供的密码生成器随机生成的，具有 128 个字符。
   e. 然后，使用 **LSA SetInformationTrustedDomain** 调用修改新的 TDO，以确保信任所支持的加密类型被正确设置：
      i. **RC4_HMAC_MD5** 加密类型被启用，即使由于活动目录的设计方式导致 RC4 密钥没有在使用。

ii. **AES128_CTS_HMAC_SHA1_96** 和 **AES256_CTS_HMAC_SHA1_96** 加密类型被启用。

6. 对于林信任，请验证是否可通过 **LSA SetInformationTrustedDomain** 调用来到达林中域。

7. 使用 **LSA RSetForestTrustInformation** 调用，添加有关其他林（与 AD 通信时的 IdM，与 IdM 通信时的 AD）的信任拓扑信息。



注意

此步骤可能会由于以下 3 个原因之一导致冲突：

1. SID 命名空间冲突，报告为 **LSA_SID_DISABLED_CONFLICT** 错误。无法解决此冲突。
2. NetBIOS 命名空间冲突，报告为 **LSA_NB_DISABLED_CONFLICT** 错误。无法解决此冲突。
3. DNS 命名空间与顶级名称(TLN)的冲突，报告为 **LSA_TLN_DISABLED_CONFLICT** 错误。如果 TLN 是因另一个林造成的，则 IdM 服务器可以自动解决它。

要解决 TLN 冲突，IdM 服务器需要执行以下步骤：

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

只有通过带有可以更改林信任的 AD 管理员特权的 **ipa trust-add** 命令进行身份验证，IdM 服务器才能解决这些冲突。如果您没有这些特权的访问权限，则原始林的管理员必须手动执行 Windows UI 的 **活动目录域和信任** 部分中提到的步骤。

8. 如果不存在，为可信域创建 ID 范围。

9. 对于林信任，请查询林根的活动目录域控制器以获取有关林拓扑的详细信息。IdM 服务器使用此信息为可信林中的任何其他域创建额外的 ID 范围。

其他资源

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

34.9.2. 建立 AD 信任的先决条件清单

您可以使用以下清单来查看创建 AD 域信任的先决条件。

表 34.4. 表

组件	配置	其它详情
产品版本	您的活动目录域使用受支持的 Windows 服务器版本。	Windows 服务器支持的版本
AD 管理员特权	活动目录管理帐户必须是以下组之一的成员： • AD 林中的 **Enterprise Admin (EA)** 组 • AD 林的林根域中的 **Domain Admins (DA)** 组	
网络	所有 IdM 服务器的 Linux 内核中都启用了 IPv6 支持。	IdM 中的 IPv6 要求
日期和时间	验证两个服务器上的日期和时间设置是否匹配。	IdM 的时间服务要求
加密类型	以下 AD 帐户有 AES 加密密钥： • AD 管理员 • AD 用户帐户 • AD 服务 如果您最近在 AD 中启用了 AES 加密，请使用以下步骤生成新的 AES 密钥： 1. 在林中重新建立任何 AD 域间的信任关系。 2. 更改 AD 管理员、用户帐户和服务的密码。	• 支持 IdM 中的加密类型 • 使用 GPO 在 Active Directory 中启用 AES 加密类型
firewall	您已在 IdM 服务器和 AD 域控制器上为双向通信开放了所有必要的端口。	IdM 和 AD 间的通信所需的端口

组件	配置	其它详情
DNS	• IdM 和 AD 各自都有唯一的主 DNS 域。 • IdM 和 AD DNS 域不能重叠。 • LDAP 和 Kerberos 服务的正确的 DNS 服务(SRV)记录。 • 您可以解析信任中所有 DNS 域的 DNS 记录。 • Kerberos 域名称是主 DNS 域名的大写版本。例如，DNS 域 **example.com** 具有对应的 Kerberos 域 **EXAMPLE.COM**	为信任配置 DNS 和域设置
Topology	确保试图与您配置为信任控制器的 IdM 服务器建立信任。	信任控制器和信任代理

34.9.3. 收集尝试建立 AD 信任的调试日志

如果您在 IdM 环境和 AD 域间建立信任时遇到问题，请使用以下步骤启用详细的错误记录，以便您可以收集尝试建立信任的日志。您可以查看这些日志来帮助进行故障排除，或者您可以在红帽技术支持问题单中提供这些信息。

先决条件

- 您需要 root 权限来重启 IdM 服务。

流程

1. 要为 IdM 服务器启用调试，请创建具有以下内容的文件 **/etc/ipa/server.conf**。

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

2. 重启 **httpd** 服务以载入调试配置。

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

3. 停止 **smb** 和 **winbind** 服务。

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

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

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

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

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

6. 删除以前的 Samba 日志。

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

7. 启动 **smb** 和 **winbind** 服务。

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

8. 在您试图建立启用了详细模式的信任时，请打印时间戳，。

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

9. 查看以下错误日志文件，以了解有关失败请求的信息：

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

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

10. 禁用调试。

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

11. *（可选）* 如果无法确定身份验证问题的原因：

    a. 收集和归档您最近生成的日志文件。

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

    b. 创建一个红帽技术支持问题单，并提供尝试的时间戳和调试日志。

其他资源

- ipa - AD 信任故障排除

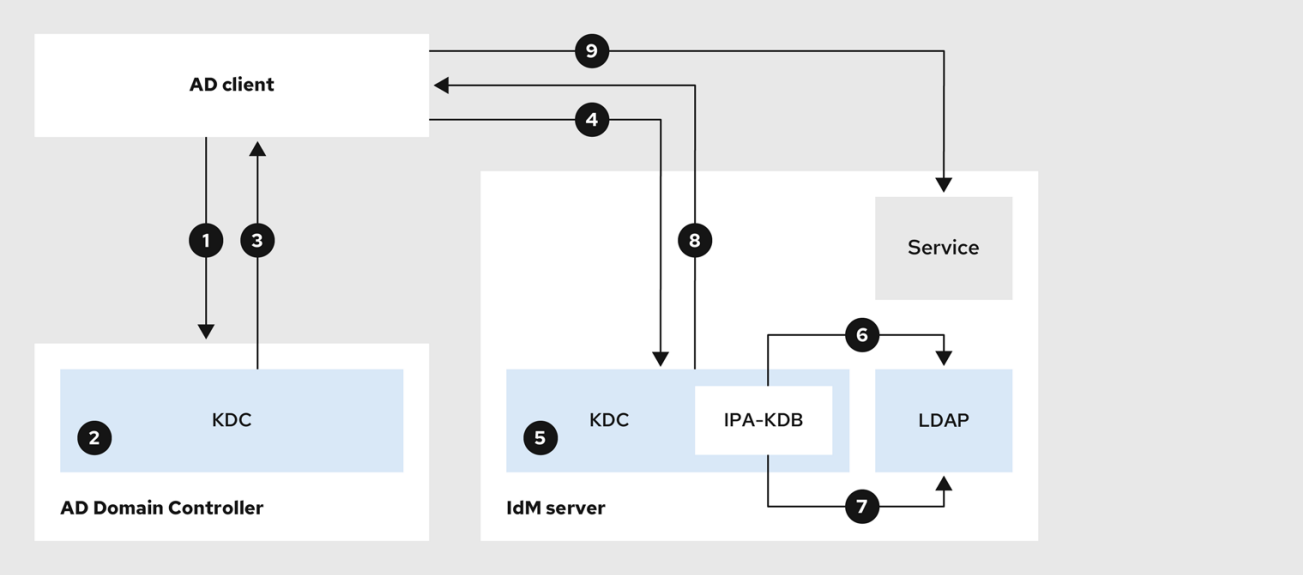
34.10. 对客户端访问其他林中的服务进行故障排除

在身份管理(IdM)和活动目录(AD)环境之间配置信任后，您可能会遇到以下问题：一个域中的客户端无法访问其他域中的服务。使用下面的图对问题进行故障排除。

34.10.1. AD 林根域中的主机请求 IdM 服务器的服务时的信息流

下图显示了当活动目录(AD)客户端请求身份验证(IdM)域中服务时的信息流。

如果您访问 AD 客户端的 IdM 服务时遇到问题，您可以使用此信息缩小故障排除范围，并识别问题源。



1. AD 客户端联系 AD Kerberos 分发中心(KDC)来在 IdM 域中为服务执行 TGS 请求。
2. AD KDC 识别该服务属于可信 IdM 域。
3. AD KDC 向客户端发送跨域票据授予票据(TGT)，以及对可信 IdM KDC 的引用。
4. AD 客户端使用跨域 TGT 向 IdM KDC 请求票据。
5. IdM KDC 验证通过跨域 TGT 传输的特权属性证书(MS-PAC)。
6. IPA-KDB 插件可能会检查 LDAP 目录，以查看是否允许外部主体获取所请求的服务的票据。
7. IPA-KDB 解码 MS-PAC、验证并过滤数据。它会在 LDAP 服务器中执行查找，以检查是否需要使用其它信息（如本地组）来扩大 MS-PAC。
8. 然后，IPA-KDB 插件对 PAC 进行编码，为其签名，将其附加到服务票据，并将其发送给 AD 客户端。
9. AD 客户端现在可以使用 IdM KDC 发布的服务票据联系 IdM 服务。

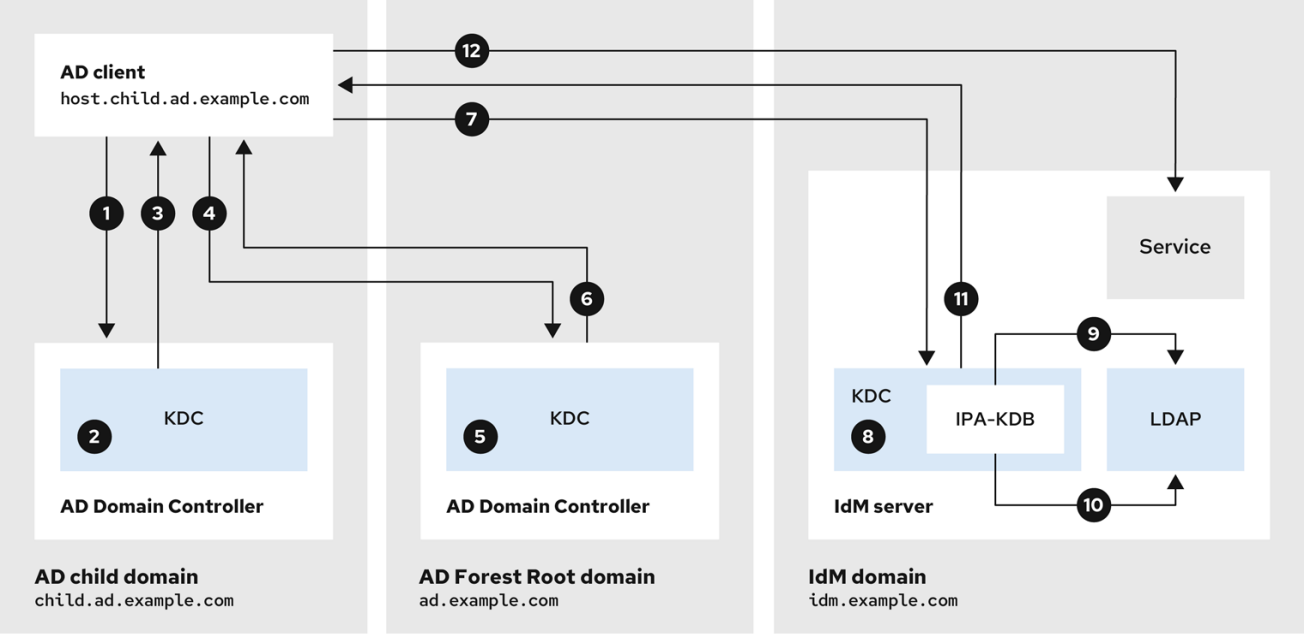
其他资源

- AD 子域中的主机请求 IdM 服务器的服务时的信息流

34.10.2. AD 子域中的主机请求 IdM 服务器的服务时的信息流

下图解释了当子域中的活动目录(AD)主机请求身份管理(IdM)域中的服务时的信息流。在这个场景中，AD 客户端联系子域中的 Kerberos 分发中心(KDC)，然后联系 AD 林根中的 KDC，最后联系 IdM KDC 以请求访问 IdM 服务。

如果您在访问 AD 客户端的 IdM 服务时遇到问题，并且您的 AD 客户端属于 AD 林根的子域，那么您可以使用这些信息缩小故障排除的范围，并识别问题源。



1. AD 客户端在其自己的域中联系 AD Kerberos Distribution Center(KDC)，以执行对 IdM 域中服务的 TGS 请求。
2. 子域 **child.ad.example.com** 中的 AD KDC（子域）识别服务属于可信的 IdM 域。
3. 子域中的 AD KDC 向客户端发送 AD 林根域 **ad.example.com** 的引用票据。
4. AD 客户端联系 AD 林根域中的 KDC，以获取 IdM 域中的服务。
5. 林根域中的 KDC 识别服务属于可信的 IdM 域。
6. AD KDC 向客户端发送跨域票据授予票据(TGT)，以及对可信 IdM KDC 的引用。
7. AD 客户端使用跨域 TGT 向 IdM KDC 请求票据。
8. IdM KDC 验证通过跨域 TGT 传输的特权属性证书(MS-PAC)。
9. IPA-KDB 插件可能会检查 LDAP 目录，以查看是否允许外部主体获取所请求的服务的票据。
10. IPA-KDB 解码 MS-PAC、验证并过滤数据。它会在 LDAP 服务器中执行查找，以检查是否需要使用其它信息（如本地组）来扩大 MS-PAC。
11. 然后，IPA-KDB 插件对 PAC 进行编码，为其签名，将其附加到服务票据，并将其发送给 AD 客户端。
12. AD 客户端现在可以使用 IdM KDC 发布的服务票据联系 IdM 服务。

其他资源

- AD 林根域中的主机请求 IdM 服务器的服务时的信息流

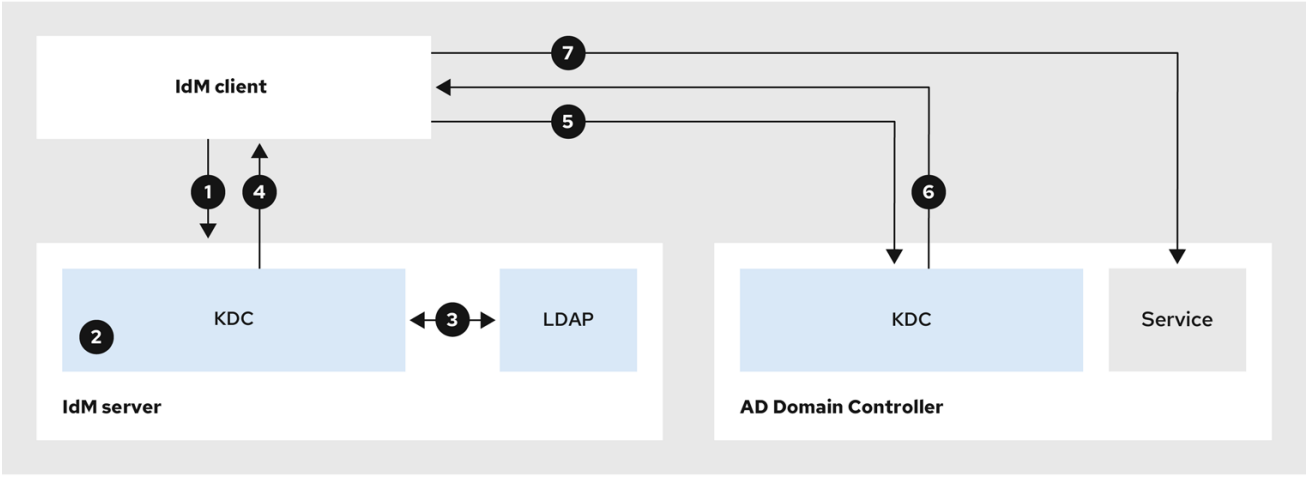
34.10.3. IdM 客户端请求 AD 服务器的服务时的信息流

下图解释了当您在 IdM 和 AD 之间配置了双向信任时，身份管理(IdM)客户端请求活动目录(AD)域中的服务时的信息流。

如果您访问 IdM 客户端的 AD 服务时遇到问题，您可以使用此信息缩小故障排除的范围，并识别问题源。

注意

默认情况下，IdM 建立到 AD 的单向信任，这意味着无法为 AD 林中的资源发出跨域票据授予票据(TGT)。为了能够请求可信 AD 域中服务的票据，请配置双向信任。



1. IdM 客户端为了其要联系的 AD 服务，请求 IdM Kerberos 分发中心(KDC)的票据授予票据。
2. IdM KDC 识别服务属于 AD 域，验证域是否已知并可信，以及是否允许客户端请求该域的服务。
3. 使用 IdM 目录服务器关于用户主体的信息，IdM KDC 创建一个跨域 TGT，其中包含有关用户主体的特权属性证书(MS-PAC)记录。
4. IdM KDC 向 IdM 客户端发回一个跨域 TGT。
5. IdM 客户端联系 AD KDC 来请求 AD 服务的票据，显示包含 IdM KDC 提供的 MS-PAC 的跨域 TGT。
6. AD 服务器验证和过滤 PAC，并返回 AD 服务的票据。
7. IPA 客户端现在可以联系 AD 服务。

其他资源

- 单向信任和双向信任

34.11. 使用命令行删除信任

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

先决条件

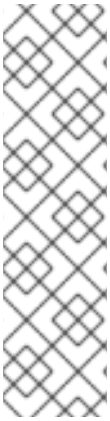
- 您已作为 IdM 管理员获得了 Kerberos 单。详情请参阅 Web UI 中的登录到 IdM: 使用 Kerberos ticket。

流程

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

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

2. 从 Active Directory 配置中删除信任对象。



注意

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

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

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

验证步骤

- 使用 **ipa trust-show** 命令来确认信任已删除。

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

其他资源

- 删除对 AD 的信任后删除 ID 范围

34.12. 使用 IDM WEB UI 删除信任

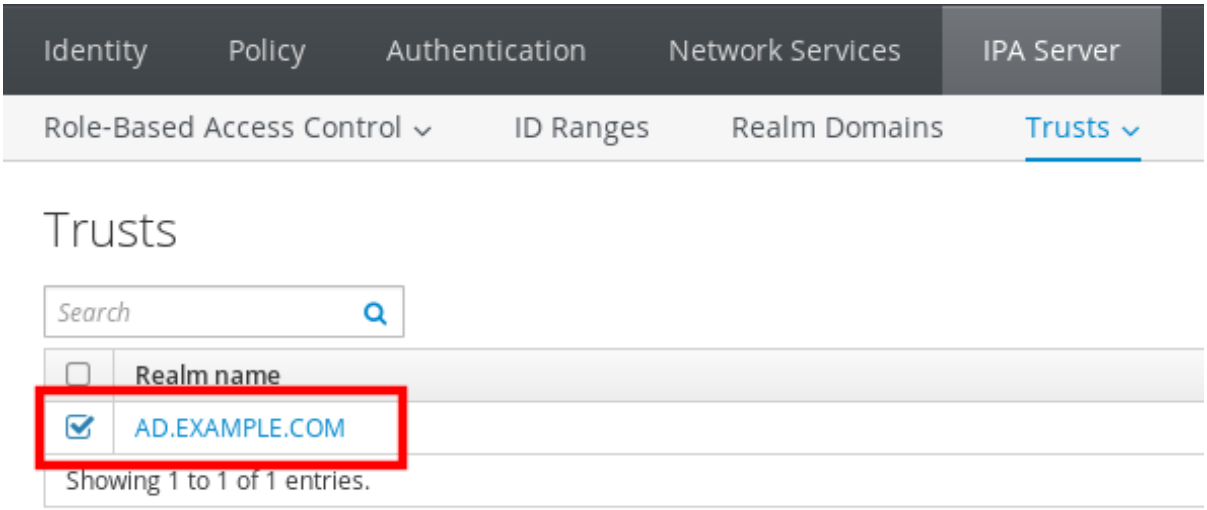
按照以下流程，使用 IdM Web UI 删除身份管理(IdM)/活动目录(AD)信任。

先决条件

- 您已获得 Kerberos ticket。详情请参阅 Web UI 中的登录到 IdM: 使用 Kerberos ticket 。

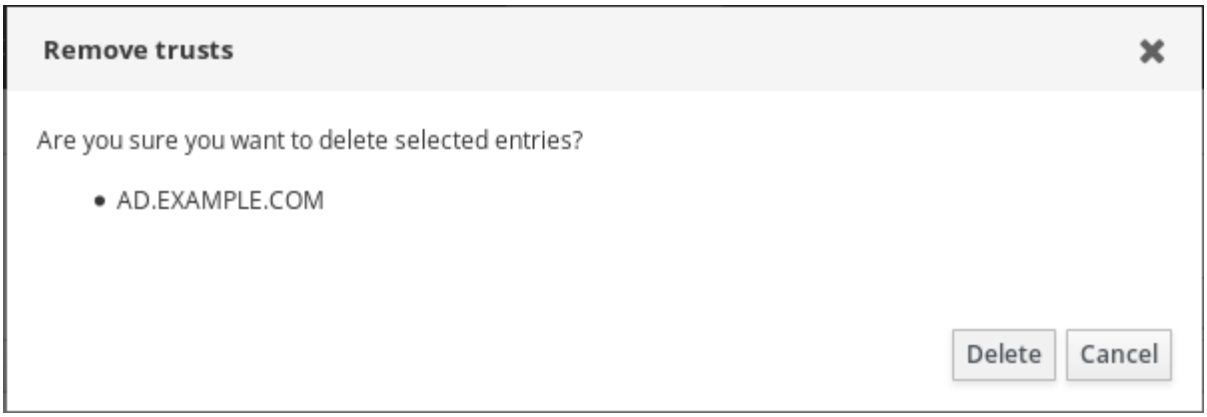
流程

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



5. 点击 **Delete** 按钮。

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



7. 从 Active Directory 配置中删除信任对象。

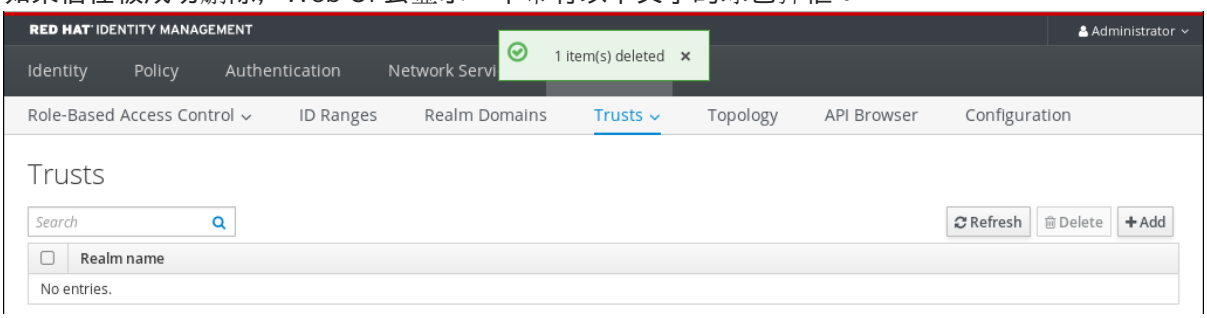
注意

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

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

验证步骤

- 如果信任被成功删除，Web UI 会显示一个带有以下文字的绿色弹框：



其他资源

- 删除对 AD 的信任后删除 ID 范围

34.13. 使用 ANSIBLE 删除信任

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

先决条件

- 您已作为 IdM 管理员获得了 Kerberos 单。详情请参阅 Web UI 中的登录到 IdM: 使用 Kerberos ticket。
- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名(FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（也就是在其上执行 **ansible-freeipa** 模块的节点）是 IdM 域的一部分，来作为 IdM 客户端、服务器或副本。

流程

1. 进入您的 ***~/MyPlaybooks/*** 目录：

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

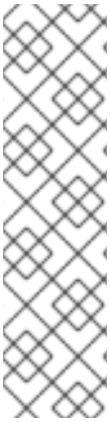
2. 使用以下内容创建 **del-trust.yml** playbook：

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

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

在示例中，**realm** 定义 AD 领域名称字符串。

3. 保存该文件。
4. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory del-trust.yml
```



注意

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

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

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

验证步骤

- 使用 **ipa trust-show** 命令来确认信任已删除。

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

其他资源

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

34.14. 删除对 AD 的信任后删除 ID 范围

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

警告

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

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

先决条件

- 您已删除了对 AD 环境的信任。

流程

1. 显示所有当前正在使用的 ID 范围：

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

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

3. 删除范围：

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

4. 重启 SSSD 服务，来删除对您已删除的 ID 范围的引用。

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

其他资源

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