Red Hat Enterprise Linux 9

规划身份管理

规划 IdM 环境的基础架构和服务集成

Last Updated: 2024-06-26

Red Hat Enterprise Linux 9 规划身份管理

规划 IdM 环境的基础架构和服务集成

法律通告

摘要

身份管理(IdM)提供了一种集中且统一的方法来管理身份存储、身份验证和授权策略。 要成功在您的环境中集成 IdM，请了解 IdM 组件并规划安装。例如，为故障转移和负载平衡规划复制拓扑，集成到活动目录(AD)、DNS 区域的结构和证书颁发机构(CA)，以及备份和恢复场景。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

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

第 1 章 RHEL 中的 IDM 和访问控制概述

了解如何使用身份管理(IdM)来集中身份管理、执行安全控制并遵守最佳实践和安全策略。探索 Linux 和 Windows 环境中的 IdM 实施的常见客户场景和解决方案。

1.1. IDM 简介

身份管理(IdM)提供了一种集中且统一的方法，在基于 Linux 的域中管理身份存储、身份验证、策略和授权策略。

Red Hat Enterprise Linux 中 IdM 的目标

IdM 可显著降低单独管理不同服务以及在不同机器上使用不同工具的管理开销。

IdM 是一个用于中央化身份、策略和授权的软件解决方案，它支持：

- Linux 操作系统环境的高级特性
- 统一大型的 Linux 机器组
- 与 Active Directory 的原生集成

IdM 创建一个基于 Linux 并由 Linux 控制的域：

- IdM 基于现有的原生 Linux 工具和协议构建。它有自己的进程和配置，但其底层的技术已在 Linux 系统中广泛使用，并被 Linux 管理员信任。
- IdM 服务器和客户端是 Red Hat Enterprise Linux 机器。IdM 客户端也可以是支持标准协议的其它 Linux 和 UNIX 发行版本。Windows 客户端不能是 IdM 域的成员，但用户登录到 Active Directory (AD) 管理的 Windows 系统可以连接到 Linux 客户端或访问由 IdM 管理的服务。这可以通过在 AD 和 IdM 域间建立跨林信任来实现。

在多个 Linux 服务器中管理身份及策略

*没有 IdM：*每个服务器都单独管理。所有密码都保存在本地机器上。IT 管理员管理每台计算机上的用户，单独设置身份验证和授权策略，并且维护本地密码。然而，用户通常会依赖其他中央化的解决方案，例如直接与 AD 集成。可使用几种不同的解决方案直接与 AD 集成：

- 旧 Linux 工具（不推荐使用）
- 基于 Samba winbind 的解决方案（针对特定用例推荐）
- 基于第三方软件的解决方案（通常需要其他供应商的许可证）
- 基于 SSSD 的解决方案（针对大多数用例的原生 Linux 推荐）

*使用 IdM：*IT 管理员可以：

- 在一个中央位置管理用户的身份：IdM 服务器
- 同时对多个机器统一应用策略
- 使用基于主机的访问控制、委托和其他规则为用户设置不同的访问级别
- 集中管理权限升级规则
- 定义如何挂载主目录

企业级 SSO

如果是 IdM Enterprise，单点登录（SSO）会通过 Kerberos 协议实现。此协议在基础架构级别中很受欢迎，并启用带有 SSH、LDAP、NFS、CUPS 或 DNS 等服务的 SSO。也可以使用不同 Web 堆栈（Apache、EAP 和 Django 等）的 Web 服务将 Kerberos 用于 SSO。但是，实践显示，使用基于 SSO 的 OpenID Connect 或 SAML 对于 Web 应用更为方便。若要桥接两个层，建议部署一种身份提供程序 (IdP) 解决方案，该解决方案可以将 Kerberos 身份验证转换为 OpenID Connect 凭证或 SAML 断言。基于 Keycloak 开源项目的 Red Hat SSO 技术是此类 IdP 的示例。

*没有 IdM：*用户每次访问服务或应用程序时都会提示用户输入密码。这些密码可能有所不同，用户必须记住使用哪个凭证。

*使用 IdM：*在用户登录系统后，他们可以访问多个服务和应用程序，无需重复提供自己的身份凭证。这有助于：

- 提高可用性
- 降低以不安全方式写入或保存密码的安全风险
- 提高用户的生产率

管理一个混合了 Linux 和 Windows 的环境

*没有 IdM：*Windows 系统在 AD 林中管理，但开发、生产和其他团队有许多 Linux 系统。AD 环境中排除了 Linux 系统。

*使用 IdM：*IT 管理员可以：

- 使用原生 Linux 工具管理 Linux 系统
- 将 Linux 系统整合到由 Active Directory 集中管理的环境中，并保留集中用户存储。
- 根据需要轻松部署新的 Linux 系统。
- 迅速响应业务需求，并在不依赖于其他团队的情况下做出与管理 Linux 构架相关的决定，避免延迟。

IdM 与标准 LDAP 目录相对

标准 LDAP 目录（如 Red Hat Directory Server）是一个通用目的目录：可以定制为适应各种使用案例。

- Schema：一种可针对大量条目（如用户、计算机、网络实体、物理设备或设施）自定义的灵活方案。
- 通常用作：用于存储其他应用的数据的后端目录，如在 Internet 上提供服务的业务应用程序。

IdM 具有特定目的：管理内部、企业内部身份，以及与这些身份相关的身份验证和授权策略。

- Schema：定义一组与其目的相关的特定条目的特定架构，如用于用户身份或机器身份的条目。
- 通常，身份和验证服务器用于在企业或项目边界内管理身份。

Red Hat Directory Server 和 IdM 的底层目录服务器技术是相同的。但是，IdM 被优化来管理企业内部的身份。这限制了其总体可扩展性，但也带来了一些好处：更简单的配置、更好的资源管理自动化和提高企业身份管理效率。

其他资源

- Red Hat Enterprise Linux 博客上的 身份管理或 Red Hat Directory Server - 我应该用哪个
- 有关标准协议的知识库文章

1.2. 常见 IDM 客户场景及其解决方案

了解 Linux 和 Windows 环境中常见身份管理和访问控制用例的示例，以及它们的解决方案。

场景 1

情况

您是贵公司的 Windows 管理员。
除了 Windows 系统外，您还需要管理一些 Linux 系统。

因为您无法将环境的任何部分控制委派给 Linux 管理员，所以您必须处理 Active Directory (AD) 中的所有安全控制。

解决方案

将 Linux 主机直接集成到 AD。
如果您希望在 LDAP 服务器中集中定义 **sudo** 规则，您必须在 AD 域控制器 (DC) 中实施模式扩展。如果您没有实施此扩展的权限，请考虑安装身份管理(IdM)- 请参阅下面的 Scenario 3。因为 IdM 已经包含 schema 扩展，您可以在 IdM 中直接管理 **sudo** 规则。

如果您期望将来需要更多 Linux 技能，请进一步建议

与 Linux 社区联系，了解他人如何管理身份：用户、主机和服务。
研究最佳实践。

您需要更加熟悉 Linux：

- 尽可能使用 RHEL web 控制台。
- 尽可能在命令行中使用简单命令。
- 参加红帽系统管理课程。

场景 2

情况

您是贵公司的 Linux 管理员。
您的 Linux 用户需要不同级别的公司资源访问权限。

您需要密切的集中访问控制您的 Linux 机器。

解决方案

安装 IdM 并将您的用户迁移到其中。

如果您期望公司在未来扩展，请进一步建议

安装 IdM 后，配置 基于主机的访问控制 和 sudo 规则。这些是保持安全最佳实践限制访问权限和最小特权所必需的。
为满足您的安全目标，开发一种统一的身份和访问管理 (IAM) 策略，它使用协议来保护基础架构和应用程序层。

场景 3

情况

您是贵公司的 Linux 管理员，您必须将 Linux 系统与公司 Windows 服务器集成。您希望保持对 Linux 系统的唯一访问权限控制者。
不同的用户需要对 Linux 系统有不同的访问级别，但它们都位于 AD 中。

解决方案

由于 AD 控制不够强大，因此您必须在 Linux 端配置对 Linux 系统的访问控制。安装 IdM 并建立 IdM-AD 信任。

进一步建议增强环境安全性

安装 IdM 后，配置 基于主机的访问控制 和 sudo 规则。这些是保持安全最佳实践限制访问权限和最小特权所必需的。
为满足您的安全目标，开发一个统一的 Identity and Access Management (IAM)策略，它使用协议来保护基础架构和应用程序层。

场景 4

情况

作为安全管理员，您必须在所有环境中管理身份和访问，包括所有红帽产品。您必须在一个位置管理所有身份，并在所有平台、云和产品中保持访问控制。

解决方案

集成 IdM、红帽单点登录、Red Hat Satellite 、Red Hat Ansible Automation Platform 和其他红帽产品。

场景 5

情况

作为国防部 (DoD) 或 Intelligence Community (IC) 环境的安全性和系统管理员，您需要使用智能卡或 RSA 身份验证。您需要使用 PIV 证书或 RSA 令牌。

解决方案

1. 在 IdM 中配置证书映射。
2. 如果存在 IdM-AD 信任，请确保已启用 GSSAPI 委派。
3. 为 RSA 令牌配置 IdM 中的 radius 配置。
4. 为智能卡验证配置 IdM 服务器和 IdM 客户端。

其他资源

- 使用 Ansible 自动化您的 IdM 任务，以减少客户端配置时间和复杂性，并减少错误。

1.3. IDM 服务器和客户端简介

Identity Management (IdM) 域包括以下类型的系统：

IdM 客户端

IdM 客户端是注册了服务器的 Red Hat Enterprise Linux 系统，并配置为使用这些服务器中的 IdM 服务。
客户端与 IdM 服务器交互来访问由它们提供的服务。例如，客户端使用 Kerberos 协议来执行身份验证，并获取企业单点登录(SSO)的票据，使用 LDAP 获取身份和策略信息，使用 DNS 检测服务器和服务所在的位置，以及如何连接它们。

IdM 服务器

IdM 服务器是响应 IdM 域内身份、认证和授权请求的 Red Hat Enterprise Linux 系统。在大多数部署中，集成的证书颁发机构 (CA) 也安装 IdM 服务器。
IdM 服务器是身份和策略信息的中央仓库。IdM 服务器也可以托管域成员使用的任何可选服务：

- 证书颁发机构 (CA)
- 密钥恢复授权中心 (KRA)
- DNS
- Active Directory (AD) 信任控制器
- Active Directory (AD) 信任代理

IdM 服务器也是嵌入式 IdM 客户端。与自己注册的客户端一样，服务器可以提供与其他客户端相同的功能。

为了为大量客户端以及冗余和可用性提供服务，IdM 允许在单一域中的多个 IdM 服务器中进行部署。可以部署最多 60 个服务器。这是 IdM 域中目前支持的最大 IdM 服务器数，也称为副本。IdM 服务器为客户端提供不同的服务。不是所有的服务器都需要提供所有可能的服务。每个服务器中都总是可用的 Kerberos 和 LDAP 等服务器组件。CA、DNS、Trust Controller 或 Vault 等其它服务都是可选的。这意味着不同的服务器在部署中通常会扮演不同的角色。

如果您的 IdM 拓扑包含一个集成的 CA，则一个服务器具有证书撤销列表 (CRL) publisher 服务器 的角色，一个服务器则拥有 CA 续订服务器的角色。

默认情况下，安装的第一个 CA 服务器承担这两个角色，但您可以将这些角色分配到单独的服务器。

警告

*CA 续订服务器*对您的 IdM 部署至关重要，因为它是负责跟踪 CA 子系统 证书和密钥的域中的唯一系统。有关如何从影响您的 IdM 部署的灾难中恢复的详情，请参阅 使用身份管理执行灾难恢复。

要获得冗余和负载平衡，管理员需要通过创建现有服务器的*副本*来创建附加服务器。在创建副本时，IdM 会克隆现有服务器的配置。副本与初始服务器的核心配置共享，包括有关用户、系统、证书和配置策略的内部信息。

注意

除了 *CA renewal* 和 *CRL publisher* 角色外，副本和从中创建副本的服务器的功能完全相同。因此，术语***服务器（server）***和***副本（replica）***名会根据上下文互换使用。

1.4. 安装 IDM 客户端支持的 RHEL 版本

IdM 服务器在 Red Hat Enterprise Linux 9 的最新次版本上运行的身份管理部署支持在最新次版本上运行的客户端：

- RHEL 7
- RHEL 8
- RHEL 9

注意

虽然其他客户端系统（如 Ubuntu）可以与 IdM 9 服务器一起使用，但红帽不对这些客户端提供支持。

1.5. RHEL 中的 IDM 和访问控制：中央化和本地化的比较

在 Red Hat Enterprise Linux 中，您可以使用集中工具对整个系统域管理身份和访问控制策略，或使用本地工具管理单一系统。

在多个 Red Hat Enterprise Linux 服务器中管理身份和策略

使用 Identity Management IdM，IT 管理员可以：

- 在一个中央位置维护身份和分组机制：IdM 服务器
- 集中管理不同类型的凭证，如密码、PKI 证书、OTP 令牌或 SSH 密钥
- 同时对多个机器统一应用策略
- 为外部 Active Directory 用户管理 POSIX 和其他属性
- 使用基于主机的访问控制、委托和其他规则为用户设置不同的访问级别
- 集中管理权限升级规则 (sudo) 和强制访问控制（SELinux 用户映射）
- 维护中央 PKI 基础架构和 secret 存储
- 定义如何挂载主目录

没有 IdM:

- 每台服务器单独管理
- 所有密码都保存在本地机器中
- IT 管理员管理每台机器上的用户，单独设置身份验证和授权策略，并维护本地密码

1.6. IDM 术语

Active Directory 林（forest）

Active Directory (AD) 林是由一个或多个域树组成的集合，共享一个通用的全局目录、目录架构、逻辑结构和目录配置。林（forest）代表了可以访问用户、计算机、组和其他对象的安全边界。如需更多信息，请参阅微软的林文档

Active Directory 全局目录

全局目录是活动目录(AD)的一项功能，允许域控制器提供有关林中任何对象的信息，无论对象是否是域控制器域的成员。启用全局目录功能的域控制器称为全局目录服务器。全局目录为多域 Active Directory Domain Services (AD DS) 中每个域中的所有对象提供一个可搜索的目录。

Active Directory 安全标识符

安全标识符 (SID) 是分配给 Active Directory 中对象的唯一 ID 编号，如用户、组或主机。它在功能上等同于 Linux 中的 UID 和 GID。

Ansible play

Ansible play 是 Ansible playbook 的构建块。Play 的目标是将一组主机映射到由 Ansible 任务表示的一些定义良好的角色。

Ansible playbook

Ansible playbook 是包含一个或多个 Ansible play 的文件。如需更多信息，请参阅有关 playbook 的官方 Ansible 文档。

Ansible 任务

Ansible 任务是 Ansible 中的操作单元。一个 Ansible play 可以包含多个任务。每个任务的目标是使用非常具体的参数执行模块。Ansible 任务是一组可通过特定 Ansible 角色或模块实现广泛定义状态的指令，并根据角色或模块的变量进行调优。如需更多信息，请参阅官方 Ansible 任务文档。

Apache Web 服务器

Apache HTTP 服务器（统称为 Apache）是一个免费的、开源的跨平台 Web 服务器应用程序，根据 Apache License 2.0 的条款发布。Apache 在万维网的初始成长中发挥了关键作用，目前是领先的 HTTP 服务器。其进程名称为 **httpd**，是 *HTTP daemon* 的缩写。红帽身份管理(IdM)使用 Apache Web 服务器来显示 IdM Web UI，并协调组件之间的通信，如目录服务器和证书颁发机构等。

证书

证书是一个电子文件，用于识别个人、服务器、公司或其他实体并将该身份与公钥关联。比如某个驱动程序的许可或论坛，证书可提供个人身份的可识别验证。公钥加密使用证书来解决身份模拟问题。

IdM 中的证书颁发机构(CA)

发布数字证书的实体。在 Red Hat Identity Management 中，主 CA 是 **ipa**，IdM CA。**ipa** CA 证书是以下类型之一：

- 自签名。在本例中，**ipa** CA 是 root CA。
- 外部签名。在这种情况下，**ipa** CA 会从属到外部 CA。

在 IdM 中，您还可以创建多个 **子 CA（sub-CA）**。子 CA 是其证书是以下类型之一的 IdM CA：

- 由 **ipa** CA 签名。
- 由自身和 **ipa** CA 之间的任意中间 CA 签名。子 CA 的证书不能是自签名的。

另请参阅 规划您的 CA 服务。

跨林信任

在两个 Kerberos 域间建立一个信任的访问关系，允许一个域中的用户和服务访问另一个域中的资源。通过 Active Directory (AD) 林根域和 IdM 域间的跨林信任，来自 AD 林域中的用户可以与 IdM 域中的 Linux 机器和服务交互。从 AD 的角度来看，身份管理代表一个独立的 AD 域。如需更多信息，请参阅信任会如何工作。

目录服务器

目录服务器集中管理用户身份和应用程序信息。它提供独立于操作系统、基于网络的注册表，用于存储应用程序设置、用户配置文件、组数据、策略和访问控制信息。网络上的每个资源都被目录服务器视为一个对象。有关特定资源的信息存储为与该资源或对象相关联的属性集合。红帽目录服务器符合

LDAP 标准。

DNS PTR 记录

DNS 指针 (PTR) 记录将主机的 IP 地址解析为域或主机名。PTR 记录与 DNS A 和 AAAA 记录（将主机名解析为 IP 地址）相反。DNS PTR 记录启用反向 DNS 查找。PTR 记录存储在 DNS 服务器上。

DNS SRV 记录

DNS 服务 (SRV) 记录定义域中可用服务的主机名、端口号、传输协议、优先级和权重。您可以使用 SRV 记录来定位 IdM 服务器和副本。

域控制器 (DC)

域控制器 (DC) 是响应域中安全身份验证请求的主机，并且控制对该域中资源的访问。IdM 服务器作为 IdM 域的 DC 工作。DC 验证用户、存储用户帐户信息，以及实施域的安全策略。当用户登录某个域时，DC 会检查并验证其凭据并允许或拒绝访问。

完全限定域名

完全限定域名 (FQDN) 是一个域名，用于指定主机在域名系统 (DNS) 层次结构中的确切位置。在父域 **example.com** 中具有主机名 **myhost** 的设备具有 FQDN **myhost.example.com**。通过 FQDN 可以将设备与其他域中名为 **myhost** 的任何其他主机区分开来。

如果您使用 DNS 自动发现在主机 **machine1** 上安装 IdM 客户端，并且正确配置了 DNS 记录，则需要 **machine1** 的 FQDN。如需更多信息，请参阅 IdM 的主机名和 DNS 要求。

GSSAPI

通用安全服务应用程序接口（GSSAPI 或 GSS-API）使开发人员能够抽象其应用程序是如何保护发送到对等应用程序的数据。安全服务提供商可以将常见流程调用的 GSSAPI 实现作为其安全软件的库来提供。这些库为那些编写只使用独立于供应商的 GSSAPI 来编写应用程序的人提供了一个兼容 GSSAPI 的接口。凭借这种灵活性，开发人员不必针对任何特定平台、安全机制、保护类型或传输协议量身定制其安全实现。

Kerberos 是主流的 GSSAPI 机制实施，它允许 Red Hat Enterprise Linux 和 Microsoft Windows Active Directory Kerberos 实现与 API 兼容。

隐藏的副本

隐藏的副本是一个 IdM 副本，它正在运行所有服务且可用，但其服务器角色被禁用，客户端无法发现其副本，因为它在 DNS 中没有 SRV 记录。

隐藏副本主要设计用于备份、批量导入和导出等服务，或者需要关闭 IdM 服务的操作。因为没有客户端使用隐藏的副本，管理员可以在不影响任何客户端的情况下暂时关闭这个主机上的服务。如需更多信息，请参 隐藏的副本模式。

HTTP 服务器

请参阅 Web 服务器。

ID 映射

SSSD 可以使用 AD 用户的 SID 在名为 ID *映射的过程中以算法生成 POSIX ID*。ID 映射会在 AD 中的 SID 和 Linux 中的 ID 之间创建一个映射。

- 当 SSSD 检测到新的 AD 域时，它会为这个新域分配一个可用的 ID 范围。因此，每个 AD 域在每个 SSSD 客户端机器上都有一个相同的 ID 范围。
- 当 AD 用户第一次登录到 SSSD 客户端机器时，SSSD 会在 SSSD 缓存中为用户创建一个条目，包括基于用户的 SID 和该域的 ID 范围的 UID。
- 由于 AD 用户的 ID 是以一致的方式从同一 SID 生成的，所以用户在登录到任何 Red Hat Enterprise Linux 系统时都有相同的 UID 和 GID。

ID 范围

ID 范围是分配给 IdM 拓扑或特定副本的 ID 数范围。您可以使用 ID 范围为新用户、主机和组指定有效的 UID 和 GID 范围。ID 范围用于避免 ID 号冲突。IdM 中有两个不同的 ID 范围：

- *IdM ID 范围*
  使用此 ID 范围为整个 IdM 拓扑中的用户和组定义 UID 和 GID。安装第一个 IdM 服务器会创建 IdM ID 范围。创建后您无法修改 IdM ID 范围。但是，您可以创建一个额外的 IdM ID 范围，例如当原始 ID 接近耗尽时。

- *分布式数字分配 (44) ID 范围*
  使用此 ID 范围定义创建新用户时使用的副本的 UID 和 GID。第一次将新用户或主机条目添加到 IdM 副本中，可为该副本分配一个 DNA ID 范围。管理员可以修改 ID 范围，但新定义必须位于现有的 IdM ID 范围内。

  请注意，IdM 范围与 DNA 范围相匹配，但它们并没有相互连接。如果您更改了一个范围，请确保更改另一个范围以进行匹配。

如需更多信息，请参阅 ID 范围。

ID 视图

通过 ID 视图，您可以为 POSIX 用户或组属性指定新值，并定义要应用新值的客户端和主机。例如，您可以使用 ID 视图来：

- 为不同的环境定义不同的属性值。
- 将之前生成的属性值替换为不同的值。

在 IdM-AD 信任设置中，**Default Trust View** 是应用到 AD 用户和组的 ID 视图。使用 **Default Trust View**，您可以为 AD 用户和组定义自定义 POSIX 属性，从而覆盖 AD 中定义的值。

如需更多信息，请参阅使用 ID 视图覆盖 IdM 客户端中的用户属性值 。

IdM CA 服务器

安装并运行 IdM 证书颁发机构 (CA) 服务的 IdM 服务器。
备选名称： **CA 服务器**

IdM 部署

用于指代整个 IdM 安装的术语。您可以通过回答以下问题来描述您的 IdM 部署：

- 您的 IdM 是一个试部署还是一个生产环境的部署？
  - 您有多少个 IdM 服务器？
- 您的 IdM 部署包含 一个集成的 CA？
  - 如果是，则集成的 CA 是自签名还是外部签名？
  - 如果是，则在哪些服务器上 CA 角色 可用？KRA 角色在哪些服务器上可用？
- 您的 IdM 部署是否包含 一个集成的 DNS？
  - 如果是，则在哪些服务器上提供 DNS 角色？
- 您的 IdM 是否在与 AD 林的信任协议中部署？
  - 如果是，则在哪些服务器中 AD 信任控制器或 AD 信任代理角色 可用？

IdM 服务器和副本

要在 IdM 部署中安装第一个服务器，您必须使用 **ipa-server-install** 命令。
然后，管理员可以使用 **ipa-replica-install** 命令在安装的第一个服务器之外安装**副本**。默认情况下，安装副本会与从中创建其的 IdM 服务器创建 复制协议 ，从而能够向其余 IdM 接收和发送更新。

所安装的第一个服务器与副本之间没有功能差异。两者都是全功能读/写 IdM 服务器。

已弃用的名称： **master 服务器**

IdM CA 续订服务器

如果您的 IdM 拓扑包含一个集成证书颁发机构 (CA)，则一台服务器会具有唯一的 CA renewal server 角色。这个服务器维护并更新 IdM 系统证书。
默认情况下，您安装的第一个 CA 服务器将履行此角色，但您可以将任何 CA 服务器配置为 CA 续订服务器。在没有集成 CA 的部署中，没有 CA 续订服务器。

已弃用的名称： **master CA**

IdM CRL publisher 服务器

如果您的 IdM 拓扑包含一个集成证书颁发机构 (CA)，则一台服务器会具有唯一的 Certificate revocation list (CRL) publisher server 角色。此服务器负责维护 CRL。
默认情况下，履行 **CA 续订服务器**角色的服务器也承担此角色，但您可以将任何 CA 服务器配置为 CRL 发布程序服务器。在没有集成 CA 的部署中，没有 CRL 发布程序服务器。

IdM 拓扑

涉及 IdM 解决方案结构的术语，特别是各个数据中心和集群之间的复制协议。

Kerberos 认证指示符

身份验证指示符附加到 Kerberos 票据中，并代表用于获取票据的初始验证方法：

- **otp** 双因素身份验证（密码 + 一次性密码）
- **radius** 用于 Remote Authentication Dial-In User Service (RADIUS) 验证（通常用于 802.1x 验证）
- **pkinit** 用于 Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)，智能卡或证书验证。
- **hardened** 用于强化密码以阻止暴力尝试

如需更多信息，请参阅 Kerberos 身份验证指标。

Kerberos keytab

密码是用户的默认验证方法，但 keytabs 是主机和服务的默认验证方法。Kerberos keytab 是包含 Kerberos 主体及其关联的加密密钥列表的文件，因此服务可以检索其自己的 Kerberos 密钥并验证用户身份。
例如，每个 IdM 客户端都有一个 **/etc/krb5.keytab** 文件，该文件存储了 **host** 主体的信息，代表 Kerberos 域中的客户端计算机。

Kerberos 主体

唯一的 Kerberos 主体可识别 Kerberos 网域中的每个用户、服务和主机：

实体	命名规则	示例
用户	**identifier@REALM**	**admin@EXAMPLE.COM**
服务	**service/fully-qualified-hostname@REALM**	**http/server.example.com@EXAMPLE.COM**
主机	**host/fully-qualified-hostname@REALM**	**host/client.example.com@EXAMPLE.COM**

Kerberos 协议

Kerberos 是一种网络身份验证协议，通过使用密钥加密为客户端和服务器应用提供强大的身份验证。IdM 和 Active Directory 使用 Kerberos 来验证用户、主机和服务。

Kerberos realm

Kerberos 域（realm）包括由 Kerberos 密钥分发中心 (KDC) 管理的所有主体。在 IdM 部署中，Kerberos 域包括所有 IdM 用户、主机和服务。

Kerberos ticket 策略

Kerberos 密钥分发中心 (KDC) 通过连接策略强制实施票据访问控制，并通过票据生命周期策略管理 Kerberos 票据的持续时间。例如，默认的全局票据生命周期为一天，默认的全局最大续订期限为一周。

如需更多信息，请参阅 IdM Kerberos ticket 策略类型。

密钥分发中心 (KDC)

Kerberos 密钥分发中心 (KDC) 是充当管理 Kerberos 凭据信息的中央可信权威的服务。KDC 发出 Kerberos 票据并确保来自 IdM 网络内实体的数据的真实性。

如需更多信息，请参阅 IdM KDC 的角色。

LDAP

轻量级目录访问协议(LDAP)是一个开放的、厂商中立的应用程序协议，用于通过网络访问和维护分布式目录信息服务。此规范的一部分是目录信息树(DIT)，它以由目录服务条目的可辨识名称(DN)组成的分层树状结构来表示数据。LDAP 是 ISO X.500 标准描述的用于网络中目录服务的目录访问协议(DAP)的一种"轻量级"版本。

轻量级子 CA

在 IdM 中，轻量级子 CA 是证书颁发机构 (CA)，其证书由 IdM root CA 签名，或属于它的一个 CA。轻量级子 CA 只为特定目的发布证书，例如用来保护 VPN 或 HTTP 连接。

如需更多信息，请参阅限制应用程序只信任某个证书子集。

密码策略

密码策略是特定 IdM 用户组的密码必须满足的一组条件。这些条件可以包括以下参数：

- 密码的长度
- 使用的字符类的数目
- 密码的最长生命周期。

如需更多信息，请参阅什么是密码策略。

POSIX 属性

POSIX 属性是用于维护操作系统间兼容性的用户属性。
在 Red Hat Identity Management 环境中，用户的 POSIX 属性包括：

- **cn**，用户名
- **uid**，帐户名称（登录）
- **uidNumber**，用户编号 (UID)
- **gidNumber**，主组号 (GID)
- **homeDirectory** （用户的主目录）

在 Red Hat Identity Management 环境中，组的 POSIX 属性包括：

- **cn**，组的名称
- **gidNumber**，组号 (GID)

这些属性将用户和组标识为单独的实体。

复制协议

复制协议是同一 IdM 部署的两个 IdM 服务器之间的协议。复制协议确保两个服务器之间不断复制数据和配置。
IdM 使用两种复制协议：*域复制*协议，用于复制身份信息，*证书复制*协议，用于复制证书信息。

如需更多信息，请参阅：

- 复制协议
- 确定正确的副本数
- 在拓扑中连接副本
- 副本拓扑示例

智能卡

智能卡是用来控制对资源访问的可移动设备或者卡。它们可以是具有嵌入式集成电路 (IC) 芯片、小型 USB 设备（如 Yubikey）或其他类似设备的固定信用卡卡。智能卡允许用户将智能卡连接到主机计算机来提供验证，而该主机上的软件与智能卡中存储的密钥材料交互以验证用户。

SSSD

系统安全服务守护进程 (SSSD) 是在 RHEL 主机上管理用户身份验证和用户授权的系统服务。SSSD 可选择性地保留一个从远程供应商获取的用户身份和凭证缓存，以便进行离线身份验证。如需更多信息，请参阅了解 SSSD 及其优势。

SSSD 后端

SSSD 后端（通常称为数据提供程序）是一个 SSSD 子进程，它管理和创建 SSSD 缓存。这个过程与 LDAP 服务器通讯，执行不同的查询并在缓存中保存结果。它还针对 LDAP 或 Kerberos 进行在线身份验证，并将访问和密码策略应用到登录的用户。

票据 (TGT)

向 Kerberos 密钥分发中心 (KDC) 进行身份验证后，用户会收到一组票据授予票据 (TGT)，这是一组临时凭证，可用于向其他服务（如网站和电子邮件）请求访问票据。

使用 TGT 请求进一步访问为用户提供了单点登录体验，因为用户只需要验证一次就可以访问多个服务。TGT 是可续订的，Kerberos ticket 策略则决定了票据续订限制以及访问控制。

如需更多信息，请参阅管理 Kerberos ticket 策略。

Web 服务器

Web 服务器是接受 Web 内容请求的计算机软件和底层硬件，如页面、镜像或应用程序。用户代理（如 Web 浏览器）使用 HTTP 网络协议来请求特定的资源、用来分发 Web 内容或其安全变体 HTTPS。Web 服务器以资源的内容或错误消息来进行响应。Web 服务器也可以接受和存储用户代理发送的资源。红帽身份管理(IdM)使用 Apache Web 服务器来显示 IdM Web UI，并协调组件之间的通信，如目录服务器和证书颁发机构(CA)。请参阅 Apache Web server。

附加术语表

如果您在这个术语表中找不到身份管理术语，请查看目录服务器和证书系统术语：

- 目录服务器 11 术语表
- 证书系统 9 术语表

第 2 章 IDM 中的故障转移、负载平衡和高可用性

身份管理（IdM）为 IdM 客户端提供了内置的故障转移机制，为 IdM 服务器提供了负载平衡和高可用性功能。

2.1. 客户端故障转移功能

- 默认情况下，IdM 客户端中的 **SSSD** 服务被配置为使用 DNS 中的服务（SRV）资源记录来自动决定要连接的最佳 IdM 服务器。此行为由 **/etc/sssd/sssd.conf** 文件的 **ipa_server** 参数中的 **_srv_** 选项控制：

```
[root@client ~]# cat /etc/sssd/sssd.conf

[domain/example.com]
id_provider = ipa
ipa_server = _srv_, server.example.com
...
```

  如果 IdM 服务器离线，IdM 客户端中的 SSSD 服务会自动连接到另一个 IdM 服务器。

- 如果您希望因为性能原因绕过 DNS 查找，请从 **ipa_server** 参数中删除 **_srv_** 条目，并指定客户端应该连接的 IdM 服务器，按首选顺序排列：

```
[root@client ~]# cat /etc/sssd/sssd.conf

[domain/example.com]
id_provider = ipa
ipa_server = server1.example.com, server2.example.com
...
```

2.2. 服务器端负载平衡和服务可用性

您可以通过安装多个 IdM 副本在 IdM 中实现负载平衡和高可用性：

- 如果您的网络分布在不同的地理位置，可以通过为每个数据中心配置多个 IdM 副本来缩短 IdM 客户端和最快的服务器间的路径。
- 红帽支持最多有 60 个副本的环境。
- IdM 复制机制提供主动/主动服务可用性：所有 IdM 副本的服务都同时可用。

注意

红帽建议不要将 IdM 和其它负载均衡或高可用性（HA）软件合并。

许多第三方高可用性解决方案假定使用主动/被动模式，并可能导致 IdM 服务出现不必要的中断。其他解决方案使用虚拟 IP 或每个集群服务使用一个主机名。所有这些方法通常不适用于 IdM 所提供的服务。另外，它们与 Kerberos 的集成效果也不好，从而降低了部署的整体安全性和稳定性。

第 3 章 规划副本拓扑

请参考为您的用例确定适当的副本拓扑的指导。

3.1. 多个副本服务器作为用于高性能和灾难恢复的解决方案

您可以通过创建现有 IdM 服务器的副本来实现身份管理(IdM)服务的持续功能和高可用性。

当您创建适当数量的 IdM 副本时，您可以使用负载均衡在多个服务器间分发客户端请求，以优化 IdM 服务的性能。使用 IdM，您可以在地理分散的数据中心中放置额外的服务器，以反映您的企业组织结构。这样，IdM 客户端和最接近可访问服务器之间的路径会被缩短。另外，拥有多个服务器可允许为更多客户端分散负载和扩展。

复制 IdM 服务器也是缓解或防止服务器丢失的常见备份机制。例如，如果一个服务器失败，剩余的服务器将继续向域提供服务。您还可以根据剩余的服务器创建新副本来恢复丢失的服务器。

3.2. IDM 服务器和客户端简介

Identity Management (IdM) 域包括以下类型的系统：

IdM 客户端

IdM 客户端是注册了服务器的 Red Hat Enterprise Linux 系统，并配置为使用这些服务器中的 IdM 服务。
客户端与 IdM 服务器交互来访问由它们提供的服务。例如，客户端使用 Kerberos 协议来执行身份验证，并获取企业单点登录(SSO)的票据，使用 LDAP 获取身份和策略信息，使用 DNS 检测服务器和服务所在的位置，以及如何连接它们。

IdM 服务器

IdM 服务器是响应 IdM 域内身份、认证和授权请求的 Red Hat Enterprise Linux 系统。在大多数部署中，集成的证书颁发机构 (CA) 也安装 IdM 服务器。
IdM 服务器是身份和策略信息的中央仓库。IdM 服务器也可以托管域成员使用的任何可选服务：

- 证书颁发机构 (CA)
- 密钥恢复授权中心 (KRA)
- DNS
- Active Directory (AD) 信任控制器
- Active Directory (AD) 信任代理

IdM 服务器也是嵌入式 IdM 客户端。与自己注册的客户端一样，服务器可以提供与其他客户端相同的功能。

为了为大量客户端以及冗余和可用性提供服务，IdM 允许在单一域中的多个 IdM 服务器中进行部署。可以部署最多 60 个服务器。这是 IdM 域中目前支持的最大 IdM 服务器数，也称为副本。IdM 服务器为客户端提供不同的服务。不是所有的服务器都需要提供所有可能的服务。每个服务器中都总是可用的 Kerberos 和 LDAP 等服务器组件。CA、DNS、Trust Controller 或 Vault 等其它服务都是可选的。这意味着不同的服务器在部署中通常会扮演不同的角色。

如果您的 IdM 拓扑包含一个集成的 CA，则一个服务器具有证书撤销列表 (CRL) publisher 服务器 的角色，一个服务器则拥有 CA 续订服务器的角色。

默认情况下，安装的第一个 CA 服务器承担这两个角色，但您可以将这些角色分配到单独的服务器。

警告

*CA 续订服务器*对您的 IdM 部署至关重要，因为它是负责跟踪 CA 子系统证书和密钥的域中的唯一系统。有关如何从影响您的 IdM 部署的灾难中恢复的详情，请参阅使用身份管理执行灾难恢复。

要获得冗余和负载平衡，管理员需要通过创建现有服务器的*副本*来创建附加服务器。在创建副本时，IdM 会克隆现有服务器的配置。副本与初始服务器的核心配置共享，包括有关用户、系统、证书和配置策略的内部信息。

注意

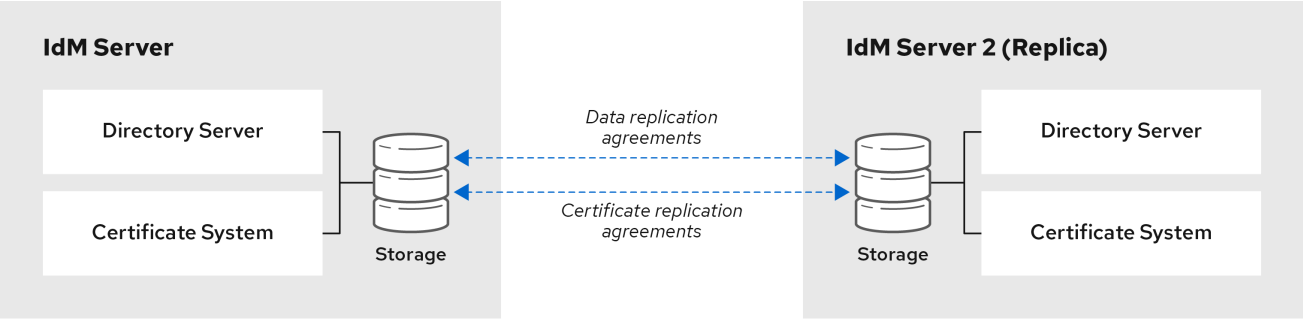
除了 *CA renewal* 和 *CRL publisher* 角色外，副本和从中创建副本的服务器的功能完全相同。因此，术语***服务器（server）***和***副本（replica）***名会根据上下文互换使用。

3.3. 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 3.1. 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。

3.4. 决定拓扑中合适数量的 IDM 副本的指南

规划 IdM 拓扑，使其与您所在机构的要求匹配，并确保最佳性能和服务可用性。

在每个数据中心中设置至少两个副本

在每个数据中心中至少部署两个副本，以确保一个服务器出现故障时，副本可以接管并处理请求。

为您的客户端设置足够数量的服务器

一个 IdM 服务器可为 2000 - 3000 个客户端提供服务。这假设客户端每天会多次查询服务器，但不会每分钟都查询一次。如果您预期使用更频繁的查询，请计划更多的服务器。

设置足够数量的证书颁发机构（CA）副本

只有安装了 CA 角色的副本才能复制证书数据。如果使用 IdM CA，请确保您的环境至少有两个带有证书复制协议的 CA 副本。

在单个 IdM 域中设置最多 60 个副本

红帽支持最多有 60 个副本的环境。

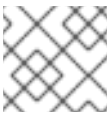
3.5. 拓扑中连接 IDM 副本的指南

将每个副本连接到至少两个其他副本

配置额外的复制协议确保信息不仅在初始副本和您安装的第一个服务器之间复制，而且在其他副本之间复制。

将副本连接到最多四个其他副本（这并不是硬要求）

每个服务器有大量的复制协议不会带来很大的好处。接收副本一次只能被另外一个副本更新，而其他复制协议则处于闲置状态。每个副本有超过四个复制协议通常意味着资源不足。



注意

本建议适用于证书复制协议和域复制协议。

每个副本有四个复制协议的限制有两个例外：

- 如果某些副本没有在线或没有响应时，您需要使用故障切换路径。
- 在大型部署中，您需要特定节点间的其他直接链接。

配置大量复制协议可能会对整体性能造成负面影响：当拓扑中的多个复制协议正在发送更新时，某些副本可能会在进入更新和传出更新之间在更改日志数据库文件出现高竞争。

如果您决定每个副本使用更多复制协议，请确保您没有遇到复制问题和延迟。但请注意，但距离大及存在大量中间节点时也可能造成延迟问题。

相互连接数据中心中的副本

这样可保证数据中心中的域复制。

将每个数据中心连接到至少两个其他数据中心

这样可确保数据中心间的域复制。

至少使用一对复制协议连接数据中心

如果数据中心 A 和 B 有从 A1 到 B1 的复制协议，当存在从 A2 到 B2 的复制协议时，可确保其中一个服务器停止工作时复制可在两个数据中心之间继续。

3.6. 副本拓扑示例

您可以使用以下示例之一创建可靠的副本拓扑。

图 3.2. 带有四个数据中心的副本拓扑，各自具有与复制协议连接的四个服务器

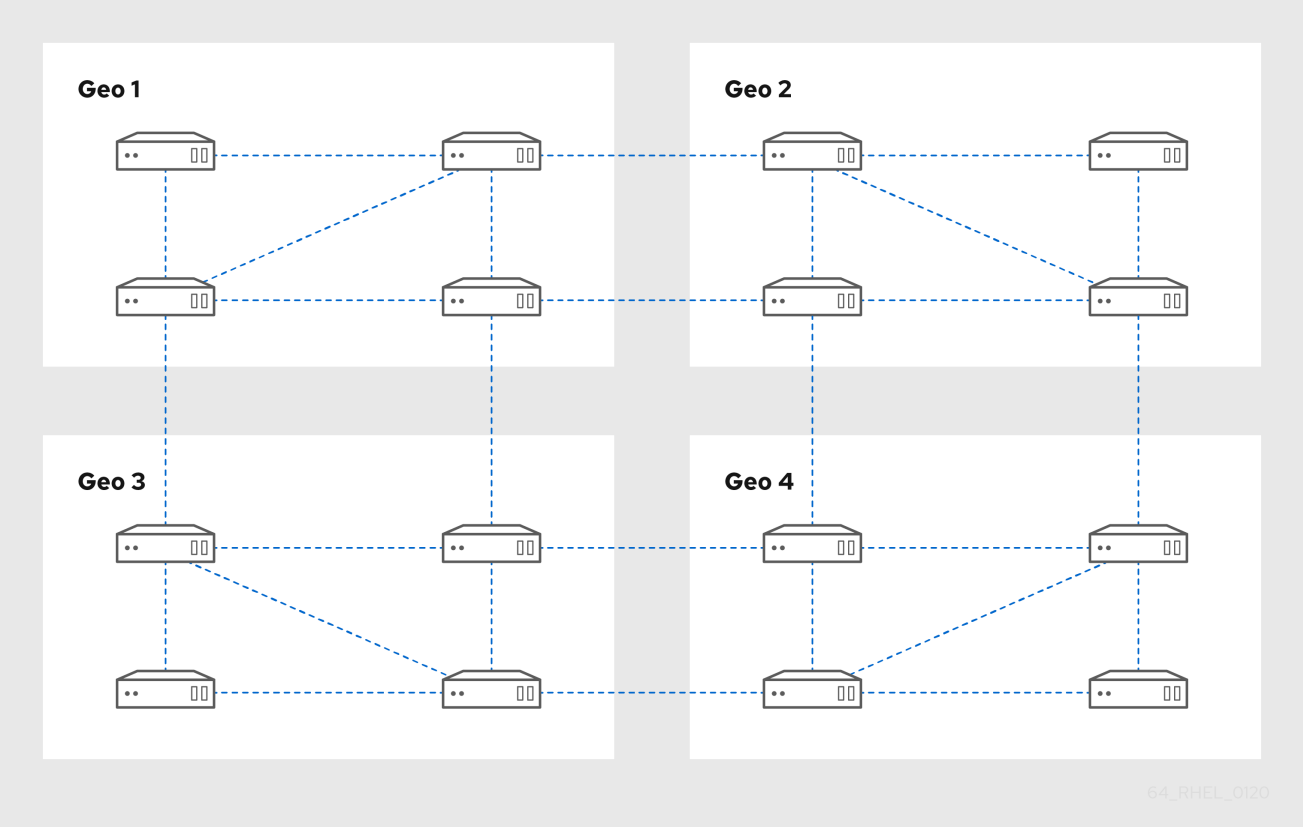
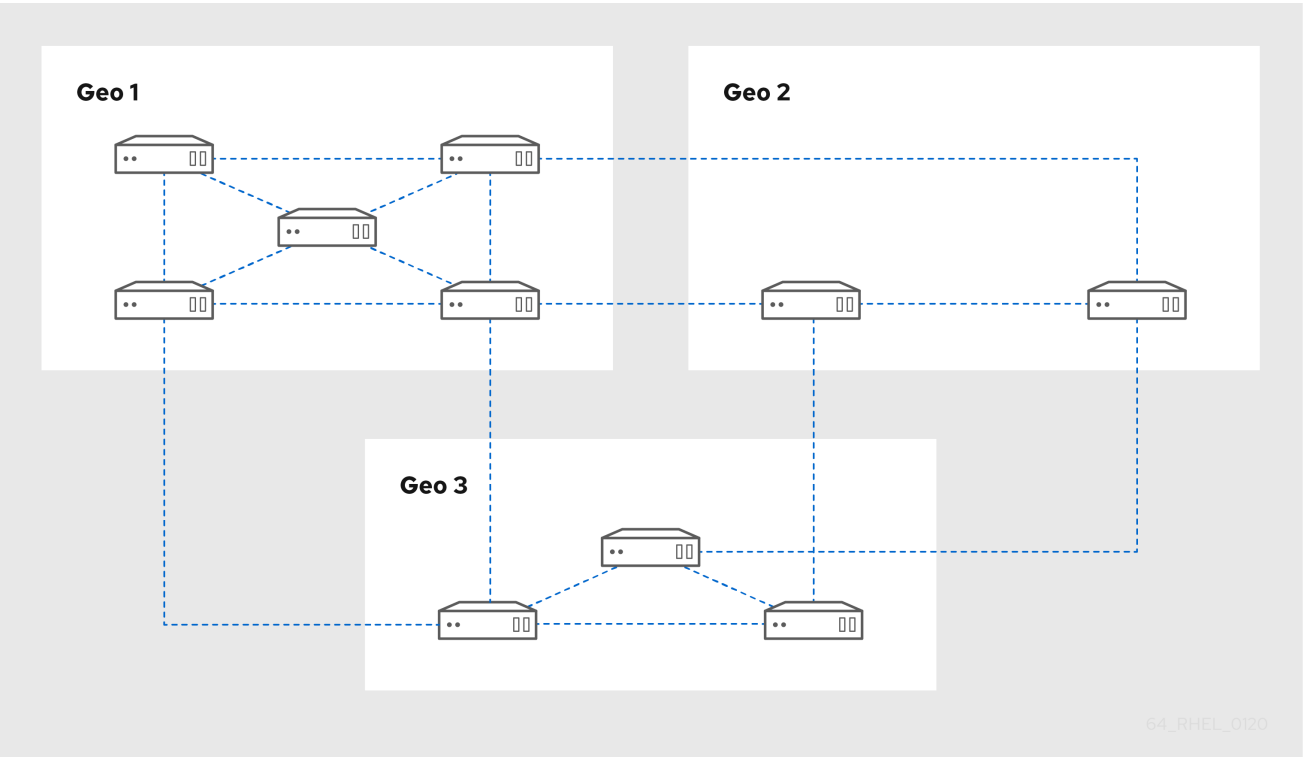


图 3.3. 带有三个数据中心的副本拓扑，每个拓扑都有不同的服务器，它们都通过复制协议互连



3.7. 隐藏的副本模式

隐藏的副本是一个 IdM 服务器，它具有所有运行的服务并可用。但是，隐藏的副本在 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。

默认情况下，当您设置副本时，安装程序会在 DNS 中自动创建服务 (SRV) 资源记录。这些记录可让客户端自动发现副本及其服务。当将副本作为隐藏安装时，请将 **--hidden-replica** 参数传递给 **ipa-replica-install** 命令。

隐藏副本主要针对可能会破坏客户端的专用服务设计。例如，IdM 的完整备份需要关闭服务器中的所有 IdM 服务。因为没有客户端使用隐藏的副本，管理员可以在不影响任何客户端的情况下暂时关闭这个主机上的服务。

其他用例包括 IdM API 或 LDAP 服务器上的高负载操作，如大量导入或广泛查询。

在备份隐藏的副本前，您必须安装集群中使用的所有必需服务器角色，特别是如果使用集成 CA 时的证书颁发机构角色。因此，在新主机上的隐藏副本中恢复备份始终会导致常规副本。

其它资源

- 安装身份管理副本
- 备份和恢复 IdM
- 演示或提升隐藏副本.

第 4 章 规划您的 DNS 服务和主机名

身份管理 (IdM) 在 IdM 服务器中提供不同类型的 DNS 配置。以下小节描述了它们，并提供了有关如何确定最适合您的用例的建议。

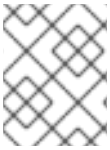
4.1. IDM 服务器中的 DNS 服务

您可以使用或不集成的 DNS 安装 Identity Management (IdM) 服务器。

表 4.1. 带有集成的 DNS 和没有集成的 DNS IdM 的比较

	带有集成的 DNS	没有集成的 DNS
概述：	IdM 为 IdM 域运行自己的 DNS 服务。	IdM 使用由外部 DNS 服务器提供的 DNS 服务。
限制：	IdM 提供的集成 DNS 服务器只支持与 IdM 部署和维护相关的功能。它不支持通用 DNS 服务器的一些高级功能。具体限制如下： • IdM DNS 名称服务器必须是其区域的权威。 • 支持的记录类型是 A, AAAA, A6, AFSDB,CERT, CNAME, DLV, DLV, DNAME, DS, KX, LOC, MX, NAPTR, NS, PTR, SRV, SSHFP, TLSA, TXT 和 URI。 • 不支持拆分 DNS，也称为拆分视图, 拆分地平线, 脑裂 DNS。 • 如果 DNS 名称服务器在多核环境中重新启动，则有已知问题。例如，如果日志轮转导致名称服务器重新启动，则名称服务器可能会崩溃。如果您必须使用多核设置，允许 **systemd** 在出现故障时重新启动名称服务器。	DNS 没有与原生 IdM 工具集成。例如，IdM 不会在拓扑更改后自动更新 DNS 记录。
这最适合于：	IdM 部署中的基本使用情况。 当 IdM 服务器管理 DNS 时，DNS 与原生 IdM 工具紧密集成，这样可启用自动化一些 DNS 记录管理任务。	需要 IdM DNS 范围之外的高级 DNS 功能的环境。 带有良好 DNS 基础架构的环境，其中您要继续使用外部 DNS 服务器。

即使将身份管理服务器用作主 DNS 服务器，其他外部 DNS 服务器仍可用作二级服务器。例如，如果您的环境已经使用另一个 DNS 服务器，例如与 Active Directory (AD) 集成的 DNS 服务器，您只能将 IdM 主域委派给与 IdM 集成的 DNS。不需要将 DNS 区域迁移到 IdM DNS。



注意

如果您需要在 Subject 备用名称 (SAN) 扩展中使用 IP 地址的 IdM 客户端发布证书，则必须使用 IdM 集成 DNS 服务。

4.2. 规划 DNS 域名和 KERBEROS 域名和 KERBEROS 域名的指南

安装第一个身份管理 (IdM) 服务器时，安装会提示输入 IdM 域的主 DNS 名称和 Kerberos 域名称。这些指南可帮助您正确设置名称。

警告

您将无法在安装该服务器后更改 IdM 主域名和 Kerberos 域名称。不要希望通过更改名称从测试环境移到生产环境，例如从 ***lab.example.com*** 更改为 ***production.example.com***。

服务记录的独立 DNS 域

确保用于 IdM 的*主 DNS 域*不与任何其他系统共享。这有助于避免 DNS 级别的冲突。

正确的 DNS 域名委托

确定您在 DNS 域的公共 DNS 树中具有有效委托。不要使用没有委托给您的域名，即使是在私有网络中。

多标签 DNS 域

不要使用单标签域名，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**。

唯一的 Kerberos 域名

确保域名不与任何其他现有 Kerberos 域名称冲突，例如 Active Directory (AD) 使用的名称。

Kerberos realm name 是主 DNS 名称的大写版本

考虑把 realm 的名称设置为主（primary）DNS 域名 (***example.com***) 的大写形式（***EXAMPLE.COM***）。

警告

如果您没有将 Kerberos 域名设置为主 DNS 名称的大写版本，则将无法使用 AD 信任。

有关规划 DNS 域名和 Kerberos 域名的附加备注

- 一个 IdM 部署总是代表一个 Kerberos 域。
- 您可以从多个不同 DNS 域（***example.com***、***example.net***、***example.org***）把 IdM 客户端加入到单个 Kerberos realm (***EXAMPLE.COM***)。
- IdM 客户端不需要位于主 DNS 域中。例如，如果 IdM 域是 ***idm.example.com***，客户端可以位于 ***client.example.com*** 域中，但必须在 DNS 域和 Kerberos 域之间配置清晰的映射。

注意

创建映射的标准方法是使用 **_kerberos** TXT DNS 记录。IdM 集成的 DNS 会自动添加这些记录。

规划 DNS 转发

- 如果要对整个 IdM 部署只使用一个转发器，请配置 **全局转发器**。
- 如果您的公司在分布在地理位置分散的多个位置，那么全局转发器可能是不切实际的。配置 **每台服务器转发器**.
- 如果您的公司有一个无法从公共互联网解析的内部 DNS 网络，请配置一个 **forward zone** 和 **zone forwarders**，以便 IdM 域中的主机可以解析其他内部 DNS 网络上的主机。

第 5 章 规划您的 CA 服务

Red Hat Enterprise Linux 中的身份管理 (IdM) 提供不同类型的证书颁发机构 (CA) 配置。以下小节描述了不同的场景，并为您提供最适合您的用例的建议。

CA 主题 DN

证书颁发机构 (CA) 主题区分名称 (DN) 是 CA 的名称。它必须在 Identity Management (IdM) CA 基础架构中具有全局唯一性，且在安装后不可更改。如果您需要 IdM CA 进行外部签名，您可能需要咨询外部 CA 管理员有关您的 IdM CA 主题 DN 应采用的形式。

5.1. IDM 服务器中的 CA 服务

您可以使用集成 IdM 证书颁发机构 (CA) 或者没有 CA 安装 Identity Management (IdM) 服务器。

表 5.1. 带有集成 CA 和没有集成 CA 的 IdM 的比较

	集成的 CA	没有 CA
概述：	IdM 使用自己的公钥基础架构 (PKI) 服务及 *CA 签名证书*在 IdM 域中创建和签署证书。 ● 如果 root CA 是集成的 CA，IdM 将使用自签名的 CA 证书。 ● 如果 root CA 是外部 CA，集成的 IdM CA 会从属到外部 CA。IdM 使用的 CA 证书由外部 CA 签名，但 IdM 域的所有证书都由集成证书系统实例发布。 ● 集成的 CA 也可以为用户、主机或服务发布证书。 外部 CA 可以是企业 CA 或第三方 CA。	IdM 不会设置其自身 CA，而是使用来自外部 CA 的签名主机证书。 安装没有 CA 的服务器需要您从第三方认证机构请求以下证书： ● LDAP 服务器证书 ● Apache 服务器证书 ● PKINIT 证书 ● 发布 LDAP 和 Apache 服务器证书的 CA 完整 CA 证书链
限制：	如果集成的 CA 属于外部 CA，则在 IdM 域中发布的证书可能会受到外部 CA 为各种证书属性设置的限制，例如： ● 有效周期。 ● 对 IDM CA 或其下级发布的证书可能出现的主题名称的限制。 ● 限制 IDM CA 是否可以自己签发从属 CA 证书，或者如何"依赖"下级证书链。	在 IdM 外部管理证书会导致许多其他活动，例如： ● 创建、上传和更新证书是一个手动过程。 ● **certmonger** 服务不跟踪 IPA 证书（LDAP 服务器、Apache 服务器和 PKINIT 证书），也不会在证书即将过期时通知您。管理员必须为外部发布的证书设置通知，或者对这些证书设置跟踪请求（如果管理员希望 **certmonger** 跟踪它们）。
这最适合于：	允许您创建和使用自己的证书基础架构的环境。	在非常罕见的情况下，基础架构内的限制不允许您安装与服务器集成的证书服务。

注意

从自签名 CA 切换到外部签名 CA 或其他方式，以及更改外部 CA 签发 IdM CA 证书，即使安装后也可以更改哪些外部 CA 证书。即使在没有 CA 的安装后也可以配置集成 CA。如需了解更多详细信息，请参阅安装 IdM 服务器：带有集成 DNS，没有 CA。

其他资源

- 了解 IdM 在内部使用的证书

5.2. CA 服务分布指南

以下步骤为您的证书颁发机构 (CA) 服务的分发提供指导。

流程

1. 在拓扑中的多个服务器中安装 CA 服务。
   没有配置 CA 的副本将所有证书操作请求转发到拓扑中的 CA 服务器。

警告

如果您丢失了具有 CA 的所有服务器，则将丢失所有 CA 配置，而没有恢复的可能。在这种情况下，您必须配置一个新的 CA，并发布和安装新证书。

2. 维护足够数量的 CA 服务器来处理部署的 CA 请求。

有关适当数量的 CA 服务器的建议，请查看下表：

表 5.2. 设置适当数量的 CA 服务器的指南

部署的描述	推荐的 CA 服务器数目
签发大量证书的部署	三个或四个 CA 服务器
在多个区域之间具有带宽或可用性问题的部署	每个区域有一个 CA 服务器，部署中至少有三个服务器
所有其他部署	两个 CA 服务器

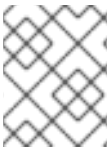
重要

如果并发证书请求数量不是很高，则拓扑中有四个 CA 服务器通常就足够了。超过四个 CA 服务器之间的复制进程可以增加处理器使用率，导致性能下降。

5.3. IDM 中的随机序列号

从 RHEL 9.1 开始，身份管理(IdM)包括 **dogtagpki 11.2.0**，它允许您使用随机序列号版本 3 (RSNv3)。**ansible-freeipa ipaserver** 角色包括带有 RHEL 9.3 更新的 **ipaserver_random_serial_numbers** 变量。

启用 RSNv3 后，IdM 为 PKI 中的证书和请求生成完全随机的序列号，而不管理范围。在重新安装 IdM 时，RSNv3 也会阻止冲突。每个证书序列号的大小最多为 40 位十进制值，因为 RSNv3 对序列号使用 128 位随机值。这使得数字实际上是随机的。



注意

在以前的版本中，Dogtag 上游项目使用基于范围的序列号，以确保跨多个克隆的唯一性。但是，基于这种体验，Dogtag 团队确定基于范围的序列号不适合具有短期证书的云环境。

RSNv3 仅支持新的 IdM CA 安装。默认情况下，在使用 **ipa-server-install** 命令安装主 IdM 服务器时，您安装了第一个 IdM CA。但是，如果您最初安装没有 CA 的 IdM 环境，您可以在以后使用 **ipa-ca-install** 命令添加 CA 服务。要启用 RSNv3，请使用带有 **--random-serial-numbers** 选项的 **ipa-server-install** 或 **ipa-ca-install** 命令。

如果启用了，则需要对部署中的所有公钥基础设施(PKI)服务使用 RSNv3，包括 CA 和密钥恢复授权 (KRA)。安装 KRA 时会执行一个检查，以便在底层 CA 上启用了 RSNv3 时自动启用 RSNv3 。

其他资源

- 随机序列号 v3 (RSNv3)

第 6 章 计划与 AD 集成

以下小节介绍了将 Red Hat Enterprise Linux 与 Active Directory (AD) 集成的选项。

6.1. LINUX 系统直接集成到活动目录中

在直接集成中，Linux 系统直接连接到活跃目录（AD）。可能会有以下类型的集成：

与系统安全性服务守护进程（SSSD）集成

SSSD 可将 Linux 系统连接到不同的身份和验证存储： AD、Identity Management（IdM）或者通用 LDAP 或 Kerberos 服务器。
与 SSSD 集成的主要要求：

- 当与 AD 集成时，SSSD 默认只能在单个 AD 林中正常工作。对于多林设置，请配置手动域枚举。
- 远程 AD 林必须信任本地林，以确保 **idmap_ad** 插件正确处理远程林用户。

SSSD 支持直接和间接集成。它还允许在不需要大量迁移成本的情况下，从一个集成方法切换到另一个集成方法。

与 Samba Winbind 集成

Samba 套件的 Winbind 组件会在 Linux 系统中模拟 Windows 客户端并与 AD 服务器沟通。
与 Samba Winbind 集成的主要要求：

- 在多林 AD 设置中直接与 Winbind 集成需要双向信托。
- Linux 系统本地域的双向路径必须存在于远程 AD 林中的用户域中，以允许 **idmap_ad** 插件提供远程 AD 域中用户的完整信息。

建议

- SSSD 满足 AD 集成的大部分用例，并提供强大的解决方案作为客户端系统和不同类型的身份和身份验证提供商 - AD、IdM、Kerberos 和 LDAP 之间的通用网关。
- 建议在您要在其上部署 Samba FS 的 AD 域成员服务器中部署 winbind。

6.2. 使用身份管理将 LINUX 系统间接集成到活动目录中

在间接集成中，Linux 系统首先连接到中央服务器，然后连接到 Active Directory (AD)。间接集成使管理员能够集中管理 Linux 系统和策略，而 AD 的用户则可透明地访问 Linux 系统和服务。

基于与 AD 的跨林信任进行集成

身份管理 (IdM) 服务器充当控制 Linux 系统的中央服务器。建立与 AD 的跨域 Kerberos 信任，使 AD 中的用户能够登录访问 Linux 系统和资源。IdM 作为一个独立的林，利用了 AD 支持的林级信任。
使用信任时：

- AD 用户可以访问 IdM 资源。
- IdM 服务器和客户端可以解析 AD 用户和组群的身份。
- AD 用户和组根据 IdM 定义的条件访问 IdM，如基于主机的访问控制。

- AD 用户和组仍在 AD 端进行管理。

基于同步进行集成

这个方法基于 WinSync 工具。WinS 同步复制协议可将用户帐户从 AD 与 IdM 同步。

警告

WinSync 已不再在 Red Hat Enterprise Linux 8 中活跃开发。间接整合的首选解决方案是跨林信任。

基于同步的集成限制包括：

- 组没有从 IdM 和 AD 同步。
- 用户在 AD 和 IdM 中会重复。
- WinSync 只支持单个 AD 域。
- AD 中只有一个域控制器可用来将数据同步到一个 IdM 实例。
- 用户密码必须同步，这需要在 AD 域的所有域控制器中安装 PassSync 组件。
- 配置同步后，所有 AD 用户必须在 PassSync 同步前手动更改密码。

6.3. 决定直接和间接集成的指南

这些指南可帮助您决定哪种类型的集成适合您的用例。

要连接到活跃目录的系统数

连接少于 30-50 个系统（并不是一个硬限制）

如果您的连接少于 30-50 的系统，请考虑直接集成。间接集成可能会带来不必要的开销。

连接超过 30-50 个系统（非硬限制）

如果您的连接超过 30-50 个系统，请考虑使用与 Identity Management 的间接集成。使用这个方法，您可以从 Linux 系统的集中管理中受益。

管理少量 Linux 系统，但预计这个数字会迅速增长

在这种情况下，请考虑间接集成以避免在以后迁移环境。

部署新系统及其类型的频率

以严格方式部署裸机系统

如果您部署新系统很少，且它们通常是裸机系统，请考虑直接集成。在这种情况下，直接集成通常是最简单方便的。

频繁部署虚拟系统

如果您经常部署新系统，且它们通常是按需调配的虚拟系统，请考虑间接集成。通过间接集成，您可以使用中央服务器动态管理新系统，并与 Red Hat Satellite 等编配工具集成。

活动目录是所需的身份验证提供程序

您的内部策略是否规定所有用户都必须针对 Active Directory 进行身份验证？

您可以选择直接或间接集成。如果您使用间接集成身份管理和 Active Directory 之间的信任，访问 Linux 系统的用户会根据 Active Directory 进行验证。Active Directory 中存在的策略会在身份验证过程中执行并强制执行。

第 7 章 规划 IDM 和 AD 间的跨林信任

Active Directory (AD) 和身份管理 (IdM) 是管理各种核心服务（如 Kerberos、LDAP、DNS 和证书服务）的两个替代环境。*跨林信任*关系通过使所有核心服务无缝交互，以透明的方式集成这两种不同环境。以下小节提供了有关如何计划和设计跨林信任部署的建议。

7.1. IDM 和 AD 之间的跨林信任和外部信任

IdM 和 AD 之间的跨林信任

在纯 Active Directory (AD) 环境中，跨林信任连接两个单独的 AD 林根域。当您在 AD 和 IdM 间创建跨林信任时，IdM 域会作为一个单独的域单独进入 AD。然后在 AD 林根域和 IdM 域间建立了信任关系。因此，来自 AD 林的用户可以访问 IdM 域中的资源。

IdM 可以与一个 AD 林或多个不相关的论坛建立信任。

注意

可以在*跨域信任*中连接两个单独的 Kerberos 域。但是，Kerberos 域仅涉及身份验证，而不涉及身份和授权操作中涉及的其他服务和协议。因此，建立 Kerberos 跨域信任不足以让一个域的用户访问另一个域中的资源。

对 AD 域的外部信任

外部信任是指 IdM 和 Active Directory 域之间的信任关系。虽然地理信任始终需要在 IdM 和 Active Directory 林的根域之间建立一个信任,但外部信任可以从 IdM 到林内的任何域建立。

7.2. 信任控制器和信任代理

身份管理 (IdM) 提供以下类型的 IdM 服务器，它们支持信任 Active Directory (AD)：

信任控制器

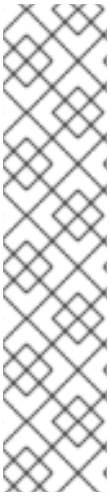
可针对 AD 域控制器执行身份查找的 IdM 服务器。他们还运行 Samba 套件，以便他们能够与 AD 建立信任关系。AD 域控制器在建立并确认对 AD 的信任时会联系信任控制器。AD-enrolled 机器为 Kerberos 身份验证请求与 IdM 信任控制器通信。
配置信任时会创建第一个信任控制器。如果您在不同地理位置有多个域控制器，请使用 **ipa-adtrust-install** 命令将 RHEL IdM 服务器指定为这些位置的信任控制器。

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

信任代理

可以从 RHEL IdM 客户端针对 AD 域控制器解析身份查找的 IdM 服务器。与信任控制器不同，信任代理无法处理 Kerberos 身份验证请求。

除了信任代理和控制器外，IdM 域还可以包含标准的 IdM 服务器。但是这些服务器并不和 AD 进行通讯。因此，与这些标准服务器通信的客户端无法解析 AD 用户和组，也无法验证和授权 AD 用户。



注意

IdM 服务器没有配置为运行 Trust Controller 或 Trust Agent 角色，除非完成以下操作之一：

- 您使用 **ipa-server-install** 或 **ipa-replica-install** 安装服务器或副本（使用 **--setup-ad** 选项）。
- 您可以在 IdM 服务器上运行 **ipa-adtrust-install** 命令，以配置 Trust Controller 角色。
- 您可以在 Trust Controller 上运行 **ipa-adtrust-install --add-agents** 命令，将另一个 IdM 副本指定为 Trust Agent。
  默认情况下，IdM 服务器在没有这些操作的情况下无法从可信域解析用户和组。

表 7.1. 比较信任控制器和信任代理支持的功能

功能	信任代理	信任控制器
解析 AD 用户和组	是	是
注册运行来自可信 AD 的用户访问的 IdM 客户端	是	是
添加、修改或删除信任协议	否	是
将信任代理角色分配给 IdM 服务器	否	是

在规划部署信任控制器和信任代理时，请考虑以下指南：

- 每个 IdM 部署至少配置两个信任控制器。
- 在每个数据中心中至少配置两个信任控制器。

如果您希望创建额外的信任控制器，或者现有信任控制器失败，请通过提升信任代理或标准服务器来创建新的信任控制器。要做到这一点，在 IdM 服务器中使用 **ipa-adtrust-install** 工具。

重要

您不能将现有信任控制器降级到信任代理。

7.3. 单向信任和双向信任

在某种程度上，身份管理 (IdM) 信任 Active Directory (AD)，但 AD 不信任 IdM。AD 用户可以访问 IdM 域中的资源，但 IdM 中的用户无法访问 AD 域中的资源。IdM 服务器使用特殊帐户连接到 AD，并读取随后通过 LDAP 传送到 IdM 客户端的身份信息。

对于双向信任，IdM 用户可以向 AD 验证，AD 用户可向 IdM 验证。AD 用户可以对 IdM 域中的资源进行身份验证并访问，就像信任案例的一种方式一样。IdM 用户可以进行身份验证，但无法访问 AD 中的大多数资源。它们只能在 AD 网站访问不需要任何访问控制检查的 Kerberized 服务。

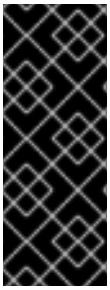
为了授予对 AD 资源的访问权限，IdM 需要实施全局目录服务。这个服务还不存在于当前 IdM 服务器版本中。因此，IdM 和 AD 之间的双向信任几乎相当于 IdM 和 AD 间的单向信任功能。

7.4. 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，但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，请执行以下部分中概述的配置之一。



重要

如果 IdM 在 FIPS 模式下，IdM-AD 集成会因为 AD 只支持使用 RC4 或 AES HMAC-SHA1 加密而无法工作，而 FIPS 模式下的 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，该策略只能用在通用标准评估的系统上。

7.4.1. 在 AD 中启用 AES 加密（推荐）

要确保 AD 林中活动目录(AD)域之间的信任支持强大的 AES 加密类型，请参阅以下 Microsoft 文章 AD DS: 安全:访问信任域中资源时的 Kerberos "Unsupported etype" 错误

7.4.2. 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
```

7.4.3. 在 RHEL 中启用 RC4 支持

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

流程

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

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

2. 重启主机。

7.4.4. 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。

7.5. 可信域的 KERBEROS FAST

Kerberos 灵活身份验证安全隧道(FAST)也称为活动目录(AD)环境中的 Kerberos armoring。Kerberos FAST 为客户端与密钥分发中心(KDC)之间的 Kerberos 通信提供额外的安全层。在 IdM 中，KDC 运行在 IdM 服务器上，FAST 会被默认启用。IdM 中的双因素身份验证(2FA)也需要启用 FAST。

在 AD 中，AD 域控制器(DC)上默认禁用 Kerberos armoring。您可以在 **Tools>Group Policy Management>Default Domain Controller Policy** 的域控制器中启用它：

- 右键点 **Default Domain Controller Policy**，再选择 **编辑**。进入到 **Computer Configuration>Policies>Administrative Templates>System>KDC**，双击 **KDC support for claims, compound authentication, and Kerberos armoring**。

为声明启用 KDC 支持后，策略设置允许以下选项：

- "不支持"
- "支持"
- "始终提供声明"
- "未发送更多身份验证请求"

Kerberos FAST 在 IdM 客户端的 Kerberos 客户端库中实现。您可以将 IdM 客户端配置为对所有发布 FAST 的可信域使用 FAST 或根本不使用 Kerberos FAST 。如果您在可信 AD 林中启用了 Kerberos armoring，则 IdM 客户端默认使用 Kerberos FAST。FAST 通过密钥的帮助建立起一个安全隧道。为了保

护与可信域的域控制器的连接，Kerberos FAST 必须从可信域获得跨域 Ticket Granting Ticket Granting Ticket (TGT)，因为这些密钥仅在 Kerberos 域中有效。Kerberos FAST 使用 IdM 客户端的 Kerberos 主机密钥来在 IdM 服务器的帮助下请求跨领域的 TGT。这只在 AD 林信任 IdM 域时才可以正常工作。这意味着需要双向信任。

如果 AD 策略需要强制使用 Kerberos FAST，则需要在 IdM 域和 AD 林间建立双向信任。您必须在连接建立之前规划此项，因为 IdM 和 AD 必须有方向和信任类型的记录。

如果您已建立单向信任，请运行 **ipa trust-add ... --two-way=true** 命令来删除现有信任协议并创建双向信任。这需要使用管理凭据。当 IdM 尝试从 AD 端删除现有信任协议，因此需要 AD 访问的管理员权限。如果您使用共享的机密而不是 AD 管理帐户建立原始信任，那么它会以双向方式重新创建信任，并只在 IdM 一侧更改可信的域对象。Windows 管理员必须使用 Windows UI 重复相同的步骤，才能选择双向信任并使用同一共享 secret 来重新创建信任。

如果无法使用双向信任，则必须在所有 IdM 客户端上禁用 Kerberos FAST。来自可信 AD 林的用户可以通过密码或直接智能卡进行身份验证。要禁用 Kerberos FAST，请在 **[domain]** 部分的 **sssd.conf** 文件中添加以下设置：

```
krb5_use_fast = never
```

请注意，当验证是基于 ssh-keys、GSSAPI 身份验证或 使用远程 Windows 客户端的智能卡进行 ssh 时，您不需要使用此选项。这些方法不使用 Kerberos FAST，因为 IdM 客户端不必与 DC 通信。另外，在 IdM 客户端上禁用 FAST 后，双因素验证 IdM 功能也不可用。

7.6. AD 用户的 POSIX 和 ID 映射 ID 范围类型

身份管理(IdM)根据用户的 POSIX 用户 ID(UID)和组 ID(GID)强制实行访问控制规则。但是，活动目录(AD)用户是由安全标识符(SID)标识的。AD 管理员可以配置 AD 来存储 AD 用户和组的 POSIX 属性，如 **uidNumber**、**gidNumber** 、**UNIXHomeDirectory** 或 **loginShell**。

您可以通过使用 **ipa-ad-trust-posix** ID range 建立信任，来配置跨林信任引用此信息：

```
[server ~]# ipa trust-add --type=ad ad.example.com --admin administrator --password  --range-type=ipa-ad-trust-posix
```

如果您没有在 AD 中存储 POSIX 属性，则系统安全服务守护进程(SSSD)可以根据在称为 **ID 映射** 的进程中用户的 SID 来一致地映射一个唯一的 UID。您可以通过使用 **ipa-ad-trust** ID range 创建信任来明确地选择此行为：

```
[server ~]# ipa trust-add --type=ad ad.example.com --admin administrator --password  --range-type=ipa-ad-trust
```

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明确选择 POSIX ID 范围类型。

其他资源

- 为 AD 用户自动映射私有组的选项

7.7. 用于自动为 AD 用户映射私有组的选项：POSIX 信任

Linux 环境中的每个用户都有一个主用户组。Red Hat Enterprise Linux(RHEL)使用用户私有组(UPG)模式：UPG 与其创建的用户的名称相同，并且该用户是 UPG 的唯一成员。

如果您已为 AD 用户分配了 UID，但没有添加 GID，您可以通过调整该 ID 范围的 auto_private_groups 设置来根据其 UID 将 SSSD 配置成自动为用户映射私有组。

默认情况下，auto_private_groups 选项对于 POSIX 信任中使用的 **ipa-ad-trust-posix** ID ranges 被设为 false。使用此配置，SSSD 会从每个 AD 用户条目中检索 **uidNumber** 和 **gidNumber**。

auto_private_groups = false

SSSD 将 **uidNumber** 值分配给用户的 UID，将 **gidNumber** 分配给用户的 GID。AD 中必须存在具有此 GID 的组，否则无法解析该用户。下表显示了您是否能够根据不同的 AD 配置解析 AD 用户。

表 7.2. 当 POSIX ID 范围的auto_private_groups 变量设为 false 时 SSSD 的行为

AD 中的用户配置	id username 的输出
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** 未定义 • 在 AD 中没有 **gidNumber** = 4000 的组。	SSSD 无法解析用户。

AD 中的用户配置	id username 的输出
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** = 4000 • 在 AD 中没有 **gidNumber** = 4000 的组。	SSSD 无法解析用户。
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** = 4000 • AD 有 **gidNumber** = 4000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(adgroup@ad-domain.com) groups=4000(adgroup@ad-domain.com), …**

如果 AD 用户没有在 AD 中配置的主组，或者其 **gidNumber** 不对应于现有的组，则 IdM 服务器将无法正确解析该用户，因为它无法查找用户所属的所有组。要临时解决这个问题，您可以通过将 **auto_private_groups** 选项设为 **true** 或 **混合** 来在 SSSD 中启用自动私有组映射：

auto_private_groups = true

SSSD 始终映射设置了 **gidNumber** 的私有组，以匹配 AD 用户条目中的 **uidNumber**。

表 7.3. 当 POSIX ID 范围的 auto_private_groups 变量设为 true 时 SSSD 的行为

AD 中的用户配置	id username 的输出
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** 未定义 • AD 没有 GID=4000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** = 5000 • AD 没有具有 **gidNumber** = 5000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**

AD 中的用户配置	id username 的输出
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** = 4000 • AD 没有 **gidNumber** = 4000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**
AD 用户条目有： • **uidNumber** = 4000 • **gidNumber** = 5000 • AD 有 **gidNumber** = 5000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**

auto_private_groups = hybrid

如果 **uidNumber** 值匹配 **gidNumber**，但没有具有此 **gidNumber** 的组，则 SSSD 会将私有组映射为用户的主用户组，其 **gidNumber** 与 **uidNumber** 匹配。如果 **uidNumber** 和 **gidNumber** 值不同，并且有一个具有此 **gidNumber** 的组，则 SSSD 会使用 **gidNumber** 的值。

表 7.4. 当 POSIX ID 范围的auto_private_groups 变量设为 hybrid 时 SSSD 的行为

AD 中的用户配置	id username 的输出
具有以下情况的 AD 用户条目： • **uidNumber** = 4000 • **gidNumber** 未定义 • AD 没有 **gidNumber** = 4000 的组。	SSSD 无法解析用户。
具有以下情况的 AD 用户条目： • **uidNumber** = 4000 • **gidNumber** = 5000 • AD 没有具有 **gidNumber** = 5000 的组。	SSSD 无法解析用户。
具有以下情况的 AD 用户条目： • **uidNumber** = 4000 • **gidNumber** = 4000 • AD 没有 **gidNumber** = 4000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=4000(aduser@ad-domain.com) groups=4000(aduser@ad-domain.com), …**

AD 中的用户配置	id username 的输出
具有以下情况的 AD 用户条目： • **uidNumber** = 4000 • **gidNumber** = 5000 • AD 有 **gidNumber** = 5000 的组。	**# id aduser@AD-DOMAIN.COMuid=4000(aduser@ad-domain.com) gid=5000(aduser@ad-domain.com) groups=5000(adgroup@ad-domain.com), …**

其他资源

- AD 用户的 POSIX 和 ID 映射 ID 范围类型
- 在 CLI 上为 POSIX ID 范围启用自动私有组映射
- 在 IdM WebUI 中为 POSIX ID range 启用自动私有组映射

7.8. 用于自动为 AD 用户映射私有组的选项： ID 映射信任

Linux 环境中的每个用户都有一个主用户组。Red Hat Enterprise Linux(RHEL)使用用户私有组(UPG)模式：UPG 与其创建的用户的名称相同，并且该用户是 UPG 的唯一成员。

如果您已为 AD 用户分配了 UID，但没有添加 GID，您可以通过调整该 ID 范围的 auto_private_groups 设置来根据其 UID 将 SSSD 配置成自动为用户映射私有组。

默认情况下，对于在 ID 映射信任中使用的 **ipa-ad-trust** ID ranges， **auto_private_groups** 选项被设为 **true**。通过此配置，SSSD 会根据其安全标识符(SID)计算 AD 用户的 UID 和 GID。SSSD 忽略 AD 中的任何 POSIX 属性，如 **uidNumber**、**gidNumber**，同时忽略 **primaryGroupID**。

auto_private_groups = true

SSSD 始终将设置为 GID 的私有组映射为与 UID 匹配，该 UID 基于 AD 用户的 SID。

表 7.5. 当 ID 映射 ID 范围的auto_private_groups 变量设为 true 时 SSSD 的行为

AD 中的用户配置	id username 的输出
AD 用户条目，其中： • SID 映射为 7000 • **primaryGroupID** 映射为 8000	**# id aduser@AD-DOMAIN.COMuid=7000(aduser@ad-domain.com) gid=7000(aduser@ad-domain.com) groups=7000(aduser@ad-domain.com), 8000(adgroup@ad-domain.com), …**

auto_private_groups = false

如果将 **auto_private_groups** 选项设为 **false**，SSSD 将使用 AD 条目中设置的 **primaryGroupID** 作为 GID 号。**primaryGroupID** 的默认值对应于 AD 中的 **Domain Users** 组。

表 7.6. 当 ID 映射 ID 范围的auto_private_groups 变量设为 false 时 SSSD 的行为

AD 中的用户配置	id username 的输出
AD 用户条目，其中： • SID 映射为 7000 • **primaryGroupID** 映射为 8000	**# id aduser@AD-DOMAIN.COMuid=7000(aduser@ad-domain.com) gid=8000(adgroup@ad-domain.com) groups=8000(adgroup@ad-domain.com), …**

其他资源

- AD 用户的 POSIX 和 ID 映射 ID 范围类型

7.9. 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

7.10. 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。

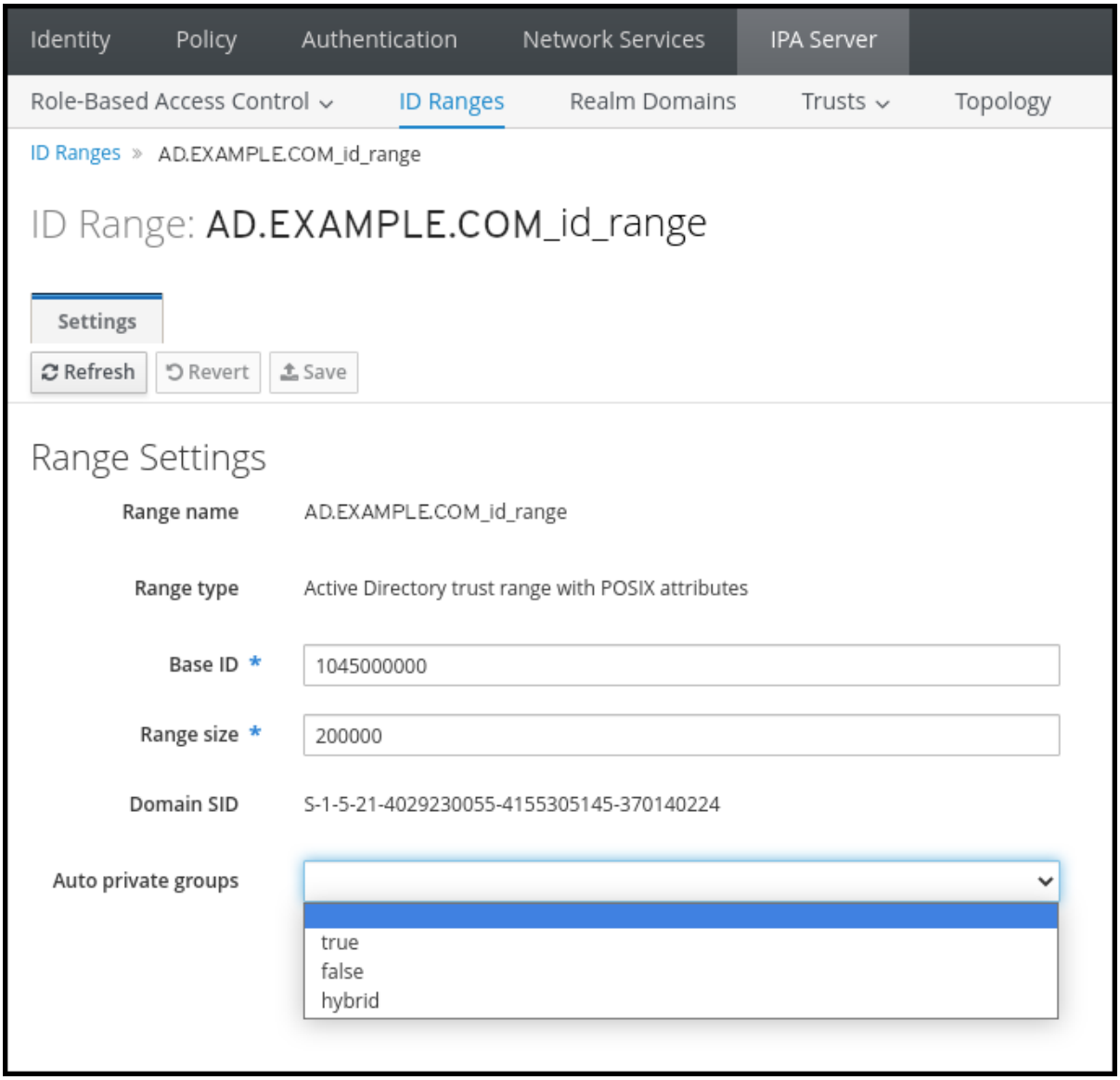
此流程解释了如何在身份管理(IdM)WebUI 中为 **auto_private_groups** SSSD 参数设置 **hybrid** 选项来为 ID range 启用自动私有组映射。因此，IdM 可以解析在 AD 中没有配置主组的 AD 用户。

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

7.11. 非 POSIX 外部组和 SID 映射

身份管理 (IdM) 使用 LDAP 管理组.Active Directory (AD) 条目没有同步或复制到 IdM，这意味着 AD 用户和组在 LDAP 服务器中没有 LDAP 对象，因此不能直接用于表达 IdM LDAP 中的组成员资格。因此，IdM 中的管理员需要创建非POSIX 外部组，作为普通 IdM LDAP 对象引用，以标记 IdM 中 AD 用户和组的组成员资格。

非 POSIX 外部组的安全 ID (SID) 由 SSSD 处理，它将 Active Directory 中的组的 SID 映射到 IdM 中的 POSIX 组。在 Active Directory 中，SID 与用户名相关联。当使用 AD 用户名访问 IdM 资源时，SSSD 会使用用户的 SID 为 IdM 域中的用户构建完整的组成员资格信息。

7.12. 为 IDM-AD 信任建立 DNS 的指南

这些规则可帮助您获得正确的 DNS 配置，从而在 Identity Management (IdM) 和 Active Directory (AD) 之间建立跨林信任。

唯一的主 DNS 域

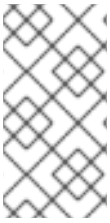
确保 AD 和 IdM 都有它们自己配置的唯一主 DNS 域。例如：

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

最方便的管理解决方案是，每个 DNS 域都由集成 DNS 服务器管理，但也可以使用任何其他标准兼容的 DNS 服务器。

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。

正确的 SRV 记录

确定主 IdM DNS 域有正确的 SRV 记录来支持 AD 信任。
对于同一 IdM 网域一部分的其他 DNS 域，在建立对 AD 的信任时不必配置 SRV 记录。原因在于 AD 域控制器不使用 SRV 记录来发现 Kerberos 密钥分发中心 (KDC)，而是基于信任名称后缀路由信息的 KDC 发现。

DNS 记录可从信任中的所有 DNS 域解析

确定所有机器都可以从所有涉及信任关系的 DNS 域解析 DNS 记录：

- 在配置 IdM DNS 时，请按照使用外部 CA 安装 IdM 服务器 所述进行操作。
- 如果您在没有集成 DNS 的情况下使用 IdM，请按照在没有集成 DNS 的情况下安装 IdM 服务器的内容进行操作。

Kerberos realm 名称作为主 DNS 域名的大写版本

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

7.13. 配置 NETBIOS 名称的指南

NetBIOS 名称通常是域名的最左侧的部分。例如：

- 在域名 ***linux.example.com*** 中，NetBIOS 名称为 **linux**。
- 在域名 ***example.com*** 中，NetBIOS 名称为 **example**。

身份管理 (IdM) 和 Active Directory (AD) 域使用不同的 NetBIOS 名称

确定 IdM 和 AD 域有不同的 NetBIOS 名称。
NetBIOS 名称对于识别 AD 域至关重要。如果 IdM 域在 AD DNS 的子域中，NetBIOS 名称对于识别 IdM 域和服务也至关重要。

NetBIOS 名称的字符限制

NetBIOS 名称的最大长度为 15 个字符。

7.14. 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 9.1 及更高版本)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

重要

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

7.15. AD 服务器发现和关联

服务器发现和关联性配置会影响身份管理(IdM)客户端在 IdM 和 AD 间的跨林信任与哪个活动目录(AD)服务器进行通信。

将客户端配置为在首选同一地理位置中的服务器，有助于防止因为客户端需要联络另一个远程数据中心的服务器而造成的时间问题及其他问题。要验证客户端是否与本地服务器进行通信，您必须确保：

- 客户端通过 LDAP 和 Kerberos 与本地 IdM 服务器沟通
- 客户端使用 Kerberos 与本地 AD 服务器沟通
- IdM 服务器中的内嵌客户端通过 LDAP 和 Kerberos 与本地 AD 服务器通信

在 IdM 客户端中配置 LDAP 和 Kerberos 的选项与本地 IdM 服务器通信

当将 IdM 与集成的 DNS 搭配使用时

默认情况下，客户端使用基于 DNS 记录的自动服务查找。在这个设置中，您还可以使用 *DNS 位置*功能配置基于 DNS 的服务发现。
要覆盖自动查找，您可以使用以下方法之一禁用 DNS 发现：

- 在 IdM 客户端安装过程中，通过命令行提供故障切换参数
- 在客户端安装后，修改系统安全服务守护进程 (SSSD) 配置

当在没有集成 DNS 的情况下使用 IdM

您必须使用以下方法之一配置客户端：

- 在 IdM 客户端安装过程中，通过命令行提供故障切换参数
- 在安装客户端后，修改 SSSD 配置

在 IdM 客户端中配置 Kerberos 以便与本地 AD 服务器通信的选项
IdM 客户端无法自动发现哪些 AD 服务器可以与哪些 AD 服务器进行通信。要手动指定 AD 服务器，修改 **krb5.conf** 文件：

- 添加 AD 域信息
- 明确列出用来通信的 AD 服务器

例如：

```
[realms]
AD.EXAMPLE.COM = {
kdc = server1.ad.example.com
kdc = server2.ad.example.com
}
```

在 IdM 服务器中配置内嵌客户端以便通过 Kerberos 和 LDAP 与本地 AD 服务器通信的选项
IdM 服务器上的内嵌客户端也是 AD 服务器的客户端。它可自动发现并使用适当的 AD 网站。

当嵌入的客户端执行发现时，它可能首先在远程位置发现 AD 服务器。如果尝试联系远程服务器用时过长，客户端可能会在不建立连接的情况下停止操作。在客户端的 **sssd.conf** 文件中使用 **dns_resolver_timeout** 选项，以增加客户端等待 DNS 解析器回复的时间。详情请查看 *sssd.conf(5)* 手册页。

嵌入式客户端配置为与本地 AD 服务器通信后，SSSD 会记住嵌入式客户端所属的 AD 站点。因此，SSSD 通常直接向本地域控制器发送 LDAP ping 以刷新其站点信息。如果站点不再存在或者同时将客户端分配到不同的站点，SSSD 会开始查询林中的 SRV 记录，并经历整个自动发现的过程。

使用 **sssd.conf** 中的 *trusted domain sections*，您还可以显式覆盖默认情况下自动发现的一些信息。

7.16. 在将 IDM 与 AD 间接集成过程中执行的操作

以下操作和请求在 IdM 到 AD 的间接集成过程中执行。

请参考这个表，了解创建身份管理 (IdM) 到 Active Directory (AD) 信任过程中执行的操作和请求，从 IdM 信任控制器到向 AD 域控制器的信任。

表 7.7. 从 IdM 信任控制器对 AD 域控制器执行的操作

操作	使用的协议	目的
针对在 IdM 信任控制器中配置的 AD DNS 解析器的 DNS 解析	DNS	发现 AD 域控制器的 IP 地址
对 AD DC 上的 UDP/UDP6 端口 389 的请求	无连接 LDAP (CLDAP)	执行 AD DC 发现

操作	使用的协议	目的
对 AD DC 上的 TCP/TCP6 端口 389 和 3268 的请求	LDAP	查询 AD 用户和组群信息
对 AD DC 上的 TCP/TCP6 端口 389 和 3268 的请求	DCE RPC 和 SMB	设置并支持 AD 的跨林信任
对 AD DC 上的 TCP/TCP6 端口 135、139、445 的请求	DCE RPC 和 SMB	设置并支持 AD 的跨林信任
根据 Active Directory 域控制器的指示，在 AD DC 上动态打开端口，可能在 49152-65535 (TCP/TCP6) 范围内	DCE RPC 和 SMB	响应 DCE RPC 端点映射器（端口 135 TCP/TCP6）的请求.
对 AD DC 上的端口 88（TCP/TCP6 和 UDP/UDP6）、464（TCP/TCP6 和 UDP/UDP6）和 749 (TCP/TCP6) 的请求	Kerberos	要获得 Kerberos 票据 ; 更改 Kerberos 密码 ; 远程管理 Kerberos

请参阅这个表，了解从 AD 域控制器创建 IdM 到 AD 信任过程中执行的操作和请求到 IdM 信任控制器。

表 7.8. 从 AD 域控制器对 IdM 信任控制器执行的操作

操作	使用的协议	目的
针对在 AD 域控制器中配置的 IdM DNS 解析器的 DNS 解析	DNS	发现 IdM 信任控制器的 IP 地址
在 IdM 信任控制器中请求 UDP/UDP6 端口 389	CLDAP	执行 IdM 信任控制器发现
对 IdM 信任控制器上的 TCP/TCP6 端口 135、139、445 的请求	DCE RPC 和 SMB	验证到 AD 的跨林信任
根据 IdM 信任控制器的指示，动态打开在 IdM 信任控制器上打开的端口，可能在 49152-65535 (TCP/TCP6) 范围内	DCE RPC 和 SMB	响应 DCE RPC 端点映射器（端口 135 TCP/TCP6）的请求.
对 IdM 信任控制器上的端口 88（TCP/TCP6 和 UDP/UDP6）、464（TCP/TCP6 和 UDP/UDP6）和 749 (TCP/TCP6) 的请求	Kerberos	要获得 Kerberos 票据 ; 更改 Kerberos 密码 ; 远程管理 Kerberos

第 8 章 备份和恢复 IDM

身份管理允许您在数据丢失事件后手动备份和恢复 IdM 系统。

在备份过程中，系统会创建一个目录来存储有关您的 IdM 设置的信息。您可以使用此备份目录恢复原始 IdM 设置。

注意

IdM 备份和恢复功能旨在帮助防止数据丢失。为了减少服务器丢失的影响并确保持续操作，请为客户端提供替代的服务器。有关建立复制拓扑的详情，请参考使用复制准备服务器丢失。

8.1. IDM 备份类型

使用 **ipa-backup** 工具，您可以创建两种类型的备份：

全服务器备份

- **包含**与 IdM 相关的所有服务器配置文件，以及 LDAP 数据交换格式 (LDIF) 文件中的 LDAP 数据
- IdM 服务必须**离**线。
- **适合**从头开始重建 IdM 部署。

只进行数据备份

- 在 LDIF 文件和复制更改日志中**包含** LDAP 数据
- IdM 服务可以为**在线或者离**线。
- **适用于** 将 IdM 数据恢复到一个过去的状态

8.2. IDM 备份文件的命名惯例

默认情况下，IdM 存储被备份为 **.tar** 存档，并保存在 **/var/lib/ipa/backup/** 目录的子目录中。

归档和子目录遵循以下命名约定：

全服务器备份

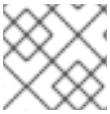
在名为 **ipa-full-*<YEAR-MM-DD-HH-MM-SS>*** 目录中的一个名为 **ipa-full.tar** 的归档，带有 GMT 时间。

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
total 3056
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

只进行数据备份

在名为 **ipa-data-*<YEAR-MM-DD-HH-MM-SS>*** 目录中的一个名为 **ipa-data.tar** 的归档，带有 GMT 时间。

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```



注意

卸载 IdM 服务器不会自动删除任何备份文件。

8.3. 创建备份时的注意事项

ipa-backup 命令的重要行为和限制包括：

- 默认情况下，**ipa-backup** 工具以离线模式运行，这会停止所有 IdM 服务。该程序会在备份完成后自动重启 IdM 服务。
- 全服务器备份必须**始终**在 IdM 服务离线的情况下运行，但可通过在线服务执行仅数据备份。
- 默认情况下，**ipa-backup** 实用程序会在包含 **/var/lib/ipa/backup/** 目录的文件系统中创建备份。红帽建议在独立于 IdM 使用的生产文件系统的文件系统中定期创建备份，并将备份归档到固定介质，如磁带或光存储。
- 考虑对 隐藏的副本 执行备份。IdM 服务可在隐藏的副本中关闭，而不会影响到 IdM 客户端。
- **ipa-backup** 实用程序检查您的 IdM 集群中使用的所有服务（如证书颁发机构(CA)、域名系统(DNS) 和密钥恢复代理 (KRA) 是否安装在您要运行备份的服务器上。如果服务器没有安装所有这些服务，**ipa-backup** 实用程序会以警告方式退出，因为在该主机上进行的备份不足以完全恢复集群。
  例如，如果您的 IdM 部署使用集成证书认证机构（CA），非副本中运行的备份将无法捕获 CA 数据。红帽建议验证执行 **ipa-backup** 的副本是否在集群安装中使用了所有 IdM 服务。

  您可以使用 **ipa-backup --disable-role-check** 命令绕过 IdM 服务器角色检查，但生成的备份不会包含完全恢复 IdM 所需的所有数据。

8.4. 创建 IDM 备份

使用 **ipa-backup** 命令在离线和在线模式中创建全服务器及仅数据备份。

先决条件

- 您必须具有 **root** 权限才能运行 **ipa-backup** 实用程序。

流程

- 要在离线模式中创建全服务器备份，请使用 **ipa-backup** 工具，而无需附加选项。

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
```

```
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- 要创建仅离线数据备份，请指定 **--data** 选项。

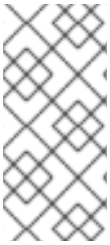
```
[root@server ~]# ipa-backup --data
```

- 要创建包含 IdM 日志文件的完整服务器备份，请使用 **--logs** 选项。

```
[root@server ~]# ipa-backup --logs
```

- 要在 IdM 服务运行时创建仅数据备份，请指定 **--data** 和 **--online** 选项。

```
[root@server ~]# ipa-backup --data --online
```



注意

如果因为 **/tmp** 目录中空间不足造成备份失败，请使用 **TMPDIR** 环境变量更改备份过程创建的临时文件的目标位置：

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

验证步骤

- 确保备份目录包含带有备份的存档。

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

其他资源

- ipa-backup 命令无法完成

8.5. 创建 GPG2 加密的 IDM 备份

您可以使用 GNU Privacy Guard (GPG) 加密来创建加密的备份。以下步骤创建了 IdM 备份并使用 GPG2 密钥对其进行加密。

先决条件

- 您已创建了 GPG2 密钥。请参阅 创建 GPG2 密钥。

流程

- 通过指定 **--gpg** 选项创建 GPG 加密备份。

```
[root@server ~]# ipa-backup --gpg
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
```

```
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

验证步骤

- 确保备份目录包含带有一个 **.gpg** 文件扩展名的加密存档。

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

其他资源

- 创建备份.

8.6. 创建 GPG2 密钥

下面的步骤描述了如何生成使用加密工具的 GPG2 密钥。

先决条件

- 您需要 **root** 权限。

流程

1. 安装并配置 **pinentry** 工具。

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. 创建一个 **key-input** 文件来生成附带您想要的详细信息的 GPG 密钥对。例如：

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. *（可选）*默认情况下，GPG2 在 **~/.gnupg** 文件中保存其密钥环。要使用自定义的密钥环位置，请将 **GNUPGHOME** 环境变量设置为只可由根用户访问的目录。

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. 根据 **key-input** 文件的内容生成一个新的 GPG2 密钥。

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. 输入密码短语来保护 GPG2 密钥。您可以使用这个密码短语访问解密的私钥。

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

6. 再输入一次来确认正确的密码短语。

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

7. 验证新 GPG2 密钥是否已成功创建。

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

验证步骤

- 列出服务器中的 GPG 密钥。

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

其他资源

- GNU Privacy Guard

8.7. 从 IDM 备份中恢复的时间

您可以通过从 IdM 备份中恢复来响应几个灾难情况：

- **对 LDAP 内容进行了不必要的更改**：条目被修改或删除，在整个部署过程中复制这些更改，您希望恢复这些更改。仅恢复数据备份会将 LDAP 条目返回到之前的状态，而不影响 IdM 配置本身。
- **基础架构全部出问题或所有 CA 实例都丢失** ：如果灾难破坏了所有证书颁发机构副本，部署会失去通过部署其他服务器来重建自身的能力。在这种情况下，恢复 CA 副本的备份并从中构建新副本。
- **在隔离服务器上进行升级失败**：操作系统可以正常工作，但 IdM 数据被破坏，因此您想要将 IdM 系统恢复到已知良好状态的原因。红帽建议与技术支持合作，以诊断和排除此问题。如果这些步骤失败，则从全服务器备份中恢复。

重要

硬件或升级失败的首选解决方案是从副本中重建丢失的服务器。如需更多信息，请参阅使用复制恢复单个服务器。

8.8. 从 IDM 备份中恢复时的注意事项

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

以下是从 IdM 备份中恢复时的主要注意事项：

- 您只能在符合最初创建备份的服务器配置的服务器中恢复备份。服务器**必**须具有：
  - 相同的主机名
  - 相同的 IP 地址
  - 同一版本的 IdM 软件
- 如果很多 IdM 服务器被恢复，恢复的服务器就成为 IdM 的唯一信息来源。其它服务器**必**须从恢复的服务器中重新初始化。
- 由于上次备份后创建的任何数据都将丢失，请不要使用备份和恢复解决方案进行正常系统维护。
- 如果服务器丢失，红帽建议重新构建服务器，方法是将其重新安装为副本，而不是从备份中恢复。创建新副本可保留当前工作环境中的数据。如需更多信息，请参阅准备使用复制进行服务器丢失。
- 备份和恢复功能只能从命令行管理，且在 IdM Web UI 中不可用。
- 您无法从位于 **/tmp** 或 **/var/tmp** 目录中的备份文件恢复。IdM 目录服务器使用 **PrivateTmp** 目录，且无法访问操作系统通常可用的 **/tmp** 或 **/var/tmp** 目录。

提示

从备份中恢复需要目标主机上安装的软件 (RPM) 版本与执行备份时安装的版本相同。因此，红帽建议从虚拟机快照而不是备份中恢复。如需更多信息，请参阅使用虚拟机快照恢复数据丢失。

8.9. 从备份中恢复 IDM 服务器

从 IdM 备份中恢复 IdM 服务器或其 LDAP 数据。

图 8.1. 本例中使用的复制拓扑

表 8.1. 本例中使用的服务器命名惯例

服务器主机名	功能
server1.example.com	需要从备份中恢复的服务器。
caReplica2.example.com	连接到 **server1.example.com** 主机的证书颁发机构 (CA) 副本。
replica3.example.com	连接到 **caReplica2.example.com** 主机的副本。

先决条件

- 您已使用 **ipa-backup** 工具为 IdM 服务器生成全服务器或者仅数据备份。请参阅 创建备份。
- 您的备份文件不在 **/tmp** 或 **/var/tmp** 目录中。
- 在从全服务器备份中执行全服务器恢复前，请从服务器中 卸载 IdM，并使用之前相同的服务器配置重新安装 IdM。

流程

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

     ```
     [root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
     ```

   - 如果备份目录不在默认位置，请输入其完整路径：

     ```
     [root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
     ```

注意

ipa-restore 实用程序自动检测该目录包含的备份类型，并且默认执行同类型的恢复。要从全服务器备份中只执行数据恢复，在 **ipa-restore** 命令中添加 **--data** 选项：

```
[root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
```

2. 输入 Directory Manager 密码。

```
Directory Manager (existing master) password:
```

3. 输入 **yes** 以确认备份中的当前数据覆盖。

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
server1.example.com
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. **ipa-restore** 工具禁用所有可用服务器的复制：

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

然后该工具将停止 IdM 服务，恢复备份并重启服务：

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

5. 重新初始化连接到恢复的服务器的所有副本：

   a. 列出 **domai** 后缀的所有复制拓扑片段，记录涉及恢复的服务器的拓扑片段。

```
[root@server1 ~]# ipa topologysegment-find domain
```

```
------------------
2 segments matched
------------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both

  Segment name: caReplica2.example.com-to-replica3.example.com
  Left node: caReplica2.example.com
  Right node: replica3.example.com
  Connectivity: both
----------------------------
Number of entries returned 2
----------------------------
```

b. 使用恢复的服务器重新初始化所有拓扑片段的 **domai** 后缀。
在本例中，使用来自 **server1** 的数据对 **caReplica2** 进行重新初始化。

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

c. 继续到证书颁发机构数据，列出 **ca** 后缀的所有复制拓扑片段。

```
[root@server1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

d. 重新初始化连接到恢复的服务器的所有 CA 副本。
在本例中，使用来自 **server1** 的数据执行 **caReplica2** 的 **csreplica** 重新初始化。

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=server1.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

6. 继续进入复制拓扑，重新初始化连续的副本，直到所有服务器都已使用恢复的服务器 **server1.example.com** 的数据进行更新。
在本例中，我们只需要使用 **caReplica2** 中的数据在 **replica3** 上重新初始化 **domai** 后缀。

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:
```

```
Update in progress, 3 seconds elapsed
Update succeeded
```

7. 清除每台服务器上 SSSD 的缓存，以避免因为数据无效而导致身份验证问题：

   a. 停止 SSSD 服务：

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

   b. 从 SSSD 中删除所有缓存的内容：

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

   c. 启动 SSSD 服务：

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

   d. 重启服务器。

其他资源

- **ipa-restore(1)** man page 还详细介绍了如何在恢复期间处理复杂复制方案。

8.10. 从加密备份中恢复

这个过程从加密的 IdM 备份恢复 IdM 服务器。**ipa-restore** 工具会自动检测 IdM 备份是否已加密，并使用 GPG2 根密钥环恢复它。

先决条件

- GPG 加密的 IdM 备份。请参阅 创建加密的 IdM 备份。
- LDAP Directory Manager 密码
- 创建 GPG 密钥时使用的口令

流程

1. 如果您在创建 GPG2 密钥时使用了自定义 keyring 位置，请验证 **$GNUPGHOME** 环境变量是否被设置为该目录。请参阅 创建 GPG2 密钥。

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

2. 为 **ipa-restore** 实用程序提供备份目录位置。

   ```
   [root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
   ```

   a. 输入 Directory Manager 密码。

   ```
   Directory Manager (existing master) password:
   ```

   b. 输入您创建 GPG 密钥时使用的密码短语。

```
┌──────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:        │
│ "GPG User (first key) <root@example.com>"                            │
│ 2048-bit RSA key, ID BF28FFA302EF4557,                               │
│ created 2020-01-13.                                                  │
│                                                                      │
│                                                                      │
│ Passphrase: <passphrase>                                             │
│                                                                      │
│       <OK>                                <Cancel>                   │
└──────────────────────────────────────────────────────────────────────┘
```

3. 重新初始化连接到恢复的服务器的所有副本。请参阅 从备份中恢复 IdM 服务器。

第 9 章 使用 ANSIBLE PLAYBOOK 备份和恢复 IDM 服务器

使用 **ipabackup** Ansible 角色，您可以自动备份 IdM 服务器，在服务器和 Ansible 控制器之间传输备份文件，并从备份中恢复 IdM 服务器。

9.1. 使用 ANSIBLE 创建 IDM 服务器的备份

您可以使用 Ansible playbook 中的 **ipabackup** 角色来创建 IdM 服务器的备份并将其存储在 IdM 服务器上。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **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 **~/MyPlaybooks/** 目录：

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

2. 创建位于 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **backup-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server.yml backup-my-server.yml
```

3. 打开 **backup-my-server.yml** Ansible playbook 文件以进行编辑。
4. 通过将您的清单文件中的 **hosts** 变量设置为主机组来调整 文件。在本例中，将其设置为 **ipaserver** 主机组：

```
---
- name: Playbook to backup IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipabackup
    state: present
```

5. 保存该文件。
6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
backup-my-server.yml
```

验证步骤

1. 登录到您备份的 IdM 服务器。
2. 验证备份是否位于 **/var/lib/ipa/backup** 目录中。

```
[root@server ~]# ls /var/lib/ipa/backup/
ipa-full-2021-04-30-13-12-00
```

其他资源

- 有关使用 **ipabackup** 角色的更多 Ansible playbook 示例，请参阅：
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
  - **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

9.2. 使用 ANSIBLE 在 ANSIBLE 控制器上创建 IDM 服务器的备份

您可以使用 Ansible playbook 中的 **ipabackup** 角色来创建 IdM 服务器的备份，并在 Ansible 控制器上自动传输它。您的备份文件名以 IdM 服务器的主机名开头。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **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. 若要存储备份，请在 Ansible 控制器上的主目录中创建一个子目录。

```
$ mkdir ~/ipabackups
```

2. 进入 **~/MyPlaybooks/** 目录：

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

3. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **backup-server-to-controller.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server-to-controller.yml backup-my-server-to-my-controller.yml
```

4. 打开 **backup-my-server-to-my-controller.yml** 文件进行编辑。
5. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. *（可选）*若要在 IdM 服务器中维护备份副本，请取消注释以下行：

```
# ipabackup_keep_on_server: true
```

6. 默认情况下，备份存储在 Ansible 控制器的当前工作目录中。要指定在第 1 步中创建的备份目录，请添加 **ipabackup_controller_path** 变量并将其设置为 **/home/user/ipabackups** 目录。

```
---
- name: Playbook to backup IPA server to controller
  hosts: ipaserver
  become: true
  vars:
    ipabackup_to_controller: true
    # ipabackup_keep_on_server: true
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

7. 保存该文件。
8. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory backup-my-server-to-my-controller.yml
```

验证步骤

- 验证备份是否位于 Ansible 控制器的 **/home/user/ipabackups** 目录中：

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

其他资源

- 有关使用 **ipabackup** 角色的更多 Ansible playbook 示例，请参阅：
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
  - **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

9.3. 使用 ANSIBLE 将 IDM 服务器的备份复制到 ANSIBLE 控制器

您可以使用 Ansible playbook 将 IdM 服务器的备份从 IdM 服务器复制到 Ansible 控制器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **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. 若要存储备份，请在 Ansible 控制器上的主目录中创建一个子目录。

```
$ mkdir ~/ipabackups
```

2. 进入 **~/MyPlaybooks/** 目录：

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

3. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **copy-backup-from-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-server.yml copy-backup-from-my-server-to-my-controller.yml
```

4. 打开 **copy-my-backup-from-my-server-to-my-controller.yml** 文件进行编辑。
5. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. 将 **ipabackup_name** 变量设置为 IdM 服务器上的 **ipabackup** 的名称，以复制到您的 Ansible 控制器。
   c. 默认情况下，备份存储在 Ansible 控制器的当前工作目录中。要指定在第 1 步中创建的目录，请添加 **ipabackup_controller_path** 变量并将其设置为 **/home/user/ipabackups** 目录。

```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_to_controller: true
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

6. 保存该文件。
7. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-server-to-my-controller.yml
```

注意

要将**所有** IdM 备份复制到控制器，请将 Ansible playbook 中的 **ipabackup_name** 变量设置为 **all** ：

```
vars:
  ipabackup_name: all
  ipabackup_to_controller: true
```

例如，请参阅 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **copy-all-backups-from-server.yml** Ansible playbook。

验证步骤

- 验证备份是否位于 Ansible 控制器上的 **/home/user/ipabackups** 目录中：

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

9.4. 使用 ANSIBLE 将 IDM 服务器的备份从 ANSIBLE 控制器复制到 IDM 服务器

您可以使用 Ansible playbook 将 IdM 服务器的备份从 Ansible 控制器复制到 IdM 服务器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **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 **~/MyPlaybooks/** 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **copy-backup-from-controller.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-controller.yml copy-backup-from-my-controller-to-my-server.yml
```

3. 打开 **copy-my-backup-from-my-controller-to-my-server.yml** 文件进行编辑。

4. 通过设置以下变量来调整文件：

   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

   b. 将 **ipabackup_name** 变量设置为 Ansible 控制器上 **ipabackup** 的名称，以复制到 IdM 服务器。

```
---
- name: Playbook to copy a backup from controller to the IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_from_controller: true

  roles:
  - role: ipabackup
    state: copied
```

5. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-controller-to-my-server.yml
```

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

9.5. 使用 ANSIBLE 从 IDM 服务器中删除备份

您可以使用 Ansible playbook 从 IdM 服务器中删除备份。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：

- 您使用 Ansible 版本 2.14 或更高版本。
- 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
- 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
- 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。

- 目标节点（这是执行 **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 ~/MyPlaybooks/ 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成 **remove-backup-from-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/remove-backup-from-server.yml remove-backup-from-my-server.yml
```

3. 打开 **remove-backup-from-my-server.yml** 文件以进行编辑。
4. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。
   b. 将 **ipabackup_name** 变量设置为 **ipabackup** 的名称，以从 IdM 服务器中删除。

```
---
- name: Playbook to remove backup from IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00

  roles:
  - role: ipabackup
    state: absent
```

5. 保存该文件。
6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory remove-backup-from-my-server.yml
```

注意

要从 IdM 服务器中删除**所有** IdM 备份，将 Ansible playbook 中的 **ipabackup_name** 变量设置为 **all** ：

```
vars:
  ipabackup_name: all
```

作为一个示例，请参阅 **/usr/share/doc/ansible-freeipa/playbooks** 目录中的 **remove-all-backups-from-server.yml** Ansible playbook。

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

9.6. 使用 ANSIBLE 从服务器中存储的备份中恢复 IDM 服务器

您可以使用 Ansible playbook 从该主机上存储的备份中恢复 IdM 服务器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **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。
- 您知道 LDAP Directory Manager 密码。

流程

1. 进入 **~/MyPlaybooks/** 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成一个 **restore-server.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/restore-server.yml restore-my-server.yml
```

3. 打开 **restore-my-server.yml** Ansible playbook 文件以进行编辑。
4. 通过设置以下变量来调整文件：
   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

b. 将 **ipabackup_name** 变量设置为要恢复的 **ipabackup** 的名称。

c. 将 **ipabackup_password** 变量设置为 LDAP Directory Manager 密码。

```
---
- name: Playbook to restore an IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>

  roles:
  - role: ipabackup
    state: restored
```

5. 保存该文件。

6. 运行指定清单文件和 playbook 文件的 Ansible playbook：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
restore-my-server.yml
```

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

9.7. 使用 ANSIBLE 从 ANSIBLE 控制器中存储的备份中恢复 IDM 服务器

您可以使用 Ansible playbook 从 Ansible 控制器中存储的备份中恢复 IdM 服务器。

先决条件

- 您已配置了 Ansible 控制节点以满足以下要求：
  - 您使用 Ansible 版本 2.14 或更高版本。
  - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
  - 示例假定在 ***~/MyPlaybooks/*** 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN)的 Ansible 清单文件。
  - 示例假定 **secret.yml** Ansible vault 存储了 **ipaadmin_password**。
- 目标节点（这是执行 **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。
- 您知道 LDAP Directory Manager 密码。

流程

1. 进入 **~/MyPlaybooks/** 目录：

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

2. 在 **/usr/share/doc/ansible-freeipa/playbooks** 目录中生成一个 **restore-server-from-controller.yml** 文件的副本：

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/restore-server-from-controller.yml restore-my-server-from-my-controller.yml
```

3. 打开 **restore-my-server-from-my-controller.yml** 文件进行编辑。

4. 通过设置以下变量来调整文件：

   a. 将 **hosts** 变量设置为清单文件中的主机组。在本例中，将它设置为 **ipaserver** 主机组。

   b. 将 **ipabackup_name** 变量设置为要恢复的 **ipabackup** 的名称。

   c. 将 **ipabackup_password** 变量设置为 LDAP Directory Manager 密码。

```
---
- name: Playbook to restore IPA server from controller
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_password: <your_LDAP_DM_password>
    ipabackup_from_controller: true

  roles:
  - role: ipabackup
    state: restored
```

5. 保存该文件。

6. 运行 Ansible playbook，指定清单文件和 playbook 文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory restore-my-server-from-my-controller.yml
```

其他资源

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 目录中的 **README.md** 文件。
- **/usr/share/doc/ansible-freeipa/playbooks/** 目录。

第 10 章 IDM 与红帽产品集成

查找与 IdM 集成的其他红帽产品的文档。您可以配置这些产品，以允许 IdM 用户可以访问它们的服务。

Ansible Automation Platform

设置 LDAP 身份验证

OpenShift Container Platform

配置 LDAP 身份提供程序

OpenStack Platform

将 OpenStack 身份(keystone)与红帽身份管理器(IdM)集成

Satellite

使用红帽身份管理

单点登录

SSSD 和 FreeIPA 身份管理集成

虚拟化

配置外部 LDAP 提供商

第 11 章 为 IDM 域中的 RHEL 9 WEB 控制台配置单点登录

了解如何使用 RHEL 9 web 控制台中的 Identity Management(IdM)提供的单点登录(SSO)身份验证。

优点：

- IdM 域管理员可以使用 RHEL 9 web 控制台来管理本地机器。
- IdM 域中具有 Kerberos 票据的用户不需要提供登录凭据来访问 Web 控制台。
- IdM 域已知的所有主机均可通过 RHEL 9 web 控制台本地实例的 SSH 访问。
- 不需要证书配置。控制台的 Web 服务器会自动切换到 IdM 证书颁发机构发布的证书，并被浏览器接受。

本章论述了配置用于登录到 RHEL web 控制台的 SSO 的步骤：

1. 使用 RHEL 9 web 控制台将机器添加到 IdM 域中。
   详情请参阅使用 Web 控制台将 RHEL 9 系统添加到 IdM 域中 。
2. 如果要使用 Kerberos 进行身份验证，则需要在机器上获得 Kerberos ticket。
   详情请参阅使用 Kerberos 身份验证登录到 web 控制台。
3. 允许 IdM 服务器上的管理员在任何主机上运行任何命令。
   详情请参阅为 IdM 服务器上的域管理员启用管理员的 admin sudo 访问权限

先决条件

- 在 RHEL 9 系统上安装的 RHEL web 控制台。
  详情请参阅安装 Web 控制台。
- 在使用 RHEL web 控制台的系统中安装 IdM 客户端。
  详情请查看 IdM 客户端安装。

11.1. 使用 WEB 控制台将 RHEL 9 系统添加到 IDM 域中

您可以使用 Web 控制台将 Red Hat Enterprise Linux 9 系统添加到 Identity Management(IdM)域中。

先决条件

- IdM 域正在运行，并可访问您想要加入的客户端。
- 您有 IdM 域管理员凭证。

流程

1. 登录到 RHEL web 控制台。
   详情请参阅 Web 控制台的日志记录。
2. 在 **Overview** 选项卡的 **Configuration** 字段中点 **Join Domain**。
3. 在 **Join a Domain** 对话框的 **Domain Address** 字段中输入 IdM 服务器的主机名。
4. 在 **Domain administrator name** 字段中输入 IdM 管理帐户的用户名。

5. 在域 **Domain administrator password** 中添加密码。
6. 点 **Join**。

验证步骤

1. 如果 RHEL 9 web 控制台没有显示错误，系统已加入到 IdM 域，您可以在 **System** 屏幕中看到域名。
2. 要验证该用户是否为域的成员，点 Terminal 页面并输入 **id** 命令：

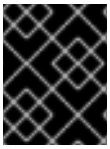
```
$ id
euid=548800004(example_user) gid=548800004(example_user)
groups=548800004(example_user) context=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
```

其它资源

- 规划身份管理
- 安装身份管理
- 管理 IdM 用户、组、主机和访问控制规则

11.2. 使用 KERBEROS 身份验证登录到 WEB 控制台

将 RHEL 9 系统配置为使用 Kerberos 身份验证。



重要

使用 SSO 时，通常在 Web 控制台中拥有任何管理特权。这只有在您配置了免密码 sudo 时有效。Web 控制台不以交互方式询问 sudo 密码。

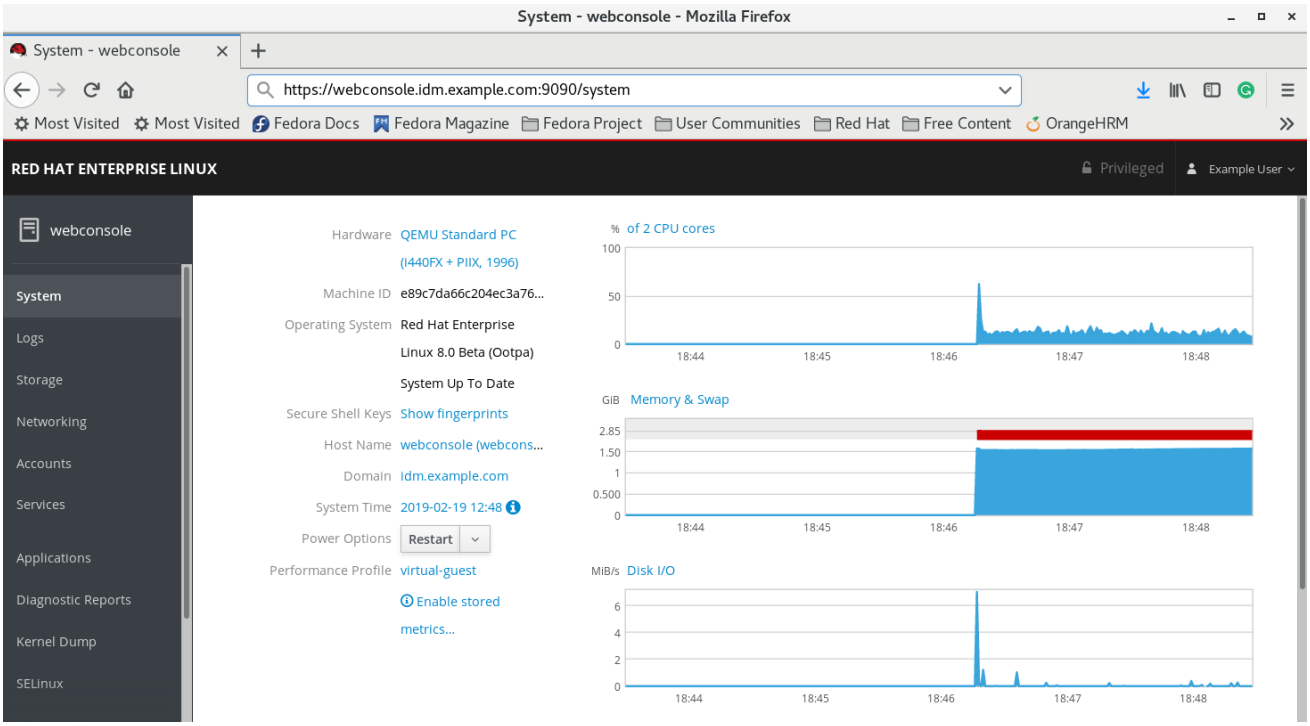
先决条件

- IdM 域在您的公司环境中运行并可访问。
  详情请参阅使用 Web 控制台将 RHEL 9 系统添加到 IdM 域中 。
- 在您要通过 RHEL web 控制台连接和管理的远程系统中启用 **cockpit.socket** 服务。
  详情请参阅安装 Web 控制台。
- 如果系统没有使用 SSSD 客户端管理的 Kerberos ticket，请尝试使用 **kinit** 程序手动请求 ticket。

流程

使用以下地址登录到 RHEL web 控制台：**https://dns_name:9090**

此时，您已成功连接到 RHEL web 控制台，您可以使用配置启动。



11.3. 为 IDM 服务器上的域管理员启用管理员 SUDO 访问权限

您可以使用 RHEL web 控制台，允许域管理员在身份管理(IdM)域中的任何主机上使用任何命令。

要实现这一目的，请启用对 IdM 服务器安装过程中自动创建的 **admins** 用户组的 sudo 访问权限。如果您对组运行 **ipa-advise** 脚本，则添加到 **admins** 组中的所有用户都获得 sudo 权限。

先决条件

- 服务器运行 IdM 4.7.1 或更高版本。

流程

1. 连接到 IdM 服务器。
2. 运行 ipa-advise 脚本：

```
$ ipa-advise enable-admins-sudo | sh -ex
```

如果控制台没有显示错误，则 **admins** 组对 IdM 域中的所有机器有 sudo 权限。

第 12 章 IDM 目录服务器 RFC 支持

身份管理(IdM)中的目录服务器组件支持许多与 LDAP 相关的注释请求(RFC)。

其它资源

- 目录服务器 RFC 支持
- 规划和设计目录服务器