Red Hat Enterprise Linux 9

迁移到 RHEL 9 上的身份管理

将 RHEL 8 IdM 环境升级到 RHEL 9，并将外部 LDAP 解决方案迁移到 IdM

Last Updated: 2024-06-28

Red Hat Enterprise Linux 9 迁移到 RHEL 9 上的身份管理

将 RHEL 8 IdM 环境升级到 RHEL 9，并将外部 LDAP 解决方案迁移到 IdM

法律通告

摘要

红帽仅支持 Red Hat Enterprise Linux (RHEL)上的身份管理(IdM)。如果您在 RHEL 8 或 LDAP 目录上运行 IdM，您可以将这些解决方案迁移到 RHEL 9 上的 IdM 。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

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

部分 I. 将 IDM 从 RHEL 8 迁移到 RHEL 9

第 1 章 将 IDM 环境从 RHEL 8 服务器迁移到 RHEL 9 服务器

要将 RHEL 8 IdM 环境升级到 RHEL 9，您必须首先为 RHEL 8 IdM 环境添加新的 RHEL 9 IdM 副本，然后停用 RHEL 8 服务器。迁移涉及将 Red Hat Enterprise Linux (RHEL) 8 服务器中的所有身份管理(IdM)数据和配置移到 RHEL 9 服务器。

警告

- 不支持将 RHEL 8 IdM 服务器原位升级到 RHEL 9。
- 有关在 FIPS 模式的 RHEL 8 IdM 部署中添加 RHEL 9 IdM 副本的更多信息，请参阅 *采用 RHEL 9 的注意事项* 中的 身份管理 部分。
- 将 IdM 副本升级到 RHEL 9.2 后，IdM Kerberos 分发中心(KDC)可能无法向没有为其分配安全标识符(SID)的用户发出票据授予票据(TGT)。因此，用户无法登录到其帐户。
  要临时解决这个问题，请通过在拓扑中的另一个 IdM 副本上以 IdM 管理员身份运行 **evince ipa config-mod --enable-sid --add-sids** 来生成 SID。之后，如果用户仍然无法登录，请检查目录服务器错误日志。您可能需要调整 ID 范围使其包含用户 POSIX 身份。
- 不支持直接从 RHEL 7 或更早版本迁移到 RHEL 9。要正确更新 IdM 数据，您必须执行增量迁移。
  例如，要将 RHEL 7 IdM 环境迁移到 RHEL 9：
  a. 从 RHEL 7 服务器迁移到 RHEL 8 服务器。请参阅 迁移到 RHEL 8 上的身份管理。
  b. 如本节所述，从 RHEL 8 服务器迁移到 RHEL 9 服务器。

这部分描述了如何将所有身份管理(IdM)数据和配置从 Red Hat Enterprise Linux(RHEL)8 服务器 **迁移**到 RHEL 9 服务器。

迁移步骤包括：

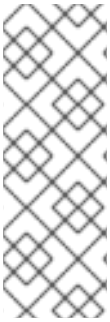
1. 配置 RHEL 9 IdM 服务器并将其作为副本添加到您当前的 RHEL 8 IdM 环境中。详情请参阅安装 RHEL 9 Replica。
2. 使 RHEL 9 服务器成为证书颁发机构(CA)续订服务器。详情请参阅 将 CA 续订服务器角色分配给 RHEL 9 IdM 服务器。
3. 在 RHEL 8 服务器上停止证书撤销列表(CRL)的生成，并将 CRL 请求重定向到 RHEL 9 副本。详情请参阅在 RHEL 8 IdM CA 服务器中停止 CRL 生成 。
4. 在 RHEL 9 服务器上启动 CRL 的生成。详情请参阅在新的 RHEL 9 IdM CA 服务器中启动 CRL 生成。
5. 停止并弃用原始 RHEL 8 CA 续订服务器。详情请参阅停止和弃用 RHEL 8 服务器 。

在以下步骤中：

- **rhel9.example.com** 是 RHEL 9 系统，它将成为新的 CA 续订服务器。
- **rhel8.example.com** 是原始 RHEL 8 CA 续订服务器。要识别哪个 Red Hat Enterprise Linux 8 服务器是 CA 续订服务器，在任何 IdM 服务器上运行以下命令：

```
[root@rhel8 ~]# ipa config-show | grep "CA renewal"
IPA CA renewal master: rhel8.example.com
```

如果您的 IdM 部署没有使用 IdM CA，在 RHEL 8 中运行的任何 IdM 服务器都可以是 **rhel8.example.com**。



注意

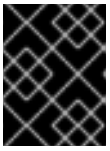
只有 在您的 IdM 部署使用嵌入式证书颁发机构(CA)时，才完成以下章节中的步骤：

- 为 RHEL 9 IdM 服务器分配 CA 续订服务器角色
- 在 RHEL 8 IdM CA 服务器中停止 CRL 生成
- 在新的 RHEL 9 IdM CA 服务器中启动 CRL 生成

1.1. 将 IDM 从 RHEL 8 迁移到 9 的先决条件

在 **rhel8.example.com** 上：

1. 将系统升级到最新的 RHEL 8 版本。



重要

如果您要迁移到 RHEL 9.0，请不要更新至比 RHEL 8.6 较新的版本。RHEL 9.1 仅支持从 RHEL 8.7 迁移。

2. 将 **ipa-*** 软件包更新至其最新版本：

```
[root@rhel8 ~]# dnf update ipa-*
```

警告

当升级多个身份管理(IdM)服务器时，在每次升级之间至少等待 10 分钟。

当两个或更多个服务器同时升级，或在不同升级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。

在 **rhel9.example.com** 上：

1. 在系统上已安装了最新版本的Red Hat Enterprise Linux。如需更多信息，请参阅 执行标准的 RHEL 9 安装。

2. 确保系统是注册到 **rhel8.example.com** IdM 服务器授权域的 IdM 客户端。如需更多信息，请参阅安装 IdM 客户端：基本场景 。

3. 确定系统满足 IdM 服务器安装的要求。请参阅为 IdM 服务器安装准备系统。

4. 确保时间服务器 **rhel8.example.com** 同步：

```
[root@rhel8 ~]# ntpstat
synchronised to NTP server (ntp.example.com) at stratum 3
  time correct to within 42 ms
  polling server every 1024 s
```

5. 确定系统已授权安装 IdM 副本。请参阅授权 IdM 客户端中的副本安装。

6. 将 **ipa-*** 软件包更新至其最新版本：

```
[root@rhel8 ~]# dnf update ipa-*
```

其他资源

- 要决定您要在新的 IdM 主服务器 **rhel9.example.com** 上安装哪些服务器角色，请查看以下链接：
  - 有关 IdM 中 CA 服务器角色的详情，请参阅 规划您的 CA 服务。
  - 有关 IdM 中 DNS 服务器角色的详情，请参阅 规划您的 DNS 服务和主机名。
  - 有关基于 IdM 和活动目录(AD)之间跨林信任的集成的详情，请参阅 规划 IdM 和 AD 之间的跨林信任。
- 要在 RHEL 9 中为 IdM 安装特定的服务器角色，您需要从特定的 IdM 软件仓库下载软件包：安装 IdM 服务器所需的软件包。
- 要将系统从 RHEL 8 升级到 RHEL 9，请参阅 从 RHEL 8 升级到 RHEL 9 。

1.2. 安装 RHEL 9 副本

1. 列出 RHEL 8 环境中存在哪些服务器角色：

```
[root@rhel8 ~]# ipa server-role-find --status enabled --server rhel8.example.com
----------------------
3 server roles matched
----------------------
  Server name: rhel8.example.com
  Role name: CA server
  Role status: enabled

  Server name: rhel8.example.com
  Role name: DNS server
  Role status: enabled
[... output truncated ...]
```

2. （可选）如果 **rhel8.example.com** 使用 rhel8.example.com 使用的 **rhel9.example.com** 的相同的 per-server 转发器，请查看 **rhel8.example.com** 的 per-server 转发器：

```
[root@rhel8 ~]# ipa dnsserver-show rhel8.example.com
----------------------------
1 DNS server matched
----------------------------
  Server name: rhel8.example.com
  SOA mname: rhel8.example.com.
  Forwarders: 192.0.2.20
  Forward policy: only
------------------------------------------------
Number of entries returned 1
------------------------------------------------
```

3. 在 **rhel9.example.com** 上安装 IdM 服务器软件，将其配置为 RHEL 8 IdM 服务器的副本，包括 **rhel8.example.com** 上存在的所有服务器角色。要安装上例中的角色，请使用 **ipa-replica-install** 命令的这些选项：

   - **--setup-ca** 用来设置证书系统组件
   - **--setup-dns** 和 **--forwarder** 来配置集成 DNS 服务器，并设置每服务器转发器来处理 IdM 域外的 DNS 查询

   注意

   另外，如果您的 IdM 部署与 Active Directory(AD)属于信任关系，请将 **--setup-adtrust** 选项添加到 **ipa-replica-install** 命令中，以便在 **rhel9.example.com** 上配置 AD 信任功能。

   - **--ntp-server** 指定 NTP 服务器，或者 **--ntp-pool** 指定 NTP 服务器池
     要设置其使用 IP 地址为 192.0.2.20 的每服务器转发器、IP 地址为 192.0.2.1 的 IdM 服务器，并与 **ntp.example.com** NTP 服务器同步：

     ```
     [root@rhel9 ~]# ipa-replica-install --setup-ca --ip-address 192.0.2.1 --setup-dns --forwarder 192.0.2.20 --ntp-server ntp.example.com
     ```

     您不需要指定 RHEL 8 IdM 服务器本身，因为如果 DNS 工作正常，**rhel9.example.com** 将使用 DNS 自动发现来找到它。

4. [可选] 将您的外部 **NTP** 时间服务器的 **_ntp._udp** 服务(SRV)记录添加到新安装的 IdM 服务器的 DNS，即 **rhel9.example.com**。IdM DNS 中时间服务器的 SRV 记录可确保将来的 RHEL 9 副本和客户端安装被自动配置为与 **rhel9.example.com** 使用的时间服务器同步。这是因为 **ipa-client-install** 会查找 **_ntp._udp** DNS 条目，除非在安装命令行界面(CLI)上提供了 **--ntp-server** 或 **--ntp-pool** 选项。

验证

1. 验证 IdM 服务是否在 **rhel9.example.com** 上运行：

   ```
   [root@rhel9 ~]# ipactl status
   Directory Service: RUNNING
   [... output truncated ...]
   ipa: INFO: The ipactl command was successful
   ```

2. 验证 **rhel9.example.com** 的服务器角色是否与 **rhel8.example.com** 相同：

```
[root@rhel9 ~]# kinit admin
[root@rhel9 ~]# ipa server-role-find --status enabled --server rhel9.example.com
----------------------
2 server roles matched
----------------------
  Server name: rhel9.example.com
  Role name: CA server
  Role status: enabled

  Server name: rhel9.example.com
  Role name: DNS server
  Role status: enabled
```

3. （可选）显示 **rhel8.example.com** 和 **rhel9.example.com** 之间的复制协议详情：

```
[root@rhel9 ~]# ipa-csreplica-manage list --verbose rhel9.example.com
Directory Manager password:

rhel8.example.com
last init status: None
last init ended: 1970-01-01 00:00:00+00:00
last update status: Error (0) Replica acquired successfully: Incremental update succeeded
last update ended: 2019-02-13 13:55:13+00:00
```

4. （可选）如果您的 IdM 部署与 AD 有一个信任关系，请验证它是否正常工作：

   a. 验证 Kerberos 配置

   b. 尝试在 **rhel9.example.com** 上解析 AD 用户：

```
[root@rhel9 ~]# id aduser@ad.domain
```

5. 验证 **rhel9.example.com** 是否已与 **NTP** 服务器同步：

```
[root@rhel8 ~]# chronyc tracking
Reference ID    : CB00710F (ntp.example.com)
Stratum         : 3
Ref time (UTC)  : Wed Feb 16 09:49:17 2022
[... output truncated ...]
```

其他资源

- DNS 配置优先级
- IdM 的时间服务要求

1.3. 为 RHEL 9 IDM 服务器分配 CA 续订服务器角色

如果您的 IdM 部署使用嵌入的证书颁发机构(CA)，请将 CA renewal server 角色分配给 Red Hat Enterprise Linux (RHEL) 9 IdM 服务器。

在 **rhel9.example.com** 上，将 **rhel9.example.com** 配置为新的 CA 续订服务器：

1. 配置 **rhel9.example.com** 以处理 CA 子系统证书续订：

```
[root@rhel9 ~]# ipa config-mod --ca-renewal-master-server rhel9.example.com
  ...
  IPA masters: rhel8.example.com, rhel9.example.com
  IPA CA servers: rhel8.example.com, rhel9.example.com
  IPA CA renewal master: rhel9.example.com
```

输出确认更新成功。

2. 在 **rhel9.example.com** 上，启用证书更新器任务：

   a. 打开 **/etc/pki/pki-tomcat/ca/CS.cfg** 配置文件进行编辑。

   b. 删除 **ca.certStatusUpdateInterval** 条目，或者将其设置为所需的间隔（以秒为单位）。默认值为 **600**。

   c. 保存并关闭 **/etc/pki/pki-tomcat/ca/CS.cfg** 配置文件。

   d. 重启 IdM 服务：

   ```
   [user@rhel9 ~]$ ipactl restart
   ```

3. 在 **rhel8.example.com** 上，禁用证书更新器任务：

   a. 打开 **/etc/pki/pki-tomcat/ca/CS.cfg** 配置文件进行编辑。

   b. 将 **ca.certStatusUpdateInterval** 改为 **0**，或者如果以下条目不存在，就添加它：

   ```
   ca.certStatusUpdateInterval=0
   ```

   c. 保存并关闭 **/etc/pki/pki-tomcat/ca/CS.cfg** 配置文件。

   d. 重启 IdM 服务：

   ```
   [user@rhel8 ~]$ ipactl restart
   ```

1.4. 在 RHEL 8 IDM CA 服务器中停止 CRL 生成

如果您的 IdM 部署使用嵌入的证书颁发机构(CA)，请在 IdM CRL 发布程序服务器上停止生成证书撤销列表(CRL)。

先决条件

- 您必须以 root 身份登录。

步骤

1. （可选）验证 **rhel8.example.com** 正在生成 CRL：

```
[root@rhel8 ~]# ipa-crlgen-manage status
CRL generation: enabled
Last CRL update: 2021-10-31 12:00:00
Last CRL Number: 6
The ipa-crlgen-manage command was successful
```

2. 在 **rhel8.example.com** 服务器上停止生成 CRL：

```
[root@rhel8 ~]# ipa-crlgen-manage disable
Stopping pki-tomcatd
Editing /var/lib/pki/pki-tomcat/conf/ca/CS.cfg
Starting pki-tomcatd
Editing /etc/httpd/conf.d/ipa-pki-proxy.conf
Restarting httpd
CRL generation disabled on the local host. Please make sure to configure CRL generation on another master with ipa-crlgen-manage enable.
The ipa-crlgen-manage command was successful
```

3. （可选）检查 **rhel8.example.com** 服务器是否停止了生成 CRL：

```
[root@rhel7 ~]# ipa-crlgen-manage status
```

rhel8.example.com 服务器停止生成 CRL。下一步是在 **rhel9.example.com** 上启用生成 CRL。

1.5. 在新的 RHEL 9 IDM CA 服务器中启动 CRL 生成

如果您的 IdM 部署使用嵌入的证书颁发机构(CA)，请在新的 Red Hat Enterprise Linux (RHEL) 9 IdM CA 服务器上启动证书撤销列表(CRL)生成。

先决条件

- 您必须以 root 用户身份登录 **rhel9.example.com** 机器。

步骤

1. 要在 **rhel9.example.com** 上生成 CRL，请使用 **ipa-crlgen-manage enable** 命令：

```
[root@rhel9 ~]# ipa-crlgen-manage enable
Stopping pki-tomcatd
Editing /var/lib/pki/pki-tomcat/conf/ca/CS.cfg
Starting pki-tomcatd
Editing /etc/httpd/conf.d/ipa-pki-proxy.conf
Restarting httpd
Forcing CRL update
CRL generation enabled on the local host. Please make sure to have only a single CRL generation master.
The ipa-crlgen-manage command was successful
```

验证步骤

- 要检查是否启用了 CRL 生成，请使用 **ipa-crlgen-manage status** 命令：

```
[root@rhel8 ~]# ipa-crlgen-manage status
CRL generation: enabled
Last CRL update: 2021-10-31 12:10:00
Last CRL Number: 7
The ipa-crlgen-manage command was successful
```

1.6. 停止并退出 RHEL 8 服务器

1. 确保所有数据（包括最新的更改）已从 **rhel8.example.com** 正确迁移到 **rhel9.example.com**。例如：

   a. 在 **rhel8.example.com** 上添加一个新用户：

   ```
   [root@rhel8 ~]# ipa user-add random_user
   First name: random
   Last name: user
   ```

   b. 检查该用户是否已复制到 **rhel9.example.com** ：

   ```
   [root@rhel9 ~]# ipa user-find random_user
   --------------
   1 user matched
   --------------
     User login: random_user
     First name: random
     Last name: user
   ```

2. 确保分布式数字分配(DNA) ID 范围被分配给 **rhel9.example.com** 。使用以下方法之一：

   - 通过创建另一个测试用户，直接在 **rhel9.example.com** 上激活 DNA 插件：

   ```
   [root@rhel9 ~]# ipa user-add another_random_user
   First name: another
   Last name: random_user
   ```

   - 将特定的 DNA ID 范围分配给 **rhel9.example.com** ：

     i. 在 **rhel8.example.com** 上，显示 IdM ID 范围：

     ```
     [root@rhel8 ~]# ipa idrange-find
     ----------------
     3 ranges matched
     ----------------
       Range name: EXAMPLE.COM_id_range
       First Posix ID of the range: 196600000
       Number of IDs in the range: 200000
       First RID of the corresponding RID range: 1000
       First RID of the secondary RID range: 100000000
       Range type: local domain range
     ```

     ii. 在 **rhel8.example.com** 上，显示分配的 DNA ID 范围：

     ```
     [root@rhel8 ~]# ipa-replica-manage dnarange-show
     rhel8.example.com: 196600026-196799999
     rhel9.example.com: No range set
     ```

     iii. 减少分配给 **rhel8.example.com** 的 DNA ID 范围，以便一部分对 **rhel9.example.com** 可用：

```
[root@rhel8 ~]# ipa-replica-manage dnarange-set rhel8.example.com
196600026-196699999
```

iv. 将 IdM ID 范围的剩余部分分配给 **rhel9.example.com** ：

```
[root@rhel8 ~]# ipa-replica-manage dnarange-set rhel9.example.com
196700000-196799999
```

3. 停止 **rhel8.example.com** 中的所有 IdM 服务，将域发现强制到新的 **rhel9.example.com** 服务器。

```
[root@rhel8 ~]# ipactl stop
Stopping CA Service
Stopping pki-ca:                                   [  OK  ]
Stopping HTTP Service
Stopping httpd:                                    [  OK  ]
Stopping MEMCACHE Service
Stopping ipa_memcached:                            [  OK  ]
Stopping DNS Service
Stopping named:                                    [  OK  ]
Stopping KPASSWD Service
Stopping Kerberos 5 Admin Server:                  [  OK  ]
Stopping KDC Service
Stopping Kerberos 5 KDC:                           [  OK  ]
Stopping Directory Service
Shutting down dirsrv:
    EXAMPLE-COM...                                 [  OK  ]
    PKI-IPA...                                     [  OK  ]
```

之后，**ipa** 工具将通过远程过程调用(RPC)联系新的服务器。

4. 通过在 RHEL 9 服务器中执行删除命令，从拓扑中删除 RHEL 8 服务器。详情请参阅 卸载 IdM 服务器。

第 2 章 将 IDM 客户端从 RHEL 8 升级到 RHEL 9

与 IdM 服务器不同，支持将 IdM 客户端从 RHEL 8 原位升级到 RHEL 9。Leapp 原位升级实用程序进行所有必要的配置更改。

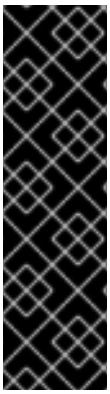
部分 II. 从外部源迁移到 IDM

第 3 章 从非 RHEL LINUX 发行版上的 FREEIPA 迁移到 RHEL 9 上的 IDM

要将非 RHEL Linux 发行版上的 FreeIPA 部署迁移到 RHEL 9 服务器上的身份管理(IdM)部署，您必须首先将新的 RHEL 9 IdM 证书颁发机构(CA)副本添加到现有的 FreeIPA 环境中，将与证书相关的角色传给它，然后停用非 RHEL FreeIPA 服务器。

警告

不支持使用 Convert2RHEL 工具执行非 RHEL FreeIPA 服务器到 RHEL 9 IdM 服务器的原位升级。



重要

因为 **SHA-1** 算法的使用在 RHEL 9 中的 **DEFAULT** 系统范围加密策略中被禁用了，所以如果 RHEL 9 系统在同一 IdM 部署中被用作非 RHEL-9 系统，则可能会出现多个已知问题。详情请查看：

- Red Hat Enterprise Linux 9.0 发行注记
- Red Hat Enterprise Linux 9.1 的发行注记
- Red Hat Enterprise Linux 9.2 发行注记

重要

将 IdM 副本升级到 RHEL 9.2 后，IdM Kerberos 分发中心(KDC)可能无法向没有为其分配安全标识符(SID)的用户发出票据授予票据(TGT)。因此，用户无法登录到其帐户。

要临时解决这个问题，请通过在拓扑中的另一个 IdM 副本上以 IdM 管理员身份运行 **evince ipa config-mod --enable-sid --add-sids** 来生成 SID。之后，如果用户仍然无法登录，请检查目录服务器错误日志。您可能需要调整 ID 范围使其包含用户 POSIX 身份。

先决条件

在 RHEL 9 系统上：

1. 在系统上已安装了最新版本的Red Hat Enterprise Linux。如需更多信息，请参阅 执行标准的 RHEL 9 安装。
2. 确保系统是注册到 FreeIPA 服务器授权的域的 IdM 客户端。如需更多信息，请参阅安装 IdM 客户端：基本场景 。
3. 确定系统满足 IdM 服务器安装的要求。请参阅为 IdM 服务器安装准备系统。
4. 确定系统已授权安装 IdM 副本。请参阅授权 IdM 客户端中的副本安装。

在非 RHEL FreeIPA 服务器上：

1. 确定您知道系统与之同步的时间服务器：

```
[root@freeipaserver ~]# ntpstat
synchronised to NTP server (ntp.example.com) at stratum 3
   time correct to within 42 ms
   polling server every 1024 s
```

2. 将 **ipa-*** 软件包更新至其最新版本：

```
[root@freeipaserver ~]# dnf update ipa-*
```

步骤

1. 要执行迁移，请按照 将 IdM 环境从 RHEL 8 服务器迁移到 RHEL 9 服务器 中的步骤进行操作，使用您的非 RHEL FreeIPA CA 副本作为 RHEL 8 服务器：

   a. 配置 RHEL 9 服务器，并将其作为 IdM 副本添加到非 RHEL Linux 发行版的当前 FreeIPA 环境中。详情请参阅安装 RHEL 9 副本 。

   b. 使 RHEL 9 复制证书颁发机构(CA)续订服务器。详情请参阅 将 CA 续订服务器角色分配给 RHEL 9 IdM 服务器。

   c. 在非 RHEL 服务器上停止生成证书撤销列表(CRL)，并将 CRL 请求重定向到 RHEL 9 副本。详情请参阅在 RHEL 8 IdM CA 服务器中停止 CRL 生成 。

   d. 在 RHEL 9 服务器上开始生成 CRL。详情请参阅在新的 RHEL 9 IdM CA 服务器中启动 CRL 生成。

   e. 停止并弃用原来的非 RHEL FreeIPA CA 续订服务器。详情请参阅停止和弃用 RHEL 8 服务器。

其他资源

- 将 IdM 环境从 RHEL 8 服务器迁移到 RHEL 9 服务器

第 4 章 从 LDAP 目录迁移到 IDM

如果您之前为身份和身份验证查找部署了 LDAP 服务器，您可以将查找服务迁移到身份管理(IdM)。IdM 提供了一个迁移工具来帮助您执行以下任务：

- 传输用户帐户，包括密码和组成员身份，而不会丢失数据。
- 避免在客户端上进行昂贵的配置更新。

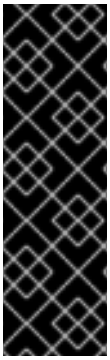
此处描述的迁移过程假定一个简单的部署场景，其中在 LDAP 中有一个名字空间，在 IdM 中有一个名字空间。对于更复杂的环境，如有多个名字空间或自定义模式的环境，请联系红帽支持服务。

4.1. 从 LDAP 迁移到 IDM 时的注意事项

从 LDAP 服务器移至身份管理(IdM)的过程有以下阶段：

- 迁移 *客户端*。仔细规划此阶段。确定您当前基础架构中的每个客户端都使用哪些服务。例如，这些服务可能包括 Kerberos 或系统安全服务守护进程(SSSD)。然后，确定您可以在最终的 IdM 部署中使用哪些服务。如需更多信息，请参阅 当从 LDAP 迁移到 IdM 时规划客户端配置 。
- 迁移 *数据*。
- 迁移 *密码*。仔细规划此阶段。除了密码，IdM 还需要每个用户帐户的 Kerberos 哈希。 在从 LDAP 迁移到 IdM 时规划密码迁移 中涵盖了一些注意事项和密码迁移路径。

您可以首先迁移服务器部分，然后迁移客户端，或首先迁移客户端，然后迁移服务器。有关两种迁移类型的更多信息，请参阅 LDAP 到 IdM 的迁移序列 。



重要

强烈建议您在尝试迁移真实的 LDAP 环境前设置测试 LDAP 环境并测试迁移过程。在测试环境时，请执行以下操作：

1. 在 IdM 中创建测试用户，并将迁移的用户的输出与测试用户的输出进行比较。确保迁移的用户包含测试用户上存在的最小属性和对象类集合。
2. 将迁移的用户的输出（如 IdM 上所示）与源用户进行比较，如原始 LDAP 服务器上所示。确保导入的属性不会复制两次，并且它们具有正确的值。

4.2. 在从 LDAP 迁移到 IDM 时规划客户端配置

身份管理(IdM)可以支持多种不同的客户端配置，具有不同功能、灵活性和安全性。根据操作系统以及您的 IT 维护优先级，确定最适合每个客户的配置。还要考虑客户端的功能区域：开发计算机通常需要的配置与生产服务器或用户笔记本电脑不同。

重要

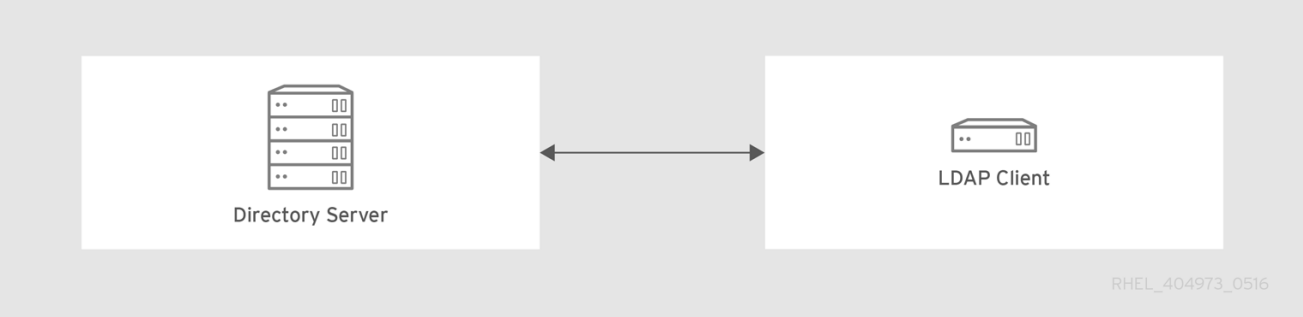
大多数环境都混合有客户端连接到 IdM 域的不同方式。管理员必须决定哪种场景最适合每个客户端。

4.2.1. 初始的、迁移前的客户端配置

在决定身份管理(IdM)中客户端配置的细节之前，请首先确定当前的、迁移前配置的具体信息。

要迁移的几乎所有 LDAP 部署的初始状态是，有一个提供身份和身份验证服务的 LDAP 服务。

图 4.1. 基本的 LDAP 目录和客户端配置



Linux 和 Unix 客户端使用 PAM_LDAP 和 NSS_LDAP 库来直接连接 LDAP 服务。这些库允许客户端从 LDAP 目录检索用户信息，就像数据存储在 **/etc/passwd** 或 **/etc/shadow** 中一样。在现实环境中，如果客户端使用 LDAP 进行身份查找，使用 Kerberos 进行身份验证或其他配置，则基础架构可能更为复杂。

身份管理(IdM)服务器与 LDAP 目录不同，特别是在模式支持和目录树的结构方面。有关这些差异的更多背景，请参阅 当从 LDAP 迁移到 IdM 时规划客户端配置 中的 **将 IdM 与标准 LDAP 目录进行对比** 部分。这些差异可能会影响数据，特别是目录树，这会影响条目名称。但是，这些差异对客户端配置和将客户端迁移到 IdM 的影响不大。

4.2.2. 推荐的 RHEL 客户端配置

注意

描述的客户端配置只支持 RHEL 6.1 及之后的版本以及 RHEL 5.7 之后的版本，它支持最新版本的 SSSD 和 **ipa-client** 软件包。可以配置 RHEL 的旧版本，如 可选的支持的配置 中所述。

Red Hat Enterprise Linux(RHEL)中的系统安全服务守护进程(SSSD)使用特殊的 PAM 和 NSS 库：**pam_ss** 和 **nss_sss**。使用这些库，SSSD 可以与身份管理(IdM)紧密集成，并从其完整的身份验证和身份功能中获益。SSSD 具有一些有用的特性，如缓存身份信息，因此即使与中央服务器的连接丢失，用户也可以登录。

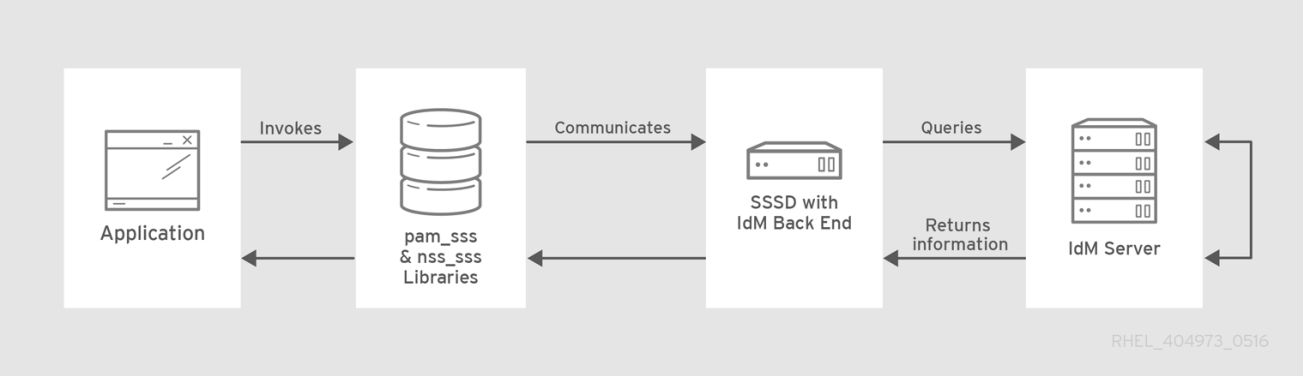
与使用 **pam_ldap** 和 **nss_ldap** 库的通用 LDAP 目录服务不同，SSSD 通过定义 *域* 来在身份和身份验证信息之间建立关系。SSSD 中的域定义以下后端功能：

- 认证
- 身份查找
- 权限
- 密码更改

然后，SSSD 域配置为使用 *提供者* 来为任何一个或所有这些功能提供信息。域配置始终需要一个 *身份* 提供者。其他三个提供者是可选的；如果未定义身份验证、访问或密码提供者，则身份提供者用于此功能。

SSSD 可以对所有后端功能使用 IdM 。这是理想的配置，因为它提供完整的 IdM 功能，与通用的 LDAP 身份提供者或 Kerberos 身份验证不同。例如，在日常操作中，SSSD 在 IdM 中强制执行基于主机的访问控制规则和安全功能。

图 4.2. 客户端和带有 IdM 后端的 SSSD



ipa-client-install 脚本自动将 SSSD 配置为对所有其后端服务使用 IdM，以便默认使用推荐的配置设置 RHEL 客户端。

附加信息

- 了解 SSSD 及其优势

4.2.3. 替代的支持的配置

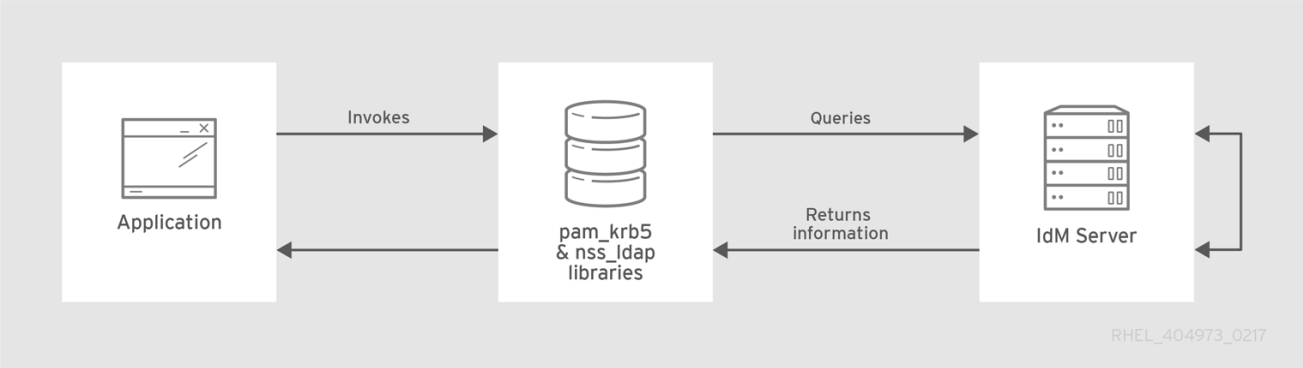
UNIX 和 Linux 系统（如 Mac、Solaris、HP-UX、AIX 和 Scientific Linux）支持身份管理(IdM)管理的所有服务，但不使用 SSSD。同样，旧的 Red Hat Enterprise Linux(RHEL)版本（特别是 6.1 和 5.6）支持 SSSD，但有一个旧版本，它不支持 IdM 作为身份提供者。

如果不能对系统使用 SSSD 的现代版本，则可以通过以下方式配置客户端：

- 客户端使用 **nss_ldap** 连接到 IdM 服务器，就像它是用于身份查找的 LDAP 目录服务器一样。
- 客户端使用 **pam_krb5** 连接到 IdM 服务器，就像它是常规的 Kerberos KDC 一样。

有关配置 *带有旧版本的 SSSD 的 RHEL 客户端* 以使用 IdM 服务器作为其身份提供商及其 Kerberos 身份验证域的更多信息，请参阅 RHEL 7 *系统级身份验证指南* 中的 为 SSSD 配置身份和身份验证提供商 部分。

图 4.3. 客户端与带有 LDAP 和 Kerberos 的 IdM



通常，这通常是对客户端使用最安全配置的最佳实践。这意味着 SSSD 或 LDAP 用于身份，Kerberos 用于身份验证。但是，对于某些维护情况和 IT 结构，您可能需要使用最简单的情景：通过在客户端上使用 **nss_ldap** 和 **pam_ldap** 库将 LDAP 配置为提供身份和身份验证。

4.3. 在从 LDAP 迁移到 IDM 时规划密码迁移

在将用户从 LDAP 迁移到身份管理(IdM)之前，需要回答的一个关键问题是是否迁移用户密码。可用的选项如下：

迁移没有密码的用户

可以更快地执行，但需要管理员和用户进行更多的手动操作。在某些情况下，这是唯一可用的选项：例如，如果 原始的 LDAP 环境存储了明文用户密码，或者如果 密码不符合 IdM 中定义的密码策略要求。

在迁移无密码的用户帐户时，您可以重置所有用户密码。迁移的用户被分配一个临时密码，在第一次登录时更改该密码。有关如何重置密码的更多信息，请参阅 HREL 7 IdM 文档中的 更改和重置用户密码。

迁移带密码的用户

提供更顺畅的过渡，但还需要在迁移和转换过程中并行管理 LDAP 目录和 IdM。其原因在于，默认情况下，IdM 使用 Kerberos 进行身份验证，并且要求每个用户除标准用户密码外还有存储在 IdM 目录服务器中的 Kerberos 哈希。要生成哈希，需要以明文形式将用户密码提供给 IdM 服务器。在创建新用户密码时，密码会在被哈希处理前以明文形式提供，并存储在 IdM 中。但是，当用户从 LDAP 目录迁移时，相关的用户密码已被哈希处理，因此无法生成相应的 Kerberos 密钥。

重要

默认情况下，用户无法验证到 IdM 域或访问 IdM 资源，除非它们有 Kerberos 哈希 - 即使用户帐户已经存在。有一个临时解决方案：在 IdM 中使用 LDAP 身份验证，而不是 Kerberos 身份验证。在这个临时解决方案中，用户不需要 Kerberos 哈希。但是，这个临时解决方案限制了 IdM 的功能，我们不推荐。

以下小节解释了如何迁移用户及其密码：

- 在将 LDAP 迁移到 IdM 时迁移密码的方法
  - 使用网页
  - 使用 SSSD
- 规划明文 LDAP 密码的迁移
- 规划不满足 IdM 要求的 LDAP 密码的迁移

4.3.1. 在将 LDAP 迁移到 IdM 时迁移密码的方法

要在不强制用户更改密码的情况下将用户帐户从 LDAP 迁移到身份管理(IdM)，您可以使用以下方法：

方法 1: 使用迁移网页

告诉用户一次将其 LDAP 凭据输入到 IdM Web UI 中的特殊页面 ***https://ipaserver.example.com/ipa/migration***。在后台运行的脚本随后捕获明文密码，并使用密码和合适的 Kerberos 哈希正确更新用户帐户。

方法 2（推荐）：使用 SSSD

通过使用系统安全服务守护进程(SSSD)生成所需的用户密钥来缓解迁移对用户的影响。对于具有大量用户的部署，或者用户不应承担密码更改所带来的负担的部署，这是最佳方案。

工作流

1. 用户尝试使用 SSSD 登录到机器。
2. SSSD 尝试对 IdM 服务器执行 Kerberos 身份验证。
3. 即使用户在系统中存在，但会出现错误为 *key type is not supported* 的身份验证失败，因为 Kerberos哈希不存在。
4. SSSD 通过安全连接执行纯文本 LDAP 绑定。
5. IdM 截获此绑定请求。如果用户有 Kerberos 主体，但没有 Kerberos 哈希，则 IdM 身份提供者会生成哈希，并将其存储在用户条目中。
6. 如果身份验证成功，SSSD 会断开与 IdM 的连接，并再次尝试 Kerberos 身份验证。这一次，请求会成功，因为条目中存在哈希。

使用方法 2 时，整个过程对用户不可见。他们登录客户端服务，但请注意他们的密码已从 LDAP 移到 IdM。

4.3.2. 规划明文 LDAP 密码的迁移

尽管大多数部署中 LDAP 密码都被加密存储，但可能有一些用户或一些环境对用户条目使用明文密码。

当用户从 LDAP 服务器迁移到 IdM 服务器时，他们的明文密码不会被迁移，因为 IdM 不允许明文密码。相反，会为每个用户创建一个 Kerberos 主体，keytab 设为 true，密码设为过期。这意味着 IdM 要求用户在下次登录时重置密码。如需更多信息，请参阅 规划不满足 IdM 要求的 LDAP 密码的迁移 。

4.3.3. 规划不满足 IdM 要求的 LDAP 密码的迁移

如果原始目录中的用户密码不符合身份管理(IdM)中定义的密码策略，则迁移后密码将无效。

当用户通过输入 **kinit** 第一次尝试获得 IdM 域中的 Kerberos 票据授权票据(TGT)时，会自动完成密码重置。强制用户更改其密码：

```
[migrated_idm_user@idmclient ~]$ kinit
Password for migrated_idm_user@IDM.EXAMPLE.COM:
Password expired.  You must change it now.
Enter new password:
Enter it again:
```

4.4. 进一步的迁移注意事项和要求

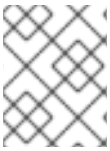
当您计划从 LDAP 服务器迁移到身份管理(IdM)时，请确保您的 LDAP 环境能够使用 IdM 迁移脚本。

4.4.1. 支持迁移的 LDAP 服务器

从 LDAP 服务器到 IdM 的迁移过程使用一个特殊的脚本 **ipa migrate-ds** 来执行迁移。此脚本对 LDAP 目录的结构和 LDAP 条目有具体的要求。仅支持对符合 LDAPv3 的目录服务的迁移，其中包括几个通用目录：

- Sun ONE 目录服务器
- Apache 目录服务器
- OpenLDAP

从 LDAP 服务器到 IdM 的迁移已使用红帽目录服务器和 OpenLDAP 进行了测试。



注意

Microsoft 活动目录 *不支持* 使用迁移脚本进行迁移，因为它不是符合 LDAPv3 的目录。如需从活动目录进行迁移的帮助，请联系红帽专业服务。

4.4.2. LDAP 环境迁移要求

LDAP 服务器和身份管理(IdM)存在许多不同的配置场景，这会影响迁移过程的顺畅性。对于示例迁移流程，这些是环境的假设：

- 正在将一个 LDAP 目录域迁移到一个 IdM 域。不涉及整合。
- 用户密码作为哈希存储在 LDAP 目录中。有关支持的哈希列表，请参阅 红帽目录服务器文档 中红帽目录服务器 10 部分中的 *配置、命令和文件参考* 标题中的密码存储模式部分。
- LDAP 目录实例是身份存储和身份验证方法。客户端机器配置为使用 **pam_ldap** 或 **nss_ldap** 库来连接 LDAP 服务器。
- 条目仅使用标准的 LDAP 模式。包含自定义对象类或属性的条目不会迁移到 IdM。
- **migrate-ds** 命令只迁移以下帐户：
  - 哪些包含 **gidNumber** 属性的账户。**posixAccount** 对象类需要此属性。
  - 哪些包含 **sn** 属性的账户。**person** 对象类需要此属性。

4.4.3. IdM 系统迁移要求

对于约 10,000 个用户和 10 个组的中等大小的目录，必须具有足够强大的目标 IdM 系统才能允许处理迁移。迁移的最低要求是：

- 4 个核
- 4GB RAM
- 30GB 磁盘空间
- 2 MB 的 SASL 缓冲区，这是 IdM 服务器的默认大小
  如果出现迁移错误，请增加缓冲大小：

```
[root@ipaserver ~]# ldapmodify -x -D 'cn=directory manager' -w password -h
ipaserver.example.com -p 389

dn: cn=config
changetype: modify
replace: nsslapd-sasl-max-buffer-size
nsslapd-sasl-max-buffer-size: 4194304

modifying entry "cn=config"
```

  设置 **nsslapd-sasl-max-buffer-size** 值（以字节为单位）。

其他资源

- IdM 服务器硬件建议

4.4.4. 用户和组 ID 号

当从 LDAP 迁移到 IdM 部署时，请确保部署之间没有用户 ID (UID)和组 ID (GID)冲突。迁移前，请验证：

- 您知道您的 LDAP ID 范围。
- 您知道您的 IdM ID 范围。
- LDAP 服务器上的 UID 和 GID 和 RHEL 系统或 IdM 部署中的现有 UID 或 GID 之间没有重叠。
- 迁移的 LDAP UID 和 GID 适合 IdM ID 范围。
  - 如果需要，在迁移前创建一个新的 IdM ID 范围。

其他资源

- 添加新的 IdM ID 范围

4.4.5. 关于 sudo 规则的注意事项

如果您将 **sudo** 与 LDAP 一起使用，则您必须手动将存储在 LDAP 中的 **sudo** 规则迁移到身份管理(IdM)。红帽建议您在 IdM 中重新创建 netgroups 来作为 hostgroups。对于不使用 SSSD **sudo** 提供者的 **sudo** 配置，IdM 自动将 hostgroups 显示为传统的 netgroups。

4.4.6. LDAP 到 IdM 的迁移工具

身份管理(IdM)使用特定命令 **ipa migrate-ds** 来执行迁移过程，以便 LDAP 目录数据被正确格式化并干净地导入到 IdM 服务器中。使用 **ipa migrate-ds** 时，远程系统用户（由 **--bind-dn** 选项指定的）必须具有对 **userPassword** 属性的读权限，否则将不能迁移密码。

IdM 服务器必须配置为在迁移模式下运行，然后才可以使用迁移脚本。详情请参阅 将 LDAP 服务器迁移到 IdM。

4.4.7. 提高 LDAP 到 IdM 的迁移性能

LDAP 迁移本质上是 IdM 服务器中 389 目录服务器(DS)实例的一个专门的导入操作。调优 389 DS 实例以获得更好的导入操作性能，有助于提高整体迁移性能。

有两个参数会直接影响导入性能：

- **nsslapd-cachememsize** 属性定义条目缓存允许的大小。这是一个缓冲区，其自动设置为总缓存大小的 80%。对于大规模导入操作，您可以增加此参数以及可能的内存缓存本身。这一改进将提高目录服务处理大量条目或具有大量属性的条目的效率。
  有关如何使用 **dsconf** 命令修改属性的详情，请参阅 调整条目缓存大小。

- 系统 **ulimit** 配置选项设置系统用户允许的最大进程数。处理大型数据库可能会超出限制。如果发生这种情况，请增大值：

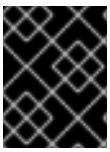
  ```
  [root@server ~]# ulimit -u 4096
  ```

其他资源

- 调整 IdM 目录服务器性能

4.4.8. LDAP 到 IdM 的迁移序列

迁移到 IdM 时有四个主要步骤，但它们的顺序根据您要首先迁移 *服务器* 还是 *客户端* 而有所不同。



重要

客户端优先和服务器优先迁移都提供了常规迁移流程，但它们可能无法在每个环境中都正常工作。在尝试迁移真实的 LDAP 环境之前，请设置测试 LDAP 环境，并测试迁移过程。

客户端优先迁移

SSSD 用于在配置身份管理(IdM)服务器时更改客户端配置：

1. 部署 SSSD。
2. 重新配置客户端来连接到当前 LDAP 服务器，然后故障转移到 IdM。
3. 安装 IdM 服务器。
4. 使用 IdM **ipa migrate-ds** 脚本迁移用户数据。这会从 LDAP 目录导出数据、IdM 模式的格式，然后将它导入到 IdM。
5. 使 LDAP 服务器下线，并允许客户端透明地故障转移到 IdM。

服务器优先迁移

LDAP 到 IdM 的迁移首先是：

1. 安装 IdM 服务器。
2. 使用 IdM **ipa migrate-ds** 脚本迁移用户数据。这会从 LDAP 目录导出数据，为 IdM 模式格式化数据，然后将其导入到 IdM 中。
3. *可选*。部署 SSSD。
4. 重新配置客户端来连接到 IdM。不可能简单地替换 LDAP 服务器。IdM 目录树- 因此用户条目 DN - 与之前的目录树不同。
   虽然要求必须重新配置客户端，但不需要立即重新配置客户端。更新的客户端可以指向 IdM 服务器，而其他客户端则指向旧的 LDAP 目录，从而在数据迁移后可允许合理的测试和过渡阶段。

注意

不要长时间并行运行 LDAP 目录服务和 IdM 服务器。这增加了用户数据在两个服务间不一致的风险。

4.5. 自定义从 LDAP 到 IDM 的迁移

您可以使用 **ipa migrate-ds** 命令将身份验证和授权服务从 LDAP 服务器迁移到身份管理(IdM)。如果没有附加选项，命令会获取目录的 LDAP URL，来根据常见的默认设置迁移和导出数据。

您可以使用不同的 **ipa migrate-ds** 命令选项来自定义迁移过程，以及数据如何被识别和导出。如果您的 LDAP 目录树具有唯一的结构，或者您知道必须排除某些条目或条目中的某些属性，则可以自定义迁移。

4.5.1. 从 LDAP 迁移到 IdM 的过程中自定义绑定 DN 和基本 DN 的示例

使用 **ipa migrate-ds** 命令来从 LDAP 迁移到身份管理(IdM)。如果没有附加选项，命令会获取目录的 LDAP URL，来根据常见的默认设置迁移和导出数据。以下是修改默认设置的示例：

```
# ipa migrate-ds ldap://ldap.example.com:389
```

自定义绑定 DN

默认情况下，DN "**cn=Directory Manager**" 用于绑定到远程 LDAP 目录。使用 **--bind-dn** 选项来指定自定义绑定 DN：

```
# ipa migrate-ds ldap://ldap.example.com:389 --bind-dn=cn=Manager,dc=example,dc=com
```

自定义命名上下文

如果 LDAP 服务器命名上下文与 IdM 中使用的不同，对象的基本 DN 会被转换。例如：**uid=*user*,ou=Person,dc=ldap,dc=example,dc=com** 被迁移到 **uid=*user*,ou=Person,dc=idm,dc=example,dc=com**。使用 **--base-dn** 选项，您可以更改容器子树的目标，因此设置远程 LDAP 服务器上用于迁移的基本 DN：

```
# ipa migrate-ds --base-dn="ou=people,dc=example,dc=com" ldap://ldap.example.com:389
```

其他资源

- **ipa migrate-ds --help**

4.5.2. 特定子树的迁移

默认目录结构将人员条目置于 **ou=People** 子树中，并将组条目置于 **ou=Groups** 子树中。这些子树是这些不同类型的目录数据的容器条目。如果您不将任何选项用于 **migrate-ds** 命令，则 工具假定给定的 LDAP 目录使用 **ou=People** 和 **ou=Groups** 结构。

许多部署可能具有完全不同的目录结构，或者您可能只想导出原始目录树的某些部分。作为管理员，您可以使用以下选项来指定源 LDAP 服务器上不同用户或组子树的 RDN：

- **--user-container**
- **--group-container**

注意

在这两种情况下，子树都必须是相对区分名称(RDN)，并且必须相对于基本 DN。例如，您可以使用 **--user-container=ou=Employees** 迁移 **>ou=Employees,dc=example,dc=com** 目录树。

例如：

```
[ipaserver ~]# ipa migrate-ds --user-container=ou=employees \
--group-container="ou=employee groups" ldap://ldap.example.com:389
```

另外，还可在 **ipa migrate-ds** 命令中添加 **--scope** 选项来设置范围：

- **onelevel** ：默认的。仅迁移指定容器中的条目。

- **subtree** ：指定容器中的条目以及所有子容器都被迁移。
- **base** ：仅迁移指定的对象本身。

4.5.3. 条目的包含和排除

默认情况下，**ipa migrate-ds** 脚本导入具有 **person** 对象类的每个用户条目，以及具有 **groupOfUniqueNames** 或 **groupOfNames** 对象类的每个组条目。

在某些迁移路径中，可能需要导出特定类型的用户和组，或者需要排除特定的用户和组。您可以通过在查找用户或组条目时设置要搜索的对象类来选择要包括哪个用户和组 *类型*。

当您对不同的 *用户* 类型使用自定义对象类时，此选项特别有用。例如，以下命令仅迁移具有自定义 **fullTimeEmployee** 对象类的用户：

```
[root@ipaserver ~]# ipa migrate-ds --user-objectclass=fullTimeEmployee
ldap://ldap.example.com:389
```

由于不同类型的组，这对于仅迁移某些类型的 *组* （如用户组），同时排除其他类型的组（如证书组）也非常有用，。例如：

```
[root@ipaserver ~]# ipa migrate-ds --group-objectclass=groupOfNames --group-
objectclass=groupOfUniqueNames ldap://ldap.example.com:389
```

根据对象类指定要迁移的用户和组条目，可以隐式地将所有其他用户和组从迁移中排除。

或者，除了少量条目之外，迁移所有用户和组条目也很有用。您可以在迁移该类型的所有其他用户或组帐户时排除特定的用户或组帐户。例如，这仅排除一个 hobbies 组和两个用户：

```
[root@ipaserver ~]# ipa migrate-ds --exclude-groups="Golfers Group" --exclude-
users=idmuser101 --exclude-users=idmuser102 ldap://ldap.example.com:389
```

exclude 语句应用到与 **uid** 中模式匹配的用户，以及在 **cn** 属性中与其匹配的组。

您可以迁移常规对象类，但排除该类的特定条目。例如，这特别包括具有 **fullTimeEmployee** 对象类的用户，但排除了三个管理者：

```
[root@ipaserver ~]# ipa migrate-ds --user-objectclass=fullTimeEmployee --exclude-
users=jsmith --exclude-users=bjensen --exclude-users=mreynolds
ldap://ldap.example.com:389
```

4.5.4. 条目属性的排除

默认情况下，用户或组条目的每个属性和对象类都将被迁移。在某些场景中，由于带宽和网络的约束，或者由于属性数据不再相关，这可能不太现实。例如，如果在用户在加入身份管理(IdM)域时为其分配了新用户证书，那么迁移 **userCertificate** 属性就毫无用处。

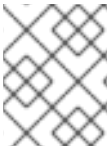
您可以通过在 **migrate-ds** 命令中使用以下选项来忽略特定的对象类和属性：

- **--user-ignore-objectclass**
- **--user-ignore-attribute**
- **--group-ignore-objectclass**

- **--group-ignore-attribute**

例如，要为用户排除 **userCertificate** 属性和 **strongAuthenticationUse** 对象类，为组排除 **groupOfCertificate** 对象类：

```
[root@ipaserver ~]# ipa migrate-ds --user-ignore-attribute=userCertificate --user-ignore-objectclass=strongAuthenticationUser --group-ignore-objectclass=groupOfCertificates ldap://ldap.example.com:389
```



注意

确保不要忽略任何必需的属性。另外，在排除对象类时，请确保排除该对象类只支持的任何属性。

其他资源

- LDAP 环境迁移要求

4.5.5. 从 LDAP 迁移到 IdM 时使用的模式和模式兼容特性

身份管理(IdM)使用 RFC2307bis 模式来定义用户、主机、主机组和其他网络身份。但是，如果用作迁移源的 LDAP 服务器使用 RFC2307 模式，请在使用 **ipa migrate-ds** 命令时指定 **--schema** 选项：

```
[root@ipaserver ~]# ipa migrate-ds --schema=RFC2307 ldap://ldap.example.com:389
```

另外，IdM 具有内置 **模式兼容特性**，其允许 IdM 为不支持 RFC2307bis 的系统重新格式化数据。兼容插件默认为启用，这意味着目录服务器会计算用户和组的替代视图，并在 **cn=users,cn=compat,dc=example,dc=com** 容器条目中提供此视图。它通过在启动时预先计算其条目内容来实现，并根据需要刷新其条目。

建议在迁移过程中禁用此特性，以减少系统开销。

4.6. 将 LDAP 服务器迁移到 IDM

您可以使用 **ipa migrate-ds** 命令将身份验证和授权服务从 LDAP 服务器迁移到身份管理(IdM)。

警告

这是一个通用的迁移流程，可能在每个环境中不一定能正常工作。

强烈建议您在尝试迁移真实的 LDAP 环境前设置测试 LDAP 环境并测试迁移过程。在测试环境时，请执行以下操作：

1. 在 IdM 中创建测试用户，并将迁移的用户的输出与测试用户的输出进行比较。
2. 将迁移的用户的输出（如 IdM 上所示）与源用户进行比较，如原始 LDAP 服务器上所示。

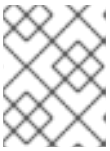
有关更多的指导，请参见下面的 **验证** 部分。

先决条件

- 有 LDAP 目录的管理员特权。
- 如果已安装 IdM，则您有 IdM 的管理员权限。
- 您以 **root** 身份登录到要在其上执行以下流程的 RHEL 系统。
- 您已阅读并理解了以下章节：
  - 从 LDAP 迁移到 IdM 时的注意事项。
  - 在从 LDAP 迁移到 IdM 时规划客户端配置。
  - 从 LDAP 迁移到 IdM 时规划密码迁移。
  - 进一步的迁移注意事项和要求。
  - 自定义从 LDAP 到 IdM 的迁移。

步骤

1. 如果 IdM 尚未安装：在安装了现有 LDAP 目录的不同机器上安装 IdM 服务器，包括任何自定义 LDAP 目录模式。详情请参阅 安装身份管理。



注意

自定义用户或组模式在 IdM 中的支持有限。它们可能会在迁移过程中导致问题，因为对象定义不兼容。

2. 出于性能考虑，禁用兼容插件：

```
# ipa-compat-manage disable
```

有关模式兼容特性以及为迁移禁用它的好处的更多信息，请参阅 从 LDAP 迁移到 IdM 时的模式和模式兼容功能。

3. 重启 IdM 目录服务器实例：

```
# systemctl restart dirsrv.target
```

4. 配置 IdM 服务器来允许迁移：

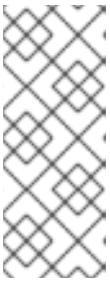
```
# ipa config-mod --enable-migration=TRUE
```

通过将 **--enable-migration** 设为 TRUE，您可以执行以下操作：

- 在 LDAP 添加操作过程中允许预哈希密码。
- 如果初始 Kerberos 身份验证失败，则将 SSSD 配置为尝试密码迁移序列。如需更多信息，请参阅 将密码从 LDAP 迁移到 IdM 时的使用 SSSD 中的工作流部分。

5. 运行 IdM 迁移脚本 **ipa migrate-ds** 以及与您的用例相关的选项。如需更多信息，请参阅 自定义从 LDAP 到 IdM 的迁移。

```
# ipa migrate-ds --your-options ldap://ldap.example.com:389
```



注意

如果您没有在前面的步骤中禁用兼容插件，请将 **--with-compat** 选项添加到 **ipa migrate-ds** ：

```
# ipa migrate-ds --your-options --with-compat
ldap://ldap.example.com:389
```

6. 重新启用兼容插件：

```
# ipa-compat-manage enable
```

7. 重启 IdM 目录服务器：

```
# systemctl restart dirsrv.target
```

8. 当所有用户已迁移密码后，禁用迁移模式：

```
# ipa config-mod --enable-migration=FALSE
```

9. [可选] 当所有用户都已迁移后，重新配置非 SSSD 客户端以使用 Kerberos 身份验证，即 **pam_krb5**，而不是 LDAP 身份验证，即 **pam_ldap**。如需更多信息，请参阅 RHEL 7 *系统级身份验证指南*中的配置 Kerberos 客户端。

10. 让用户生成哈希的 Kerberos 密码。选择 从 LDAP 迁移到 IdM 时规划密码迁移 中描述的方法之一。

- 如果您决定使用 SSSD 方法 ：
  - 将已安装 SSSD 的客户端从 LDAP 目录移到 IdM 目录，并将它们注册为 IdM 的客户端。这会下载所需的密钥和证书。
    在 Red Hat Enterprise Linux 客户端上，可以使用 **ipa-client-install** 命令来实现。例如：

```
# ipa-client-install --enable-dns-update
```

- 如果您决定使用 IdM 迁移 web 页面 方法：
  - 指示用户使用迁移网页登录到 IdM：

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

11. 要监控用户迁移过程，请查询现有的 LDAP 目录，以查看哪些用户帐户拥有密码，但还没有 Kerberos 主体键。

```
$ ldapsearch -LL -x -D 'cn=Directory Manager' -w secret -b
'cn=users,cn=accounts,dc=example,dc=com' '(&(!(krbprincipalkey=))(userpassword=))'
uid
```

注意

在过滤器两边包含单引号，以便 shell 不会对其进行解释。

12. 当所有客户端和用户的迁移完成后，请停用 LDAP 目录。

验证

1. 使用 **ipa user-add** 命令来在 IdM 中创建测试用户。将迁移的用户的输出与测试用户的输出进行比较。确保迁移的用户包含测试用户上存在的最小属性和对象类集合。例如：

```
$ ipa user-show --all testing_user
dn: uid=testing_user,cn=users,cn=accounts,dc=idm,dc=example,dc=com
User login: testing_user
First name: testing
Last name: user
Full name: testing user
Display name: testing user
Initials: tu
Home directory: /home/testing_user
GECOS: testing user
Login shell: /bin/sh
Principal name: testing_user@IDM.EXAMPLE.COM
Principal alias: testing_user@IDM.EXAMPLE.COM
Email address: testing_user@idm.example.com
UID: 1689700012
GID: 1689700012
Account disabled: False
Preserved user: False
Password: False
Member of groups: ipausers
Kerberos keys available: False
ipauniqueid: 843b1ac8-6e38-11ec-8dfe-5254005aad3e
mepmanagedentry: cn=testing_user,cn=groups,cn=accounts,dc=idm,dc=example,dc=com
objectclass: top, person, organizationalperson, inetorgperson, inetuser, posixaccount,
krbprincipalaux, krbticketpolicyaux, ipaobject,
        ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry
```

2. 将迁移的用户的输出（如 IdM 上所示）与源用户进行比较，如原始 LDAP 服务器上所示。确保导入的属性不会复制两次，并且它们具有正确的值。

其他资源

- 通过 SSL 从 LDAP 迁移到 IdM

4.7. 通过 SSL 从 LDAP 迁移到 IDM

您可以使用 **ipa migrate-ds** 命令将身份验证和授权服务从 LDAP 服务器迁移到身份管理(IdM)。按照以下流程加密迁移过程中传输的数据。

警告

这是一个通用的迁移流程，可能在每个环境中不一定能正常工作。

强烈建议您在尝试迁移真实的 LDAP 环境前设置测试 LDAP 环境并测试迁移过程。在测试环境时，请执行以下操作：

1. 在 IdM 中创建测试用户，并将迁移的用户的输出与测试用户的输出进行比较。
2. 将迁移的用户的输出（如 IdM 上所示）与源用户进行比较，如原始 LDAP 服务器上所示。

有关更多的指导，请参见下面的 **验证** 部分。

先决条件

- 有 LDAP 目录的管理员特权。
- 如果已安装 IdM，则您有 IdM 的管理员权限。
- 您以 **root** 身份登录到要在其上执行以下流程的 RHEL 系统。
- 您已阅读并理解了以下章节：
  - 从 LDAP 迁移到 IdM 时的注意事项。
  - 在从 LDAP 迁移到 IdM 时规划客户端配置。
  - 从 LDAP 迁移到 IdM 时规划密码迁移。
  - 进一步的迁移注意事项和要求。
  - 自定义从 LDAP 到 IdM 的迁移。

步骤

1. 将签发远程 LDAP 服务器证书的 CA 证书存储在未来 IdM 服务器的文件中。例如：**/tmp/remote.crt**。

2. 按照将 将 LDAP 服务器迁移到 IdM 中描述的步骤操作。但是，对于在迁移过程中加密的 LDAP 连接，请使用 URL 中的 **ldaps** 协议，并将 **--ca-cert-file** 选项传给 **ipa migrate-ds** 命令。例如：

```
# ipa migrate-ds --ca-cert-file=/tmp/remote.crt --your-other-options
ldaps://ldap.example.com:636
```

验证

1. 使用 **ipa user-add** 命令来在 IdM 中创建测试用户。将迁移的用户的输出与测试用户的输出进行比较。确保迁移的用户包含测试用户上存在的最小属性和对象类集合。例如：

```
$ ipa user-show --all testing_user
dn: uid=testing_user,cn=users,cn=accounts,dc=idm,dc=example,dc=com
User login: testing_user
First name: testing
Last name: user
Full name: testing user
Display name: testing user
Initials: tu
Home directory: /home/testing_user
GECOS: testing user
Login shell: /bin/sh
Principal name: testing_user@IDM.EXAMPLE.COM
Principal alias: testing_user@IDM.EXAMPLE.COM
Email address: testing_user@idm.example.com
UID: 1689700012
GID: 1689700012
Account disabled: False
Preserved user: False
Password: False
Member of groups: ipausers
Kerberos keys available: False
ipauniqueid: 843b1ac8-6e38-11ec-8dfe-5254005aad3e
mepmanagedentry: cn=testing_user,cn=groups,cn=accounts,dc=idm,dc=example,dc=com
objectclass: top, person, organizationalperson, inetorgperson, inetuser, posixaccount,
krbprincipalaux, krbticketpolicyaux, ipaobject,
        ipasshuser, ipaSshGroupOfPubKeys, mepOriginEntry
```

2. 将迁移的用户的输出（如 IdM 上所示）与源用户进行比较，如原始 LDAP 服务器上所示。确保导入的属性不会复制两次，并且它们具有正确的值。