Red Hat Enterprise Linux 9

访问身份管理服务

登录到 IdM 并管理其服务

Last Updated: 2024-06-26

Red Hat Enterprise Linux 9 访问身份管理服务

登录到 IdM 并管理其服务

法律通告

摘要

在 Red Hat Identity Management (IdM)中执行管理任务前，您必须登录到该服务。当您使用命令行或 IdM Web UI 登录时，您可以在 IdM 中使用 Kerberos 和一次性密码作为身份验证方法。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

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

第 1 章 从命令行登录到身份管理

身份管理(IdM)使用 Kerberos 协议来支持单点登录。单点登录意味着用户仅输入一次正确的用户名和密码，就可以访问 IdM 服务，而无需系统再次提示输入凭证。

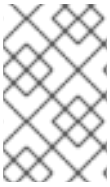
重要

在 IdM 中，系统安全服务守护进程(SSSD)在用户成功登录到带有相应 Kerberos 主体名的 IdM 客户端机器上的桌面环境后，会自动为用户获取票据授予票(TGT)。这意味着登录后，用户不需要使用 **kinit** 工具来访问 IdM 资源。

如果您已清除 Kerberos 凭证缓存或者 Kerberos TGT 已过期，您需要手动请求 Kerberos ticket 以访问 IdM 资源。以下章节介绍了在 IdM 中使用 Kerberos 的基本用户操作。

1.1. 使用 KINIT 手动登录到 IDM

按照以下流程，使用 **kinit** 工具手动向身份管理(IdM)环境进行身份验证。**kinit** 工具代表 IdM 用户获取并缓存 Kerberos 票据授予票(TGT)。



注意

只有在初始 Kerberos TGT 被销毁了或者过期了，才使用这个流程。作为 IdM 用户，当登录到本地机器时，您也会自动登录到 IdM。这意味着登录后，您不需要使用 **kinit** 工具来访问 IdM 资源。

流程

1. 要登录到 IdM

   - 在当前登录到本地系统的用户的用户名下，使用 **kinit**，而不指定用户名。例如，如果您在本地系统中以 **example_user** 身份登录：

     ```
     [example_user@server ~]$ kinit
     Password for example_user@EXAMPLE.COM:
     [example_user@server ~]$
     ```

     如果本地用户的用户名与 IdM 中的任何用户条目都不匹配，则身份验证尝试失败：

     ```
     [example_user@server ~]$ kinit
     kinit: Client 'example_user@EXAMPLE.COM' not found in Kerberos database while
     getting initial credentials
     ```

   - 使用不对应于本地用户名的 Kerberos 主体，将所需的用户名传给 **kinit** 工具。例如，要以 **admin** 用户身份登录：

     ```
     [example_user@server ~]$ kinit admin
     Password for admin@EXAMPLE.COM:
     [example_user@server ~]$
     ```

2. 另外，要验证登录是否成功，请使用 **klist** 工具来显示缓存的 TGT。在以下示例中，缓存包含了 **example_user** 主体的票，这意味着在这个特定的主机上，当前只允许 **example_user** 访问 IdM 服务：

```
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: example_user@EXAMPLE.COM

Valid starting     Expires            Service principal
11/10/2019 08:35:45  11/10/2019 18:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

1.2. 销毁用户的活动的 KERBEROS 票

按照以下流程清除包含用户的活跃 Kerberos 票据的凭证缓存。

流程

1. 销毁您的 Kerberos 票：

```
[example_user@server ~]$ kdestroy
```

2. （可选）检查 Kerberos 票是否已被销毁：

```
[example_user@server ~]$ klist
klist: Credentials cache keyring 'persistent:0:0' not found
```

1.3. 为 KERBEROS 身份验证配置外部系统

按照以下流程配置外部系统，以便身份管理(IdM)用户可以使用他们的 Kerberos 凭证从外部系统登录到 IdM。

当您的基础架构包含多个域或重叠域时，在外部系统上启用 Kerberos 身份验证非常有用。如果系统尚未通过 **ipa-client-install** 注册到任何 IdM 域，它也很有用。

要从不属于 IdM 域成员的系统启用对 IdM 的 Kerberos 身份验证，请在外部系统上定义特定于 IdM 的 Kerberos 配置文件。

先决条件

- **krb5-workstation** 软件包已安装在外部系统上。
  要查找是否安装了该软件包，请使用以下 CLI 命令：

```
# dnf list installed krb5-workstation
Installed Packages
krb5-workstation.x86_64    1.16.1-19.el8     @BaseOS
```

流程

1. 将 **/etc/krb5.conf** 文件从 IdM 服务器复制到外部系统。例如：

```
# scp /etc/krb5.conf root@externalsystem.example.com:/etc/krb5_ipa.conf
```

警告

不要覆盖外部系统上现有的 **krb5.conf** 文件。

2. 在外部系统上，将终端会话设置为使用复制的 IdM Kerberos 配置文件：

```
$ export KRB5_CONFIG=/etc/krb5_ipa.conf
```

KRB5_CONFIG 变量仅在退出之前暂时存在。要防止其丢失，请使用其他文件名导出变量。

3. 将 Kerberos 配置代码段从 **/etc/krb5.conf.d/** 目录复制到外部系统。

外部系统上的用户现在可以使用 **kinit** 工具对 IdM 服务器进行身份验证。

1.4. 其它资源

- **krb5.conf(5)** 手册页。
- **kinit(1)** 手册页。
- **klist(1)** 手册页。
- **kdestroy(1)** 手册页。

第 2 章 查看、启动和停止身份管理服务

身份管理(IdM)服务器是作为域控制器(DC)的 Red Hat Enterprise Linux 系统。很多不同的服务在 IdM 服务器上运行，最重要的是目录服务器、证书颁发机构(CA)、DNS 和 Kerberos。

2.1. IDM 服务

有许多不同服务可以在 IdM 服务器和客户端上安装并运行。

IdM 服务器托管的服务列表

以下大多数服务并没严格要求安装到 IdM 服务器上。例如，您可以在 IdM 域外的外部服务器上安装诸如证书颁发机构(CA)或 DNS 服务器等服务。

Kerberos

krb5kdc 和 **kadmin** 服务

IdM 使用 **Kerberos** 协议来支持单点登录。使用 Kerberos，用户只需提供一次正确的用户名和密码，就可以访问 IdM 服务，而系统不需要再次提示输入凭证。

Kerberos 分为两部分：

- **krb5kdc** 服务是 Kerberos 身份验证服务和密钥分发中心(KDC)守护进程。
- **kadmin** 服务是 Kerberos 数据库管理程序。

有关如何在 IdM 中使用 Kerberos 进行身份验证的详情，请参考 从命令行登录到身份管理 和 在 Web UI 中登录到 IdM：使用 Kerberos 票据。

LDAP 目录服务器

dirsrv 服务

IdM **LDAP 目录服务器** 实例存储所有 IdM 信息，例如，与 Kerberos、用户帐户、主机条目、服务、策略、DNS 等相关的信息。LDAP 目录服务器实例基于与 红帽目录服务器 相同的技术。但是，它被调优为特定于 IdM 的任务。

证书颁发机构

pki-tomcatd 服务

集成的 **证书颁发机构(CA)** 基于与 与红帽证书系统 相同的技术。**pki** 是用于访问证书系统服务的命令行界面。

如果您单独创建并提供了所有必需的证书，则您还可以安装没有集成 CA 的服务器。

如需更多信息，请参阅 规划您的 CA 服务。

域名系统(DNS)

named 服务

IdM 使用 **DNS** 进行动态服务发现。IdM 客户端安装工具可使用 DNS 的信息来自动配置客户端机器。客户端注册到 IdM 域后，它使用 DNS 来定位域中的 IdM 服务器和服务。Red Hat Enterprise Linux 中的 DNS（域名系统）协议的 **BIND** （Berkeley 互联网名称域）实现包括 **命名的** DNS 服务器。**named-pkcs11** 是使用对 PKCS#11 加密标准的原生支持构建的 BIND DNS 服务器版本。

如需更多信息，请参阅 规划 DNS 服务和主机名。

Apache HTTP 服务器

httpd 服务

Apache HTTP Web 服务器提供了 IdM Web UI，还管理证书颁发机构和其他 IdM 服务之间的通信。

Samba/ Winbind

SMB 和 **winbind** 服务

Samba 在 Red Hat Enterprise Linux 中实现了服务器消息块(SMB)协议，也称为通用互联网文件系统(CIFS)协议。通过 smb 服务，SMB 协议可让您访问服务器上的资源，如文件共享和共享打印机。如果您使用活动目录(AD)环境配置了信任，'Winbind' 服务将管理 IdM 服务器和 AD 服务器之间的通信。

一次性密码(OTP)验证

ipa-otpd 服务

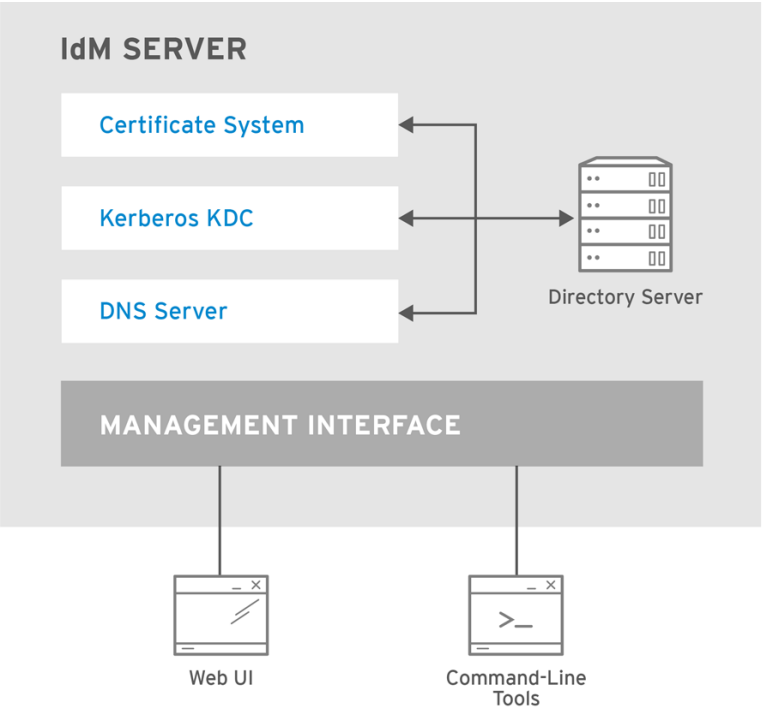
一次性密码(OTP)是由身份验证令牌为一个会话生成的密码，作为双因素身份验证的一部分。OTP 身份验证在 Red Hat Enterprise Linux 中是通过 **ipa-otpd** 服务实现的。

如需更多信息，请参阅 使用一次性密码登录到身份管理 Web UI。

OpenDNSSEC

ipa-dnskeysyncd 服务

OpenDNSSEC 是一个 DNS 管理器，自动化了跟踪 DNS 安全扩展(DNSSEC)密钥和区域签名的过程。**ipa-dnskeysyncd** 服务管理 IdM 目录服务器和 OpenDNSSEC 之间的同步。



IdM 客户端托管的服务列表

- **系统安全服务守护进程** ：**sssd** 服务

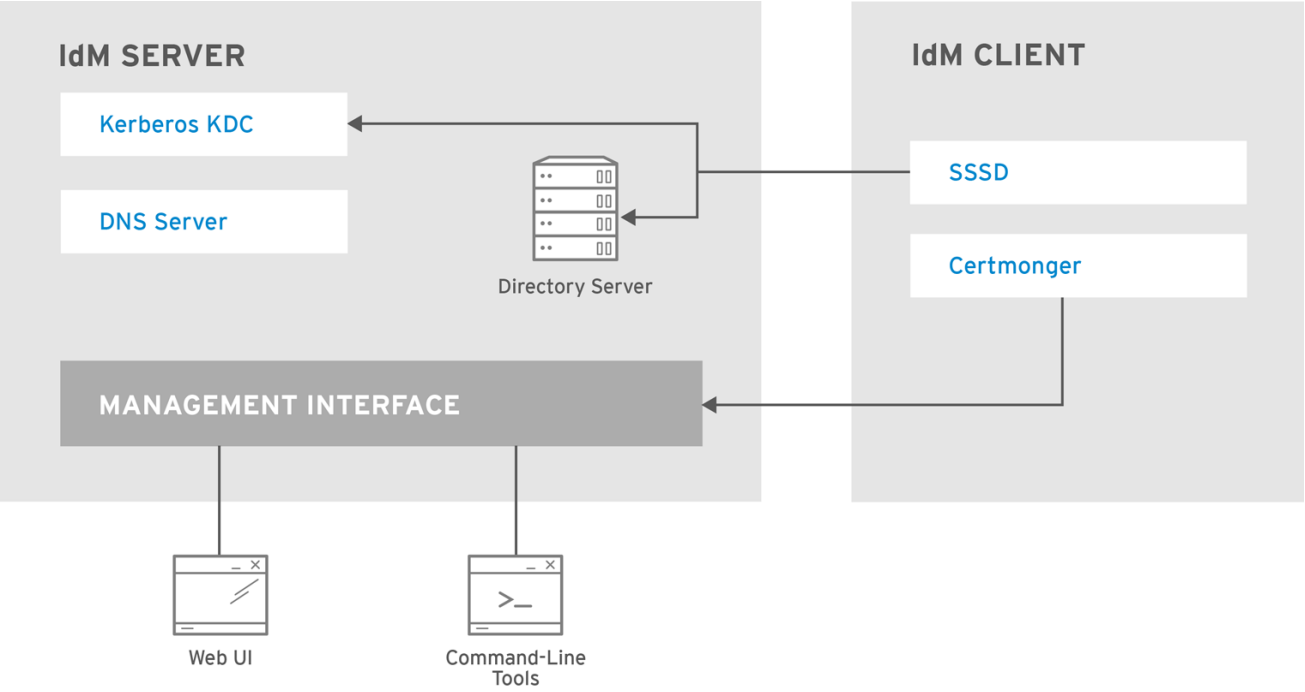
系统安全服务守护进程 (SSSD)是客户端应用程序，其管理用户身份验证和缓存凭据。缓存可让本地系统在 IdM 服务器不可用或客户端离线时能够继续正常的身份验证操作。

如需更多信息，请参阅了解 SSSD 及其优势。

- Certmonger ：**certmonger** 服务

certmonger 服务监控并更新客户端上的证书。它可以为系统上的服务请求新的证书。

如需更多信息，请参阅 使用 certmonger 为服务获取 IdM 证书 。

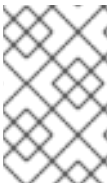


2.2. 查看 IDM 服务的状态

要查看 IdM 服务器上配置的 IdM 服务的状态，请运行 **ipactl status** 命令：

```
[root@server ~]# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
pki-tomcatd Service: RUNNING
smb Service: RUNNING
winbind Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

服务器上 **ipactl status** 命令的结果取决于您的 IdM 配置。例如，如果 IdM 部署不包含 DNS 服务器，则 **named** 服务不会出现在列表中。



注意

您不能使用 IdM Web UI 来查看在特定 IdM 服务器上运行的所有 IdM 服务的状态。可以在 IdM Web UI 的 **Identity → Services** 选项卡中查看在不同服务器上运行的 Kerberized 服务。

您可以启动或停止整个服务器，或仅单个服务。

要启动、停止或重启整个 IdM 服务器，请参阅：

- 启动和停止整个身份管理服务器

要启动、停止或重启单个 IdM 服务，请参阅：

- 启动和停止单个身份管理服务

要显示 IdM 软件的版本，请参阅：

- 显示 IdM 软件版本的方法

2.3. 启动和停止整个身份管理服务器

使用 **ipa** systemd 服务停止、启动或重启整个 IdM 服务器以及所有安装的服务。使用 **systemctl** 工具控制 **ipa** systemd 服务，确保所有服务都以适当的顺序停止、启动或重启。**ipa** systemd 服务也会在启动 IdM 服务之前升级 RHEL IdM 配置，并在管理 IdM 服务时使用合适的 SELinux 上下文。您不需要有一个有效的 Kerberos 票据来运行 **systemctl ipa** 命令。

ipa systemd 服务命令

启动整个 IdM 服务器：

```
# systemctl start ipa
```

停止整个 IdM 服务器：

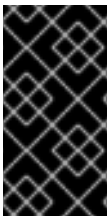
```
# systemctl stop ipa
```

重启整个 IdM 服务器：

```
# systemctl restart ipa
```

要显示组成 IdM 的所有服务的状态，请使用 **ipactl** 工具：

```
# ipactl status
```



重要

- 不要直接使用 **ipactl** 工具来启动、停止或重启 IdM 服务。使用 **systemctl ipa** 命令，其在可预测的环境中调用 **ipactl** 工具。
- 您不能使用 IdM Web UI 来执行 **ipactl** 命令。

2.4. 启动和停止单个身份管理服务

通常不建议手动更改 IdM 配置文件。然而，在某些情况下，需要管理员来执行特定服务的手动配置。在这种情况下，使用 **systemctl** 工具来停止、启动或重启单个 IdM 服务。

例如，自定义目录服务器行为，而不修改其他 IdM 服务后使用 **systemctl**：

```
# systemctl restart dirsrv@REALM-NAME.service
```

另外，在最初使用活动目录部署 IdM 信任时，请修改 **/etc/sssd/sssd.conf** 文件，并添加：

- 在远程服务器具有高延迟的环境中用来调整超时配置选项的特定参数
- 用于调整活动目录站点关联性的特定参数
- 覆盖某些不是由全局 IdM 设置提供的配置选项

要应用您在 **/etc/sssd/sssd.conf** 文件中所做的更改：

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

需要运行 **systemctl restart sssd.service**，因为系统安全服务守护进程(SSSD)不会自动重新读取或重新应用其配置。

请注意，对于影响 IdM 身份范围的更改，建议完全重启服务器。

重要

要重启多个 IdM 域服务，请始终使用 **systemctl restart ipa**。由于与 IdM 服务器一起安装的服务之间的依赖关系，这些服务启动和停止的顺序至关重要。**ipa** systemd 服务确保服务以适当的顺序启动和停止。

有用的 systemctl 命令

要启动特定的 IdM 服务：

```
# systemctl start name.service
```

要停止特定的 IdM 服务：

```
# systemctl stop name.service
```

要重启特定的 IdM 服务：

```
# systemctl restart name.service
```

要查看特定的 IdM 服务的状态：

```
# systemctl status name.service
```

重要

您不能使用 IdM Web UI 来启动或停止在 IdM 服务器上运行的单个服务。您只能使用 Web UI 来修改 Kerberized 服务的设置，方法是导航到 **Identity → Services**，并选择服务。

其它资源

- 启动和停止整个身份管理服务器

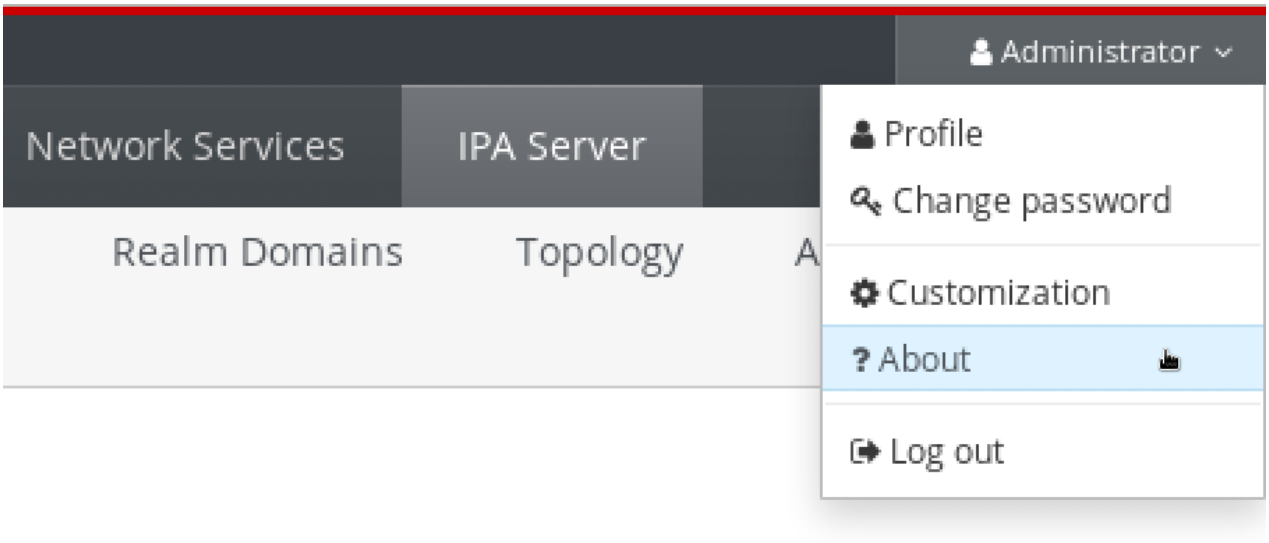
2.5. 显示 IDM 软件版本的方法

您可以使用以下命令显示 IdM 版本号：

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

通过 WebUI 显示版本

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



使用 ipa 命令显示版本

在命令行中使用 **ipa --version** 命令。

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

使用 rpm 命令显示版本

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

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

第 3 章 IDM 命令行工具简介

了解有关使用身份管理(IdM)命令行工具的基础知识。

先决条件

- 已安装并可访问 IdM 服务器。
  详情请参阅 安装身份管理。
- 要使用 IPA 命令行界面，请通过有效的 Kerberos 票据向 IdM 进行身份验证。

3.1. 什么是 IPA 命令行界面

IPA 命令行界面(CLI)是身份管理(IdM)管理的基本命令行界面。

它支持很多管理 IdM 的子命令，如 **ipa user-add** 命令来添加新用户。

IPA CLI 允许您：

- 在网络中添加、管理或删除用户、组、主机和其他对象。
- 管理证书。
- 搜索条目。
- 显示和列出对象。
- 设置访问权限。
- 获取正确命令语法的帮助。

3.2. IPA 帮助是什么

IPA 帮助是 IdM 服务器的内置文档系统。

IPA 命令行界面(CLI)从加载的 IdM 插件模块中生成可用的帮助主题。要使用 IPA 帮助工具，您必须：

- IdM 服务器已安装并运行。
- 使用有效的 Kerberos 票据进行了身份验证。

输入没有选项的 **ipa help** 命令会显示有关基本帮助用法和最常见的命令示例的信息。

您可以对不同的 **ipa help** 用例使用以下选项：

```
$ ipa help [TOPIC | COMMAND | topics | commands]
```

- **[]** - 方括号表示所有参数都是可选的，您可以只写 **ipa help**，命令就可执行。
- | - 管道符表示 **或** 。因此，您可以使用基本的 **ipa help** 命令指定 **TOPIC**、**COMMAND** 或 **topics**、**commands** ：
  - **topics** – 您可以运行命令 **ipa help topics** 来显示 IPA 帮助涵盖的主题列表，如 **user**、**cert**、**server** 等。

- **TOPIC** – 大写字母的 TOPIC 是一个变量。因此，您可以指定一个特定的主题，例如 **ipa help user**。
- **commands** – 您可以输入命令 **ipa help commands** 来显示 IPA 帮助所涵盖的命令列表，如 **user-add**、**ca-enable**、**server-show** 等。
- **COMMAND** – 大写字母的 COMMAND 是一个变量。因此，您可以指定一个的命令，例如 **ipa help user-add**。

3.3. 使用 IPA 帮助主题

以下流程描述了如何在命令行界面中使用 IPA 帮助。

流程

1. 打开一个终端，接到 IdM 服务器。
2. 输入 **ipa help topics** 来显示帮助所涵盖的主题列表。

```
$ ipa help topics
```

3. 选择其中一个主题，按照以下模式创建一个命令： **ipa help *[topic_name]***。添加在上一步中列出的主题之一，而不是 **topic_name** 字符串。
在这个示例中，我们使用以下主题：**user**

```
$ ipa help user
```

4. 如果 IPA 帮助输出太长，您不能整个文本，请用以下语法：

```
$ ipa help user | less
```

然后您可以向下滚动，并阅读全部帮助。

IPA CLI 显示 **user** 主题的帮助页。阅读完概述后，您可以看到许多使用主题命令的模式示例。

3.4. 使用 IPA HELP 命令

以下流程描述了如何在命令行界面中创建 IPA 帮助命令。

流程

1. 打开一个终端，接到 IdM 服务器。
2. 输入 **ipa help commands** 来显示 help 所涵盖的命令列表。

```
$ ipa help commands
```

3. 选择一个命令，并按照下模式创建一个help 命令： **ipa help *<COMMAND>***。添加在上一步中列出的其中一个命令，而不是 **<COMMAND>** 字符串。

```
$ ipa help user-add
```

其它资源

- **ipa** 手册页。

3.5. IPA 命令的结构

IPA CLI 区分以下命令类型：

- **内置命令** – IdM 服务器中可用的内置命令。
- **插件提供的命令**

IPA 命令的结构允许您管理各种类型的对象。例如：

- 用户，
- 主机、
- DNS 记录、
- 证书、

以及许多其他信息。

对于大多数这些对象，IPA CLI 包括以下命令来：

- 添加（**add**）
- 修改(**mod**)
- 删除(**del**)
- 搜索（**find**）
- 显示（**show**）

命令具有以下结构：

ipa user-add, **ipa user-mod**, **ipa user-del**, **ipa user-find**, **ipa user-show**

ipa host-add, **ipa host-mod**, **ipa host-del**, **ipa host-find**, **ipa host-show**

ipa dnsrecord-add, **ipa dnsrecord-mod**, **ipa dnsrecord-del**, **ipa dnsrecord-find**, **ipa dnrecord-show**

您可以使用 **ipa user-add [options]** 创建用户，其中 **[options]** 是可选的。如果您只使用 **ipa user-add** 命令，脚本将逐个询问您详细信息。

要更改现有对象，您需要定义对象，因此命令还包括一个对象：**ipa user-mod USER_NAME [options]**。

3.6. 使用 IPA 命令将用户帐户添加到 IDM

以下流程描述了如何使用命令行向身份管理(IdM)数据库添加一个新用户。

先决条件

- 您需要拥有管理员特权才能将用户帐户添加到 IdM 服务器。

流程

1. 打开一个终端，接到 IdM 服务器。
2. 输入命令来添加新用户：

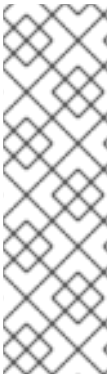
```
$ ipa user-add
```

命令运行一个脚本，提示您提供创建用户帐户所需的基本数据。

3. 在 **First name:** 字段中，输入新用户的名字，然后按 **Enter** 键。
4. 在 **Last name:** 字段中，输入新用户的姓氏，然后按 **Enter** 键。
5. 在 **User login [suggested user name]:**输入用户名，或者只是按 **Enter** 键来接受推荐的用户名。
整个 IdM 数据库的用户名必须是唯一的。如果因为用户名已存在而发生错误，使用 **ipa user-add** 命令重复该过程，并使用不同的、唯一的用户名。

添加用户名后，用户帐户被添加到 IdM 数据库，IPA 命令行界面(CLI)会打印以下输出：

```
----------------------
Added user "euser"
----------------------
User login: euser
First name: Example
Last name: User
Full name: Example User
Display name: Example User
Initials: EU
Home directory: /home/euser
GECOS: Example User
Login shell: /bin/sh
Principal name: euser@IDM.EXAMPLE.COM
Principal alias: euser@IDM.EXAMPLE.COM
Email address: euser@idm.example.com
UID: 427200006
GID: 427200006
Password: False
Member of groups: ipausers
Kerberos keys available: False
```



注意

默认情况下，没有为用户帐户设置用户密码。要在创建用户帐户时添加密码，请使用带有以下语法的 **ipa user-add** 命令：

```
$ ipa user-add --first=Example --last=User --password
```

然后 IPA CLI 会提示您添加或确认用户名和密码。

如果已创建了该用户，您可以使用 **ipa user-mod** 命令添加密码。

其它资源

- 运行 **ipa help user-add** 命令来了解有关参数的更多信息。

3.7. 使用 IPA 命令修改 IDM 中的用户帐户

您可以为每个用户帐户更改多个参数。例如，您可以为用户添加新密码。

基本命令语法与 **user-add** 语法不同，因为您需要定义要对其执行更改的现有用户帐户，例如，添加密码。

先决条件

- 您需要具有管理员特权才能修改用户帐户。

流程

1. 打开一个终端，接到 IdM 服务器。
2. 输入 **ipa user-mod** 命令，指定要修改的用户，以及任何选项，如添加密码的 **--password** ：

```
$ ipa user-mod euser --password
```

命令将运行脚本，您可以在其中添加新密码。

3. 输入新密码并按 **Enter** 键。

IPA CLI 打印以下输出：

```
----------------------
Modified user "euser"
----------------------
User login: euser
First name: Example
Last name: User
Home directory: /home/euser
Principal name: euser@IDM.EXAMPLE.COM
Principal alias: euser@IDM.EXAMPLE.COM
Email address: euser@idm.example.com
UID: 427200006
GID: 427200006
Password: True
Member of groups: ipausers
Kerberos keys available: True
```

现在，为帐户设置了用户密码，用户可以登录 IdM 了。

其它资源

- 运行 **ipa help user-mod** 命令来了解有关参数的更多信息。

3.8. 如何为 IDM 工具提供值列表

身份管理(IdM)将多值属性的值存储在列表中。

IdM 支持以下提供多值列表的方法：

- 在同一命令调用中多次使用相同的命令行参数：

```
$ ipa permission-add --right=read --permissions=write --permissions=delete ...
```

- 或者，您可以将列表用大括号括起来，在这种情况下，shell 执行展开：

```
$ ipa permission-add --right={read,write,delete} ...
```

上面的示例显示了命令 **permission-add**，它为对象添加权限。示例中没有提及对象。需要添加要为其添加权限的对象，而不是 **...**。

当您从命令行更新此类多值属性时，IdM 会使用新列表完全覆盖以前的值列表。因此，当更新多值属性时，您必须指定整个新列表，而不只是您要添加的单个值。

例如，在以上命令中，权限列表包括读、写和删除。当您决定使用 **permission-mod** 命令更新列表时，您必须添加所有的值，否则未提及的值将被删除。

示例 1: -ipa permission-mod 命令更新所有以前添加的权限。

```
$ ipa permission-mod --right=read --right=write --right=delete ...
```

或者

```
$ ipa permission-mod --right={read,write,delete} ...
```

示例 2 - ipa permission-mod 命令会删除 **--right=delete** 参数，因为它没有包含在命令中：

```
$ ipa permission-mod --right=read --right=write ...
```

或者

```
$ ipa permission-mod --right={read,write} ...
```

3.9. 如何在 IDM 工具中使用特殊字符

将包含特殊字符的命令行参数传递给 **ipa** 命令时，请使用反斜杠(\)转义这些字符。例如，常见的特殊字符包括尖括号（< 和 >）、and(&)、星号(*)或竖线(|)。

例如，要转义星号(*)：

```
$ ipa certprofile-show certificate_profile --out=exported\*profile.cfg
```

包含未转义特殊字符的命令无法按预期工作，因为 shell 无法正确解析这些字符。

第 4 章 从命令行搜索身份管理条目

以下章节描述了如何使用 IPA 命令，其可帮助您查找或显示对象。

4.1. 列出 IDM 条目的概述

您可以使用 **ipa *-find** 命令帮助您搜索特定类型的 IdM 条目。

要列出所有 **find** 命令，请使用以下 ipa help 命令：

```
$ ipa help commands | grep find
```

您可能需要检查特定的用户是否包含在 IdM 数据库中。然后您可以使用以下命令列出所有用户：

```
$ ipa user-find
```

要列出其指定属性包含关键字的用户组：

```
$ ipa group-find keyword
```

例如，**ipa group-find *admin*** 命令列出了其名称或描述包含字符串 **admin** 的所有组：

```
----------------
3 groups matched
----------------
  Group name: admins
  Description: Account administrators group
  GID: 427200002

  Group name: editors
  Description: Limited admins who can edit other users
  GID: 427200002

  Group name: trust admins
  Description: Trusts administrators group
```

在搜索用户组时，您还可以将搜索结果限制为包含特定用户的组：

```
$ ipa group-find --user=user_name
```

搜索不包含特定用户的组：

```
$ ipa group-find --no-user=user_name
```

4.2. 显示特定条目的详情

使用 **ipa *-show** 命令显示特定 IdM 条目的详情。

流程

- 要显示名为 *server.example.com* 的主机的详情：

```
$ ipa host-show server.example.com

Host name: server.example.com
Principal name: host/server.example.com@EXAMPLE.COM
...
```

4.3. 调整搜索大小和时间限制

有些查询（比如请求 IdM 用户列表）可能会返回大量条目。通过调优这些搜索操作，您可以在运行 **ipa *-find** 命令时提高服务器的总体性能，例如 **ipa user-find**，并在 Web UI 中显示相应的列表。

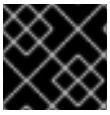
搜索大小限制

定义从客户端 CLI 发送发送到服务器的请求或从访问 IdM Web UI 的浏览器返回的最大条目数。
默认： 100 条目。

搜索时间限制

定义服务器等待搜索运行的最长时间（以秒为单位）。搜索达到这个限制后，服务器将停止搜索并返回该时间里发现的条目。
默认： 2 秒。

如果您将值设为 **-1**，IdM 在搜索时不会应用任何限制。



重要

如果设置的搜索大小或时间限制太大，则可能会对服务器性能造成负面影响。

4.3.1. 在命令行中调整搜索大小和时间限制

以下流程描述了在命令行中调整搜索大小和时间限制：

- 全局
- 对于一个特定条目

流程

1. 要在 CLI 中显示当前搜索时间和大小限制，请使用 **ipa config-show** 命令：

```
$ ipa config-show

Search time limit: 2
Search size limit: 100
```

2. 要为所有查询调整 **全局** 限制，请使用 **ipa config-mod** 命令，并添加 **--searchrecordslimit** 和 **--searchtimelimit** 选项。例如：

```
$ ipa config-mod --searchrecordslimit=500 --searchtimelimit=5
```

3. 要仅为特定查询 **暂时** 调整限制，请在命令中添加 **--sizelimit** 或 **--timelimit** 选项。例如：

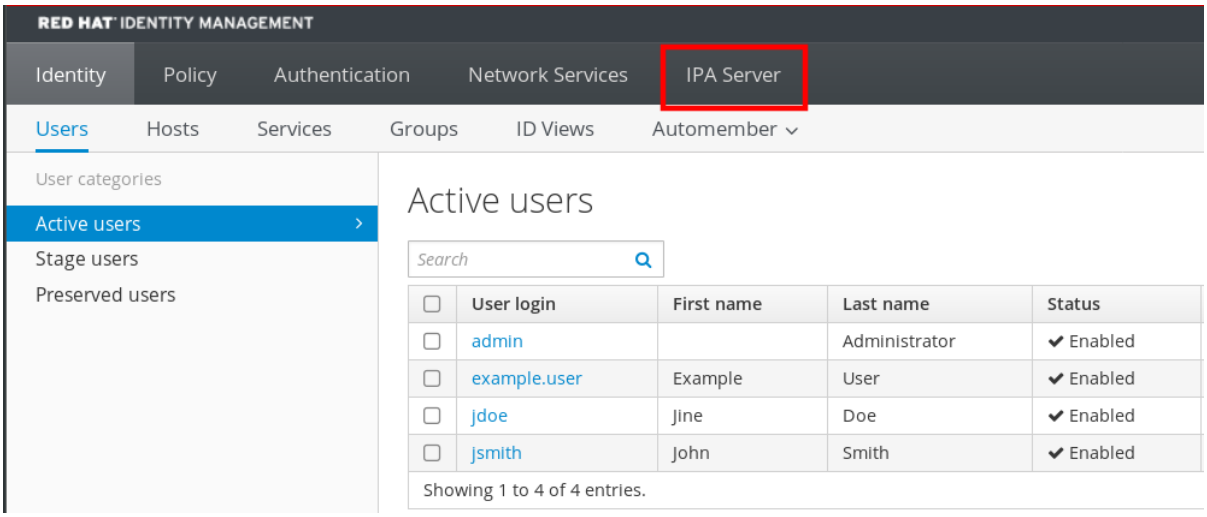
```
$ ipa user-find --sizelimit=200 --timelimit=120
```

4.3.2. 在 Web UI 中调整搜索大小和时间限制

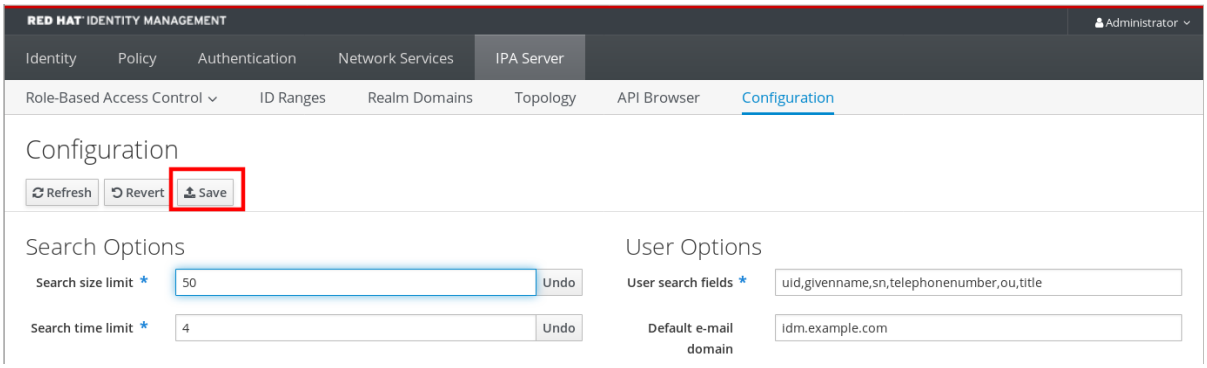
以下流程描述了在 IdM Web UI 中调整全局搜索大小和时间限制。

流程

1. 登录到 IdM Web UI。
2. 点 **IPA Server**。



3. 在 **IPA Server** 选项卡中点 **Configuration**。
4. 在**搜索选项**区域中设置所需的值。
   默认值为：
   - 搜索大小限制：100 个条目
   - 搜索时间限值：2 秒
5. 点页面顶部的 **Save**。



第 5 章 在 WEB 浏览器中访问 IDM WEB UI

IdM （身份管理）Web UI 是一个 IdM 管理的 Web 应用程序，是 IdM 命令行界面(CLI)的图形替代方案。

5.1. 什么是 IDM WEB UI

IdM （身份管理）Web UI 是一个 IdM 管理的 Web 应用程序。您可以以以下方式访问 IdM Web UI：

- **IdM 用户：** 有限的一组操作，具体取决于为 IdM 服务器中的用户授予的权限。基本上，活动的 IdM 用户可以登录 IdM 服务器，并配置他们自己的帐户。它们无法更改其他用户的设置或 IdM 服务器的设置。
- **管理员：** 对 IdM 服务器具有完整访问权限。
- **活动用户：** 一组操作，具体取决于授予用户的权限。活动目录用户现在可以是身份管理的管理员。详情请参阅 启用 AD 用户来管理 IdM。

5.2. 支持访问 WEB UI 的 WEB 浏览器

身份管理(IdM)支持以下浏览器来连接到 Web UI：

- Mozilla Firefox 38 及更新的版本
- Google Chrome 46 及更新的版本

注意

如果您的浏览器尝试使用 TLS v1.3，您可能会遇到使用智能卡访问 IdM Web UI 的问题。

```
[ssl:error] [pid 125757:tid 140436077168384] [client 999.999.999.999:99999] AH:
verify client post handshake
[ssl:error] [pid 125757:tid 140436077168384] [client 999.999.999.999:99999]
AH10158: cannot perform post-handshake authentication
[ssl:error] [pid 125757:tid 140436077168384] SSL Library Error: error:14268117:SSL
routines:SSL_verify_client_post_handshake:extension not received
```

这是因为，最新的浏览器版本没有默认启用 TLS Post-Handshake Authentication(PHA)，或者不支持 PHA。对于网站的一部分，PHA 只需要 TLS 客户端证书，比如使用智能卡验证访问 IdM Web UI 时。

要在 Mozilla Firefox 68 及更新的版本中解决这个问题，请启用 TLS PHA：

1. 在地址栏中输入 **about:config** 以访问 Mozilla Firefox 首选项菜单。
2. 在搜索栏中输入 **security.tls.enable_post_handshake_auth**。
3. 点击切换按钮将参数设为 true。

要解决 Chrome （其目前不支持 PHA）的问题，请禁用 TLS v1.3：

1. 打开 **/etc/httpd/conf.d/ssl.conf** 配置文件。
2. 将 **-TLSv1.3** 添加到 **SSLProtocol** 选项中：

```
SSLProtocol all -TLSv1 -TLSv1.1 -TLSv1.3
```

3. 重启 **httpd** 服务：

```
service httpd restart
```

请注意，IdM 管理 **ssl.conf** 文件，并可能会在软件包更新过程中覆盖其内容。在更新 IdM 软件包后验证自定义设置。

5.3. 访问 WEB UI

以下流程描述了首次使用密码登录到 IdM（身份管理）Web UI。

第一次登录后，您可以将 IdM 服务器配置为使用以下方式进行身份验证：

- Kerberos 票据
  详情请查看 身份管理中的 Kerberos 验证。
- 智能卡
  详情请参阅 为智能卡身份验证配置 IdM 服务器。
- 一次性密码(OTP) - 可将其与密码和 Kerberos 身份验证结合使用。
  详情请参阅 身份管理中的一次性密码(OTP)身份验证。

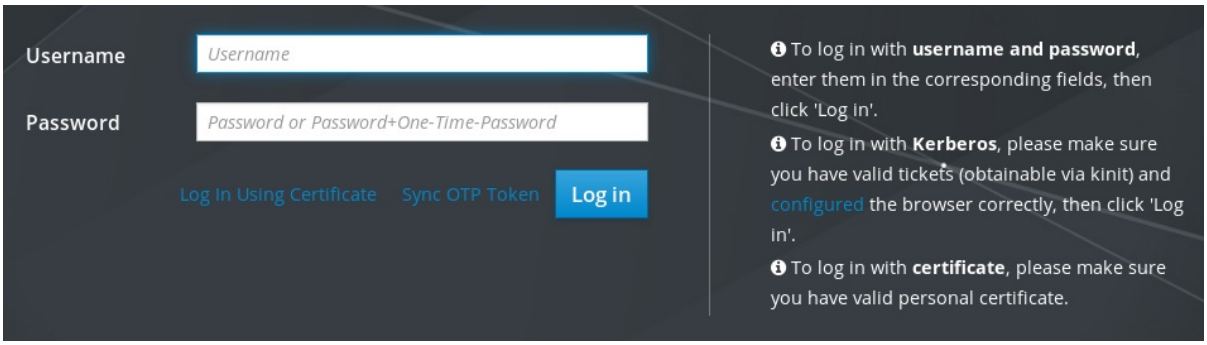
流程

1. 在浏览器地址栏中输入 IdM 服务器 URL。名称类似以下示例：

```
https://server.example.com
```

   您只需要将 **server.example.com** 更改为您 IdM 服务器的 DNS 名称。

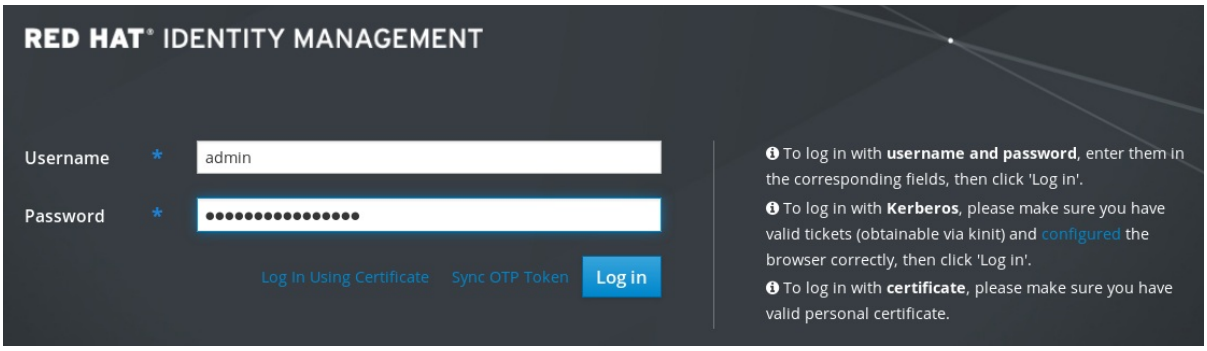
   这会在您的浏览器中打开 IdM Web UI 登录屏幕。



   - 如果服务器没有响应或者登录屏幕没有打开，请检查您要连接的 IdM 服务器上的 DNS 设置。
   - 如果您使用自签名证书，浏览器会发出警告。检查证书并接受安全例外以进行登录。为避免安全异常，请安装由证书颁发机构签名的证书。

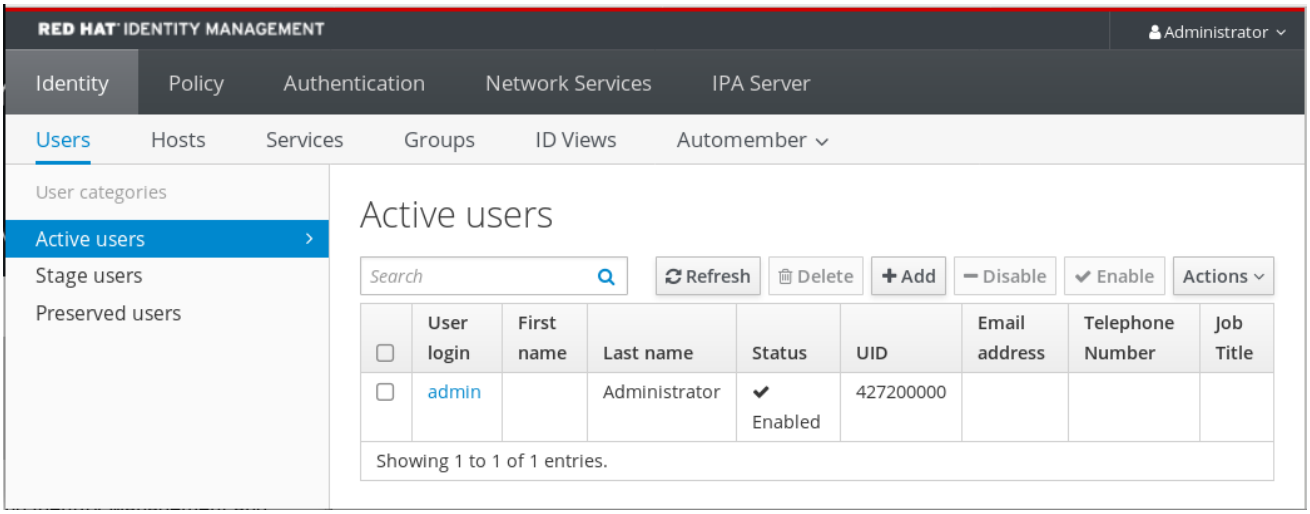
2. 在 Web UI 登录屏幕上，输入您在 IdM 服务器安装过程中添加的管理员帐户凭证。详情请参阅 安装身份管理服务器：带有集成 DNS 的，带有集成 CA 的。

   如果您已经进入到 IdM 服务器中，您还可以输入您的个人帐户凭证。



3. 单击 **Log in**。

登录成功后，您可以开始配置 IdM 服务器。


RED HAT IDENTITY MANAGEMENT
Administrator
Identity
Policy
Authentication
Network Services
IPA Server
Users
Hosts
Services
Groups
ID Views
Automember
User categories
Active users
Stage users
Preserved users
Active users
Search
Refresh
Delete
Add
Disable
Enable
Actions
User login
First name
Last name
Status
UID
Email address
Telephone Number
Job Title
admin
Administrator
Enabled
427200000
Showing 1 to 1 of 1 entries.

第 6 章 在 WEB UI 中登录到 IDM: 使用 KERBEROS 票据

了解更多有关如何配置您的环境，以使用 Kerberos 身份验证，使 Kerberos 能够登录到 IdM Web UI，并访问 IdM。

先决条件

- 在网络环境中已安装 IdM 服务器
  详情请参阅 在 Red Hat Enterprise Linux 9 中安装身份管理

6.1. 身份管理中的 KERBEROS 身份验证

身份管理(IdM)使用 Kerberos 协议来支持单点登录。单点登录身份验证允许您仅提供一次正确的用户名和密码，然后您就可以访问身份管理服务了，而系统不再提示输入凭据。

如果正确配置了 DNS 和证书设置，IdM 服务器会在安装后立即提供 Kerberos 身份验证。详情请参阅 安装身份管理。

要在主机上使用 Kerberos 身份验证，请安装：

- IdM 客户端
  详情请参阅 为身份管理客户端安装准备系统。
- krb5conf 软件包

6.2. 使用 KINIT 手动登录到 IDM

按照以下流程，使用 **kinit** 工具手动向身份管理(IdM)环境进行身份验证。**kinit** 工具代表 IdM 用户获取并缓存 Kerberos 票据授予票(TGT)。

注意

只有在初始 Kerberos TGT 被销毁了或者过期了，才使用这个流程。作为 IdM 用户，当登录到本地机器时，您也会自动登录到 IdM。这意味着登录后，您不需要使用 **kinit** 工具来访问 IdM 资源。

流程

1. 要登录到 IdM
   - 在当前登录到本地系统的用户的用户名下，使用 **kinit**，而不指定用户名。例如，如果您在本地系统中以 **example_user** 身份登录：

     ```
     [example_user@server ~]$ kinit
     Password for example_user@EXAMPLE.COM:
     [example_user@server ~]$
     ```

     如果本地用户的用户名与 IdM 中的任何用户条目都不匹配，则身份验证尝试失败：

     ```
     [example_user@server ~]$ kinit
     kinit: Client 'example_user@EXAMPLE.COM' not found in Kerberos database while
     getting initial credentials
     ```

- 使用不对应于本地用户名的 Kerberos 主体，将所需的用户名传给 **kinit** 工具。例如，要以 **admin** 用户身份登录：

```
[example_user@server ~]$ kinit admin
Password for admin@EXAMPLE.COM:
[example_user@server ~]$
```

2. 另外，要验证登录是否成功，请使用 **klist** 工具来显示缓存的 TGT。在以下示例中，缓存包含了 **example_user** 主体的票，这意味着在这个特定的主机上，当前只允许 **example_user** 访问 IdM 服务：

```
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: example_user@EXAMPLE.COM

Valid starting      Expires             Service principal
11/10/2019 08:35:45  11/10/2019 18:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

6.3. 为 KERBEROS 身份验证配置浏览器

要启用使用 Kerberos 票据的身份验证，您可能需要浏览器配置。

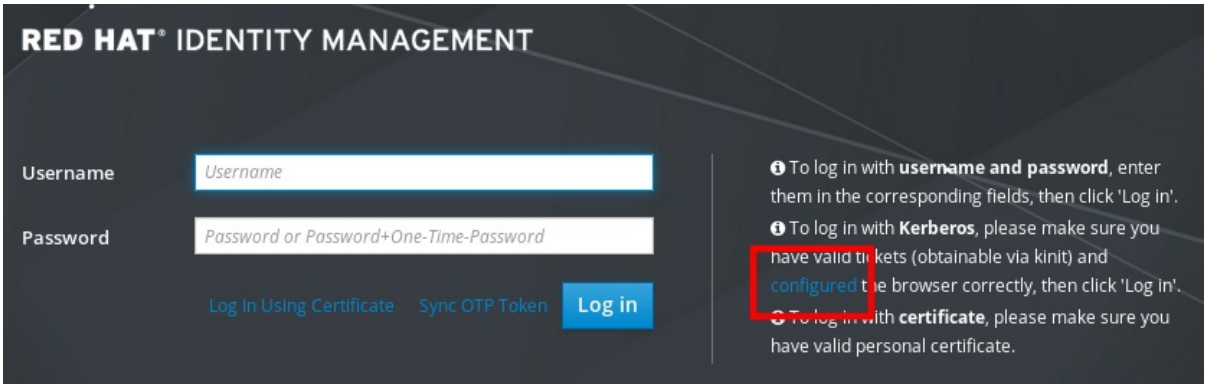
以下步骤可帮助您支持 Kerberos 协商以访问 IdM 域。

每个浏览器支持 Kerberos 的方式不同，并且需要不同的设置。IdM Web UI 包含对以下浏览器的指南：

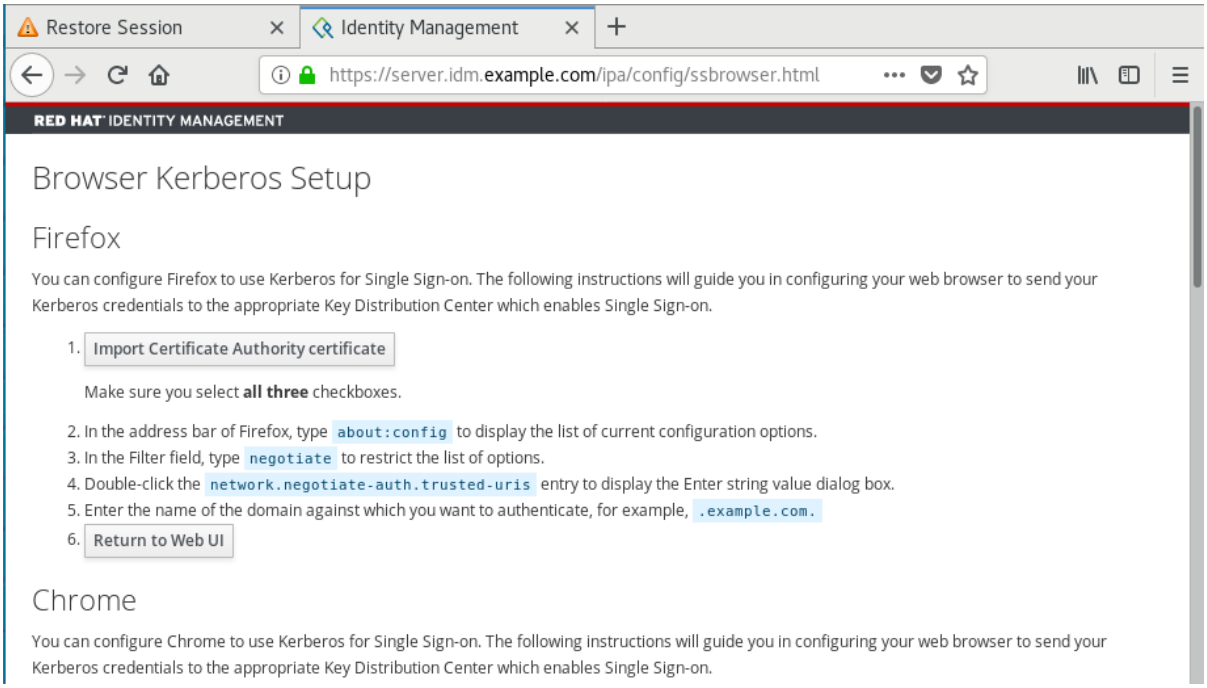
- Firefox
- Chrome

流程

1. 在 Web 浏览器中打开 IdM Web UI 登录对话框。
2. 在 Web UI 登录屏幕上，单击浏览器配置的链接。



3. 按照配置页面中的步骤进行操作。



设置完成后，切回到 IdM Web UI，并单击 **Log in**。

6.4. 使用 KERBEROS 票据登录到 WEB UI

按照以下流程，使用 Kerberos 票据授予票(TGT)登录到 IdM Web UI。

TGT 在预定义的时间过期。默认的时间间隔为 24 小时，您可以在 IdM Web UI 中更改它。

时间间隔过期后，您需要续订票据：

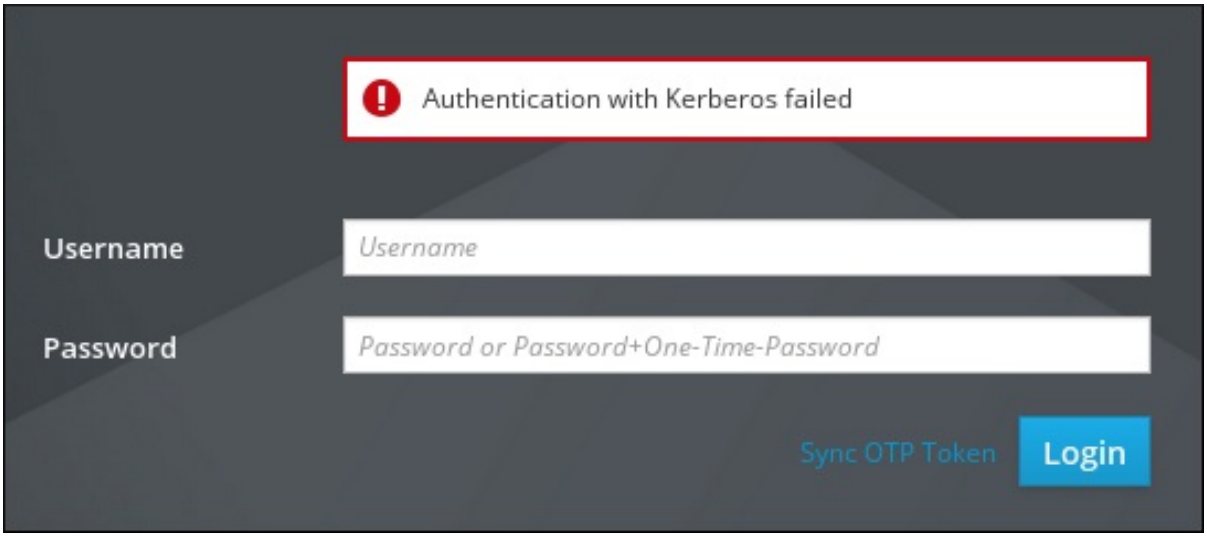
- 使用 kinit 命令。
- 在 Web UI 登录对话框中使用 IdM 登录凭据。

流程

- 打开 IdM Web UI。
  如果 Kerberos 身份验证正常工作，并且您拥有有效的票据，则将自动对您进行身份验证，并打开 Web UI。

  如果票据过期了，需要首先使用凭证进行身份验证。但是，下次 IdM Web UI 将自动打开，而不会打开登录对话框。

  如果您看到错误消息 **Authentication with Kerberos failed**，请验证您的浏览器是否已针对 Kerberos 身份验证进行了配置。请参阅 为 Kerberos 身份验证配置浏览器。



6.5. 为 KERBEROS 身份验证配置外部系统

按照以下流程配置外部系统，以便身份管理(IdM)用户可以使用他们的 Kerberos 凭证从外部系统登录到 IdM。

当您的基础架构包含多个域或重叠域时，在外部系统上启用 Kerberos 身份验证非常有用。如果系统尚未通过 **ipa-client-install** 注册到任何 IdM 域，它也很有用。

要从不属于 IdM 域成员的系统启用对 IdM 的 Kerberos 身份验证，请在外部系统上定义特定于 IdM 的 Kerberos 配置文件。

先决条件

- **krb5-workstation** 软件包已安装在外部系统上。
  要查找是否安装了该软件包，请使用以下 CLI 命令：

```
# dnf list installed krb5-workstation
Installed Packages
krb5-workstation.x86_64    1.16.1-19.el8    @BaseOS
```

流程

1. 将 **/etc/krb5.conf** 文件从 IdM 服务器复制到外部系统。例如：

```
# scp /etc/krb5.conf root@externalsystem.example.com:/etc/krb5_ipa.conf
```

> **警告**
>
> 不要覆盖外部系统上现有的 **krb5.conf** 文件。

2. 在外部系统上，将终端会话设置为使用复制的 IdM Kerberos 配置文件：

```
$ export KRB5_CONFIG=/etc/krb5_ipa.conf
```

-

KRB5_CONFIG 变量仅在退出之前暂时存在。要防止其丢失，请使用其他文件名导出变量。

3. 将 Kerberos 配置代码段从 **/etc/krb5.conf.d/** 目录复制到外部系统。
4. 在外部系统上配置浏览器，如 为 Kerberos 身份验证配置浏览器 中所述。

外部系统上的用户现在可以使用 **kinit** 工具对 IdM 服务器进行身份验证。

6.6. 活动目录用户的 WEB UI 登录

要为活动目录用户启用 Web UI 登录，请在 **Default Trust View** 中为每个活动目录用户定义一个 ID 覆盖。例如：

```
[admin@server ~]$ ipa idoverrideuser-add 'Default Trust View' ad_user@ad.example.com
```

其它资源

- 为活动目录用户使用 ID 视图

第 7 章 使用一次性密码登录到身份管理 WEB UI

可以通过多种方法保护对 IdM Web UI 的访问。最基本的一种是密码身份验证。

要提高密码身份验证的安全性，您可以添加第二个步骤，并需要自动生成的一次性密码(OTP)。最常见的用法是将与用户帐户连接的密码与由硬件或软件令牌生成的有时间限制的一次性密码结合起来。

以下章节可帮助到您：

- 了解 OTP 身份验证在 IdM 中的工作方式。
- 在 IdM 服务器上配置 OTP 身份验证。
- 为 IdM 中的 OTP 验证配置 RADIUS 服务器。
- 创建 OTP 令牌，并将它们与您电话中的 FreeOTP 应用程序同步。
- 使用用户密码和一次性密码的组合，向 IdM Web UI 进行身份验证。
- 在 Web UI 中重新同步令牌.
- 以 OTP 或 RADIUS 用户身份检索一个 IdM 票据授予票据

7.1. 先决条件

- 在 web 浏览器中访问 IdM Web UI

7.2. 身份管理中的一次性密码(OTP)身份验证

一次性密码可为您的身份验证安全性增加一步。身份验证使用您的密码 + 自动生成的一次性密码。

要生成一次性密码，您可以使用硬件或软件令牌。IdM 同时支持软件和硬件令牌。

身份管理支持以下两个标准的 OTP 机制：

- 基于 HMAC 的一次性密码(HOTP)算法是基于计数器的。HMAC 代表哈希消息身份验证代码。
- 基于时间的一次性密码(TOTP)算法是 HOTP 的扩展，来支持基于时间的移动因子。

重要

IdM 不支持活动目录信任用户的 OTP 登录。

7.3. 在 WEB UI 中启用一次性密码

身份管理(IdM)管理员可以全局或单独为 IdM 用户启用双因素身份验证(2FA)。用户在命令行或者 Web UI 登录对话框中的专用字段中的常规密码之后输入一次性密码(OTP)，在这些密码之间没有空格。

启用 2FA 与强制执行 2FA 不同。如果您使用基于 LDAP-binds 的登录，IdM 用户仍可以只通过输入密码来进行身份验证。但是，如果您使用基于 **krb5** 的登录，则强制使用 2FA。在以后的发行版本中，红帽计划为管理员提供一个选择以下内容之一的配置选项：

- 允许用户设置自己的令牌。在这种情况下，LDAP-binds 仍然不会强制执行 2FA，虽然基于 **krb5** 的登录会强制执行 2FA。

- 不允许用户设置自己的令牌。在这种情况下，在 LDAP-binds 和基于 **krb5** 的登录中都会强制执行 2FA。

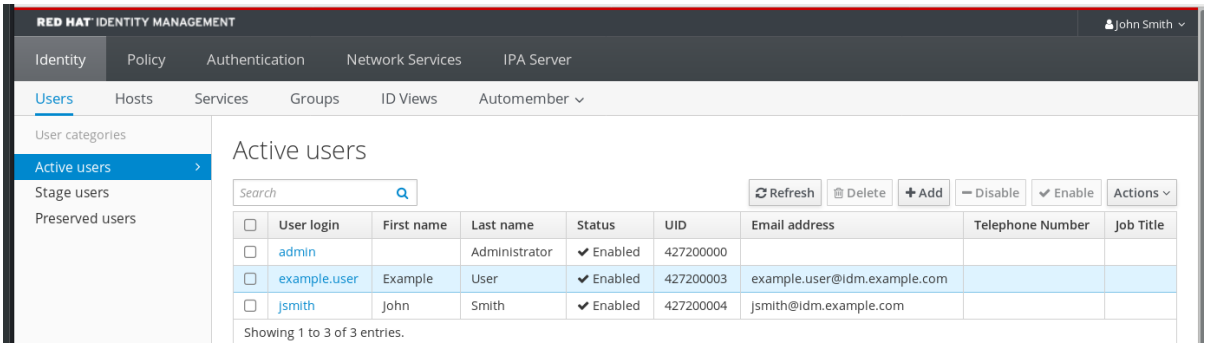
完成此流程，以使用 IdM Web UI 为单独的 **example.user** IdM 用户启用 2FA。

先决条件

- 管理特权

流程

1. 使用 IdM **admin** 权限登录到 IdM Web UI。
2. 打开 **Identity → Users → Active users**选项卡。



3. 选择 **example.user** 以打开用户设置。
4. 在 **User authentication types** 中，选择 **Two factor authentication (password + OTP)**。
5. 点击 **Save**。

此时，为 IdM 用户启用了 OTP 身份验证。

现在，您或 **example.user** 必须向 **example.user** 帐户分配一个新的令牌 ID。

7.4. 在 IDM 中为 OTP 验证配置 RADIUS 服务器

要启用从专有一次性密码(OTP)解决方案迁移到身份管理(IdM)原生的 OTP 解决方案的大型部署，IdM 提供了一种将 OTP 验证卸载到用户子集的第三方 RADIUS 服务器的方法。管理员创建一组 RADIUS 代理，其中每个代理只能引用一个 RADIUS 服务器。如果需要寻址多个服务器，建议创建一个指向多个 RADIUS 服务器的虚拟 IP 解决方案。

例如，此类解决方案必须在 **keepalived** 守护进程的帮助下，在 RHEL IdM 之外构建。然后，管理员将这些代理集中的一个分配给用户。只要用户分配了 RADIUS 代理集，IdM 就会绕过所有其他身份验证机制。

注意

IdM 不为第三方系统中的令牌提供任何令牌管理或同步支持。

完成流程，来为 OTP 验证配置 RADIUS 服务器，并将用户添加到代理服务器中：

先决条件

- radius 用户验证方法已启用。详情请参阅 在 Web UI 中启用一次性密码。

流程

1. 添加 RADIUS 代理：

```
$ ipa radiusproxy-add proxy_name --secret secret
```

命令提示您插入所需的信息。

RADIUS 代理的配置需要在客户端和服务器之间使用通用 secret 来包装凭证。在 **--secret** 参数中指定此 secret。

2. 将用户分配给添加的代理：

```
ipa user-mod radiususer --radius=proxy_name
```

3. 如果需要，配置要发送到 RADIUS 的用户名：

```
ipa user-mod radiususer --radius-username=radius_user
```

因此，RADIUS 代理服务器开始处理用户 OTP 身份验证。

当用户准备好迁移到 IdM 原生 OTP 系统时，您可以简单地删除用户的 RADIUS 代理分配。

7.4.1. 当在较慢的网络中运行 RADIUS 服务器时，更改 KDC 的超时值

在某些情况下，比如在较慢的网络中运行 RADIUS 代理，身份管理(IdM) Kerberos 分发中心(KDC)会在 RADIUS 服务器响应前关闭连接，因为在等待用户输入令牌时连接超时了。

要更改 KDC 的超时设置：

1. 更改 **/var/kerberos/krb5kdc/kdc.conf** 文件中 **[otp]** 部分中 **timeout** 参数的值。例如，要将超时设置为 **120** 秒：

```
[otp]
DEFAULT = {
  timeout = 120
  ...
}
```

2. 重启 **krb5kdc** 服务：

```
# systemctl restart krb5kdc
```

其他资源

- 如何在 FIPS 模式下配置 FreeRADIUS 身份验证 知识库文章

7.5. 在 WEB UI 中添加 OTP 令牌

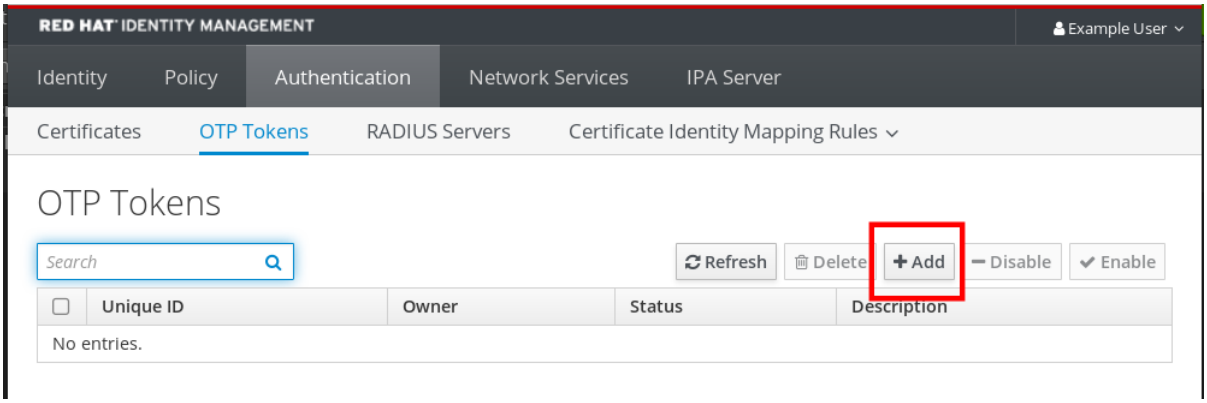
下面的章节帮助您将令牌添加到 IdM Web UI，以及您的软件令牌生成器中。

先决条件

- IdM 服务器上的活跃用户帐户。
- 管理员已在 IdM Web UI 中为特定用户帐户启用了 OTP。
- 生成 OTP 令牌的软件设备，如 FreeOTP。

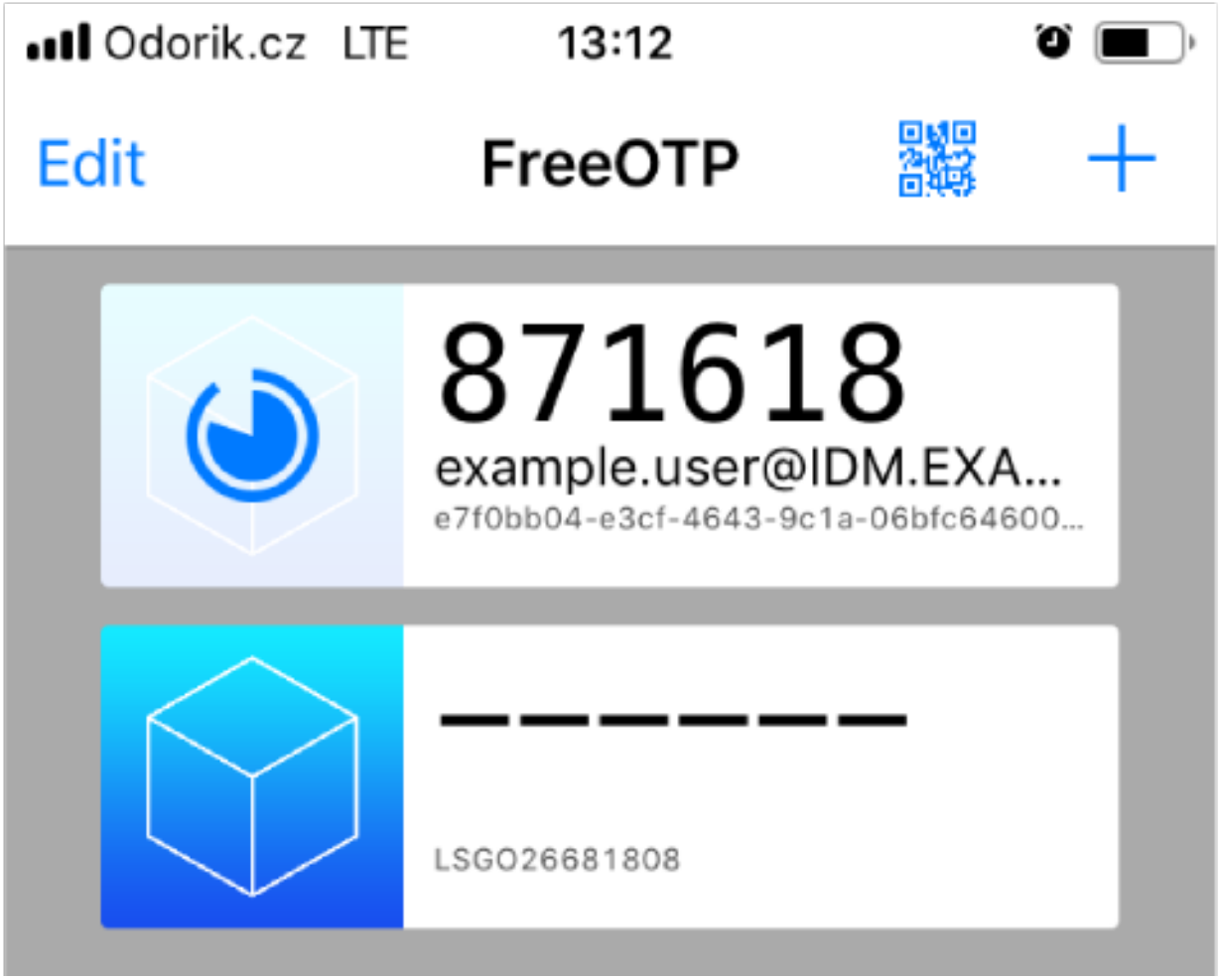
流程

1. 使用您的用户名和密码登录到 IdM Web UI。
2. 要在您的手机中创建令牌，请打开 **Authentication → OTP Tokens**选项卡。
3. 点击 **Add**。



4. 在 **Add OTP 令牌**对话框中，保留所有内容未填充，并点击 **Add**。
   在这个阶段，IdM 服务器在服务器上创建一个带有默认参数的令牌，并打开一个带有 QR 代码的页面。
5. 将 QR 代码复制到您的手机。
6. 单击 **OK** 来关闭 QR 代码。

现在，您可以生成一次性密码，并使用它们登录到 IdM Web UI。



7.6. 使用一次性密码登录到 WEB UI

按照以下流程，使用一次性密码(OTP)首次登录到 IdM Web UI。

先决条件

- OTP 配置在身份管理服务器上为用于 OTP 身份验证的用户帐户启用 OTP 配置。管理员和用户本身也可以启用 OTP。
  要启用 OTP 配置，请参阅 在 Web UI 中启用一次性密码。
- 生成 OTP 令牌的硬件或软件设备已配置。

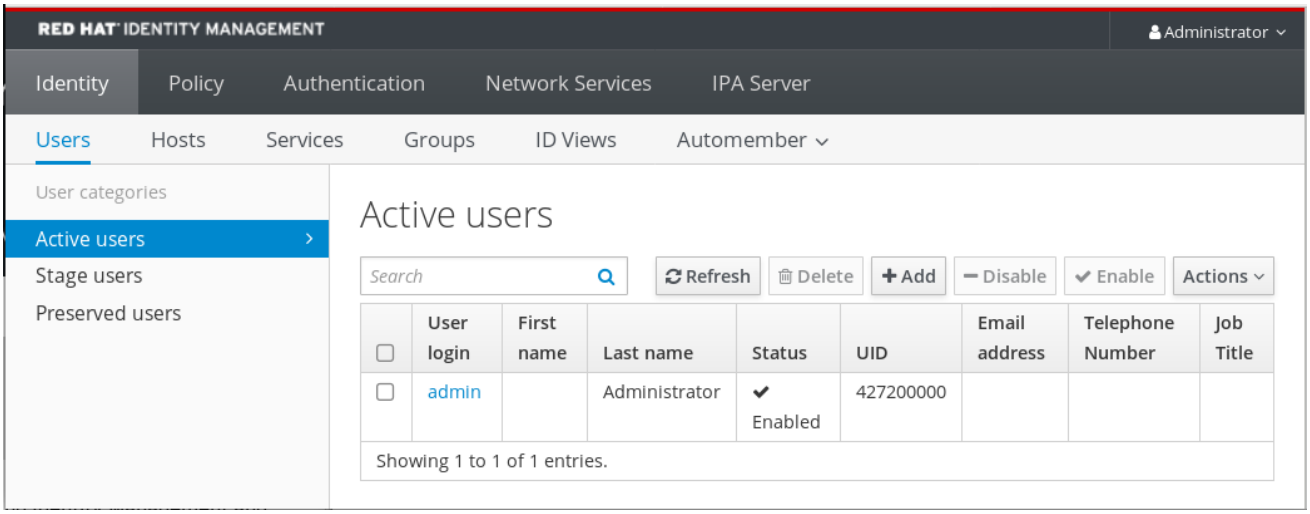
流程

1. 在身份管理登录屏幕中，输入您的用户名或 IdM 服务器管理员帐户的用户名。
2. 为上面输入的用户名添加密码。
3. 在您的设备上生成一次性密码。
4. 在密码后面输入一次性密码（不带空格）。
5. 点击 **Log in**。
   如果身份验证失败，请同步 OTP 令牌。

   如果您的 CA 使用自签名证书，则浏览器会发出警告。检查证书并接受安全例外以进行登录。

如果 IdM Web UI 未打开，请验证您的身份管理服务器的 DNS 配置。

登录成功后，会出现 IdM Web UI。



7.7. 使用 WEB UI 同步 OTP 令牌

如果使用 OTP 登录（一次性密码）失败，OTP 令牌不会被正确同步。

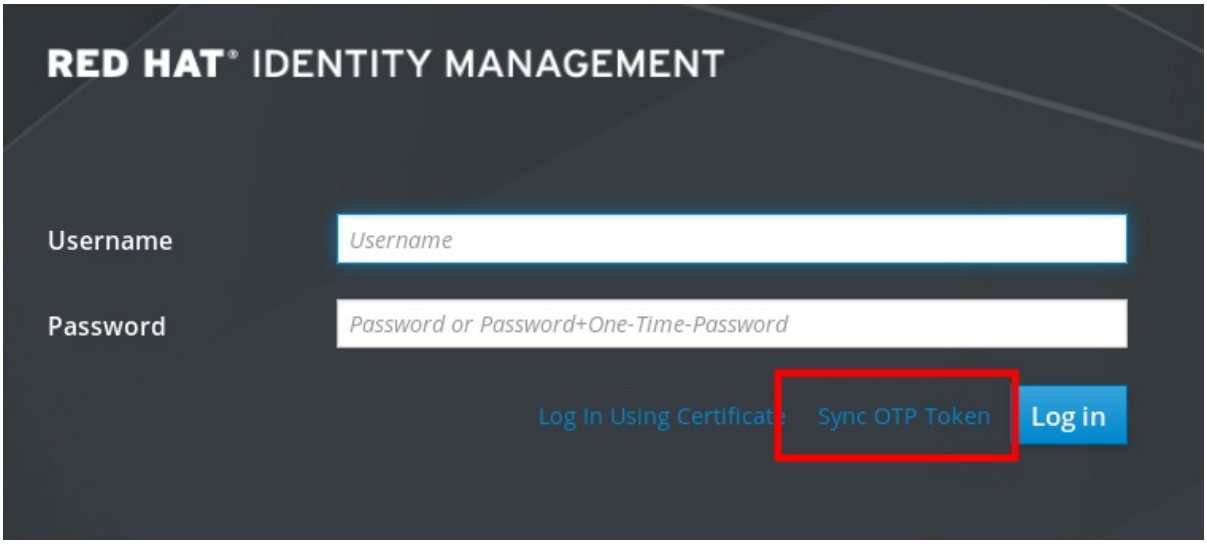
以下文本描述了令牌重新同步。

先决条件

- 登录屏幕已打开。
- 生成 OTP 令牌的设备已配置。

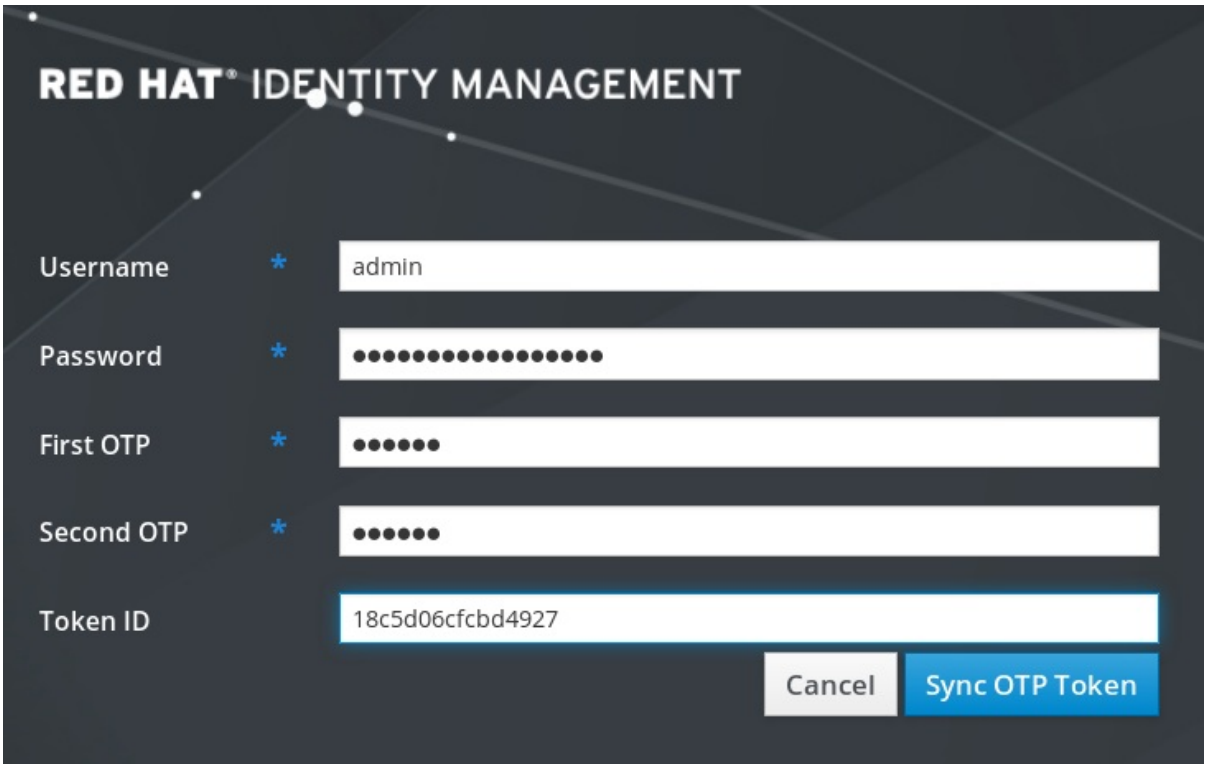
流程

1. 在 IdM Web UI 登录屏幕上，单击 **Sync OTP Token**。



2. 在登录屏幕中，输入您的用户名和身份管理密码。
3. 生成一次性密码，并将它输入到 **First OTP** 字段中。
4. 再生成一次性密码，并将它输入到 **Second OTP** 字段中。

5. （可选）输入令牌 ID。



6. 单击 **Sync OTP Token**。

同步成功后，您可以登录到 IdM 服务器。

7.8. 更改过期的密码

身份管理的管理员可以强制您在下一次登录时更改密码。这意味着，在更改密码之前，您无法成功登录到 IdM Web UI。

您第一次登录到 Web UI 时可能会出现密码过期。

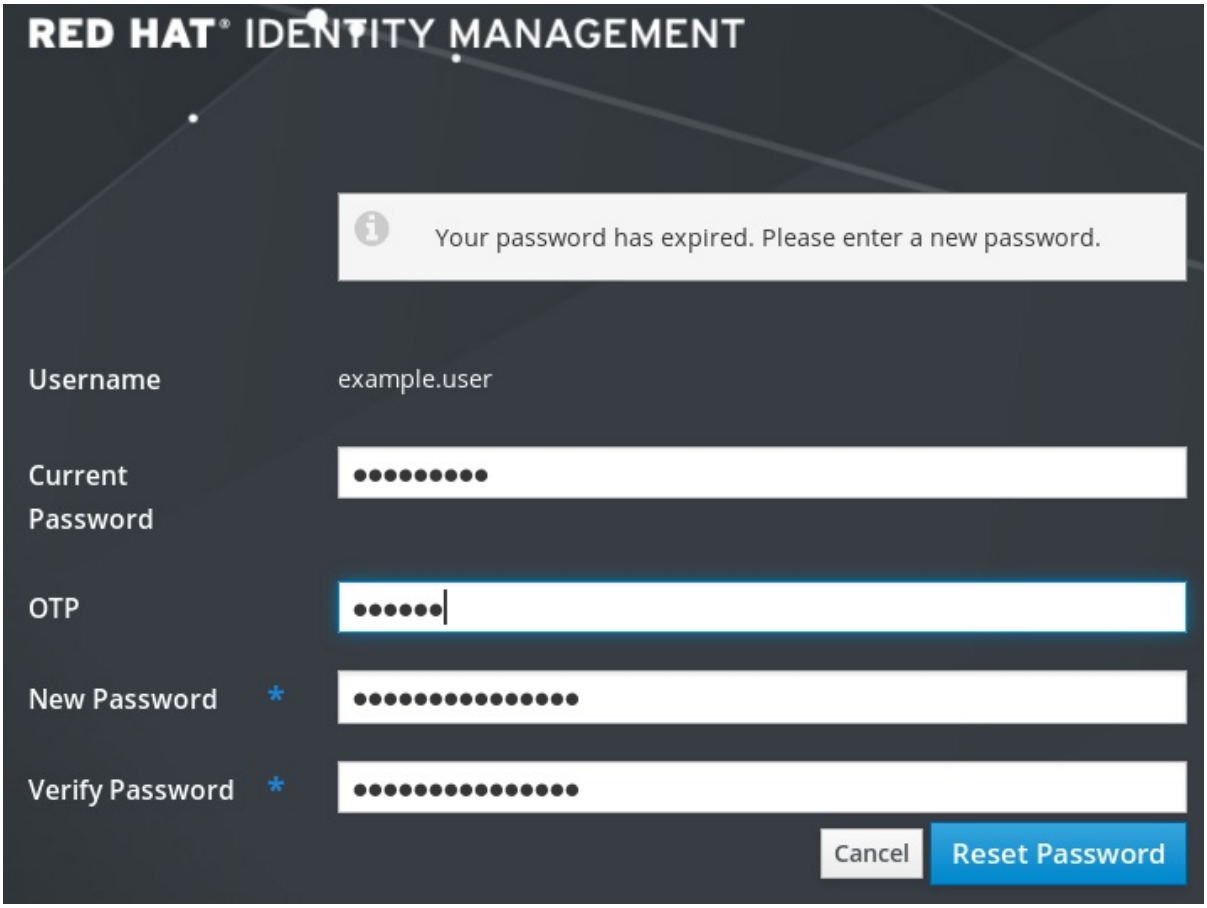
如果出现密码过期对话框，请按照流程中的说明操作。

先决条件

- 登录屏幕已打开。
- IdM 服务器的活动帐户。

流程

1. 在密码过期登录屏幕中，输入用户名。
2. 为上面输入的用户名添加密码。
3. 在 OTP 字段中，如果使用一次性密码身份验证，请生成一次性密码。
   如果您没有启用 OTP 身份验证，请将该字段留空。
4. 输入两次新密码进行验证。
5. 单击 **Reset Password**。



成功更改密码后，将显示常见的登录对话框。使用新密码登录。

7.9. 以 OTP 或 RADIUS 用户身份检索一个 IDM 票据授予票据

要以 OTP 用户身份检索一个 Kerberos 票据授予票据(TGT)，请请求一个匿名 Kerberos 票据，并通过 Secure Tunneling (FAST)通道启用 Flexible Authentication，以便在 Kerberos 客户端和 Kerberos 分发中心(KDC)之间提供一个安全连接。

先决条件

- 您的 IdM 客户端和服务器使用 RHEL 9.1 或更高版本。
- 您的 IdM 客户端和服务器使用 SSSD 2.7.0 或更高版本。
- 您已为所需用户帐户启用了 OTP。

流程

1. 运行以下命令来初始化凭证缓存：

```
[root@client ~]# kinit -n @IDM.EXAMPLE.COM -c FILE:armor.ccache
```

请注意，这个命令会创建 **armor.ccache** 文件，每当请求一个新的 Kerberos 票据时，您需要指向该文件。

2. 运行以下命令来请求一个 Kerberos 票据：

```
[root@client ~]# kinit -T FILE:armor.ccache <username>@IDM.EXAMPLE.COM
Enter your OTP Token Value.
```

-

验证

- 显示您的 Kerberos 票据信息：

```
[root@client ~]# klist -C
Ticket cache: KCM:0:58420
Default principal: <username>@IDM.EXAMPLE.COM

Valid starting     Expires            Service principal
05/09/22 07:48:23  05/10/22 07:03:07  krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
config: fast_avail(krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM) = yes
08/17/2022 20:22:45  08/18/2022 20:22:43
krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM
config: pa_type(krbtgt/IDM.EXAMPLE.COM@IDM.EXAMPLE.COM) = 141
```

pa_type = 141 表示 OTP/RADIUS 身份验证。

第 8 章 IDENTITY MANAGEMENT 安全设置

了解身份管理的与安全相关功能的更多信息。

8.1. IDENTITY MANAGEMENT 如何应用默认安全设置

默认情况下，Identity Management (IdM) 使用系统范围的加密策略。这个策略的好处是您不需要手动强化独立的 IdM 组件。

重要

红帽建议您使用系统范围的加密策略。更改单个安全设置可能会破坏 IdM 的组件。

其他资源

- 请参阅 **crypto-policies(7)** 手册页。

8.2. IDENTITY MANAGEMENT 中的匿名 LDAP 绑定

默认情况下，启用匿名绑定到 Identity Management(IdM)LDAP 服务器。匿名绑定可以公开某些配置设置或目录值。但是，一些实用程序（如 **realmd 或** 较旧的 RHEL 客户端）需要启用匿名绑定来发现注册客户端时的域设置。

其它资源

- 禁用匿名绑定

8.3. 禁用匿名绑定

您可以使用 LDAP 工具重置 **nsslapd-allow-anonymous-access** 属性来禁用 Identity Management(IdM)389 Directory Server 实例上的匿名绑定。

这些是 **nsslapd-allow-anonymous-access** 属性的有效值：

- **on**: 允许所有匿名绑定（默认）
- **rootdse** ： 仅允许匿名绑定进行 DSE 信息
- **off** ： 不允许任何匿名绑定

红帽不推荐通过将属性设置为 **off** 来完全禁止匿名绑定，因为这也会阻止外部客户端检查服务器配置。LDAP 和 Web 客户端不一定是域客户端，因此它们会匿名连接，以读取 root DSE 文件来获取连接信息。

将 **nsslapd-allow-anonymous-access** 属性的值更改为 **rootdse**，您允许访问 root DSE 和服务器配置而无需访问目录数据。

警告

某些客户端依赖于匿名绑定来发现 IdM 设置。另外，对于没有使用身份验证的传统客户端，compat 树可能无法正常工作。只有在您的客户端不需要匿名绑定时才执行这个流程。

先决条件

- 您可以作为 Directory Manager 进行身份验证，以写入到 LDAP 服务器。
- 您可以以 **root** 用户身份进行身份验证以重启 IdM 服务。

流程

1. 将 **nsslapd-allow-anonymous-access** 属性更改为 **rootdse**。

```
$ ldapmodify -x -D "cn=Directory Manager" -W -h server.example.com -p 389
Enter LDAP Password:
dn: cn=config
changetype: modify
replace: nsslapd-allow-anonymous-access
nsslapd-allow-anonymous-access: rootdse

modifying entry "cn=config"
```

2. 重启 389 Directory 服务器实例以加载新设置。

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

验证

- 显示 **nsslapd-allow-anonymous-access** 属性的值。

```
$ ldapsearch -x -D "cn=Directory Manager" -b cn=config -W -h server.example.com  -p 389
nsslapd-allow-anonymous-access | grep nsslapd-allow-anonymous-access
Enter LDAP Password:
# requesting: nsslapd-allow-anonymous-access
nsslapd-allow-anonymous-access: rootdse
```

其它资源

- Directory Server 11 文档中的 nsslapd-allow-anonymous-access
- Identity Management 中的匿名 LDAP 绑定

第 9 章 IDM 日志文件和目录

使用以下小节来监控、分析并排除 Identity Management (IdM) 的独立组件：

- LDAP
- Apache Web 服务器
- 证书系统
- Kerberos
- DNS
- Custodia

另外，您可以监控、分析 IdM 服务器和客户端 并对其进行故障排除， 并在 IdM 服务器中启用审计日志。

9.1. IDM 服务器和客户端日志文件和目录

下表显示 Identity Management (IdM) 服务器和客户端用来记录信息的目录和文件。您可以使用文件和目录排除安装错误。

目录或文件	描述
/var/log/ipaserver-install.log	IdM 服务器的安装日志。
/var/log/ipareplica-install.log	IdM 副本的安装日志。
/var/log/ipaclient-install.log	IdM 客户端的安装日志。
/var/log/sssd/	SSSD 的日志文件。您可以在 sssd.conf 文件中或使用 sssctl 命令启用 SSSD 的详细日志记录。
~/.ipa/log/cli.log	日志文件，用于远程过程调用(RPC)返回的错误以及 **ipa** 实用程序的响应。在主目录中为运行工具的实际用户创建家目录。此用户可能具有与 IdM 用户主体不同的用户名，这是在试图执行失败的 **ipa** 命令前获取 ticket (TGT) 的 IdM 用户。例如，如果您以 **root** 身份登录系统，并且获取了 IdM **admin** 的 TGT，则错误会登录到 **/root/.ipa/log/cli.log** 文件。
/etc/logrotate.d/	DNS、SSSD、Apache、Tomcat 和 Kerberos 的日志轮转策略。
/etc/pki/pki-tomcat/logging.properties	这个链接指向 **/usr/share/pki/server/conf/logging.properties** 的默认证书颁发机构日志记录配置。

其它资源

- IdM 服务器安装故障排除
- IdM 客户端安装故障排除

- IdM 副本安装故障排除
- IdM 中 SSSD 身份验证故障排除

9.2. 目录服务器日志文件

下表显示 Identity Management (IdM) 目录服务器 (DS) 实例用来记录信息的目录和文件。您可以使用文件和目录对 DS 相关问题进行故障排除。

表 9.1. 目录服务器日志文件

目录或文件	描述
/var/log/dirsrv/slapd-*REALM_NAME*/	与 IdM 服务器使用的 DS 实例关联的日志文件。这里记录的大多数操作数据都与服务器数据交互相关。
/var/log/dirsrv/slapd-*REALM_NAME*/audit	包含在 DS 配置中启用审计时所有 DS 操作的审计跟踪。 **注意** 您还可以审核 IdM API 日志访问的 Apache 错误日志。但是，因为也可以直接通过 LDAP 进行更改，因此出于审计目的，红帽建议启用更全面的 **/var/log/dirsrv/slapd-REALM_NAME/audit** 日志。
/var/log/dirsrv/slapd-*REALM_NAME*/access	包含有关试图访问域 DS 实例的详细信息。
/var/log/dirsrv/slapd-*REALM_NAME*/errors	包含有关对域 DS 实例的失败操作的详细信息。

其它资源

- 监控服务器和数据库活动
- 日志文件参考

9.3. 在 IDM 服务器中启用审计日志记录

按照以下流程，为审计目的在身份管理(IdM)服务器上启用日志记录。使用详细的日志，您可以监控数据、对问题进行故障排除，以及检查网络上的可疑活动。

注意

如果记录了大量 LDAP 更改，则 LDAP 服务可能会变得较慢，特别是在值较大时。

先决条件

- Directory Manager 密码

流程

1. 绑定到 LDAP 服务器：

```
$ ldapmodify -D "cn=Directory Manager" -W << EOF
```

2. 按 [Enter]。

3. 指定您要进行的所有修改，例如：

```
dn: cn=config
changetype: modify
replace: nsslapd-auditlog-logging-enabled
nsslapd-auditlog-logging-enabled: on
-
replace:nsslapd-auditlog
nsslapd-auditlog: /var/log/dirsrv/slapd-REALM_NAME/audit
-
replace:nsslapd-auditlog-mode
nsslapd-auditlog-mode: 600
-
replace:nsslapd-auditlog-maxlogsize
nsslapd-auditlog-maxlogsize: 100
-
replace:nsslapd-auditlog-logrotationtime
nsslapd-auditlog-logrotationtime: 1
-
replace:nsslapd-auditlog-logrotationtimeunit
nsslapd-auditlog-logrotationtimeunit: day
```

4. 通过在新行中输入 **EOF** 来指示 **ldapmodify** 命令的末尾。

5. 按 [Enter] 两次。

6. 在您要在其上启用审计日志的所有其他 IdM 服务器中重复前面的步骤。

验证

- 打开 **/var/log/dirsrv/slapd-REALM_NAME/audit** 文件：

```
389-Directory/1.4.3.231 B2021.322.1803
server.idm.example.com:636 (/etc/dirsrv/slapd-IDM-EXAMPLE-COM)

time: 20220607102705
dn: cn=config
result: 0
changetype: modify
replace: nsslapd-auditlog-logging-enabled
nsslapd-auditlog-logging-enabled: on
[...]
```

该文件不再为空，确认启用了审计。

重要

系统会记录一个更改的条目的绑定 LDAP 可分辨名称(DN)。因此，您可能必须在对日志进行后处理。例如，在 IdM Directory 服务器中，它是一个 ID 覆盖 DN，它代表修改记录的 AD 用户的身份：

```
$ modifiersName: ipaanchoruuid=:sid:s-1-5-21-19610888-1443184010-1631745340-279100,cn=default trust view,cn=views,cn=accounts,dc=idma,dc=idm,dc=example,dc=com
```

如果您有用户 SID，请使用 **pysss_nss_idmap.getnamebysid** Python 命令查找 AD 用户：

```
>>> import pysss_nss_idmap
>>> pysss_nss_idmap.getnamebysid('S-1-5-21-1273159419-3736181166-4190138427-500'))
{'S-1-5-21-1273159419-3736181166-4190138427-500': {'name': 'administrator@ad.vm', 'type': 3}}
```

其它资源

- 红帽目录服务器文档中的 核心服务器配置属性 中的审计日志配置选项
- 如何在 IPA/IDM 服务器和 Replica Servers 中启用审计日志记录 KCS 解决方案
- 目录服务器日志文件

9.4. 修改 IDM 服务器上的错误日志

按照以下流程获取有关特定类型的错误的调试信息。该示例重点是通过将错误日志级别设为 8192 来获取有关复制的详细的错误日志。要记录不同类型的信息，请在 Red Hat Directory Server 文档中 错误日志记录级别 的表中选择不同的编号。

注意

如果记录了很多类型的 LDAP 错误，则 LDAP 服务可能会变得很慢，特别是在值较大时。

先决条件

- 目录管理器密码。

流程

1. 绑定到 LDAP 服务器：

```
$ ldapmodify -x -D "cn=directory manager" -w <password>
```

2. 按 [Enter]。
3. 指定要进行的修改。例如，仅收集与复制相关的日志：

```
dn: cn=config
changetype: modify
```

```
add: nsslapd-errorlog-level
nsslapd-errorlog-level: 8192
```

4. 按 [Enter] 两次，表示 **ldapmodify** 指令的结束。这将显示 **modifying entry "cn=config"** 消息。
5. 按 [Ctrl+C] 退出 **ldapmodify** 命令。
6. 在您要在其上收集关于复制错误的详细日志的其他 IdM 服务器上重复前面的步骤。

重要

完成故障排除后，将 **nsslapd-errorlog-level** 设回 0 以防止性能问题。

其它资源

- 目录服务器错误日志记录级别

9.5. IDM APACHE 服务器日志文件

下表显示 Identity Management (IdM) Apache 服务器用来记录信息的目录和文件。

表 9.2. Apache 服务器日志文件

目录或文件	描述
/var/log/httpd/	Apache Web 服务器的日志文件。
/var/log/httpd/access_log	Apache 服务器的标准访问和错误日志。特定于 IdM 的消息会和 Apache 信息一起记录，因为 IdM Web UI 和 RPC 命令行界面使用 Apache。访问日志主要仅用于用户主体和使用的 URI，通常是 RPC 端点。错误日志包含 IdM 服务器日志。
/var/log/httpd/error_log	

其它资源

- Apache 文档中的日志文件

9.6. IDM 中的证书系统日志文件

下表显示 Identity Management (IdM) 证书系统用来记录信息的目录和文件。

表 9.3. 证书系统日志文件

目录或文件	描述
/var/log/pki/pki-ca-spawn.*time_of_installation*.log	IdM 证书颁发机构 (CA) 的安装日志。
/var/log/pki/pki-kra-spawn.*time_of_installation*.log	IdM 密钥恢复授权 (KRA) 的安装日志。

目录或文件	描述
/var/log/pki/pki-tomcat/	PKI 操作日志的顶级目录。包含 CA 和 KRA 日志。
/var/log/pki/pki-tomcat/ca/	包含与证书操作相关的日志的目录。在 IdM 中，这些日志用于服务主体、主机以及使用证书的其他实体。
/var/log/pki/pki-tomcat/kra	包含与 KRA 相关的日志的目录。
/var/log/messages	包括其它系统消息中的证书错误消息。

其它资源

- Red Hat Certificate System *管理指南*中的配置 subsystem 日志

9.7. IDM 中的 KERBEROS 日志文件

下表列出了 Kerberos 用来在 Identity Management (IdM) 中记录信息的目录和文件。

表 9.4. Kerberos 日志文件

目录或文件	描述
/var/log/krb5kdc.log	Kerberos KDC 服务器的主日志文件。
/var/log/kadmind.log	Kerberos 管理服务器的主日志文件。
这些文件的位置在 **krb5.conf** 文件中配置。在某些系统中，它们可能会有所不同。	

9.8. IDM 中的 DNS 日志文件

下表列出了 DNS 用来在 Identity Management (IdM) 中记录信息的目录和文件。

表 9.5. DNS 日志文件

目录或文件	描述
/var/log/messages	包括 DNS 错误消息和其他系统信息。默认情况下不启用此文件中的 DNS 日志记录。要启用它，请输入 **# /usr/sbin/rndc querylog** 命令。该命令生成添加到 **var/log/messages** 中的以下行： **Jun 26 17:37:33 r8server named-pkcs11[1445]: received control channel command 'querylog'** **Jun 26 17:37:33 r8server named-pkcs11[1445]: query logging is now on** 要禁用日志记录，请再次运行命令。

9.9. IDM 中的 CUSTODIA 日志文件

下表显示了 Custodia 用来记录 Identity Management (IdM) 中的目录和文件。

表 9.6. custodia 日志文件

目录或文件	描述
/var/log/custodia/	Custodia 服务的日志文件目录。

9.10. 其它资源

- 查看日志文件。您可以使用 **journalctl** 查看 **systemd** 单元文件的日志输出。