



Red Hat Enterprise Linux 9

管理智能卡验证

配置和使用智能卡验证

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

通过使用 Red Hat Identity Management (IdM)，您可以将凭证以私钥和证书的形式存储在智能卡中。然后，您可以使用此智能卡而不是密码向服务进行身份验证。管理员可以配置映射规则来减少管理开销。

目录

对红帽文档提供反馈	4
第 1 章 了解智能卡验证	5
1.1. 什么是智能卡	5
1.2. 什么是智能卡验证	5
1.3. RHEL 中的智能卡验证选项	6
1.4. 管理智能卡及其内容的工具	6
1.5. 证书和智能卡验证	7
1.6. IDM 中智能卡验证所需的步骤	7
1.7. 使用 ACTIVE DIRECTORY 发布的证书的智能卡验证所需的步骤	8
第 2 章 为智能卡验证配置身份管理	9
2.1. 为智能卡验证配置 IDM 服务器	9
2.2. 使用 ANSIBLE 为智能卡验证配置 IDM 服务器	11
2.3. 为智能卡验证配置 IDM 客户端	14
2.4. 使用 ANSIBLE 为智能卡验证配置 IDM 客户端	16
2.5. 在 IDM WEB UI 的用户条目中添加证书	18
2.6. 在 IDM CLI 中向用户条目中添加证书	20
2.7. 安装用来管理和使用智能卡的工具	21
2.8. 准备智能卡并将证书和密钥上传到智能卡	21
2.9. 使用智能卡登录到 IDM	23
2.10. 在 IDM 客户端中使用智能卡验证登录到 GDM	24
2.11. 在 SU 命令中使用智能卡验证	25
第 3 章 为 IDM 中智能卡验证配置 ADCS 发布的证书	26
3.1. 信任配置和证书使用量所需的 WINDOWS 服务器设置	26
3.2. 使用 SFTP 从 ACTIVE DIRECTORY 复制证书	26
3.3. 使用 ADCS 证书为智能卡身份验证配置 IDM 服务器和客户端	27
3.4. 转换 PFX 文件	29
3.5. 安装用来管理和使用智能卡的工具	29
3.6. 准备智能卡并将证书和密钥上传到智能卡	30
3.7. 在 SSSD.CONF 中配置超时	31
3.8. 为智能卡身份验证创建证书映射规则	32
第 4 章 用于配置身份验证的证书映射规则	33
第 5 章 使用 WEB 控制台为集中管理的用户配置智能卡验证	34
5.1. 实现中央管理用户的智能卡验证	34
5.2. 安装用来管理和使用智能卡的工具	34
5.3. 准备智能卡并将证书和密钥上传到智能卡	35
5.4. 为 WEB 控制台启用智能卡验证	36
5.5. 使用智能卡登录到 WEB 控制台	37
5.6. 为智能卡用户启用无密码的 SUDO 验证	38
5.7. 限制用户会话和内存以防止 DOS 攻击	39
第 6 章 使用本地证书配置智能卡验证	41
6.1. 创建本地证书	41
6.2. 将证书复制到 SSSD 目录中	44
6.3. 安装用来管理和使用智能卡的工具	45
6.4. 准备智能卡并将证书和密钥上传到智能卡	45
6.5. 使用智能卡验证配置 SSH 访问	47
第 7 章 使用 AUTHSELECT 配置智能卡验证	49

7.1. 适用于智能卡的证书	49
7.2. 配置您的系统以启用智能卡和密码验证	49
7.3. 配置您的系统以强制智能卡验证	50
7.4. 配置智能卡认证，使它在取出智能卡时进行锁定	50
第 8 章 使用智能卡进行远程向 SUDO 进行身份验证	52
8.1. 在 IDM 中创建 SUDO 规则	52
8.2. 为 SUDO 设置 PAM 模块	53
8.3. 使用智能卡远程连接到 SUDO	53
第 9 章 使用带有智能卡的 PKINIT 以 ACTIVE DIRECTORY 用户身份进行身份验证	55
第 10 章 使用智能卡对身份验证进行故障排除	57
10.1. 测试系统中的智能卡访问	57
10.2. 使用 SSSD 对智能卡验证进行故障排除	60
10.3. 验证 IDM KERBEROS KDC 可以使用 PKINIT 和 CA 证书正确位置	62
10.4. 增加 SSSD 超时	64
10.5. 证书映射和匹配规则故障排除	64

对红帽文档提供反馈

我们感谢您对我们文档的反馈。帮助我们如何进行改进。

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** 字段中输入您的建议以改进。包括文档相关部分的链接。
5. 点对话框底部的 **Create**。

第 1 章 了解智能卡验证

使用基于智能卡的验证是使用密码进行验证的替代选择。您可以将用户凭证以私钥和证书的形式存储在智能卡上，并使用证书、特殊的软件和硬件来访问它们。将智能卡放在读卡器或 USB 端口中，并为智能卡提供 PIN 代码，而不是提供您的密码。

这部分论述了如何使用智能卡以及智能卡验证的工作方式。它描述了可以用来读取和操作智能卡内容的工具。它还提供了示例用例，并描述了 IdM 服务器和 IdM 客户端用于智能卡验证的设置。



注意

如果要开始使用智能卡验证，请参阅硬件要求：[RHEL9 中的智能卡支持](#)。

1.1. 什么是智能卡

智能卡是一个物理设备，通常是一个带有微处理器的塑料板卡，它可以使用保存在卡中的证书进行个人验证。个人验证意味着，您可以象使用用户密码一样使用智能卡。

您可以将用户凭证以私钥和证书的形式存储在智能卡上，并使用特殊的软件和硬件来访问它们。您可以将智能卡放在读卡器或 USB 插座中，并为智能卡提供 PIN 代码，而不是提供您的密码。

1.2. 什么是智能卡验证

基于公钥的验证和基于证书的身份验证是两个广泛使用的、基于密码验证的替代选择。使用公钥和私钥而不是您的密码确认您的身份。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。

如果使用智能卡验证，您的用户凭证（您的公钥和私钥和证书）保存在智能卡中，且只能在智能卡插入读卡机并提供了一个个人身份码（PIN）后才能使用。这需要您拥有物理设备（智能卡）并知道其 PIN 时，因此智能卡验证被认为是双因素验证类型。

1.2.1. IdM 中智能卡验证示例

以下示例描述了在 IdM 中使用智能卡的两个简单场景。

1.2.1.1. 使用智能卡登录到您的系统

您可以使用智能卡以本地用户对 RHEL 系统进行身份验证。如果您的系统被配置为强制智能卡登录，则会提示您插入智能卡并输入其 PIN，如果失败，则无法登录到您的系统。或者，您可以将您的系统配置为使用智能卡验证或者您的用户名和密码进行验证。在这种情况下，如果您没有插入智能卡，会提示您输入您的用户名和密码。

1.2.1.2. 登陆到 GDM 并在移除卡时进行锁定

如果您在 RHEL 系统中配置了智能卡验证，您可以设置 在移除卡时进行锁定。如果您登录到 GNOME 显示管理器 (GDM) 并移除智能卡，则屏幕锁定会被启用，您必须重新插入智能卡并使用 PIN 验证来解锁屏幕。您不能使用您的用户名和密码进行验证。



注意

如果您登录到 GDM 并移除智能卡，则屏幕锁定会被启用，您必须重新插入智能卡并使用 PIN 验证来解锁屏幕。

1.3. RHEL 中的智能卡验证选项

您可以使用 **authselect** 命令, **authselect enable-feature <smartcardoption>** 配置如何在特定的身份管理(IdM)客户端中进行智能卡验证。可用的智能卡选项如下：

- **with-smartcard**: 用户可以使用用户名和密码进行身份验证，或者使用他们的智能卡进行身份验证
- **with-smartcard-required**: 用户可以使用智能卡进行验证，并禁用密码验证。您不能在没有智能卡的情况下访问该系统。使用智能卡进行身份验证后，一直保持登录状态，即使您的智能卡已从读取器中移除。



注意

with-smartcard-required 选项代表只对登陆服务（如 **login**, **gdm**, **xdm**, **xscreensaver**, 和 **gnome-screensaver**）强制只能使用智能卡进行验证。对于其它服务，如使用 **su** 或 **sudo** 来切换用户，则不会强制使用智能卡进行验证，如果没有插入您的智能卡，则会提示您输入密码。

- **with-smartcard-lock-on-removal**: 用户可以使用智能卡进行验证。但是，如果您从读取器中移除智能卡，则系统会被锁定。您不能使用密码进行验证。



注意

with-smartcard-lock-on-removal 选项仅适用于具有 GNOME 桌面环境的系统。如果您使用基于 **tty** 或控制台的系统，并且您从读卡器中删除了智能卡，则不会将您自动锁在系统之外。

如需更多信息，请参阅[使用 authselect 配置智能卡](#)。

1.4. 管理智能卡及其内容的工具

您可以使用许多不同的工具来管理保存在智能卡中的密钥和证书。您可以使用这些工具进行以下操作：

- 列出连接到系统的可用智能卡读取器。
- 列出可用的智能卡并查看其内容。
- 操作智能卡内容（密钥和证书）。

有很多工具可以提供相似的功能，但某些工具在系统的不同层上工作。智能卡由多个组件在多个层上进行管理。在较低级别上，操作系统使用 PC/SC 协议与智能卡读取器通信，此通信由 **pcsc-lite** 守护进程处理。守护进程将收到的命令转发到智能卡读取器通常通过 USB，这由低级 CCID 驱动程序处理。PC/SC 低级通信很少显示在应用程序级别。用于应用程序访问智能卡的主要方法是通过更高级别的应用程序编程界面(API)，OASIS PKCS#11 API，它将卡通信基于加密对象（例如，私钥）。智能卡厂商提供了一个共享模块，如一个 **.so** 文件，它遵循 PKCS#11 API，并作为智能卡的驱动程序。

您可以使用以下工具管理您的智能卡及其内容：

- OpenSC 工具：使用 **opensc** 中实施的驱动程序。
 - OpenSC-tool：执行智能卡操作。
 - pkcs15-tool：管理智能卡中的 PKCS#15 数据结构，如列出和读取存储在令牌中的 PIN、密钥和证书。

- `pkcs11-tool` : 管理智能卡中的 PKCS#11 数据对象, 如列出和读取令牌中存储的 PIN、密钥和证书。
- GnuTLS utils: 一个 API, 用于应用程序的 API 来启用网络传输层的安全通信, 以及访问 X.509、PKCS#12、OpenPGP 和其他结构的接口。
 - `p11tool` : 对 PKCS#11 智能卡和安全模块执行操作。
 - `certtool` : 解析和生成 X.509 证书、请求和私钥。
- 网络安全服务(NSS)工具: 一组库, 旨在支持启用了安全的客户端和服务端应用程序的跨平台开发。使用 NSS 构建的应用程序支持 SSL v3、TLS、Pce PKCS #5、PKCS #7、PKCS #11, PKCS #12、S/MIME、X.509 v3 证书和其他安全标准。
 - `modutil` : 使用安全模块数据库管理 PKCS#11 模块信息。
 - `certutil` : 管理 NSS 数据库和其它 NSS 令牌中的密钥和证书。

有关使用这些工具排除使用智能卡进行身份验证的问题的更多信息, 请参阅 [使用智能卡对身份验证进行故障排除](#)。

其他资源

- [opensc-tool man page](#)
- [pkcs15-tool man page](#)
- [pkcs11-tool man page](#)
- [p11tool man page](#)
- [certtool man page](#)
- [modutil man page](#)
- [certutil man page](#)

1.5. 证书和智能卡验证

如果您使用 Identity Management (IdM) 或 Active Directory (AD) 来管理域中的身份存储、身份验证、策略和授权策略, 则 IdM 或 AD 用于身份验证的证书会分别生成。您还可以使用外部证书颁发机构提供的证书, 在这种情况下, 您必须配置 Active Directory 或 IdM 接受来自外部提供程序的证书。如果用户不是某个域的一部分, 您可以使用本地证书颁发机构生成的证书。详情请查看以下部分:

- [为智能卡验证配置身份管理](#)
- [为 IdM 中智能卡验证配置 ADCS 发布的证书](#)
- [管理 IdM 用户、主机和服务的外部签名证书](#)
- [配置和导入本地证书到智能卡](#)

有关有资格进行智能卡验证的证书的完整列表, 请参阅 [符合智能卡的证书](#)。

1.6. IDM 中智能卡验证所需的步骤

在 Identity Management (IdM) 中使用智能卡进行身份验证前，您必须确定以下步骤：

- 为智能卡验证配置 IdM 服务器。请参阅[为智能卡验证配置 IdM 服务器](#)
- 为智能卡验证配置 IdM 客户端。请参阅[为智能卡验证配置 IdM 客户端](#)
- 将证书添加到 IdM 的用户条目。请参阅[在 IdM Web UI 的用户条目中添加证书](#)
- 在智能卡中保存密钥和证书。请参阅[智能卡中的证书](#)

1.7. 使用 **ACTIVE DIRECTORY** 发布的证书的智能卡验证所需的步骤

在使用由 Active Directory (AD) 发布的证书的智能卡验证前，您必须确定以下步骤：

- [将 CA 和用户证书从活动目录复制到 IdM 服务器和客户端](#)
- [使用 ADCS 证书为智能卡身份验证配置 IdM 服务器和客户端](#)
- [转换 PFX\(PKCS#12\)文件，以便在智能卡中保存证书和私钥。](#)
- [在 sssd.conf 文件中配置超时。](#)
- [为智能卡身份验证创建证书映射规则](#)

第 2 章 为智能卡验证配置身份管理

身份管理(IdM)支持使用如下方式的智能卡身份验证：

- IdM 证书颁发机构发布的用户证书
- 外部证书颁发机构发布的用户证书

您可以在 IdM 中为两种类型的证书配置智能卡验证。在这种情况下，**rootca.pem** CA 证书是包含可信外部证书颁发机构证书的文件。

有关 IdM 中智能卡验证的详情，请参考 [了解智能卡验证](#)。

有关配置智能卡验证的详情：

- [为智能卡验证配置 IdM 服务器](#)
- [为智能卡验证配置 IdM 客户端](#)
- [在 IdM Web UI 的用户条目中添加证书](#)
- [在 IdM CLI 中向用户条目中添加证书](#)
- [安装用来管理和使用智能卡的工具](#)
- [在智能卡中存储证书](#)
- [使用智能卡登录到 IdM](#)
- [使用智能卡身份验证配置 GDM 访问](#)
- [使用智能卡验证配置 su 访问](#)

2.1. 为智能卡验证配置 IDM 服务器

如果要为其证书是由身份管理 (IdM) CA 信任的 <EXAMPLE.ORG> 域的证书颁发机构 (CA) 发布的用户启用智能卡验证，您必须获取以下证书，以便在运行配置 IdM 服务器的 **ipa-adviser** 脚本时添加它们：

- 为 <EXAMPLE.ORG> CA 直接发布或者通过一个或多个其子 CA 发布证书的根 CA 的证书。您可以从颁发机构发布证书的网页下载证书链。详情请查看 [配置浏览器来启用证书身份验证](#) 中的步骤 1 - 4a。
- IdM CA 证书。您可以从运行 IdM CA 实例的 IdM 服务器上的 **/etc/ipa/ca.crt** 文件获取 CA 证书。
- 所有中间 CA 的证书，即介于 <EXAMPLE.ORG> CA 和 IdM CA 之间。

要为智能卡验证配置 IdM 服务器：

1. 获取 PEM 格式的 CA 证书的文件。
2. 运行内置的 **ipa-adviser** 脚本。
3. 重新加载系统配置。

先决条件

- 有到 IdM 服务器的 root 访问权限。
- 您有 root CA 证书和所有中间 CA 证书。

流程

1. 创建要进行配置的目录：

```
[root@server]# mkdir ~/SmartCard/
```

2. 进入该目录：

```
[root@server]# cd ~/SmartCard/
```

3. 获取存储在 PEM 格式文件中的相关 CA 证书。如果您的 CA 证书存储在再不同格式的文件中，如 DER，请将其转换为 PEM 格式。IdM 证书颁发机构证书采用 PEM 格式，位于 `/etc/ipa/ca.crt` 文件中。

将 DER 文件转换为 PEM 文件：

```
# openssl x509 -in <filename>.der -inform DER -out <filename>.pem -outform PEM
```

4. 为方便起见，将证书复制到您要配置目录中：

```
[root@server SmartCard]# cp /tmp/rootca.pem ~/SmartCard/
[root@server SmartCard]# cp /tmp/subca.pem ~/SmartCard/
[root@server SmartCard]# cp /tmp/issuingca.pem ~/SmartCard/
```

5. 另外，如果您使用外部证书颁发机构的证书，请使用 `openssl x509` 工具查看 PEM 格式的文件内容，来检查 **Issuer** 和 **Subject** 值是否正确：

```
[root@server SmartCard]# openssl x509 -noout -text -in rootca.pem | more
```

6. 使用管理员特权，通过内置的 `ipa-adviser` 工具生成配置脚本：

```
[root@server SmartCard]# kinit admin
[root@server SmartCard]# ipa-adviser config-server-for-smart-card-auth > config-server-for-smart-card-auth.sh
```

`config-server-for-smart-card-auth.sh` 脚本执行以下操作：

- 它配置 IdM Apache HTTP 服务器。
 - 它在 KDC（Key Distribution Center）中启用 PKINIT（Public Key Cryptography for Initial Authentication in Kerberos）。
 - 它将 IdM Web UI 配置为接受智能卡授权请求。
7. 执行脚本，将包含根 CA 和子 CA 证书的 PEM 文件添加为参数：

```
[root@server SmartCard]# chmod +x config-server-for-smart-card-auth.sh
[root@server SmartCard]# ./config-server-for-smart-card-auth.sh rootca.pem subca.pem issuingca.pem
Ticket cache:KEYRING:persistent:0:0
```

```
Default principal: admin@IDM.EXAMPLE.COM
[...]
Systemwide CA database updated.
The ipa-certupdate command was successful
```



注意

在任何子 CA 证书前，确保将根 CA 的证书添加为参数，并且 CA 或子 CA 证书还没有过期。

8. 另外，如果发布用户证书的证书颁发机构不提供任何在线证书状态协议(OCSP)响应程序，您可能需要禁用对 IdM Web UI 身份验证的 OCSP 检查：

- a. 在 `/etc/httpd/conf.d/ssl.conf` 文件中将 **SSL_OCSP_Enable** 参数设为 **off**：

```
SSL_OCSP_Enable off
```

- b. 重启 Apache 守护进程(httpd)使更改立即生效：

```
[root@server SmartCard]# systemctl restart httpd
```



警告

如果您只使用 IdM CA 发出的用户证书，不要禁用 OCSP 检查。OCSP 响应器是 IdM 的一部分。

有关如何保持 OCSP 检查处于启用状态，同时防止 IdM 服务器拒绝用户证书（如果 IdM 服务器不包含有关颁发用户证书的 CA 侦听 OCSP 服务请求的位置的信息）的说明，请参阅 [Apache mod_ssl 配置选项](#) 中的 **SSL_OCSPDefaultResponder** 指令。

该服务器现在被配置为智能卡验证。



注意

要在整个拓扑中启用智能卡验证，请在每个 IdM 服务器中运行操作过程。

2.2. 使用 ANSIBLE 为智能卡验证配置 IDM 服务器

您可以使用 Ansible 为其证书是由身份管理(IdM) CA 信任的 <EXAMPLE.ORG> 域的证书颁发机构(CA)发布的用户启用智能卡验证。要做到这一点，您必须获取以下证书，以便在运行具有 **ipasmartcard_server ansible-freeipa** 角色脚本的 Ansible playbook 时使用它们：

- 为 <EXAMPLE.ORG> CA 直接发布或者通过一个或多个其子 CA 发布证书的根 CA 的证书。您可以从颁发机构发布证书的网页下载证书链。详情请参阅 [配置浏览器以启用证书验证](#) 中的步骤 4。
- IdM CA 证书。您可以从任何 IdM CA 服务器上的 `/etc/ipa/ca.crt` 文件获取 CA 证书。
- 介于<EXAMPLE.ORG> CA 和 IdM CA 之间的所有 CA 的证书。

先决条件

- 您有访问 IdM 服务器的 **root** 权限。
- 您需要知道 IdM **admin** 密码。
- 您有根 CA 证书、IdM CA 证书以及所有中间 CA 证书。
- 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 `ipadmin_password`。
- 目标节点,也就是在其上执行 **ansible-freeipa** 模块的节点，是 IdM 域的一部分，作为 IdM 客户端、服务器或副本。

步骤

1. 如果您的 CA 证书存储在不同格式（如 **DER**）的文件中，请将其转换为 **PEM** 格式：

```
# openssl x509 -in <filename>.der -inform DER -out <filename>.pem -outform PEM
```

IdM 证书颁发机构证书采用 **PEM** 格式，位于 `/etc/ipa/ca.crt` 文件中。

2. （可选）使用 **openssl x509** 工具查看 **PEM** 格式的文件的內容，以检查 **Issuer** 和 **Subject** 值是否正确：

```
# openssl x509 -noout -text -in root-ca.pem | more
```

3. 进入您的 `~/MyPlaybooks/` 目录：

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

4. 创建专用于 CA 证书的子目录：

```
$ mkdir SmartCard/
```

5. 为方便起见，将所有必需的证书复制到 `~/MyPlaybooks/SmartCard/` 目录中：

```
# cp /tmp/root-ca.pem ~/MyPlaybooks/SmartCard/
# cp /tmp/intermediate-ca.pem ~/MyPlaybooks/SmartCard/
# cp /etc/ipa/ca.crt ~/MyPlaybooks/SmartCard/ipa-ca.crt
```

6. 在 Ansible 清单文件中指定以下内容：

- 要为智能卡验证配置的 IdM 服务器。
- IdM 管理员密码。

- CA 证书的路径按以下顺序：
 - 根 CA 证书文件
 - 中间 CA 证书文件
 - IdM CA 证书文件

文件类似如下：

```
[ipaserver]
ipaserver.idm.example.com

[ipareplicas]
ipareplica1.idm.example.com
ipareplica2.idm.example.com

[ipacluster:children]
ipaserver
ipareplicas

[ipacluster:vars]
ipaadmin_password= "{{ ipaadmin_password }}"
ipasmartcard_server_ca_certs=/home/<user_name>/MyPlaybooks/SmartCard/root-
ca.pem,/home/<user_name>/MyPlaybooks/SmartCard/intermediate-
ca.pem,/home/<user_name>/MyPlaybooks/SmartCard/ipa-ca.crt
```

7. 使用以下内容创建一个 **install-smartcard-server.yml** playbook：

```
---
- name: Playbook to set up smart card authentication for an IdM server
  hosts: ipaserver
  become: true

  roles:
  - role: ipasmartcard_server
    state: present
```

8. 保存该文件。
9. 运行 Ansible playbook。指定 playbook 文件、存储保护 **secret.yml** 文件的密码，以及清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory install-
smartcard-server.yml
```

ipasmartcard_server Ansible 角色执行以下操作：

- 它配置 IdM Apache HTTP 服务器。
 - 它在 KDC（Key Distribution Center）中启用 PKINIT（Public Key Cryptography for Initial Authentication in Kerberos）。
 - 它将 IdM Web UI 配置为接受智能卡授权请求。
10. 另外，如果发布用户证书的证书颁发机构不提供任何在线证书状态协议(OCSP)响应程序，您可能需要禁用对 IdM Web UI 身份验证的 OCSP 检查：

- a. 以 **root** 用户身份连接到 IdM 服务器：

```
ssh root@ipaserver.idm.example.com
```

- b. 在 `/etc/httpd/conf.d/ssl.conf` 文件中将 **SSLLOCSPEnable** 参数设为 **off**：

```
SSLLOCSPEnable off
```

- c. 重启 Apache 守护进程(httpd)使更改立即生效：

```
# systemctl restart httpd
```



警告

如果您只使用 IdM CA 发出的用户证书，不要禁用 OCSP 检查。OCSP 响应器是 IdM 的一部分。

有关如何保持 OCSP 检查处于启用状态，同时防止 IdM 服务器拒绝用户证书（如果 IdM 服务器不包含有关颁发用户证书的 CA 侦听 OCSP 服务请求的位置的信息）的说明，请参阅 [Apache mod_ssl 配置选项](#) 中的 **SSLLOCSPDefaultResponder** 指令。

清单文件中列出的服务器现在已被配置为进行智能卡验证。



注意

要在整个拓扑中启用智能卡验证，请将 Ansible playbook 中的 **hosts** 变量设为 **ipacluster**：

```
---
- name: Playbook to setup smartcard for IPA server and replicas
  hosts: ipacluster
  [...]
```

其他资源

- 使用 `/usr/share/doc/ansible-freeipa/playbooks/` 目录中 **ipasmartcard_server** 角色的 playbook 示例

2.3. 为智能卡验证配置 IDM 客户端

按照以下流程为智能卡验证配置 IdM 客户端。这个过程需要运行在每个 IdM 系统、客户端或服务器上，您希望在使用智能卡进行身份验证时连接到这些系统。例如，若要启用从主机 A 到主机 B 的 **ssh** 连接，需要在主机 B 上运行脚本。

作为管理员，运行这个流程来使用如下方法启用智能卡身份验证

- **ssh** 协议
详情请查看 [使用智能卡验证配置 SSH 访问](#)。

- 控制台登录
- GNOME 显示管理器(GDM)
- **su** 命令

对于向 IdM Web UI 进行身份验证，不需要此流程。向 IdM Web UI 进行身份验证涉及两个主机，它们都不必是 IdM 客户端：

- 其上运行浏览器的机器。机器可以在 IdM 域之外。
- 其上运行 **httpd** 的 IdM 服务器。

以下流程假设您在 IdM 客户端，而不是 IdM 服务器上配置智能卡身份验证。因此，您需要两台计算机：生成配置脚本的 IdM 服务器，以及运行脚本的 IdM 客户端。

先决条件

- 为智能卡验证配置了您的 IdM 服务器，如 [为智能卡验证配置 IdM 服务器](#) 所述。
- 有对 IdM 服务器和 IdM 客户端的 root 访问权限。
- 您有 root CA 证书和所有中间 CA 证书。
- 已使用 **--mkhomedir** 选项安装了 IdM 客户端，以确保远程用户可以成功登录。如果您没有创建主目录，则默认登录位置为目录结构的根目录 **/**。

步骤

1. 在 IdM 服务器上，使用管理员权限通过 **ipa-adviser** 生成配置脚本：

```
[root@server SmartCard]# kinit admin
[root@server SmartCard]# ipa-adviser config-client-for-smart-card-auth > config-client-for-smart-card-auth.sh
```

config-client-for-smart-card-auth.sh 脚本执行以下操作：

- 它配置智能卡守护进程。
- 它设置系统范围的信任存储。
- 它配置系统安全服务守护进程 (SSSD)，允许用户使用其用户名和密码或其智能卡进行验证。有关智能卡验证的 SSSD 配置集选项的详情，请参考 [RHEL 中的智能卡验证选项](#)。

2. 从 IdM 服务器中，将脚本复制到 IdM 客户端机器中选择的目录中：

```
[root@server SmartCard]# scp config-client-for-smart-card-auth.sh
root@client.idm.example.com:/root/SmartCard/
Password:
config-client-for-smart-card-auth.sh    100% 2419    3.5MB/s  00:00
```

3. 为了方便起见，将 IdM 服务器上的 PEM 格式的 CA 证书文件复制到 IdM 客户端机器上与在上一步中所使用的相同的目录中：

```
[root@server SmartCard]# scp {rootca.pem,subca.pem,issuingca.pem}
root@client.idm.example.com:/root/SmartCard/
```

```

Password:
rootca.pem          100% 1237 9.6KB/s 00:00
subca.pem           100% 2514 19.6KB/s 00:00
issuingca.pem       100% 2514 19.6KB/s 00:00

```

- 在客户端机器上执行脚本，将包含 CA 证书的 PEM 文件添加为参数：

```

[root@client SmartCard]# kinit admin
[root@client SmartCard]# chmod +x config-client-for-smart-card-auth.sh
[root@client SmartCard]# ./config-client-for-smart-card-auth.sh rootca.pem subca.pem
issuingca.pem
Ticket cache:KEYRING:persistent:0:0
Default principal: admin@IDM.EXAMPLE.COM
[...]
Systemwide CA database updated.
The ipa-certupdate command was successful

```



注意

在任何子 CA 证书前，确保将根 CA 的证书添加为参数，并且 CA 或子 CA 证书还没有过期。

现在为智能卡验证配置了客户端。

2.4. 使用 ANSIBLE 为智能卡验证配置 IDM 客户端

按照以下流程，使用 **ansible-freeipa ipasmartcard_client** 模块配置特定的身份管理(IdM)客户端，以允许 IdM 用户使用智能卡进行身份验证。运行这个流程为使用以下任一方法访问 IdM 的用户启用智能卡验证：

- **ssh** 协议
详情请查看 [使用智能卡验证配置 SSH 访问](#)。
- 控制台登录
- GNOME 显示管理器(GDM)
- **su** 命令



注意

对于向 IdM Web UI 进行身份验证，不需要此流程。向 IdM Web UI 进行身份验证涉及两个主机，它们都不必是 IdM 客户端：

- 其上运行浏览器的机器。机器可以在 IdM 域之外。
- 其上运行 **httpd** 的 IdM 服务器。

先决条件

- 您的 IdM 服务器已被配置为进行智能卡验证，如 [使用 Ansible 为智能卡验证配置 IdM 服务器](#) 中所述。
- 有对 IdM 服务器和 IdM 客户端的 root 访问权限。

- 您有根 CA 证书、IdM CA 证书以及所有中间 CA 证书。
- 您已配置了 Ansible 控制节点以满足以下要求：
 - 您使用 Ansible 版本 2.14 或更高版本。
 - 您已在 Ansible 控制器上安装了 **ansible-freeipa** 软件包。
 - 示例假定在 `~/MyPlaybooks/` 目录中，您已创建了一个带有 IdM 服务器的完全限定域名 (FQDN) 的 **Ansible 清单文件**。
 - 示例假定 `secret.yml` Ansible vault 存储了 `ipaadmin_password`。
- 目标节点,也就是在其上执行 **ansible-freeipa** 模块的节点，是 IdM 域的一部分，作为 IdM 客户端、服务器或副本。

流程

1. 如果您的 CA 证书存储在不同格式（如 **DER**）的文件中，请将其转换为 **PEM** 格式：

```
# openssl x509 -in <filename>.der -inform DER -out <filename>.pem -outform PEM
```

IdM CA 证书采用 **PEM** 格式，位于 `/etc/ipa/ca.crt` 文件中。

2. （可选）使用 **openssl x509** 工具查看 **PEM** 格式的文件的內容，以检查 **Issuer** 和 **Subject** 值是否正确：

```
# openssl x509 -noout -text -in root-ca.pem | more
```

3. 在 Ansible 控制节点上，导航到 `~/MyPlaybooks/` 目录：

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

4. 创建专用于 CA 证书的子目录：

```
$ mkdir SmartCard/
```

5. 为方便起见，将所有必需的证书复制到 `~/MyPlaybooks/SmartCard/` 目录中，例如：

```
# cp /tmp/root-ca.pem ~/MyPlaybooks/SmartCard/
# cp /tmp/intermediate-ca.pem ~/MyPlaybooks/SmartCard/
# cp /etc/ipa/ca.crt ~/MyPlaybooks/SmartCard/ipa-ca.crt
```

6. 在 Ansible 清单文件中指定以下内容：

- 要为智能卡验证配置的 IdM 客户端。
- IdM 管理员密码。
- CA 证书的路径按以下顺序：
 - 根 CA 证书文件
 - 中间 CA 证书文件

- IdM CA 证书文件

文件类似如下：

```
[ipaclients]
ipaclient1.example.com
ipaclient2.example.com

[ipaclients:vars]
ipaadmin_password=SomeADMINpassword
ipasmartcard_client_ca_certs=/home/<user_name>/MyPlaybooks/SmartCard/root-
ca.pem,/home/<user_name>/MyPlaybooks/SmartCard/intermediate-
ca.pem,/home/<user_name>/MyPlaybooks/SmartCard/ipa-ca.crt
```

7. 使用以下内容创建 **install-smartcard-clients.yml** playbook：

```
---
- name: Playbook to set up smart card authentication for an IdM client
  hosts: ipaclients
  become: true

  roles:
  - role: ipasmartcard_client
    state: present
```

8. 保存该文件。
9. 运行 Ansible playbook。指定 playbook 和清单文件：

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory install-
smartcard-clients.yml
```

ipasmartcard_client Ansible 角色执行以下操作：

- 它配置智能卡守护进程。
- 它设置系统范围的信任存储。
- 它将系统安全服务守护进程(SSSD)配置为允许用户使用其用户名和密码或者智能卡进行身份验证。有关智能卡验证的 SSSD 配置集选项的详情，请参考 [RHEL 中的智能卡验证选项](#)。

清单文件的 **ipaclients** 部分中列出的客户端现在配置为进行智能卡验证。



注意

如果您使用 **--mkhomedir** 选项安装了 IdM 客户端，则远程用户将能够登录到其主目录。否则，默认登录位置是目录结构的根目录，**/**。

其他资源

- 使用 **/usr/share/doc/ansible-freeipa/playbooks/** 目录中 **ipasmartcard_server** 角色的 playbook 示例

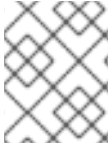
2.5. 在 IDM WEB UI 的用户条目中添加证书

按照以下流程，向 IdM Web UI 中的用户条目中添加外部证书。



注意

也可以将证书映射数据上传到 IdM 中的用户条目，而不必上传整个证书。包含完整证书或证书映射数据的用户条目可以和相应的证书映射规则一起使用，以便于系统管理员配置智能卡身份验证。详情请参阅 [配置身份验证的证书映射规则](#)。



注意

如果用户的证书由 IdM 证书颁发机构发布，则证书已存储在用户条目中，您不需要按照此流程操作。

先决条件

- 您有要添加到用户条目的证书。

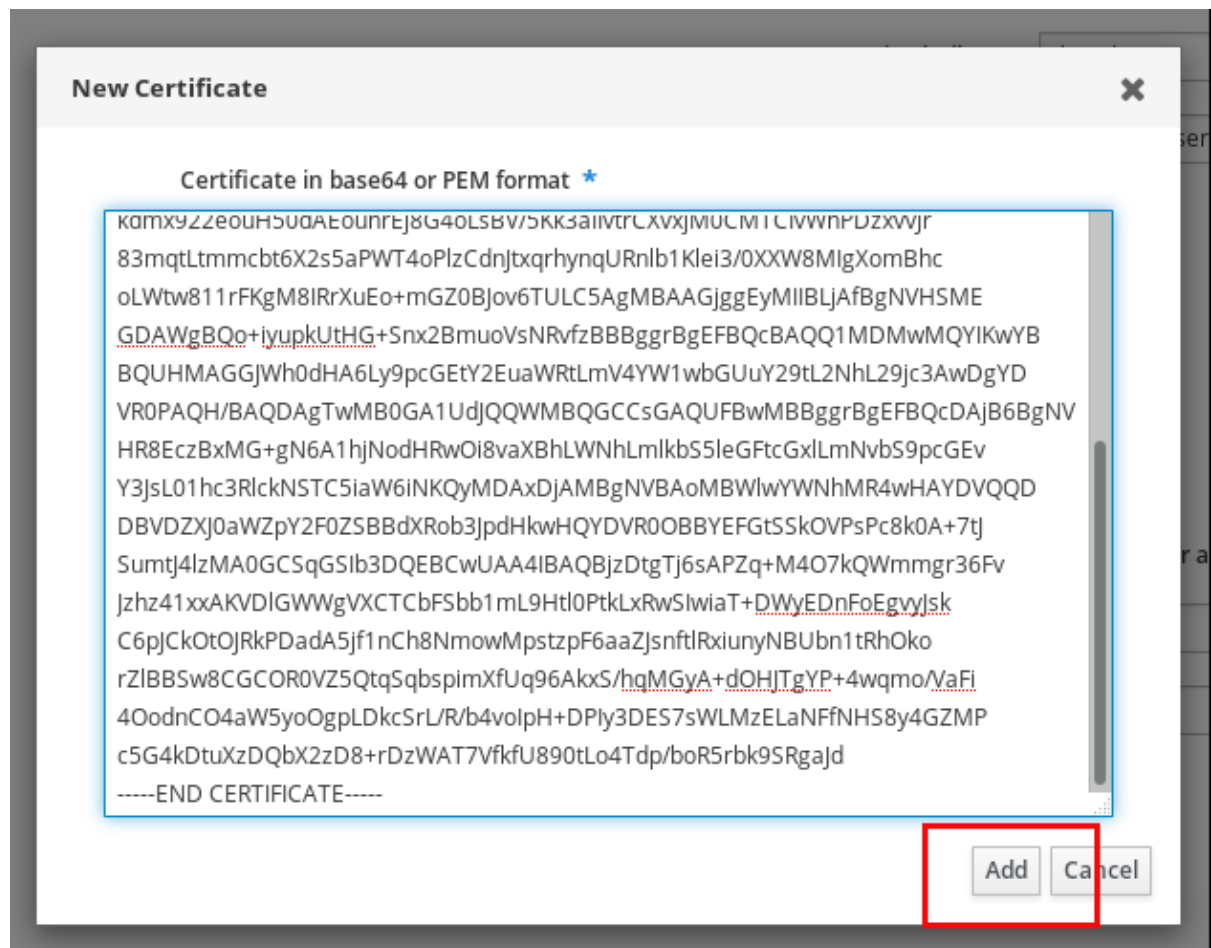
流程

1. 如果要给另一个用户添加证书，请以管理员身份登录到 IdM Web UI。要在您自己的配置文件中添加证书，您不需要管理员的凭证。
2. 导航到 **Users → Active users → sc_user**。
3. 找到 **Certificate** 选项，并单击 **Add**。
4. 在命令行界面中，使用 **cat** 工具或文本编辑器以 **PEM** 格式显示证书：

```
[user@client SmartCard]$ cat testuser.crt
```

5. 将证书从 CLI 复制并粘贴到 Web UI 中打开的窗口中。
6. 单击 **Add**。

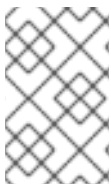
图 2.1. 在 IdM Web UI 中添加新证书



sc_user 条目现在包含一个外部证书。

2.6. 在 IDM CLI 中向用户条目中添加证书

按照以下流程，将外部证书添加到 IdM CLI 中的用户条目。



注意

也可以将证书映射数据上传到 IdM 中的用户条目，而不必上传整个证书。包含完整证书或证书映射数据的用户条目可以和相应的证书映射规则一起使用，以便于系统管理员配置智能卡身份验证。详情请参阅 [配置身份验证的证书映射规则](#)。



注意

如果用户的证书由 IdM 证书颁发机构发布，则证书已存储在用户条目中，您不需要按照此流程操作。

先决条件

- 您有要添加到用户条目的证书。

流程

1. 如果要给另一个用户添加证书，请以管理员身份登录到 IdM CLI：


```
[user@client SmartCard]$ kinit admin
```

要在您自己的配置文件中添加证书，您不需要管理员的凭证：

```
[user@client SmartCard]$ kinit sc_user
```

2. 创建一个包含证书的环境变量，该变量移除了标头和页脚，并串联成一行，这是 **ipa user-add-cert** 命令期望的格式：

```
[user@client SmartCard]$ export CERT=`openssl x509 -outform der -in testuser.crt |  
base64 -w0 -`
```

请注意，**testuser.crt** 文件中的证书必须是 **PEM** 格式。

3. 使用 **ipa user-add-cert** 命令将证书添加到 **sc_user** 的配置文件：

```
[user@client SmartCard]$ ipa user-add-cert sc_user --certificate=$CERT
```

sc_user 条目现在包含一个外部证书。

2.7. 安装用来管理和使用智能卡的工具

先决条件

- **gnutls-utils** 软件包已安装。
- **opensc** 软件包已安装。
- **pcscd** 服务正在运行。

在配置智能卡前，您必须安装相应的工具，该工具可以生成证书，并启动 **pcscd** 服务。

步骤

1. 安装 **opensc** 和 **gnutls-utils** 软件包：

```
# dnf -y install opensc gnutls-utils
```

2. 启动 **pcscd** 服务。

```
# systemctl start pcscd
```

验证步骤

- 验证 **pcscd** 服务是否已启动并运行

```
# systemctl status pcscd
```

2.8. 准备智能卡并将证书和密钥上传到智能卡

按照以下流程，使用 **pkcs15-init** 工具配置智能卡，该工具可帮助您配置：

- 擦除智能卡
- 设置新的 PIN 和可选的 PIN Unblocking Keys (PUKs)
- 在智能卡上创建新插槽
- 在插槽存储证书、私钥和公钥
- 如果需要，请锁定智能卡设置，因为某些智能卡需要这个类型的最终化



注意

pkcs15-init 工具可能无法使用所有智能卡。您必须使用您使用智能卡的工具。

先决条件

- 已安装 **opensc** 软件包，其中包括 **pkcs15-init** 工具。
如需了解更多详细信息，请参阅 [安装用于管理和使用智能卡的工具](#)。
- 该卡插入读卡器并连接到计算机。
- 您有一个要存储在智能卡上的私钥、公钥和证书。在此流程中，**testuser.key**、**testuserpublic.key** 和 **testuser.crt** 是用于私钥、公钥和证书的名称。
- 您有当前的智能卡用户 PIN 和 Security Officer PIN (SO-PIN)。

流程

1. 擦除智能卡并使用您的 PIN 验证自己：

```
$ pkcs15-init --erase-card --use-default-transport-keys
Using reader with a card: Reader name
PIN [Security Officer PIN] required.
Please enter PIN [Security Officer PIN]:
```

这个卡已经被清除。

2. 初始化智能卡，设置您的用户 PIN 和 PUK，以及您的安全响应 PIN 和 PUK：

```
$ pkcs15-init --create-pkcs15 --use-default-transport-keys \ --pin 963214 --puk 321478 --so-
pin 65498714 --so-puk 784123
Using reader with a card: Reader name
```

pkcs15-init 工具在智能卡上创建一个新插槽。

3. 为插槽设置标签和验证 ID：

```
$ pkcs15-init --store-pin --label testuser \ --auth-id 01 --so-pin 65498714 --pin 963214 --puk
321478
Using reader with a card: Reader name
```

标签设置为人类可读的值，在本例中为 **testuser**。**auth-id** 必须是两个十六进制值，在本例中设为 **01**。

4. 在智能卡的新插槽中存储并标记私钥：

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \ --auth-id 01 --id 01 --pin 963214
```

Using reader with a card: *Reader name*



注意

在存储您的私钥并将证书存储在下一步中时，您为 **--id** 指定的值必须相同。建议为 **--id** 指定自己的值，否则它们将更复杂的值由工具计算。

5. 在智能卡上的新插槽中存储并标记该证书：

```
$ pkcs15-init --store-certificate testuser.crt --label testuser_cert \ --auth-id 01 --id 01 --format pem --pin 963214
```

Using reader with a card: *Reader name*

6. 可选：在智能卡上的新插槽中保存并标记公钥：

```
$ pkcs15-init --store-public-key testuserpublic.key --label testuserpublic_key --auth-id 01 --id 01 --pin 963214
```

Using reader with a card: *Reader name*



注意

如果公钥与私钥或证书对应，请指定与私钥或证书的 ID 相同的 ID。

7. 可选：某些智能卡要求您通过锁定设置来完成卡：

```
$ pkcs15-init -F
```

此时您的智能卡在新创建的插槽中包含证书、私钥和公钥。您还创建了您的用户 PIN 和 PUK，以及安全响应 PIN 和 PUK。

2.9. 使用智能卡登录到 IDM

按照以下流程，使用智能卡登录到 IdM Web UI。

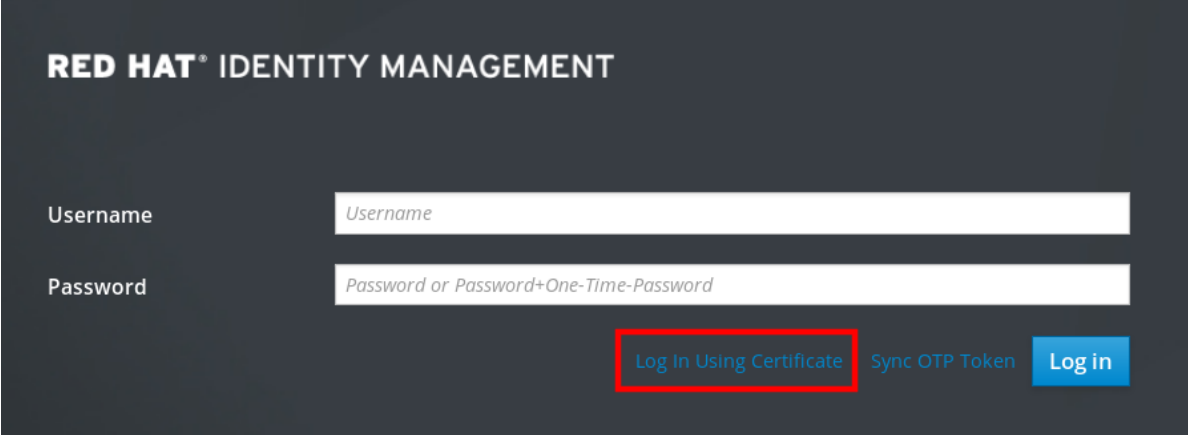
先决条件

- web 浏览器被配置为使用智能卡验证。
- IdM 服务器被配置为智能卡验证。
- 在您的智能卡中安装的证书由 IdM 服务器发出，或者已添加到 IdM 的用户条目中。
- 您知道解锁智能卡所需的 PIN。
- 智能卡已插入到读取器中。

流程

1. 在浏览器中打开 IdM Web UI。

2. 点使用证书登陆。



RED HAT® IDENTITY MANAGEMENT

Username

Password

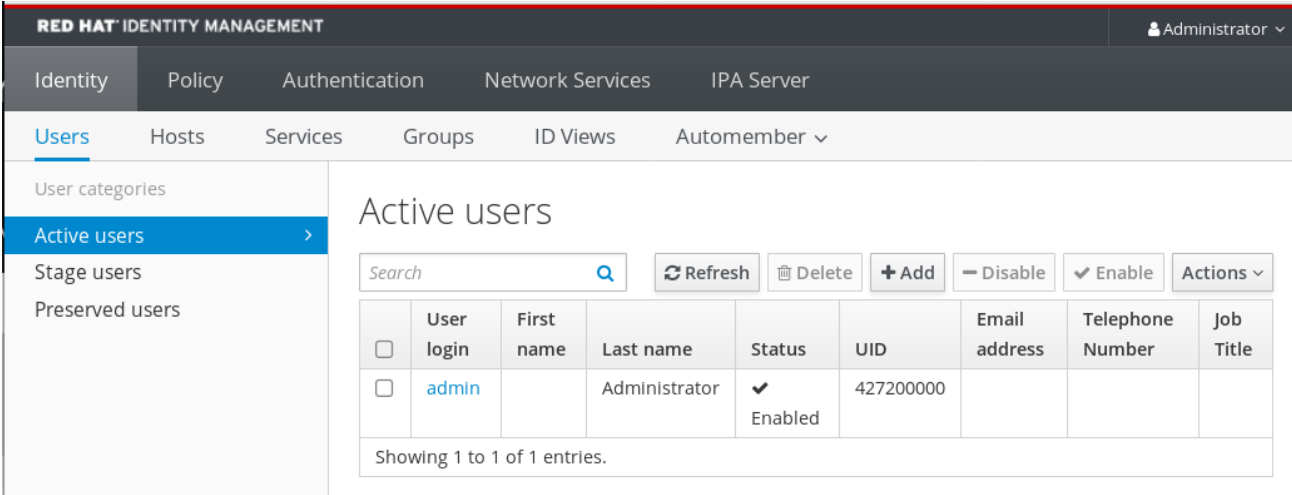
[Log In Using Certificate](#) [Sync OTP Token](#) [Log in](#)

3. 如果 **Password Required** 对话框打开，请添加 PIN 来解锁智能卡，然后单击 **OK** 按钮。此时会打开 **User Identification Request** 对话框。

如果智能卡包含多个证书，请在 **选择用于验证的证书** 下方的下拉列表中选择您要用于身份验证的证书。

4. 单击 **OK** 按钮。

现在，您已成功登录到 IdM Web UI。



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
<input type="checkbox"/>	admin		Administrator	✓ Enabled	427200000			

Showing 1 to 1 of 1 entries.

2.10. 在 IDM 客户端中使用智能卡验证登录到 GDM

GNOME 桌面管理器(GDM)需要身份验证。您可以使用您的密码，但是，您也可以使用智能卡进行身份验证。

按照以下流程，使用智能卡验证来访问 GDM。

先决条件

- 为智能卡验证配置了系统。详情请参阅[为智能卡验证配置 IdM 客户端](#)。
- 该智能卡包含您的证书和私钥。
- 该用户帐户是 IdM 域的成员。
- 智能卡上的证书通过以下方式映射到用户条目：

- 为特定用户条目分配证书。详情请参阅 [Adding a certificate to a user entry in the IdM Web UI](#) 或 [Adding a certificate to a user entry in the IdM CLI](#) 。
- 应用到该帐户的证书映射数据。详情请查看用于 [在智能卡上配置身份验证的证书映射规则](#)。

流程

1. 在读取器中插入智能卡。
2. 输入智能卡 PIN。
3. 点 **Sign In**。

您成功登录到 RHEL 系统，并且您有一张由 IdM 服务器提供的 TGT。

验证步骤

- 在 **Terminal** 中输入 **klist**，并检查结果：

```
$ klist
Ticket cache: KEYRING:persistent:1358900015:krb_cache_TObtNMd
Default principal: example.user@REDHAT.COM

Valid starting    Expires          Service principal
04/20/2020 13:58:24 04/20/2020 23:58:24 krbtgt/EXAMPLE.COM@EXAMPLE.COM
renew until 04/27/2020 08:58:15
```

2.11. 在 SU 命令中使用智能卡验证

切换到其他用户需要身份验证。您可以使用密码或证书。按照以下流程，通过 **su** 命令使用智能卡。这意味着输入 **su** 命令后，系统会提示您输入智能卡 PIN。

先决条件

- 为智能卡验证配置了您的 IdM 服务器和客户端。
 - 请参阅[为智能卡验证配置 IdM 服务器](#)
 - 请参阅[为智能卡验证配置 IdM 客户端](#)
- 该智能卡包含您的证书和私钥。请参阅[智能卡中的证书](#)
- 该卡插入读卡器并连接到计算机。

步骤

- 在终端窗口中，使用 **su** 命令切换到其他用户：

```
$ su - example.user
PIN for smart_card
```

如果配置正确，会提示您输入智能卡 PIN。

第 3 章 为 IDM 中智能卡验证配置 ADCS 发布的证书

要在 IdM 中为其证书是由活动目录(AD)证书服务发布的用户配置智能卡验证：

- 您的部署是基于身份管理(IdM)和活动目录(AD)之间的跨林信任。
- 您希望允许智能卡验证存储在 AD 中的帐户的用户。
- 证书创建并存储在活动目录证书服务(ADCS)中。

有关智能卡验证的概述，请参阅[了解智能卡验证](#)。

配置通过以下步骤完成：

- [将 CA 和用户证书从活动目录复制到 IdM 服务器和客户端](#)
- [使用 ADCS 证书为智能卡身份验证配置 IdM 服务器和客户端](#)
- [转换 PFX\(PKCS#12\)文件，以便能够将证书和私钥存储到智能卡中](#)
- [在 sssd.conf 文件中配置超时](#)
- [为智能卡身份验证创建证书映射规则](#)

先决条件

- 身份管理(IdM)和活动目录(AD)信任已安装
详情请参阅在 [IdM 和 AD 之间安装信任](#)。
- 活动目录证书服务(ADCS)已安装，并且用户证书已生成

3.1. 信任配置和证书使用量所需的 WINDOWS 服务器设置

您必须在 Windows 服务器上配置以下内容：

- 已安装活动目录证书服务(ADCS)
- 创建证书颁发机构
- [可选] 如果您正在使用证书颁发机构 Web 注册，则必须配置互联网信息服务(IIS)

导出证书：

- 密钥必须有 **2048** 位或更多
- 包括一个私钥
- 您需要一个以下格式的证书：个人信息交换 - **PKCS #12(.PFX)**
 - 启用证书隐私

3.2. 使用 SFTP 从 ACTIVE DIRECTORY 复制证书

要能够使用智能卡身份验证，您需要复制以下证书文件：

- **CER** 格式的根 CA 证书：IdM 服务器上的 **adcs-winserver-ca.cer**。

- 具有 **PFX** 格式私钥的用户证书：IdM 客户端上的 **aduser1.pfx**。



注意

这个过程预期 SSH 访问是允许的。如果 SSH 不可用，用户必须将文件从 AD 服务器复制到 IdM 服务器和客户端。

步骤

1. 从 **IdM 服务器** 连接，并将 **adcs-winserver-ca.cer** 根证书复制到 IdM 服务器：

```
root@idmserver ~]# sftp Administrator@winserver.ad.example.com
Administrator@winserver.ad.example.com's password:
Connected to Administrator@winserver.ad.example.com.
sftp> cd <Path to certificates>
sftp> ls
adcs-winserver-ca.cer  aduser1.pfx
sftp>
sftp> get adcs-winserver-ca.cer
Fetching <Path to certificates>/adcs-winserver-ca.cer to adcs-winserver-ca.cer
<Path to certificates>/adcs-winserver-ca.cer      100% 1254  15KB/s 00:00
sftp quit
```

2. 从 **IdM 客户端** 连接，并将 **aduser1.pfx** 用户证书复制到客户端：

```
[root@client1 ~]# sftp Administrator@winserver.ad.example.com
Administrator@winserver.ad.example.com's password:
Connected to Administrator@winserver.ad.example.com.
sftp> cd /<Path to certificates>
sftp> get aduser1.pfx
Fetching <Path to certificates>/aduser1.pfx to aduser1.pfx
<Path to certificates>/aduser1.pfx      100% 1254  15KB/s 00:00
sftp quit
```

现在，CA 证书保存在 IdM 服务器上，用户证书存储在客户端机器上。

3.3. 使用 ADCS 证书为智能卡身份验证配置 IDM 服务器和客户端

您必须配置 IdM（身份管理）服务器和客户端，以便能够在 IdM 环境中使用智能卡身份验证。IdM 包含进行了所有必要更改的 **ipa-adviser** 脚本：

- 安装所需的软件包
- 配置 IdM 服务器和客户端
- 将 CA 证书复制到期望的位置

您可以在 IdM 服务器中运行 **ipa-adviser**。

按照以下流程为智能卡验证配置服务器和客户端：

- 在 IdM 服务器中：准备 **ipa-adviser** 脚本，以配置您的 IdM 服务器进行智能卡验证。
- 在 IdM 服务器中：准备 **ipa-adviser** 脚本，以配置您的 IdM 客户端进行智能卡验证。

- 在 IdM 服务器中：使用 AD 证书在 IdM 服务器中应用 **ipa-adviser** 服务器脚本。
- 将客户端脚本移动到 IdM 客户端机器中。
- 在 IdM 客户端中：使用 AD 证书在 IdM 客户端中应用 **ipa-adviser** 客户端脚本。

先决条件

- 证书已复制到 IdM 服务器。
- 获取 Kerberos 票据。
- 以具有管理权限的用户身份登录。

步骤

1. 在 IdM 服务器中，使用 **ipa-adviser** 脚本来配置客户端：

```
[root@idmsvr ~]# ipa-adviser config-client-for-smart-card-auth > sc_client.sh
```

2. 在 IdM 服务器中，使用 **ipa-adviser** 脚本来配置服务器：

```
[root@idmsvr ~]# ipa-adviser config-server-for-smart-card-auth > sc_server.sh
```

3. 在 IdM 服务器中执行脚本：

```
[root@idmsvr ~]# sh -x sc_server.sh adcs-winsvr-ca.cer
```

- 它配置 IdM Apache HTTP 服务器。
- 它在 KDC（Key Distribution Center）中启用 PKINIT（Public Key Cryptography for Initial Authentication in Kerberos）。
- 它将 IdM Web UI 配置为接受智能卡授权请求。

4. 将 **sc_client.sh** 脚本复制到客户端系统中：

```
[root@idmsvr ~]# scp sc_client.sh root@client1.idm.example.com:/root
Password:
sc_client.sh          100% 2857  1.6MB/s  00:00
```

5. 将 Windows 证书复制到客户端系统中：

```
[root@idmsvr ~]# scp adcs-winsvr-ca.cer root@client1.idm.example.com:/root
Password:
adcs-winsvr-ca.cer    100% 1254  952.0KB/s  00:00
```

6. 在客户端系统中运行客户端脚本：

```
[root@idmclient1 ~]# sh -x sc_client.sh adcs-winsvr-ca.cer
```

CA 证书以正确格式安装在 IdM 服务器和客户端系统中，下一步是将用户证书复制到智能卡本身。

3.4. 转换 PFX 文件

在将 PFX(PKCS#12)文件存储到智能卡之前，您必须：

- 将文件转换为 PEM 格式
- 将私钥和证书提取到两个不同的文件中

先决条件

- PFX 文件被复制到 IdM 客户端机器中。

流程

1. 在 IdM 客户端中，采用 PEM 格式：

```
[root@idmclient1 ~]# openssl pkcs12 -in aduser1.pfx -out aduser1_cert_only.pem -clcerts -nodes
Enter Import Password:
```

2. 将密钥提取到单独的文件中：

```
[root@idmclient1 ~]# openssl pkcs12 -in adduser1.pfx -nocerts -out adduser1.pem > adduser1.key
```

3. 将公共证书提取到单独的文件中：

```
[root@idmclient1 ~]# openssl pkcs12 -in adduser1.pfx -clcerts -nokeys -out aduser1_cert_only.pem > aduser1.crt
```

此时，您可以将 **aduser1.key** 和 **aduser1.crt** 存储到智能卡。

3.5. 安装用来管理和使用智能卡的工具

先决条件

- **gnutls-utils** 软件包已安装。
- **opensc** 软件包已安装。
- **pcscd** 服务正在运行。

在配置智能卡前，您必须安装相应的工具，该工具可以生成证书，并启动 **pcscd** 服务。

步骤

1. 安装 **opensc** 和 **gnutls-utils** 软件包：

```
# dnf -y install opensc gnutls-utils
```

2. 启动 **pcscd** 服务。

```
# systemctl start pcscd
```

验证步骤

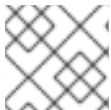
- 验证 **pcscd** 服务是否已启动并运行

```
# systemctl status pcscd
```

3.6. 准备智能卡并将证书和密钥上传到智能卡

按照以下流程，使用 **pkcs15-init** 工具配置智能卡，该工具可帮助您配置：

- 擦除智能卡
- 设置新的 PIN 和可选的 PIN Unblocking Keys (PUKs)
- 在智能卡上创建新插槽
- 在插槽存储证书、私钥和公钥
- 如果需要，请锁定智能卡设置，因为某些智能卡需要这个类型的最终化



注意

pkcs15-init 工具可能无法使用所有智能卡。您必须使用您使用智能卡的工具。

先决条件

- 已安装 **opensc** 软件包，其中包括 **pkcs15-init** 工具。
如需了解更多详细信息，请参阅 [安装用于管理和使用智能卡的工具](#)。
- 该卡插入读卡器并连接到计算机。
- 您有一个要存储在智能卡上的私钥、公钥和证书。在此流程中，**testuser.key**、**testuserpublic.key** 和 **testuser.crt** 是用于私钥、公钥和证书的名称。
- 您有当前的智能卡用户 PIN 和 Security Officer PIN (SO-PIN)。

流程

1. 擦除智能卡并使用您的 PIN 验证自己：

```
$ pkcs15-init --erase-card --use-default-transport-keys
Using reader with a card: Reader name
PIN [Security Officer PIN] required.
Please enter PIN [Security Officer PIN]:
```

这个卡已经被清除。

2. 初始化智能卡，设置您的用户 PIN 和 PUK，以及您的安全响应 PIN 和 PUK：

```
$ pkcs15-init --create-pkcs15 --use-default-transport-keys \ --pin 963214 --puk 321478 --so-
pin 65498714 --so-puk 784123
Using reader with a card: Reader name
```

pkcs15-init 工具在智能卡上创建一个新插槽。

3. 为插槽设置标签和验证 ID：

```
$ pkcs15-init --store-pin --label testuser \ --auth-id 01 --so-pin 65498714 --pin 963214 --puk 321478
Using reader with a card: Reader name
```

标签设置为人类可读的值，在本例中为 **testuser**。**auth-id** 必须是两个十六进制值，在本例中设为 **01**。

4. 在智能卡的新插槽中存储并标记私钥：

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \ --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```

**注意**

在存储您的私钥并将证书存储在下一步中时，您为 **--id** 指定的值必须相同。建议为 **--id** 指定自己的值，否则它们将更复杂的值由工具计算。

5. 在智能卡上的新插槽中存储并标记该证书：

```
$ pkcs15-init --store-certificate testuser.crt --label testuser_cert \ --auth-id 01 --id 01 --format pem --pin 963214
Using reader with a card: Reader name
```

6. 可选：在智能卡上的新插槽中保存并标记公钥：

```
$ pkcs15-init --store-public-key testuserpublic.key --label testuserpublic_key --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```

**注意**

如果公钥与私钥或证书对应，请指定与私钥或证书的 ID 相同的 ID。

7. 可选：某些智能卡要求您通过锁定设置来完成卡：

```
$ pkcs15-init -F
```

此时您的智能卡在新创建的插槽中包含证书、私钥和公钥。您还创建了您的用户 PIN 和 PUK，以及安全响应 PIN 和 PUK。

3.7. 在 SSSD.CONF 中配置超时

使用智能卡证书进行身份验证的时间可能比 SSSD 使用的默认超时时间更长。超时时间可能是由以下原因造成的：

- 慢的读取器
- 从物理设备转发到虚拟环境

- 保存在智能卡上的证书太多
- 如果使用 OCSP 验证证书，则来自 OCSP（在线证书状态协议）响应器的响应较慢

在这种情况下，您可以在 **sssd.conf** 文件中将以下超时时间延长到 60 秒：

- **p11_child_timeout**
- **krb5_auth_timeout**

先决条件

- 您必须以 root 身份登录。

步骤

1. 打开 **sssd.conf** 文件：

```
[root@idmclient1 ~]# vim /etc/sss/sssd.conf
```

2. 更改 **p11_child_timeout** 的值：

```
[pam]
p11_child_timeout = 60
```

3. 更改 **krb5_auth_timeout** 的值：

```
[domain/IDM.EXAMPLE.COM]
krb5_auth_timeout = 60
```

4. 保存设置。

现在，在验证被认为出现超时故障前，与智能卡的交互可以运行 1 分钟（60 秒）。

3.8. 为智能卡身份验证创建证书映射规则

如果要将一个证书用于 AD(Active Directory)和 IdM 中拥有帐户的用户，您可以在 IdM 服务器上创建证书映射规则。

创建这样的规则后，用户可以在这两个域中使用智能卡进行验证。

有关证书映射规则的详情，请参阅 [用于配置身份验证的证书映射规则](#)。

第 4 章 用于配置身份验证的证书映射规则

在以下情况下可能需要配置证书映射规则：

- 证书是由与 IdM 域有信任关系的活动目录(AD)的证书系统发布的。
- 证书由外部证书颁发机构发布。
- IdM 环境较大，有很多用户使用智能卡的用户。在这种情况下，添加完整证书可能会比较复杂。在大多数情况下，主题和签发者是可预测的，因此与完整证书相比，更容易提前添加。

作为系统管理员，您可以创建证书映射规则，并在向特定用户签发证书前向用户条目添加证书映射数据。签发证书后，用户就可以使用证书登录，即使证书还没有上传到用户条目。

另外，因为证书会定期续订，因此证书映射规则可减少管理开销。续订用户证书时，管理员不必更新用户条目。例如，如果映射基于 **Subject** 和 **Issuer** 的值，如果新的证书具有与旧证书相同的主题和签发者，则映射仍适用。如果使用完整证书，则管理员必须将新证书上传到用户条目以替换旧证书。

设置证书映射：

1. 管理员必须将证书映射数据或完整证书加载到用户帐户中。
2. 管理员必须创建证书映射规则，以允许其帐户包含与证书信息匹配的证书映射数据条目的用户成功登录到 IdM。

创建证书映射规则后，当最终用户提供保存在 [文件系统](#) 或 [智能卡](#) 上的证书时，身份验证可以成功。



注意

密钥分发中心(KDC)有一个用于证书映射规则的缓存。缓存在第一个 **certauth** 请求时填充，它有一个 300 秒的硬编码超时。KDC 不会看到对证书映射规则的任何更改，除非它重启了或缓存过期了。

有关构成映射规则的单组组件，以及如何获取和使用它们的详细信息，请参阅 [IdM 中的身份映射规则组件](#)，以及 [获取证书中的签发者](#)，以便在 [匹配规则](#) 中使用。



注意

您的证书映射规则可取决于您使用证书的用例。例如，如果您使用带有证书的 SSH，则必须有从证书中提取公钥的完整证书。

第 5 章 使用 WEB 控制台为集中管理的用户配置智能卡验证

在 RHEL web 控制台中为集中管理的用户配置智能卡验证：

- 身份管理
- Active Directory，它在 Identity Management 的跨林信任中连接

先决条件

- 您要使用智能卡验证的系统必须是 Active Directory 或 Identity Management 域的成员。
- 用于智能卡验证的证书必须与身份管理或 Active Directory 中的特定用户关联。
有关在 Identity Management 中将证书与用户关联的详情，请参阅[在 IdM Web UI 中的用户条目中添加证书](#)，或[将证书添加到 IdM CLI 中的用户条目中](#)。

5.1. 实现中央管理用户的智能卡验证

智能卡是一个物理设备，可以使用保存在卡中的证书提供个人验证。个人验证意味着，您可以象使用用户密码一样使用智能卡。

您可以使用私钥和证书的形式在智能卡中保存用户凭证。特殊的软件和硬件可用于访问它们。您可以将智能卡插入到读取器或者 USB 套接字中，并为智能卡提供 PIN 代码，而不是提供密码。

身份管理(IdM)支持使用如下方式的智能卡身份验证：

- IdM 证书颁发机构发布的用户证书。
- Active Directory 证书服务(ADCS)证书颁发机构发布的用户证书。



注意

如果要使用智能卡验证，请参阅硬件要求：[RHEL8+ 中的智能卡支持](#)。

5.2. 安装用来管理和使用智能卡的工具

先决条件

- **gnutls-utils** 软件包已安装。
- **opensc** 软件包已安装。
- **pcscd** 服务正在运行。

在配置智能卡前，您必须安装相应的工具，该工具可以生成证书，并启动 **pcscd** 服务。

流程

1. 安装 **opensc** 和 **gnutls-utils** 软件包：

```
# dnf -y install opensc gnutls-utils
```

2. 启动 **pcscd** 服务。

■

```
# systemctl start pcscd
```

验证步骤

- 验证 **pcscd** 服务是否已启动并运行

```
# systemctl status pcscd
```

5.3. 准备智能卡并将证书和密钥上传到智能卡

按照以下流程，使用 **pkcs15-init** 工具配置智能卡，该工具可帮助您配置：

- 擦除智能卡
- 设置新的 PIN 和可选的 PIN Unblocking Keys (PUKs)
- 在智能卡上创建新插槽
- 在插槽存储证书、私钥和公钥
- 如果需要，请锁定智能卡设置，因为某些智能卡需要这个类型的最终化



注意

pkcs15-init 工具可能无法使用所有智能卡。您必须使用您使用智能卡的工具。

先决条件

- 已安装 **opensc** 软件包，其中包括 **pkcs15-init** 工具。
如需了解更多详细信息，请参阅 [安装用于管理和使用智能卡的工具](#)。
- 该卡插入读卡器并连接到计算机。
- 您有一个要存储在智能卡上的私钥、公钥和证书。在此流程中，**testuser.key**、**testuserpublic.key** 和 **testuser.crt** 是用于私钥、公钥和证书的名称。
- 您有当前的智能卡用户 PIN 和 Security Officer PIN (SO-PIN)。

步骤

1. 擦除智能卡并使用您的 PIN 验证自己：

```
$ pkcs15-init --erase-card --use-default-transport-keys
Using reader with a card: Reader name
PIN [Security Officer PIN] required.
Please enter PIN [Security Officer PIN]:
```

这个卡已经被清除。

2. 初始化智能卡，设置您的用户 PIN 和 PUK，以及您的安全响应 PIN 和 PUK：

```
$ pkcs15-init --create-pkcs15 --use-default-transport-keys \ --pin 963214 --puk 321478 --so-
pin 65498714 --so-puk 784123
Using reader with a card: Reader name
```

pkcs15-init 工具在智能卡上创建一个新插槽。

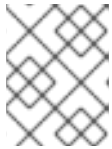
3. 为插槽设置标签和验证 ID：

```
$ pkcs15-init --store-pin --label testuser \ --auth-id 01 --so-pin 65498714 --pin 963214 --puk 321478
Using reader with a card: Reader name
```

标签设置为人类可读的值，在本例中为 **testuser**。**auth-id** 必须是两个十六进制值，在本例中设为 **01**。

4. 在智能卡的新插槽中存储并标记私钥：

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \ --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```



注意

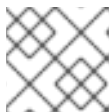
在存储您的私钥并将证书存储在下一步中时，您为 **--id** 指定的值必须相同。建议为 **--id** 指定自己的值，否则它们将更复杂的值由工具计算。

5. 在智能卡上的新插槽中存储并标记该证书：

```
$ pkcs15-init --store-certificate testuser.crt --label testuser_crt \ --auth-id 01 --id 01 --format pem --pin 963214
Using reader with a card: Reader name
```

6. 可选：在智能卡上的新插槽中保存并标记公钥：

```
$ pkcs15-init --store-public-key testuserpublic.key --label testuserpublic_key --auth-id 01 --id 01 --pin 963214
Using reader with a card: Reader name
```



注意

如果公钥与私钥或证书对应，请指定与私钥或证书的 ID 相同的 ID。

7. 可选：某些智能卡要求您通过锁定设置来完成卡：

```
$ pkcs15-init -F
```

此时您的智能卡在新创建的插槽中包含证书、私钥和公钥。您还创建了您的用户 PIN 和 PUK，以及安全响应 PIN 和 PUK。

5.4. 为 WEB 控制台启用智能卡验证

要在 web 控制台中使用智能卡验证，请在 **cockpit.conf** 文件中启用智能卡验证。

另外，您还可以在同一文件中禁用密码验证。

先决条件

- 已安装 RHEL web 控制台。

步骤

1. 使用管理员权限登录到 RHEL web 控制台。
2. 点 **Terminal**。
3. 在 `/etc/cockpit/cockpit.conf` 中，将 **ClientCertAuthentication** 设置为 **yes**：

```
[WebService]
ClientCertAuthentication = yes
```

4. 可选：在 **cockpit.conf** 中禁用基于密码的身份验证：

```
[Basic]
action = none
```

这个配置禁用了密码验证，且必须总是使用智能卡。

5. 重启 Web 控制台，以确保 **cockpit.service** 接受更改：

```
# systemctl restart cockpit
```

5.5. 使用智能卡登录到 WEB 控制台

您可以使用智能卡登录到 web 控制台。

先决条件

- 保存在智能卡中的有效证书，该证书与 Active Directory 或 Identity Management 域中的用户帐户关联。
- PIN 用于解锁智能卡。
- 已经将智能卡放入读卡器。

步骤

1. 打开 Web 浏览器，并在地址栏中添加 Web 控制台的地址。
浏览器要求您添加 PIN 保护保存在智能卡中的证书。
2. 在 **Password Required** 对话框中，输入 PIN 并点 **OK**。
3. 在 **User Identification Request** 对话框中，选择保存在智能卡中的证书。
4. 选择 **Remember this decision**。
系统下次打开这个窗口。



注意

此步骤不适用于 Google Chrome 用户。

5. 点击 OK。

您现在已连接，Web 控制台会显示其内容。

5.6. 为智能卡用户启用无密码的 SUDO 验证

您可以使用 Web 控制台为智能卡用户配置 **sudo** 和其他服务的无密码身份验证。

另一种选择是，如果您使用红帽身份管理，您可以将初始 Web 控制台证书身份验证声明为可信，以向 **sudo**、SSH 或其他服务进行身份验证。为此，Web 控制台会在用户会话中自动创建 S4U2Proxy Kerberos ticket。

先决条件

- 身份管理已安装。
- 跨林信任中与身份管理连接的活动目录。
- 设置为登录到 web 控制台的智能卡。如需更多信息，请参阅[使用 Web 控制台配置智能卡验证](#)。

步骤

1. 设置约束委派规则，以列出托管票据可以访问哪些主机。

例 5.1. 设置约束委派规则

Web 控制台会话运行主机 **host.example.com**，并应受信任，以通过 **sudo** 访问自己的主机。此外，我们还添加了第二个可信主机 - **remote.example.com**。

- 创建以下委派：
 - 运行以下命令添加特定规则可以访问的目标机器列表：

```
# ipa servicedelegationtarget-add cockpit-target
# ipa servicedelegationtarget-add-member cockpit-target \ --
principals=host/host.example.com@EXAMPLE.COM \ --
principals=host/remote.example.com@EXAMPLE.COM
```

- 要允许 Web 控制台会话(HTTP/principal)访问该主机列表，请使用以下命令：

```
# ipa servicedelegationrule-add cockpit-delegation
# ipa servicedelegationrule-add-member cockpit-delegation \ --
principals=HTTP/host.example.com@EXAMPLE.COM
# ipa servicedelegationrule-add-target cockpit-delegation \ --
servicedelegationtargets=cockpit-target
```

2. 在对应服务中启用 GSS 身份验证：

- a. 对于 sudo，在 **/etc/sss/sss.conf** 文件中启用 **pam_sss_gss** 模块：
- i. 以 root 用户身份，将域的条目添加到 **/etc/sss/sss.conf** 配置文件。

```
[domain/example.com]
pam_gssapi_services = sudo, sudo-i
```

- ii. 在第一行启用 `/etc/pam.d/sudo` 文件中的模块。

```
auth sufficient pam_sss_gss.so
```

- b. 对于 SSH，将 `/etc/ssh/sshd_config` 文件中的 `GSSAPIAuthentication` 选项更新为 `yes`。



警告

从 Web 控制台连接到远程 SSH 主机时，委派的 S4U 票据不会被转发到远程 SSH 主机。使用您的票据在远程主机上向 `sudo` 进行身份验证将无法正常工作。

验证

1. 使用智能卡登录到 web 控制台。
2. 点 **Limited access** 按钮。
3. 使用您的智能卡进行验证。

或者：

- 尝试使用 SSH 连接到其他主机。

5.7. 限制用户会话和内存以防止 DOS 攻击

证书验证被分离和隔离 **cockpit-ws** Web 服务器的实例保护，使其免受要模拟其他用户的攻击者的攻击。但是，这会引入了一个潜在的拒绝服务(DoS)攻击：远程攻击者可以创建大量证书，并将大量 HTTPS 请求发送到 **cockpit-ws** 各自使用不同的证书。

为防止这一 DoS，这些 Web 服务器实例的收集资源受到限制。默认情况下，对连接数量和内存用量限制为 200 个线程，且具有 75%（软）/ 90%（硬）内存限值。

以下流程描述了通过限制连接和内存量的资源保护。

步骤

1. 在终端中，打开 **system-cockpithttps.slice** 配置文件：

```
# systemctl edit system-cockpithttps.slice
```

2. 将 **TasksMax** 限制为 100，将 **CPUQuota** 限制为 30%：

```
[Slice]
# change existing value
TasksMax=100
# add new restriction
CPUQuota=30%
```

3. 要应用这些更改，请重启系统：

—

```
# systemctl daemon-reload  
# systemctl stop cockpit
```

现在，新的内存和用户会话限制了 **cockpit-ws** Web 服务器不受 DoS 攻击。

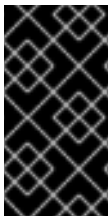
第 6 章 使用本地证书配置智能卡验证

使用本地证书配置智能卡验证：

- 主机没有连接到某个域。
- 您需要在这个主机上使用智能卡进行验证。
- 您需要使用智能卡验证配置 SSH 访问。
- 您需要使用 **authselect** 配置智能卡。

使用以下配置来实现这种情况：

- 为希望使用智能卡进行身份验证的用户获取用户证书。证书应该由在域中使用的可信认证认证机构生成。
如果您无法获得证书，您可以生成由本地证书颁发机构签名的用户证书用于测试。
- 在智能卡中保存证书和私钥。
- 为 SSH 访问配置智能卡验证。



重要

如果主机可以作为域的一部分，将主机添加到域中，并使用活动目录或者身份管理认证机构生成的证书。

有关如何为智能卡创建 IdM 证书的详情，请参考[为智能卡验证配置身份管理](#)。

先决条件

- 已安装 authselect
authselect 工具在 Linux 主机中配置用户验证，您可以使用它配置智能卡验证参数。有关 authselect 的详情，请参考[浏览 authselect](#)。
- RHEL 9 支持智能卡或者 USB 设备
详情请查看 [RHEL9 中的智能卡支持](#)。

6.1. 创建本地证书

按照以下流程执行以下任务：

- 生成 OpenSSL 证书颁发机构
- 创建证书签名请求



警告

以下步骤仅用于测试目的。由本地自签名证书颁发机构生成的证书不如使用 AD、IdM 或 RHCS 认证认证机构的安全。即使主机不是域的一部分，您仍应使用企业认证认证机构生成的证书。

流程

1. 创建可生成证书的目录，例如：

```
# mkdir /tmp/ca
# cd /tmp/ca
```

2. 设置证书（将此文本复制到 **ca** 目录中的命令行）：

```
cat > ca.cnf <<EOF
[ ca ]
default_ca = CA_default

[ CA_default ]
dir          = .
database     = \${dir}/index.txt
new_certs_dir = \${dir}/newcerts

certificate  = \${dir}/rootCA.crt
serial       = \${dir}/serial
private_key  = \${dir}/rootCA.key
RANDFILE     = \${dir}/rand

default_days = 365
default_crl_days = 30
default_md   = sha256

policy       = policy_any
email_in_dn  = no

name_opt     = ca_default
cert_opt     = ca_default
copy_extensions = copy

[ usr_cert ]
authorityKeyIdentifier = keyid, issuer

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints      = CA:true
keyUsage               = critical, digitalSignature, cRLSign, keyCertSign

[ policy_any ]
organizationName      = supplied
```

```

organizationalUnitName = supplied
commonName             = supplied
emailAddress           = optional

[ req ]
distinguished_name = req_distinguished_name
prompt             = no

[ req_distinguished_name ]
O = Example
OU = Example Test
CN = Example Test CA
EOF

```

3. 创建以下目录：

```
# mkdir certs crl newcerts
```

4. 创建以下文件：

```
# touch index.txt crlnumber index.txt.attr
```

5. 在串行文件中写入数字 01:

```
# echo 01 > serial
```

该命令在串行文件中写入数字 01。它是证书的序列号。当这个 CA 发布一个新证书时这个数字会加一。

6. 创建一个 OpenSSL root CA 密钥：

```
# openssl genrsa -out rootCA.key 2048
```

7. 创建自签名 root 认证认证机构证书：

```
# openssl req -batch -config ca.cnf \
-x509 -new -nodes -key rootCA.key -sha256 -days 10000 \
-set_serial 0 -extensions v3_ca -out rootCA.crt
```

8. 为您的用户名创建密钥：

```
# openssl genrsa -out example.user.key 2048
```

这个密钥是在本地系统中生成的，因此当密钥保存在卡中时，从系统中删除密钥。

您还可以直接在智能卡中创建密钥。要做到这一点，请遵循智能卡生产商生成的说明。

9. 创建证书签名请求配置文件（将这个文本复制到 ca 目录中的命令行中）：

```

cat > req.cnf <<EOF
[ req ]
distinguished_name = req_distinguished_name
prompt = no

```

```
[ req_distinguished_name ]
O = Example
OU = Example Test
CN = testuser

[ req_exts ]
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "testuser"
subjectKeyIdentifier = hash
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection, msSmartcardLogin
subjectAltName = otherName:msUPN;UTF8:testuser@EXAMPLE.COM,
email:testuser@example.com
EOF
```

10. 为 example.user 证书创建证书签名请求：

```
# openssl req -new -nodes -key example.user.key \
  -reqexts req_exts -config req.cnf -out example.user.csr
```

11. 配置新证书。过期期限设定为 1 年：

```
# openssl ca -config ca.cnf -batch -notext \
  -keyfile rootCA.key -in example.user.csr -days 365 \
  -extensions usr_cert -out example.user.crt
```

此时，认证颁发机构和证书被成功生成并准备好导入到智能卡。

6.2. 将证书复制到 SSSD 目录中

GNOME 桌面管理器(GDM)需要 SSSD。如果使用 GDM，则需要将 PEM 证书复制到 **/etc/sss/pki** 目录。

先决条件

- 已生成本地 CA 颁发机构和证书

流程

1. 确保已在系统中安装了 SSSD。

```
# rpm -q sssd
sssd-2.0.0.43.el8_0.3.x86_64
```

2. 创建 **/etc/sss/pki** 目录：

```
# file /etc/sss/pki
/etc/sss/pki/: directory
```

3. 将 **rootCA.crt** 作为 PEM 文件复制到 **/etc/sss/pki/** 目录中：

```
# cp /tmp/ca/rootCA.crt /etc/sss/pki/sss_auth_ca_db.pem
```


现在，您已成功生成了证书颁发机构和证书，并将其保存在 `/etc/sss/pki` 目录中。



注意

如果要与另一个应用程序共享证书颁发机构证书，您可以在 `sss.conf` 中更改位置：

- SSSD PAM 响应器：`[pam]` 部分中的 `pam_cert_db_path`
- SSSD ssh 响应器：`[ssh]` 部分中的 `ca_db`

详情请查看 **sss.conf** 的 man page。

红帽建议保留默认路径，并为 SSSD 使用专用证书颁发机构证书文件来确保此处仅列出可信的证书颁发机构。

6.3. 安装用来管理和使用智能卡的工具

先决条件

- **gnutls-utils** 软件包已安装。
- **opensc** 软件包已安装。
- **pcscd** 服务正在运行。

在配置智能卡前，您必须安装相应的工具，该工具可以生成证书，并启动 **pcscd** 服务。

步骤

1. 安装 **opensc** 和 **gnutls-utils** 软件包：

```
# dnf -y install opensc gnutls-utils
```

2. 启动 **pcscd** 服务。

```
# systemctl start pcscd
```

验证步骤

- 验证 **pcscd** 服务是否已启动并运行

```
# systemctl status pcscd
```

6.4. 准备智能卡并将证书和密钥上传到智能卡

按照以下流程，使用 **pkcs15-init** 工具配置智能卡，该工具可帮助您配置：

- 擦除智能卡
- 设置新的 PIN 和可选的 PIN Unblocking Keys (PUKs)
- 在智能卡上创建新插槽

- 在插槽存储证书、私钥和公钥
- 如果需要，请锁定智能卡设置，因为某些智能卡需要这个类型的最终化



注意

pkcs15-init 工具可能无法使用所有智能卡。您必须使用您使用智能卡的工具。

先决条件

- 已安装 **opensc** 软件包，其中包括 **pkcs15-init** 工具。
如需了解更多详细信息，请参阅 [安装用于管理和使用智能卡的工具](#)。
- 该卡插入读卡器并连接到计算机。
- 您有一个要存储在智能卡上的私钥、公钥和证书。在此流程中，**testuser.key**、**testuserpublic.key** 和 **testuser.crt** 是用于私钥、公钥和证书的名称。
- 您有当前的智能卡用户 PIN 和 Security Officer PIN (SO-PIN)。

流程

1. 擦除智能卡并使用您的 PIN 验证自己：

```
$ pkcs15-init --erase-card --use-default-transport-keys
Using reader with a card: Reader name
PIN [Security Officer PIN] required.
Please enter PIN [Security Officer PIN]:
```

这个卡已经被清除。

2. 初始化智能卡，设置您的用户 PIN 和 PUK，以及您的安全响应 PIN 和 PUK：

```
$ pkcs15-init --create-pkcs15 --use-default-transport-keys \ --pin 963214 --puk 321478 --so-
pin 65498714 --so-puk 784123
Using reader with a card: Reader name
```

pkcs15-init 工具在智能卡上创建一个新插槽。

3. 为插槽设置标签和验证 ID：

```
$ pkcs15-init --store-pin --label testuser \ --auth-id 01 --so-pin 65498714 --pin 963214 --puk
321478
Using reader with a card: Reader name
```

标签设置为人类可读的值，在本例中为 **testuser**。**auth-id** 必须是两个十六进制值，在本例中设为 **01**。

4. 在智能卡的新插槽中存储并标记私钥：

```
$ pkcs15-init --store-private-key testuser.key --label testuser_key \ --auth-id 01 --id 01 --pin
963214
Using reader with a card: Reader name
```



注意

在存储您的私钥并将证书存储在下一步中时，您为 **--id** 指定的值必须相同。建议为 **--id** 指定自己的值，否则它们将更复杂的值由工具计算。

5. 在智能卡上的新插槽中存储并标记该证书：

```
$ pkcs15-init --store-certificate testuser.crt --label testuser_crt \ --auth-id 01 --id 01 --format
pem --pin 963214
Using reader with a card: Reader name
```

6. 可选：在智能卡上的新插槽中保存并标记公钥：

```
$ pkcs15-init --store-public-key testuserpublic.key --label testuserpublic_key --auth-id 01 --id
01 --pin 963214
Using reader with a card: Reader name
```



注意

如果公钥与私钥或证书对应，请指定与私钥或证书的 ID 相同的 ID。

7. 可选：某些智能卡要求您通过锁定设置来完成卡：

```
$ pkcs15-init -F
```

此时您的智能卡在新创建的插槽中包含证书、私钥和公钥。您还创建了您的用户 PIN 和 PUK，以及安全响应 PIN 和 PUK。

6.5. 使用智能卡验证配置 SSH 访问

SSH 连接需要身份验证。您可以使用密码或证书。按照以下流程，使用保存在智能卡中的证书启用验证。

有关使用 **authselect** 配置智能卡的详情，请参考[使用 authselect 配置智能卡](#)。

先决条件

- 该智能卡包含您的证书和私钥。
- 该卡插入读卡器并连接到计算机。
- 您的用户名与证书的 SUBJECT 中的通用名称(CN)或用户 ID(UID)匹配。
- **pcscd** 服务正在您的本地计算机上运行。
详情请查看[安装用于管理和使用智能卡的工具](#)。

流程

1. 在使用智能卡验证的用户主目录中为 SSH 密钥创建新目录：

```
# mkdir /home/example.user/.ssh
```

2. 使用 **opensc** 库运行 **ssh-keygen -D** 命令以使用智能卡中的私钥检索现有公钥对，并将其添加到用户的 SSH 密钥目录的 **authorized_keys** 列表中，以便通过智能卡验证启用 SSH 访问。

```
# ssh-keygen -D /usr/lib64/pkcs11/opensc-pkcs11.so >>
~example.user/.ssh/authorized_keys
```

3. SSH 需要访问 **/.ssh** 目录和 **authorized_keys** 文件的适当配置。要设置或更改访问权限，请输入：

```
# chown -R example.user:example.user ~example.user/.ssh/
# chmod 700 ~example.user/.ssh/
# chmod 600 ~example.user/.ssh/authorized_keys
```

4. 另外，显示密钥：

```
# cat ~example.user/.ssh/authorized_keys
```

终端会显示密钥。

您可以使用以下命令验证 SSH 访问：

```
# ssh -I /usr/lib64/opensc-pkcs11.so -l example.user localhost hostname
```

如果配置成功，会提示您输入智能卡 PIN。

这个配置现在可以在本地运行。现在，您可以复制公钥并将其分发到您要使用 SSH 的所有服务器中的 **authorized_keys** 文件。

第 7 章 使用 AUTHSELECT 配置智能卡验证

这部分论述了如何配置智能卡以达到以下目的之一：

- 启用密码和智能卡验证
- 禁用密码并启用智能卡验证
- 在删除时启用锁定

先决条件

- 已安装 `authselect`
`authselect` 工具在 Linux 主机中配置用户验证，您可以使用它配置智能卡验证参数。有关 `authselect` 的详情，请参考[使用 `authselect` 配置用户身份验证](#)。
- RHEL 9 支持的智能卡或者 USB 设备
详情请查看[RHEL9 中的智能卡支持](#)。

7.1. 适用于智能卡的证书

在使用 **`authselect`** 配置智能卡前，您必须将证书导入您的卡中。您可以使用以下工具生成证书：

- Active Directory(AD)
- 身份管理(IdM)
有关如何创建 IdM 证书的详情，请参阅[请求新用户证书并将其导出到客户端](#)。
- 红帽认证系统(RHCS)
详情请参阅[使用企业安全客户端管理智能卡](#)。
- 第三方认证机构 (CA)
- 本地认证认证机构。如果用户不是某个域的一部分或用于测试,您可以使用本地认证认证机构生成的证书。
有关如何创建并导入本地证书到智能卡的详情，请参阅[配置和导入本地证书到智能卡](#)。

7.2. 配置您的系统以启用智能卡和密码验证

按照以下流程在您的系统中启用智能卡和密码验证。

先决条件

- 智能卡包含您的证书和私钥。
- 在读卡器中插入卡并连接到计算机。
- **`authselect`** 工具已安装在您的系统中。

步骤

- 输入以下命令允许智能卡和密码验证：

```
# authselect select sssd with-smartcard --force
```

此时，智能卡验证会被启用。但是如果您忘记携带了智能卡，密码验证仍可以正常工作。

7.3. 配置您的系统以强制智能卡验证

authselect 工具可让您在系统中配置智能卡验证，并禁用默认密码验证。**authselect** 命令包括以下选项：

- **with-smartcard** -- 除了密码验证外，启用智能卡验证
- **with-smartcard-required** – 启用智能卡验证，禁用密码验证



注意

with-smartcard-required 选项只对使用智能卡进行特定登录服务时才强制执行，如 **login**、**gdm**、**xdm**、**kdm**、**xscreensaver**、**gnome-screensaver** 和 **kscreensaver**。其他服务（如 **su** 或 **sudo**）默认情况下不使用智能卡验证，并将继续提示您输入密码。

先决条件

- 智能卡包含您的证书和私钥。
- 在读卡器中插入卡并连接到计算机。
- **authselect** 工具安装在您的本地系统中。

步骤

- 输入以下命令强制智能卡验证：

```
# authselect select sssd with-smartcard with-smartcard-required --force
```



注意

运行此命令后，密码验证将无法正常工作，您只能使用智能卡登录。在运行此命令之前，确保智能卡验证正在运行，或者您会被锁定于您的系统。

7.4. 配置智能卡认证，使它在取出智能卡时进行锁定

authselect 服务可让您配置智能卡验证，以便在从读取器中删除智能卡后立即锁定屏幕。**authselect** 命令必须包括以下变量：

- **with-smartcard** – 启用智能卡验证
- **with-smartcard-required** – 启用专用智能卡验证（禁用密码验证）
- **with-smartcard-lock-on-removal** – 在智能卡被取出后会强制登出



注意

with-smartcard-lock-on-removal 选项仅适用于具有 GNOME 桌面环境的系统。如果您使用基于 **tty** 或控制台的系统，并且您从读卡器中删除了智能卡，则不会将您自动锁在系统之外。

先决条件

- 智能卡包含您的证书和私钥。
- 在读卡器中插入卡并连接到计算机。
- **authselect** 工具安装在您的本地系统中。

步骤

- 输入以下命令启用智能卡验证、禁用密码验证并在删除时强制锁定：

```
# authselect select sssd with-smartcard with-smartcard-required with-smartcard-lock-on-removal --force
```

现在，当您取出卡时，屏幕会锁定。您必须重新插入智能卡来解锁它。

第 8 章 使用智能卡进行远程向 SUDO 进行身份验证

这部分论述了如何使用智能卡远程对 `sudo` 进行身份验证。在 **ssh-agent** 服务本地运行且无法将 **ssh-agent** 套接字转发到远程机器后，您可以使用 `sudo` PAM 模块中的 SSH 身份验证协议进行远程验证。

在使用智能卡进行本地登录后，您可以通过 SSH 登录到远程机器并运行 **sudo** 命令，而无需使用智能卡验证的 SSH 转发来提示输入密码。

在本示例中，客户端通过 SSH 连接到 IPA 服务器，并在 IPA 服务器中使用保存在智能卡中的凭证运行 `sudo` 命令。

- 在 IdM 中创建 `sudo` 规则
- 为 `sudo` 设置 PAM 模块
- 使用智能卡远程连接到 `sudo`

8.1. 在 IDM 中创建 SUDO 规则

按照以下流程，在 IdM 中创建 `sudo` 规则，以便 **ipausers1** 权限在远程主机上运行 `sudo`。

在本示例中，**less** 和 **whoami** 命令被添加为 `sudo` 命令来测试该流程。

先决条件

- IdM 用户已创建。在本例中，用户名为 **ipausers1**。
- 您有远程运行 `sudo` 的系统的主机名。在本示例中，主机是 **server.ipa.test**。

步骤

1. 创建名为 **adminrule** 的 `sudo` 规则，允许用户运行命令。

```
ipa sudorule-add adminrule
```

2. 添加 **less** 和 **whoami** 作为 `sudo` 命令：

```
ipa sudocmd-add /usr/bin/less
ipa sudocmd-add /usr/bin/whoami
```

3. 将 **less** 和 **whoami** 命令添加到 **adminrule** 中：

```
ipa sudorule-add-allow-command adminrule --sudocmds /usr/bin/less
ipa sudorule-add-allow-command adminrule --sudocmds /usr/bin/whoami
```

4. 将 **ipausers1** 用户添加到 **adminrule** 中：

```
ipa sudorule-add-user adminrule --users ipausers1
```

5. 将运行 **sudo** 的主机添加到 **adminrule** 中：

```
ipa sudorule-add-host adminrule --hosts server.ipa.test
```


其他资源

- 请参阅 `ipa sudorule-add --help`。
- 请参阅 `ipa sudocmd-add --help`。

8.2. 为 SUDO 设置 PAM 模块

按照以下流程，在运行 `sudo` 的任何主机上安装和设置 `pam_ssh_agent_auth.so` PAM 模块以进行 `sudo` 身份验证。

步骤

1. 安装 PAM SSH 代理：

```
dnf -y install pam_ssh_agent_auth
```

2. 在任何其他 `auth` 条目之前，将 `pam_ssh_agent_auth.so` 添加到 `/etc/pam.d/sudo` 文件的 `authorized_keys_command`:

```
#%PAM-1.0
auth sufficient pam_ssh_agent_auth.so
authorized_keys_command=/usr/bin/sss_ssh_authorizedkeys
auth include system-auth
account include system-auth
password include system-auth
session include system-auth
```

3. 要在运行 `sudo` 命令时启用 SSH 代理转发功能，请将以下内容添加到 `/etc/sudoers` 文件中：

```
Defaults env_keep += "SSH_AUTH_SOCK"
```

这允许从存储在 IPA/SSSD 中的智能卡中的公钥在无需输入密码的情况下向 `sudo` 进行身份验证。

4. 重启 `sssd` 服务：

```
systemctl restart sssd
```

其他资源

- 请参阅 `pam` man page。

8.3. 使用智能卡远程连接到 SUDO

按照以下流程，配置 SSH 代理和客户端，以使用智能卡远程连接到 `sudo`。

先决条件

- 您已在 IdM 中创建了 `sudo` 规则。
- 您已为您要在远程系统上运行 `sudo sudo` 身份验证安装并设置了 `pam_ssh_agent_auth` PAM 模块。

步骤

1. 启动 SSH 代理（如果尚未运行）。

```
eval `ssh-agent`
```

2. 将您的智能卡添加到 SSH 代理。提示时输入您的 PIN：

```
ssh-add -s /usr/lib64/opensc-pkcs11.so
```

3. 使用启用了 ssh-agent 转发的 SSH 连接到需要远程运行 **sudo** 的系统。使用 **-A** 选项：

```
ssh -A ipauser1@server.ipa.test
```

验证步骤

- 使用 **sudo** 运行 **whoami** 命令：

```
sudo /usr/bin/whoami
```

插入智能卡时，不会提示您输入 PIN 或密码。



注意

如果 SSH 代理被配置为使用其他源，如 GNOME Keyring，且您在删除智能卡后运行 **sudo** 命令，您可能不会提示您输入 PIN 或密码，因为其他源可能提供了对有效私钥的访问。要检查所有身份的公钥是否被 SSH 代理知道，请运行 **ssh-add -L** 命令。

其他资源

- [使用 OpenSSH 的两个系统间使用安全通讯](#)
- [通过 ssh-agent，使用 SSH 密钥连接到远程机器](#)

第 9 章 使用带有智能卡的 PKINIT 以 ACTIVE DIRECTORY 用户身份进行身份验证

Active Directory (AD) 用户可以使用智能卡向加入到 IdM 的桌面客户端系统进行身份验证，并获取 Kerberos 票据授予票据(TGT)。这些票据可用于来自客户端的单点登录(SSO)身份验证。

先决条件

- 为智能卡验证配置了客户端。
- 已安装 **krb5-pkinit** 软件包。
- AD 服务器被配置为信任签发智能卡证书的证书颁发机构(CA)。将 CA 证书导入到 NTAAuth 存储(请参阅 [Microsoft 支持](#))，并将 CA 添加为可信 CA。详情请查看 Active Directory 文档。

步骤

1. 将 Kerberos 客户端配置为信任签发智能卡证书的 CA：

- a. 在 IdM 客户端上，打开 **/etc/krb5.conf** 文件。
- b. 在文件中添加以下行：

```
[realms]
AD.DOMAIN.COM = {
    pkinit_eku_checking = kpServerAuth
    pkinit_kdc_hostname = adserver.ad.domain.com
}
```

2. 如果用户证书不包含证书撤销列表(CRL)分布点扩展，请将 AD 配置为忽略撤销错误：

- a. 在纯文本文件中保存以下 REG 格式的内容，并将其导入到 Windows registry：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Kerberos\Parameters]
"UseCachedCRLOnlyAndIgnoreRevocationUnknownErrors"=dword:00000001
```

或者，您可以使用 **regedit.exe** 应用程序手动设置值。

- b. 重启 Windows 系统以应用更改。
3. 在身份管理客户端中使用 **kinit** 工具进行身份验证。使用用户名和域名指定 Active Directory 用户：

```
$ kinit -X X509_user_identity='PKCS11:opensc-pkcs11.so' ad_user@AD.DOMAIN.COM
```

X 选项指定 **opensc-pkcs11.so** 模块 作为 pre-authentication 属性。

其他资源

- **kinit(1)** 手册页。

第 10 章 使用智能卡对身份验证进行故障排除

下面的部分描述了如何在设置智能卡验证时解决您可能遇到的一些问题。

- [测试智能卡验证](#)
- [使用 SSSD 对智能卡验证进行故障排除](#)
- [验证 IdM Kerberos KDC 可以使用 PKINIT 和 CA 证书正确位置](#)
- [增加 SSSD 超时](#)
- [证书映射和匹配规则故障排除](#)

10.1. 测试系统中的智能卡访问

按照以下流程测试是否可以访问智能卡。

先决条件

- 已安装并配置了用于智能卡的 IdM 服务器和客户端。
- 您已从 **nss-tools** 软件包安装了 **certutil** 工具。
- 您有智能卡的 PIN 或密码。

步骤

1. 使用 **lsusb** 命令，验证智能卡读取器是否在操作系统中看到：

```
$ lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 072f:b100 Advanced Card Systems, Ltd ACR39U
Bus 001 Device 002: ID 0627:0001 Adomax Technology Co., Ltd
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

有关 RHEL 中经过测试和支持的智能卡和写卡器的更多信息，请参阅 [RHEL 9 中的智能卡支持](#)。

2. 确保 **pcscd** 服务和套接字已启用并正在运行：

```
$ systemctl status pcscd.service pcscd.socket

● pcscd.service - PC/SC Smart Card Daemon
   Loaded: loaded (/usr/lib/systemd/system/pcscd.service; indirect;
   vendor preset: disabled)
   Active: active (running) since Fri 2021-09-24 11:05:04 CEST; 2
   weeks 6 days ago
   TriggeredBy: ● pcscd.socket
     Docs: man:pcscd(8)
    Main PID: 3772184 (pcscd)
     Tasks: 12 (limit: 38201)
    Memory: 8.2M
       CPU: 1min 8.067s
    CGroup: /system.slice/pcscd.service
           └─3772184 /usr/sbin/pcscd --foreground --auto-exit
```

- **pcscd.socket** - PC/SC Smart Card Daemon Activation Socket
 Loaded: loaded (/usr/lib/systemd/system/pcscd.socket; enabled; vendor preset: enabled)
 Active: active (running) since Fri 2021-09-24 11:05:04 CEST; 2 weeks 6 days ago
 Triggers: ● **pcscd.service**
 Listen: /run/pcscd/pcscd.comm (Stream)
 CGroup: /system.slice/pcscd.socket

3. 使用 **p11-kit list-modules** 命令，显示有关配置的智能卡和智能卡中的令牌的信息：

```
$ p11-kit list-modules
p11-kit-trust: p11-kit-trust.so
[...]
opensc: opensc-pkcs11.so
  library-description: OpenSC smartcard framework
  library-manufacturer: OpenSC Project
  library-version: 0.20
  token: MyEID (sctest)
    manufacturer: Aventra Ltd.
    model: PKCS#15
    serial-number: 8185043840990797
    firmware-version: 40.1
    flags:
      rng
      login-required
      user-pin-initialized
      token-initialized
```

4. 验证您可以访问智能卡的内容：

```
$ pkcs11-tool --list-objects --login
Using slot 0 with a present token (0x0)
Logging in to "MyEID (sctest)".
Please enter User PIN:
Private Key Object; RSA
  label: Certificate
  ID: 01
  Usage: sign
  Access: sensitive
Public Key Object; RSA 2048 bits
  label: Public Key
  ID: 01
  Usage: verify
  Access: none
Certificate Object; type = X.509 cert
  label: Certificate
  subject: DN: O=IDM.EXAMPLE.COM, CN=idmuser1
  ID: 01
```

5. 使用 **certutil** 命令显示智能卡中的证书内容：

- a. 运行以下命令来确定证书的正确名称：

```
$ certutil -d /etc/pki/nssdb -L -h all
```

Certificate Nickname

Trust Attributes
SSL,S/MIME,JAR/XPI

Enter Password or Pin for "MyEID (sctest)":

Smart Card CA 0f5019a8-7e65-46a1-afe5-8e17c256ae00

CT,C,C

MyEID (sctest):Certificate

u,u,u

- b. 在智能卡中显示证书内容：



注意

确保证书的名称是与上一步中显示的输出完全匹配，在本例中为
MyEID(sctest):Certificate。

```
$ certutil -d /etc/pki/nssdb -L -n "MyEID (sctest):Certificate"
```

Enter Password or Pin for "MyEID (sctest)":

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 15 (0xf)

Signature Algorithm: PKCS #1 SHA-256 With RSA Encryption

Issuer: "CN=Certificate Authority,O=IDM.EXAMPLE.COM"

Validity:

Not Before: Thu Sep 30 14:01:41 2021

Not After : Sun Oct 01 14:01:41 2023

Subject: "CN=idmuser1,O=IDM.EXAMPLE.COM"

Subject Public Key Info:

Public Key Algorithm: PKCS #1 RSA Encryption

RSA Public Key:

Modulus:

[...]

Exponent: 65537 (0x10001)

Signed Extensions:

Name: Certificate Authority Key Identifier

Key ID:

e2:27:56:0d:2f:f5:f2:72:ce:de:37:20:44:8f:18:7f:

2f:56:f9:1a

Name: Authority Information Access

Method: PKIX Online Certificate Status Protocol

Location:

URI: "http://ipa-ca.idm.example.com/ca/ocsp"

Name: Certificate Key Usage

Critical: True

Usages: Digital Signature

Non-Repudiation

Key Encipherment

Data Encipherment

Name: Extended Key Usage

TLS Web Server Authentication Certificate
 TLS Web Client Authentication Certificate

Name: CRL Distribution Points

Distribution point:

URI: "http://ipa-ca.idm.example.com/ipa/crl/MasterCRL.bin"

CRL issuer:

Directory Name: "CN=Certificate Authority,O=ipaca"

Name: Certificate Subject Key ID

Data:

43:23:9f:c1:cf:b1:9f:51:18:be:05:b5:44:dc:e6:ab:
 be:07:1f:36

Signature Algorithm: PKCS #1 SHA-256 With RSA Encryption

Signature:

[...]

Fingerprint (SHA-256):

6A:F9:64:F7:F2:A2:B5:04:88:27:6E:B8:53:3E:44:3E:F5:75:85:91:34:ED:48:A8:0D:F0:31:5
 D:7B:C9:E0:EC

Fingerprint (SHA1):

B4:9A:59:9F:1C:A8:5D:0E:C1:A2:41:EC:FD:43:E0:80:5F:63:DF:29

Mozilla-CA-Policy: false (attribute missing)

Certificate Trust Flags:

SSL Flags:

User

Email Flags:

User

Object Signing Flags:

User

其他资源

- 请参阅 **certutil(1)** man page。

10.2. 使用 SSSD 对智能卡验证进行故障排除

按照以下流程，使用智能卡对使用 SSSD 的身份验证进行故障排除。

先决条件

- 已安装并配置了用于智能卡的 IdM 服务器和客户端。
- 已安装 **sssd-tools** 软件包。
- 您可以检测智能卡读取器并显示智能卡的内容。请参阅[在系统上测试智能卡访问](#)。

步骤

1. 使用 **su** 验证您可以使用智能卡进行验证：


```
$ su - idmuser1 -c 'su - idmuser1 -c whoami'
PIN for MyEID (sctest):
idmuser1
```

如果没有提示输入智能卡 PIN，且返回一个密码提示或者返回授权错误，请检查 SSSD 日志。有关登录 SSSD 的信息，请参阅 [对 IdM 中使用 SSSD 的身份验证进行故障排除](#)。以下是身份验证失败的示例：

```
$ su - idmuser1 -c 'su - idmuser1 -c whoami'
PIN for MyEID (sctest):
su: Authentication failure
```

如果 SSSD 日志指明了 **krb5_child** 的问题，类似于以下内容，则可能对您的 CA 证书有问题。要排除与证书相关的问题，请参阅 [验证 IdM Kerberos KDC 可以使用 Pkinit 以及 CA 证书正确位于](#)。

```
[Pre-authentication failed: Failed to verify own certificate (depth 0): unable to get local issuer
certificate: could not load the shared library]
```

如果 SSSD 日志表示来自 **p11_child** 或 **krb5_child** 的超时，您可能需要提高 SSSD 超时，并尝试使用智能卡再次进行身份验证。有关如何增加超时的详情，请参阅 [增加 SSSD 超时](#)。

2. 验证您的 GDM 智能卡验证配置是否正确。应返回 PAM 验证的成功消息，如下所示：

```
# sssctl user-checks -s gdm-smartcard "idmuser1" -a auth
user: idmuser1
action: auth
service: gdm-smartcard
```

```
SSSD nss user lookup result:
- user name: idmuser1
- user id: 603200210
- group id: 603200210
- geccos: idm user1
- home directory: /home/idmuser1
- shell: /bin/sh
```

```
SSSD InfoPipe user lookup result:
- name: idmuser1
- uidNumber: 603200210
- gidNumber: 603200210
- geccos: idm user1
- homeDirectory: /home/idmuser1
- loginShell: /bin/sh
```

```
testing pam_authenticate
```

```
PIN for MyEID (sctest)
pam_authenticate for user [idmuser1]: Success
```

```
PAM Environment:
- PKCS11_LOGIN_TOKEN_NAME=MyEID (sctest)
- KRB5CCNAME=KCM:
```

如果身份验证错误（类似于以下内容）被返回，请检查 SSSD 日志尝试并确定导致这个问题的原因。有关登录 SSSD 的信息，请参阅 [对 IdM 中使用 SSSD 的身份验证进行故障排除](#)。

```
pam_authenticate for user [idmuser1]: Authentication failure
```

```
PAM Environment:
```

```
- no env -
```

如果 PAM 验证仍失败，请清除您的缓存并再次运行命令。

```
# sssctl cache-remove
SSSD must not be running. Stop SSSD now? (yes/no) [yes] yes
Creating backup of local data...
Removing cache files...
SSSD needs to be running. Start SSSD now? (yes/no) [yes] yes
```

10.3. 验证 IDM KERBEROS KDC 可以使用 PKINIT 和 CA 证书正确位置

按照以下流程验证 IdM Kerberos KDC 是否可以使用 PKINIT，并描述如何正确验证您的 CA 证书。

先决条件

- 已安装并配置了用于智能卡的 IdM 服务器和客户端。
- 您可以检测智能卡读取器并显示智能卡的内容。请参阅[在系统上测试智能卡访问](#)。

步骤

1. 运行 **kinit** 工具，以 **idmuser1** 使用保存在智能卡中的证书进行验证：

```
$ kinit -X X509_user_identity=PKCS11: idmuser1
MyEID (sctest)          PIN:
```

2. 输入您的智能卡 PIN。如果没有提示输入 PIN，请检查您是否可检测智能卡读取器并显示智能卡的内容。请参阅[测试智能卡验证](#)。
3. 如果您的 PIN 被接受，系统会提示您输入密码，可能会缺少您的 CA 签名证书。

- a. 使用 **openssl** 命令，验证默认证书捆绑包文件中列出的 CA 链：

```
$ openssl crl2pkcs7 -nocrl -certfile /var/lib/ipa-client/pki/ca-bundle.pem | openssl pkcs7 -
print_certs -noout
subject=O = IDM.EXAMPLE.COM, CN = Certificate Authority

issuer=O = IDM.EXAMPLE.COM, CN = Certificate Authority
```

- b. 验证您的证书的有效性：

- i. 查找 **idmuser1** 的用户身份验证证书 ID：

```
$ pkcs11-tool --list-objects --login
[...]
Certificate Object; type = X.509 cert
```

```
label: Certificate
subject: DN: O=IDM.EXAMPLE.COM, CN=idmuser1
ID: 01
```

- ii. 从智能卡以 DER 格式读取用户证书信息：

```
$ pkcs11-tool --read-object --id 01 --type cert --output-file cert.der
Using slot 0 with a present token (0x0)
```

- iii. 将 DER 证书转换为 PEM 格式：

```
$ openssl x509 -in cert.der -inform DER -out cert.pem -outform PEM
```

- iv. 验证证书是否有有效的签发者签名到 CA：

```
$ openssl verify -CAfile /var/lib/ipa-client/pki/ca-bundle.pem <path>/cert.pem
cert.pem: OK
```

4. 如果您的智能卡包含多个证书，**kinit** 可能无法选择正确的证书进行验证。在这种情况下，您需要使用 **certid=<ID>** 选项将证书 ID 指定为 **kinit** 命令的参数。

- a. 检查保存在智能卡中的证书数量，并获取您要使用的证书 ID：

```
$ pkcs11-tool --list-objects --type cert --login
Using slot 0 with a present token (0x0)
Logging in to "MyEID (sctest)".
Please enter User PIN:
Certificate Object; type = X.509 cert
label: Certificate
subject: DN: O=IDM.EXAMPLE.COM, CN=idmuser1
ID: 01
Certificate Object; type = X.509 cert
label: Second certificate
subject: DN: O=IDM.EXAMPLE.COM, CN=ipausers1
ID: 02
```

- b. 使用证书 ID 01 运行 **kinit**：

```
$ kinit -X kinit -X X509_user_identity=PKCS11:certid=01 idmuser1
MyEID (sctest) PIN:
```

5. 运行 **klist** 查看 Kerberos 凭证缓存的内容：

```
$ klist
Ticket cache: KCM:0:11485
Default principal: idmuser1@EXAMPLE.COM

Valid starting Expires Service principal
10/04/2021 10:50:04 10/05/2021 10:49:55 krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

6. 完成后销毁您的活跃 Kerberos 票据：

```
$ kdestroy -A
```

其他资源

- 请参阅 **kinit** man page。
- 请参阅 **kdestroy** man page。

10.4. 增加 SSSD 超时

如果您在使用智能卡进行身份验证时遇到问题，请检查 **krb5_child.log** 和 **p11_child.log** 文件以查找类似如下的超时条目：

krb5_child:Timeout for child [9607] reached.....consider increasing value of krb5_auth_timeout.

如果日志文件中有一个超时条目，请尝试增加 SSSD 超时，如此过程中所述。

先决条件

- 您已为智能卡验证配置了 IdM 服务器和客户端。

步骤

1. 在 IdM 客户端中打开 **sssd.conf** 文件：

```
# vim /etc/sss/sss.conf
```

2. 在您的 domain 部分中，如 **[domain/idm.example.com]**，添加以下选项：

```
krb5_auth_timeout = 60
```

3. 在 **[pam]** 部分中，添加以下内容：

```
p11_child_timeout = 60
```

4. 清除 SSSD 缓存：

```
# sssctl cache-remove
SSSD must not be running. Stop SSSD now? (yes/no) [yes] yes
Creating backup of local data...
Removing cache files...
SSSD needs to be running. Start SSSD now? (yes/no) [yes] yes
```

增加超时后，请尝试使用智能卡再次进行身份验证。如需了解更多详细信息，请参阅[测试智能卡验证](#)。

10.5. 证书映射和匹配规则故障排除

如果您在使用智能卡验证时遇到问题，请检查您已将智能卡证书正确链接到用户。默认情况下，当用户条目包含完整证书作为 **usercertificate** 属性的一部分时，会关联一个证书。但是，如果您定义了证书映射规则，您可能已经更改了与用户关联的证书的方式。要排除证书映射和匹配规则的问题，请参阅以下部分：

- [检查证书如何映射到用户](#)
- [检查与智能卡证书关联的用户](#)



注意

如果您通过 SSH 使用智能卡进行验证，则需要将完整证书添加到 Identity Management(IdM)的用户条目中。如果您不使用 SSH 验证智能卡，您可以使用 **ipa user-add-certmapdata** 命令添加证书映射数据。

10.5.1. 检查证书如何映射到用户

默认情况下，当用户条目包含完整证书作为 **usercertificate** 属性的一部分时，会关联一个证书。但是，如果您定义了证书映射规则，您可能已经更改了与用户关联的证书的方式。按照以下流程检查您的证书映射规则。

先决条件

- 已安装并配置了 Identity Management(IdM)服务器和客户端，用于智能卡。
- 您可以检测智能卡读取器并显示智能卡的内容。请参阅[在系统上测试智能卡访问](#)。
- 您已将智能卡证书映射到 IdM 用户。请参阅[在智能卡上配置身份验证的证书映射规则](#)。

步骤

1. 验证当前为 IdM 配置的证书映射规则：

```
# ipa certmaprule-find
-----
1 Certificate Identity Mapping Rule matched
-----
Rule name: smartcardrule
Mapping rule: (ipacertmapdata=X509:<|>{issuer_dn!nss_x500}<S>{subject_dn!nss_x500})
Matching rule: <ISSUER>CN=Certificate Authority,O=IDM.EXAMPLE.COM
Enabled: TRUE
-----
Number of entries returned 1
-----
```

您可以看到定义的以下映射规则之一：

- **ipacertmapdata** 表示使用 IdM 用户条目 **certmapdata** 属性。
- **altSecurityIdentities** 指定使用 Active Directory 的用户条目名称映射属性。
- **userCertificate;binary=** 表示使用 IdM 或 AD 中的整个证书。

您可以定义许多匹配选项，但一些通常配置的选项如下：

- **<ISSUER>CN=[...]** 指定被检查的证书的 issuer 属性，以确保它与此匹配。
- **<SUBJECT>.*,DC=MY,DC=DOMAIN** 表示是否已检查证书的主题。

2. 通过在 IdM 服务器上的 **/etc/sss/sss.conf** 文件中添加 **debug_level = 9** 来启用系统安全服务守护进程(SSSD)日志：

```
[domain/idm.example.com]
...
debug_level = 9
```

3. 重启 SSSD :

```
# systemctl restart sssd
```

4. 如果正确读取映射，您应该在 `/var/log/sss/sss_idm.example.com.log` 文件中看到以下条目：

```
[be[idm.example.com]] [sdap_setup_certmap] (0x4000): Trying to add rule [smartcardrule][-1]
[<ISSUER>CN=Certificate Authority,O=IDM.EXAMPLE.COM][(|(userCertificate;binary=
{cert!bin}))(ipacertmapdata=X509:<I>{issuer_dn!nss_x500}<S>{subject_dn!nss_x500}))].
```

5. 如果您的映射规则包含无效的语法，则日志文件中可以看到类似如下的条目：

```
[be[idm.example.com]] [sss_certmap_init] (0x0040): sss_certmap initialized.
[be[idm.example.com]] [ipa_certmap_parse_results] (0x4000): Trying to add rule
[smartcardrule][-1][<ISSUER>CN=Certificate Authority,O=IDM.EXAMPLE.COM]
[(ipacertmapdata=X509:<I>{issuer_dn!x509}<S>{subject_dn})].
[be[idm.example.com]] [parse_template] (0x0040): Parse template invalid.
[be[idm.example.com]] [parse_ldap_mapping_rule] (0x0040): Failed to add template.
[be[idm.example.com]] [parse_mapping_rule] (0x0040): Failed to parse LDAP mapping rule.
[be[idm.example.com]] [ipa_certmap_parse_results] (0x0020): sss_certmap_add_rule failed
for rule [smartcardrule], skipping. Please check for typos and if rule syntax is supported.
[be[idm.example.com]] [ipa_subdomains_certmap_done] (0x0040): Unable to parse certmap
results [22]: Invalid argument
[be[idm.example.com]] [ipa_subdomains_refresh_certmap_done] (0x0020): Failed to read
certificate mapping rules [22]: Invalid argument
```

6. 检查您的映射规则语法。

```
# ipa certmaprule-show smartcardrule
Rule name: smartcardrule
Mapping rule: (|(userCertificate;binary={cert!bin}))(ipacertmapdata=X509:<I>
{issuer_dn!nss_x500}<S>{subject_dn!nss_x500}))
Matching rule: <ISSUER>CN=Certificate Authority,O=IDM.EXAMPLE.COM
Domain name: ipa.test
Enabled: TRUE
```

7. 如果需要，修改您的证书映射规则：

```
# ipa certmaprule-mod smartcardrule --maprule '(ipacertmapdata=X509:<I>
{issuer_dn!nss_x500}<S>{subject_dn!nss_x500})'
```

其他资源

- 请参阅 **sss-certmap** man page。

10.5.2. 检查与智能卡证书关联的用户

如果您在使用智能卡进行身份验证时遇到问题，请验证正确的用户是否与您的智能卡证书关联。

先决条件

- 已安装并配置了 Identity Management(IdM)服务器和客户端，用于智能卡。
- 您可以检测智能卡读取器并显示智能卡的内容。请参阅[在系统上测试智能卡访问](#)。
- 您已将智能卡证书映射到 IdM 用户。请参阅[在智能卡上配置身份验证的证书映射规则](#)。
- 您有 PEM 格式的智能卡中的证书副本，例如 **cert.pem**。

步骤

1. 验证用户是否与您的智能卡证书关联：

```
# ipa certmap-match cert.pem
-----
1 user matched
-----
Domain: IDM.EXAMPLE.COM
User logins: idmuser1
-----
Number of entries returned 1
-----
```

如果用户或域不正确，请检查您的证书如何映射到用户。请参阅[检查如何将证书映射到用户](#)。

2. 检查用户条目是否包含证书：

```
# ipa user-show idmuser1
User login: idmuser1
[...]
Certificate:MIIEejCCAUkgAwIBAgIBCzANBgkqhkiG9w0BAQsFADAzMREwDwYDVQQKDAhJ
UEEuVEVTVDEeMBwGA1UEAwwVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XD
```

3. 如果您的用户条目不包含证书，请将您的 base-64 编码证书添加到用户条目中：

- a. 创建一个包含证书的环境变量，该变量移除了标头和页脚，并串联成一行，这是 **ipa user-add-cert** 命令期望的格式：

```
$ export CERT=`openssl x509 -outform der -in idmuser1.crt | base64 -w0 -`
```

请注意，**idmuser1.crt** 文件中的证书必须采用 PEM 格式。

- b. 使用 **ipa user-add-cert** 命令将证书添加到 **idmuser1** 配置集中：

```
$ ipa user-add-cert idmuser1 --certificate=$CERT
```

- c. 清除系统安全服务守护进程(SSSD)缓存。

```
# sssctl cache-remove
SSSD must not be running. Stop SSSD now? (yes/no) [yes] yes
Creating backup of local data...
Removing cache files...
SSSD needs to be running. Start SSSD now? (yes/no) [yes] yes
```

4. 再次运行 **ipa certmap-match** 来确认用户与您的智能卡证书关联。

