Red Hat Enterprise Linux 8

将 RHEL 系统直接与 Windows Active Directory 集成

了解并配置 RHEL 系统以直接与 Active Directory 连接

Last Updated: 2021-06-07

Red Hat Enterprise Linux 8 将 RHEL 系统直接与 Windows Active Directory 集成

了解并配置 RHEL 系统以直接与 Active Directory 连接

法律通告

摘要

本文档提供如何使用 SSSD 将 RHEL 系统直接与 Windows Active Directory 集成的步骤。

目录

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。如需了解更多详细信息，请参阅 CTO Chris Wright 信息。

在身份管理中,计划使用的术语替换包括：

- ***块列表*** 替换 *黑名单*
- ***允许列表*** 替换 *白名单*
- ***从属(secondary)***替换 *slave*
- 根据上下文, *master* 将被更精确地替换为更精确的语言：
  - ***IdM 服务器*** 替换 *IdM master*
  - ***CA 续订服务器*** 替换 *CA 续订 master*
  - ***CRL publisher 服务器*** 替换 *CRL master*
  - ***多供应商*** 替换了 *multi-master*

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要提交更复杂的反馈，请创建一个 Bugzilla ticket：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 使用 SSSD 将 RHEL 系统直接连接到 AD

这部分论述了使用系统安全性服务守护进程(SSSD)将 RHEL 系统连接到 Active Directory(AD)。您需要两个组件才能将 RHEL 系统连接到 Active Directory(AD)。一个组件 SSSD 与中央身份和验证源交互,其他组件 **realmd** 会检测可用的域并配置底层 RHEL 系统服务（本例中为 SSSD）,以连接到域。

- 使用 SSSD 直接集成概述
- 支持直接集成的 Windows 平台
- 确保支持 AD 和 RHEL 中的通用加密类型
- 直接连接到 AD
- AD 供应商如何处理动态 DNS 更新
- 修改 AD 供应商的动态 DNS 设置
- AD 供应商如何处理可信域
- realm 命令

1.1. 使用 SSSD 直接集成概述

您可以使用 SSSD 访问用户目录用于身份验证和授权，并通过带有用户缓存的通用框架进以允许离线登录。SSSD 是高度可配置的,它提供了可插拔的身份验证模块(PAM)和名称交换服务(NSS)集成,以及一个用于存储本地用户的数据库以及从中央服务器获取的扩展用户数据。在把 RHEL 系统与以下身份服务器类型之一连接时，推荐使用 SSSD：

- Active Directory
- RHEL 中的身份管理（IdM）
- 任何通用 LDAP 或 Kerberos 服务器

注意

默认情况下,与 SSSD 直接集成只能在单个 AD 林中正常工作。

配置 SSSD 以将 Linux 系统直接与 AD 集成的最便捷方法是使用 **realmd** 服务。它允许调用者以标准的方式配置网络身份验证和域成员资格。**realmd** 服务自动发现有关可访问 domain 和 realm 的信息，且不需要高级配置就可以加入到 domain 和 realm。

您可以使用 SSSD 与 AD 进行直接和间接集成,并允许您从一个集成方法切换到另一个集成方法。直接集成是将 RHEL 系统引入 AD 环境的简单方法。但是,当 RHEL 系统的比例增加时,您的部署通常需要更好地集中管理与身份相关的策略,如基于主机的访问控制、sudo 或 SELinux 用户映射。在初始阶段，您可以在本地配置文件中维护 RHEL 系统的这些配置。但是，在有大量系统的情况下，使用一个置备系统（如 Red Hat Satellite）可以使对配置文件进行分发和管理的任务变得更为容易。当直接集成不再可以满足环境扩展的要求时，应该考虑使用间接集成。有关从直接集成（RHEL 客户端位于 AD 域中）到间接集成（带有信任到 AD 的 IdM）的更多信息，请参阅将 RHEL 客户端从 AD 域移动到 IdM 服务器。

有关哪些类型的集成与您的用例匹配的更多信息，请参阅间接集成和直接集成。

其它资源

- **realm(8)** man page。
- **sssd-ad(5)** man page。
- **sssd(8)** man page。

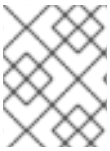
1.2. 支持直接集成的 WINDOWS 平台

您可以直接将 RHEL 系统与使用以下林和域功能级别的 Active Directory 网站集成：

- 林功能级别范围：Windows Server 2008 - Windows 服务器 2016
- 域功能级别范围：Windows Server 2008 - Windows 服务器 2016

在以下支持的操作系统中测试了直接集成：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2



注意

Windows Server 2019 没有引入新的功能级别。Windows Server 2019 使用最高功能级别是 Windows Server 2016。

1.3. 确保支持 AD 和 RHEL 中的通用加密类型

SSSD 默认支持 RC4、AES-128 和 AES-256 Kerberos 加密类型。

RHEL 8 中弃用并默认禁用 RC4 加密，因为它被视为没有较新的 AES-128 和 AES-256 加密类型安全。而 Active Directory(AD)用户凭证和 AD 域之间的信任支持 RC4 加密,且可能不支持 AES 加密类型。

如果没有通用加密类型,RHEL 主机和 AD 域间的通信可能无法正常工作,或者有些 AD 帐户可能无法验证。要避免这种情况，请修改以下配置之一：

- **在 Active Directory 中启用 AES 加密支持（推荐的选项）**:要确保 AD 林支持强大的 AES 加密类型中的 AD 域相互信任 ,请查看以下 Microsoft 文章 AD DS: Security: Kerberos "Unsupported etype" error when access a trusted domain 中
- 在**RHEL 中启用 RC4 支持**:在进行针对 AD 域控制器身份验证的每个 RHEL 主机上：

  1. 除了 **DEFAULT** 加密策略外，使用 **update-crypto-policies** 命令还启用 **AD-SUPPORT** 加密子策略。

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

  2. 重启主机。

重要

AD-SUPPORT 加密子策略仅适用于 RHEL 8.3 及更新的版本。

- 要在 RHEL 8.2 中启用对 RC4 的支持，请使用 **cipher = RC4-128+** 创建并启用自定义加密模块策略。如需了解更多详细信息，请参阅使用 policy modifiers 自定义系统范围的加密策略。
- 要在 RHEL 8.0 和 RHEL 8.1 中启用对 RC4 的支持，请将 **+rc4** 添加到 **/etc/crypto-policies/back-ends/krb5.config** 文件的 **permitted_enctypes** 选项中：

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
```

其它资源

- 有关使用 RHEL 加密策略的更多信息，请参阅安全强化指南中的使用系统范围的加密策略。

1.4. 直接连接到 AD

本节论述了如何使用 ID 映射或 POSIX 属性直接与 AD 集成。

- 使用 SSSD 发现并加入 AD 域
- 用于与 AD 集成的选项： 使用 ID 映射或 POSIX 属性
- 使用 Active Directory 中定义的 POSIX 属性连接到 AD
- 使用 SSSD 连接到不同 AD 林中的多个域

1.4.1. 使用 SSSD 发现并加入 AD 域

这个步骤描述了如何发现 AD 域并使用 SSSD 将 RHEL 系统连接到那个域。

先决条件

- 确保 RHEL 主机上的以下端口已为 AD 域控制器打开并可以被访问。

表 1.1. 使用 SSSD 将 Linux 系统直接集成到 AD 所需的端口

服务	端口	协议	备注
DNS	53	UDP 和 TCP	
LDAP	389	UDP 和 TCP	
Kerberos	88	UDP 和 TCP	
Kerberos	464	UDP 和 TCP	kadmin 用来设置和更改密码

服务	端口	协议	备注
LDAP 全局目录	3268	TCP	如果使用 **id_provider = ad** 选项
NTP	123	UDP	可选

- 确保您为 DNS 使用 AD 域控制器服务器。
- 验证两个系统中的系统时间已被同步。这样可确保 Kerberos 正常工作。

流程

1. 安装以下软件包：

```
# yum install realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. 要显示特定域的信息，请运行 **realm discover** 并添加您要发现的域名称：

```
# realm discover ad.example.com
ad.example.com
  type: kerberos
  realm-name: AD.EXAMPLE.COM
  domain-name: ad.example.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common
```

realmd 系统使用 DNS SRV 查找自动查找这个域中的域控制器。

注意

realmd 系统可以发现 Active Directory 和 Identity Management 域。如果您的环境中存在这两个域，您可以使用 **--server-software=active-directory** 选项将发现结果限制为特定类型的服务器。

3. 使用 **realm join** 命令配置本地 RHEL 系统。**realmd** 套件自动编辑所有必需的配置文件。例如，对于名为 **ad.example.com** 的域：

```
# realm join ad.example.com
```

验证步骤

- 显示 AD 用户详情，如管理员用户：

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:1450400500:1450400513:Administrator:/home/administrator
@ad.example.com:/bin/bash
```

其它资源

- 请查看 **realm(8)** man page。
- 请查看 **nmcli(1)** man page。

1.4.2. 用于与 AD 集成的选项： 使用 ID 映射或 POSIX 属性

Linux 和 Windows 系统为用户和组群使用不同的标识符：

- Linux 使用 *用户 ID*（UID）和 *组群 ID*（GID）。请参阅 *配置基本系统设置中的 管理用户和组群帐户简介*。Linux UID 和 GID 符合 POSIX 标准。
- Windows 使用 *安全 ID* (SID)。

重要

将 RHEL 系统连接到 AD 后,您可以使用 AD 用户名和密码进行身份验证。不要创建与 Windows 用户名称相同的 Linux 用户,因为重复的名称可能会导致冲突并中断验证过程。

要以 AD 用户身份验证 RHEL 系统，您必须分配了 UID 和 GID。SSSD 提供了使用 ID 映射或 POSIX 属性与 AD 集成的选项。默认是使用 ID 映射。

1.4.2.1. 为 AD 用户自动生成新的 UID 和 GID

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

- 当 SSSD 检测到新的 AD 域时,它会为新域分配一系列可用 ID。
- 当 AD 用户首次登录到 SSSD 客户端机器时,SSSD 在 SSSD 缓存中为用户创建一个条目,包括基于用户 SID 的 UID 和那个域的 ID 范围。
- 由于 AD 用户的 ID 是由同一 SID 一致生成的,所以用户在登录到任何 Red Hat Enterprise Linux 系统时具有相同的 UID 和 GID。

请参阅使用 SSSD 发现并加入 AD 域。

注意

当所有客户端系统都使用 SSSD 将 SID 映射到 Linux ID 时，映射是一致的。如果有些客户端使用不同的软件，请选择以下之一：

- 确定所有客户端都使用相同的映射算法。
- 使用 AD 中定义的显式 POSIX 属性。

1.4.2.2. 使用 AD 中定义的 POSIX 属性

AD 可以创建并存储 POSIX 属性，如 **uidNumber**、**gidNumber**、**unixHomeDirectory** 或 **loginShell**。

当使用上述 ID 映射时,SSSD 会创建新 UID 和 GID,这会覆盖 AD 中定义的值。要保留 AD 定义的值，必须在 SSSD 中禁用 ID 映射。

请参阅 使用 Active Directory 中定义的 POSIX 属性连接到 AD 。

1.4.3. 使用 Active Directory 中定义的 POSIX 属性连接到 AD

为获得最佳性能,请向 AD 全局目录发布 POSIX 属性。如果全局目录中没有 POSIX 属性，SSSD 会直接连接到 LDAP 端口上的单个域控制器。

先决条件

- 确保 RHEL 主机上的以下端口已为 AD 域控制器打开并可以被访问。

  表 1.2. 使用 SSSD 将 Linux 系统直接集成到 AD 所需的端口

服务	端口	协议	备注
DNS	53	UDP 和 TCP	
LDAP	389	UDP 和 TCP	
Kerberos	88	UDP 和 TCP	
Kerberos	464	UDP 和 TCP	kadmin 用来设置和更改密码
LDAP 全局目录	3268	TCP	如果使用 **id_provider = ad** 选项
NTP	123	UDP	可选

- 确保您为 DNS 使用 AD 域控制器服务器。
- 验证两个系统中的系统时间已被同步。这样可确保 Kerberos 正常工作。

流程

1. 安装以下软件包：

```
# yum install realmd oddjob oddjob-mkhomedir sssd adcli krb5-workstation
```

2. 使用带 **--automatic-id-mapping=no** 选项的 **realm join** 命令配置禁用了 ID 映射的本地 RHEL 系统。**realmd** 套件自动编辑所有必需的配置文件。例如，对于名为 **ad.example.com** 的域：

```
# realm join --automatic-id-mapping=no ad.example.com
```

3. 如果您已经加入某个域，可以在 SSSD 中手动禁用 ID 映射：

a. 打开 **/etc/sssd/sssd.conf** 文件。

b. 在 AD 域部分，添加 **ldap_id_mapping = false** 设置。

c. 删除 SSSD 缓存：

```
rm -f /var/lib/sss/db/*
```

d. 重启 SSSD：

```
systemctl restart sssd
```

SSSD 现在使用 AD 中的 POSIX 属性，而不是在本地创建它们。

注意

您必须为 AD 中用户配置了相关的 POSIX 属性（**uidNumber**、**gidNumber**、**unixHomeDirectory** 和 **loginShell**）。

验证步骤

- 显示 AD 用户详情，如管理员用户：

```
# getent passwd administrator@ad.example.com
administrator@ad.example.com:*:10000:10000:Administrator:/home/Administrator:/bin/bash
```

其它资源

- 有关 ID 映射和 **ldap_id_mapping** 参数的详情，请查看 **sssd-ldap(8)** man page。

1.4.4. 使用 SSSD 连接到不同 AD 林中的多个域

这个步骤描述了加入和身份验证不同林中的多个 Active Directory(AD)域,它们之间没有信任。

这个示例描述了加入两个域 **addomain1.com** 和 **addomain2.com**。使用 **realmd** 加入第一个域，并为那个域自动配置 SSSD、Kerberos 和其他工具。使用 **adcli** 加入附加域，并手动编辑配置文件使其包含这些域。

先决条件

- 确保 RHEL 主机上的以下端口已为 AD 域控制器打开并可以被访问。

表 1.3. 使用 SSSD 将 Linux 系统直接集成到 AD 所需的端口

服务	端口	协议	备注
DNS	53	UDP 和 TCP	
LDAP	389	UDP 和 TCP	
Kerberos	88	UDP 和 TCP	

服务	端口	协议	备注
Kerberos	464	UDP 和 TCP	kadmin 用来设置和更改密码
LDAP 全局目录	3268	TCP	如果使用 **id_provider = ad** 选项
NTP	123	UDP	可选

- 确保您为 DNS 使用 AD 域控制器服务器。
- 验证两个系统中的系统时间已被同步。这样可确保 Kerberos 正常工作。
- 确保在每个 AD 域中都有 AD 管理员帐户的凭证,该帐户有权将机器加入到那个域中

流程

1. 安装所需的软件包。

```
# yum install sssd realmd adcli samba-common-tools oddjob oddjob-mkhomedir
```

2. 使用 **realmd** 加入第一个 AD 域 **addomain1.com**。

```
# realm join ADDOMAIN1.COM
```

3. 将系统 keytab 重命名为唯一名称。

```
# mv /etc/krb5.keytab /etc/addomain1.com.krb5.keytab
```

4. 使用 **adcli** 加入第二个 AD 域，以及任何附加域。使用 **-K** 选项为 Kerberos keytab 指定要编写主机凭证的唯一路径。

```
# adcli join -D dc2.addomain2.com -K /etc/addomain2.com.krb5.keytab
```

5. 修改 **/etc/krb5.conf**。
   - 添加 **includedir** 选项以包含 SSSD 配置文件。
   - 使用 **dns_lookup_kdc** 选项为 AD Domain Controller 启用 DNS 查找。

```
includedir /var/lib/sss/pubconf/krb5.include.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = ADDOMAIN1.COM
 dns_lookup_realm = false
```

```
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

...
```

6. 修改 **/etc/sssd/sssd.conf** 以包含正在使用的所有 AD 域的信息。

```
[sssd]
services = nss, pam
config_file_version = 2
domains = addomain1.com, addomain2.com

[domain/addomain1.com]
id_provider = ad
access_provider = ad
krb5_keytab = /etc/addomain1.com.krb5.keytab
ldap_krb5_keytab = /etc/addomain1.com.krb5.keytab
ad_server = dc1.addomain1.com
ad_maximum_machine_account_password_age = 0
use_fully_qualified_names = true
default_shell=/bin/bash
override_homedir=/home/%d/%u

[domain/addomain2.com]
id_provider = ad
access_provider = ad
krb5_keytab = /etc/addomain2.com.krb5.keytab
ldap_krb5_keytab = /etc/addomain2.com.krb5.keytab
ad_server = dc2.addomain2.com
ad_maximum_machine_account_password_age = 0
use_fully_qualified_names = true
default_shell=/bin/bash
override_homedir=/home/%d/%u

[nss]

[pam]
```

- 对于每个 domain 部分,指定与 **krb5_keytab** 和 **ldap_krb5_keytab** 选项对应的 Kerberos keytab 的路径。
- 设置 **ad_maximum_machine_account_password_age = 0** 以禁用更新主机 Kerberos 密钥。
- 设置 **use_fully_qualified_names = true** 以区分不同域的用户。
- 设置 **override_homedir = /home/%d/%u**，使来自不同域（**%d**）的用户（**%u**）都会获得唯一的主目录。例如：用户 **linuxuser@addomain1.com** 的主目录是 **/home/addomain1.com/linuxuser**。

7. SSH 从系统密钥 b 中检索主机密钥,并通过 GSSAPI/Kerberos 提供单一登录功能。如果您想使用单点登录,将所有当前的 Kerberos 主机密钥复制到 **/etc/kbr5.keytab** 系统密钥。

```
# ktutil
```

```
ktutil:  rkt /etc/addomain1.com.krb5.keytab
ktutil:  rkt /etc/addomain2.com.krb5.keytab
ktutil:  wkt /etc/krb5.keytab
```

8. 重启并启用 SSSD 服务。

```
# systemctl restart sssd
# systemctl enable sssd
```

验证步骤

1. 显示来自每个 AD 域的用户详情：

```
# id administrator@addomain1.com
uid=1240800500(administrator@addomain1.com) gid=1240800513(domain
users@addomain1.com) groups=1240800513(domain
users@addomain1.com),1240800512(domain
admins@addomain1.com),1240800518(schema
admins@addomain1.com),1240800520(group policy creator
owners@addomain1.com),1240800572(denied rodc password replication
group@addomain1.com),1240800519(enterprise admins@addomain1.com)

# id administrator@addomain2.com
uid=1013800500(administrator@addomain2.com)
gid=1013800500(administrator@addomain2.com)
groups=1013800500(administrator@addomain2.com),1013800513(domain
users@addomain2.com)
```

2. 以来自每个域的用户身份登录，验证为该用户创建了正确的主目录。

```
# ssh administrator@addomain1.com@localhost
administrator@addomain1.com@localhost's password:
Creating directory '/home/addomain1.com/administrator'.

$ pwd
/home/addomain1.com/administrator
```

```
# ssh administrator@addomain2.com@localhost
administrator@addomain2.com@localhost's password:
Creating directory '/home/addomain2.com/administrator'.

$ pwd
/home/addomain2.com/administrator
```

1.5. AD 供应商如何处理动态 DNS 更新

Active Directory（AD）通过超时（*aging*）和删除（*scavenging*）不活跃的记录来主动维护 DNS 记录。

默认情况下，SSSD 服务会按照以下间隔刷新 RHEL 客户端的 DNS 记录：

- 身份提供程序每次上线时。
- 每次 RHEL 系统重启时。

- 在 **/etc/sssd/sssd.conf** 配置文件中的 **dyndns_refresh_interval** 选项指定的时间间隔。默认值为 **86400** 秒（24 小时）。

注意

如果您将 **dyndns_refresh_interval** 选项设置为与 DHCP 租期相同的间隔，您可以在 IP 租期被续订后更新 DNS 记录。

SSSD 使用 Kerberos/GSSAPI 为 DNS(GSS-TSIG)向 AD 服务器发送动态 DNS 更新。这意味着您只需要启用到 AD 的安全连接。

其它资源

- **sssd-ad(5)** man page。

1.6. 修改 AD 供应商的动态 DNS 设置

以下流程调整 SSSD 服务中的设置,以影响如何自动更新已加入 Active Directory 环境的 RHEL 主机的 DNS 记录。

先决条件

- 您已使用 SSSD 服务将 RHEL 主机加入到 Active Directory 环境。
- 您需要 **root** 权限来编辑 **/etc/sssd/sssd.conf** 配置文件。

流程

1. 在文本编辑器中打开 **/etc/sssd/sssd.conf** 配置文件。
2. 为您的 AD 域的 **[domain]** 部分添加以下选项,将 DNS 记录刷新间隔设置为 12 小时,禁用更新 PTR 记录,并将 DNS 记录时间到 Live(TTL)设置为 1 小时。

```
[domain/ad.example.com]
id_provider = ad
...
dyndns_refresh_interval = 43200
dyndns_update_ptr = false
dyndns_ttl = 3600
```

3. 保存并关闭 **/etc/sssd/sssd.conf** 配置文件。
4. 重启 SSSD 服务以载入配置更改。

```
[root@client ~]# systemctl restart sssd
```

注意

您可以通过将 **sssd.conf** 文件中的 **dyndns_update** 选项设置为 **false** 来禁用动态 DNS 更新：

```
[domain/ad.example.com]
id_provider = ad
...

dyndns_update = false
```

其它资源

- **sssd-ad(5)** man page

1.7. AD 供应商如何处理可信域

本节论述了，如果在 **/etc/sssd/sssd.conf** 配置文件中设置了 **id_provider = ad** 选项，SSSD 如何处理可信域。

- SSSD 只支持单个 AD 林中的域。如果 SSSD 需要从多个林访问多个域，请考虑使用带有信任的 IPA（首选方式）或 **winbindd** 服务，而不是 SSSD。
- 默认情况下,SSSD 会发现林中的所有域,并在可信域中对象请求到达时,SSSD 会尝试解决这个问题。
  如果可信域无法访问或其地理距离非常遥远，这使得它们的速度较慢，您可以在 **/etc/sssd/sssd.conf** 中设置 **ad_enabled_domains** 参数来限制 SSSD 解析对象。
- 默认情况下,您必须使用完全限定的用户名从可信域解析用户。

其它资源

- **sssd.conf(5)** man page。

1.8. REALM 命令

realmd 系统有两个主要任务：

- 在一个域中管理系统注册。
- 控制允许哪些域用户访问本地系统资源。

在 **realmd** 中，使用命令行工具 **realm** 运行命令。大多数 **realm** 命令要求用户指定该工具应执行的操作,以及执行操作的实体,如域或用户帐户。

表 1.4. realmd 命令

命令	描述
realm 命令	
discover	对网络中的域运行发现扫描。

命令	描述
join	将系统添加到指定的域中。
leave	从指定的域中删除系统。
list	列出系统的所有配置域，或者所有发现和配置的域。
登录命令	
permit	启用特定用户或配置域中的所有用户访问本地系统。
deny	限制特定用户或配置域中的所有用户访问本地系统。

有关 **realm** 命令的详情，请参考 **realm(8)** man page。

第 2 章 使用 SAMBA WINBIND 将 RHEL 系统直接连接到 AD

这部分论述了使用 Samba Winbind 将 RHEL 系统连接到 Active Directory(AD)。您需要两个组件才能将 RHEL 系统连接到 AD。一个组件（Samba Winbind）与 AD 身份和验证源交互，另一个组件（**realmd**）检测可用的域并配置底层 RHEL 系统服务，即 Samba Winbind 以连接到 AD 域。

- 使用 Samba Winbind 直接集成的概述
- 支持直接集成的 Windows 平台
- 确保支持 AD 和 RHEL 中的通用加密类型
- 将 RHEL 系统添加到 AD 域中
- realm 命令

2.1. 使用 SAMBA WINBIND 直接集成的概述

Samba Winbind 在 Linux 系统中模拟 Windows 客户端并与 AD 服务器沟通。

您可以使用 **realmd** 服务配置 Samba Winbind：

- 以标准的方式配置网络身份验证和域成员资格。
- 自动发现有关可访问 domain 和 realm 的信息。
- 不需要高级配置加入domain 或 realm。

请注意：

- 在多林 AD 设置中直接与 Winbind 集成需要双向信托。
- 远程林必须信任本地林,以确保 **idmap_ad** 插件可以正确处理远程林用户。

Samba 的 **winbindd** 服务为 Name Service Switch(NSS)提供了一个接口,并让域用户在登录到本地系统时进行身份验证。

使用 **winbindd** 提供了在不安装附加软件的情况下增强配置以共享目录和打印机的好处。详情请参阅 Deploying Different of Servers Guide 中的有关使用 Samba 作为服务器的部分。

其它资源

- 请查看 **realmd** man page。
- 请查看 **windbindd** man page。

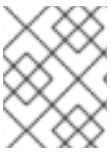
2.2. 支持直接集成的 WINDOWS 平台

您可以直接将 RHEL 系统与使用以下林和域功能级别的 Active Directory 网站集成：

- 林功能级别范围：Windows Server 2008 - Windows 服务器 2016
- 域功能级别范围：Windows Server 2008 - Windows 服务器 2016

在以下支持的操作系统中测试了直接集成：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2



注意

Windows Server 2019 没有引入新的功能级别。Windows Server 2019 使用最高功能级别是 Windows Server 2016。

2.3. 确保支持 AD 和 RHEL 中的通用加密类型

默认情况下,Samba Winbind 支持 RC4、AES-128 和 AES-256 Kerberos 加密类型。

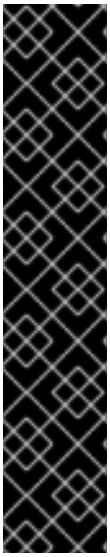
RHEL 8 中弃用并默认禁用 RC4 加密，因为它被视为没有较新的 AES-128 和 AES-256 加密类型安全。而 Active Directory(AD)用户凭证和 AD 域之间的信任支持 RC4 加密,且可能不支持 AES 加密类型。

如果没有通用加密类型,RHEL 主机和 AD 域间的通信可能无法正常工作,或者有些 AD 帐户可能无法验证。要避免这种情况，请修改以下配置之一：

- **在 Active Directory 中启用 AES 加密支持（推荐的选项）**:要确保 AD 林支持强大的 AES 加密类型中的 AD 域相互信任 ,请查看以下 Microsoft 文章 AD DS: Security: Kerberos "Unsupported etype" error when access a trusted domain 中
- 在**RHEL 中启用 RC4 支持**:在进行针对 AD 域控制器身份验证的每个 RHEL 主机上：
  1. 除了 **DEFAULT** 加密策略外，使用 **update-crypto-policies** 命令还启用 **AD-SUPPORT** 加密子策略。

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

  2. 重启主机。



重要

AD-SUPPORT 加密子策略仅适用于 RHEL 8.3 及更新的版本。

- 要在 RHEL 8.2 中启用对 RC4 的支持，请使用 **cipher = RC4-128+** 创建并启用自定义加密模块策略。如需了解更多详细信息，请参阅使用 policy modifiers 自定义系统范围的加密策略。
- 要在 RHEL 8.0 和 RHEL 8.1 中启用对 RC4 的支持，请将 **+rc4** 添加到 **/etc/crypto-policies/back-ends/krb5.config** 文件的 **permitted_enctypes** 选项中：

  ```
  [libdefaults]
  permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
  ```

其它资源

- 有关使用 RHEL 加密策略的更多信息，请参阅安全强化指南中的使用系统范围的加密策略。

2.4. 将 RHEL 系统添加到 AD 域中

这部分论述了如何使用 **realmd** 配置 Samba Winbind 将 Red Hat Enterprise Linux 系统添加到 AD 域中。

流程

1. 如果您的 AD 需要弃用的 RC4 加密类型进行 Kerberos 验证，请在 RHEL 中启用对这些密码的支持：

```
# update-crypto-policies --set DEFAULT:AD-SUPPORT
```

2. 安装以下软件包：

```
# yum install realmd oddjob-mkhomedir oddjob samba-winbind-clients \ samba-winbind samba-common-tools samba-winbind-krb5-locator
```

3. 要在域成员中共享目录或打印机，请安装 **samba** 软件包：

```
# yum install samba
```

4. 备份现有的 **/etc/samba/smb.conf** Samba 配置文件：

```
# mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
```

5. 加入域。例如，要加入名为 **ad.example.com** 的域：

```
# realm join --membership-software=samba --client-software=winbind ad.example.com
```

使用前面的命令，**realm** 工具会自动：

- 为 **ad.example.com** 域中的成员资格创建一个 **/etc/samba/smb.conf** 文件
- 在 **/etc/nsswitch.conf** 文件中为用户和组群查询添加 **winbind** 模块
- 更新 **/etc/pam.d/** 目录中的可插拔验证模块(PAM)配置文件
- 启动 **winbind** 服务并启用服务在系统引导时启动

6. 另外，还可在 **/etc/samba/smb.conf** 文件中设置备选 ID 映射后端或自定义 ID 映射设置。详情请查看 **Deploying different types of servers** 文档中 的了解和配置 Samba ID 映射 部分。

7. 编辑 **/etc/krb5.conf** 文件并添加以下部分：

```
[plugins]
  localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
  }
```

8. 验证 **winbind** 服务是否正在运行：

```
# systemctl status winbind
...
   Active: active (running) since Tue 2018-11-06 19:10:40 CET; 15s ago
```

重要

要启用 Samba 查询域用户和组群信息，必须在启动 **smb** 前运行 **winbind** 服务。

9. 如果您安装 **samba** 软件包来共享目录和打印机，请启用并启动 **smb** 服务：

```
# systemctl enable --now smb
```

验证步骤

1. 显示 AD 用户的详情，如 AD 域中的 AD 管理员帐户：

```
# getent passwd "AD\administrator"
AD\administrator:*:10000:10000::/home/administrator@AD:/bin/bash
```

2. 查询 AD 域中的域用户组成员：

```
# getent group "AD\Domain Users"
   AD\domain users:x:10000:user1,user2
```

3. 另外，还可在设置文件和目录权限时验证您可以使用域用户和组。例如，将 **/srv/samba/example.txt** 文件的拥有者设置为 **AD\administrator**，组为 **AD\Domain Users**：

```
# chown "AD\administrator":"AD\Domain Users" /srv/samba/example.txt
```

4. 验证 Kerberos 验证是否如预期正常工作：

   a. 在 AD 域成员中，为 **administrator@AD.EXAMPLE.COM** 主体获取一个 ticket：

```
# kinit administrator@AD.EXAMPLE.COM
```

   b. 显示缓存的 Kerberos ticket：

```
# klist
Ticket cache: KCM:0
Default principal: administrator@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
01.11.2018 10:00:00  01.11.2018 20:00:00
krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
        renew until 08.11.2018 05:00:00
```

5. 显示可用域：

```
# wbinfo --all-domains
BUILTIN
SAMBA-SERVER
AD
```

其它资源

- 如果您不想使用弃用的 RC4 密码，可以在 AD 中启用 AES 加密类型。请参阅 **Deploying different types of servers** 文档中 的使用 GPO 在 Active Directory 中启用 AES 加密类型 。
- 有关 **realm** 工具程序的详情，请查看 **realm(8)** man page。

2.5. REALM 命令

realmd 系统有两个主要任务：

- 在一个域中管理系统注册。
- 控制允许哪些域用户访问本地系统资源。

在 **realmd** 中，使用命令行工具 **realm** 运行命令。大多数 **realm** 命令要求用户指定该工具应执行的操作，以及执行操作的实体,如域或用户帐户。

表 2.1. realmd 命令

命令	描述
realm 命令	
discover	对网络中的域运行发现扫描。
join	将系统添加到指定的域中。
leave	从指定的域中删除系统。
list	列出系统的所有配置域，或者所有发现和配置的域。
登录命令	
permit	启用特定用户或配置域中的所有用户访问本地系统。
deny	限制特定用户或配置域中的所有用户访问本地系统。

有关 **realm** 命令的详情，请参考 **realm(8)** man page。

第 3 章 管理到 AD 的直接连接

本节论述了如何修改和管理您与 Active Directory 的连接。

先决条件

- 您已将 RHEL 系统连接到 Active Directory 域。

3.1. 修改默认的 KERBEROS 主机 KEYTAB 续订间隔

如果安装了 **adcli** 软件包，SSSD 会在 AD 环境中自动更新 Kerberos 主机 keytab 文件。如果机器帐户密码早于配置的值，守护进程会每天检查并在需要时更新它。

默认续订间隔为 30 天。要更改默认值，请按照以下步骤执行。

流程

1. 在 **/etc/sssd/sssd.conf** 文件中的 AD 供应商中添加以下参数：

```
ad_maximum_machine_account_password_age = value_in_days
```

2. 重启 SSSD：

```
# systemctl restart sssd
```

3. 要禁用自动 Kerberos 主机 keytab 续订,请设置 **ad_maximum_machine_account_password_age = 0**。

其它资源

- **adcli(8)** man page。
- **sssd.conf(5)** man page。

3.2. 从 AD 域中删除 RHEL 系统

这个步骤描述了如何从 Active Directory(AD)域中删除 RHEL 系统。

流程

1. 使用 **realm leave** 命令从身份域中删除系统。该命令从 SSSD 和本地系统中删除域配置。

```
# realm leave ad.example.com
```

注意

当客户端离开某个域时,帐户不会从 AD 中删除 ; 本地客户端配置仅会被删除。如果要删除 AD 帐户，使用 **--remove** 选项运行该命令。此时会提示您输入用户密码，且您必须有权从 Active Directory 中删除帐户。

2. 使用 **realm leave** 命令的 **-U** 选项指定不同的用户从身份域中删除系统。

默认情况下, **realm leave** 命令作为默认管理员执行。对于 AD,管理员帐户名为 **Administrator**。如果使用其他用户加入域,则可能需要以该用户的身份执行删除操作。

```
# realm leave [ad.example.com] -U [AD.EXAMPLE.COM\user]'
```

该命令首先尝试在没有凭证的情况下连接,但在需要时会提示输入密码。

验证步骤

- 验证不再配置域：

```
# realm discover [ad.example.com]
ad.example.com
   type: kerberos
   realm-name: EXAMPLE.COM
   domain-name: example.com
   configured: no
   server-software: active-directory
   client-software: sssd
   required-package: oddjob
   required-package: oddjob-mkhomedir
   required-package: sssd
   required-package: adcli
   required-package: samba-common-tools
```

其它资源

- 请查看 **realm(8)`** man page。

3.3. 在 SSSD 中设置域解析顺序来解析短 AD 用户名

默认情况下,您必须指定完全限定的用户名,如 **ad_username@ad.example.com** 和 **group@ad.example.com**,才能使用 SSSD 服务解析连接到 AD 的 RHEL 主机上的用户和组。

此流程在 SSSD 配置中设置域解析顺序,以便您可以使用简短名称解析 AD 用户和组,如 **ad_username**。这个示例配置会按照以下顺序搜索用户和组：

1. Active Directory(AD)子域 **subdomain2.ad.example.com**
2. AD 子域 **subdomain1.ad.example.com**
3. AD root domain **ad.example.com**

先决条件

- 已使用 SSSD 服务将 RHEL 主机直接连接到 AD。

流程

1. 在文本编辑器中打开 **/etc/sssd/sssd.conf** 文件。
2. 在文件的 **[sssd]** 部分设置 **domain_resolution_order** 选项。

```
domain_resolution_order = subdomain2.ad.example.com, subdomain1.ad.example.com,
ad.example.com
```

3. 保存并关闭该文件。

4. 重启 SSSD 服务以加载新的配置设置。

```
[root@ad-client ~]# systemctl restart sssd
```

验证步骤

- 您只能使用简短名称从第一个域中检索用户的用户信息。

```
[root@ad-client ~]# id <user_from_subdomain2>
uid=1916901142(user_from_subdomain2) gid=1916900513(domain users)
groups=1916900513(domain users)
```

3.4. 为域用户管理登录权限

默认情况下,会应用域端访问控制,这意味着在 AD 域本身中为 Active Directory(AD)用户定义了登录策略。此默认行为可以被覆盖,以便使用客户端访问控制。使用客户端访问控制,登录权限仅由本地策略定义。

如果某个域应用客户端访问控制,您可以使用 **realmd** 为来自该域的用户配置基本允许或拒绝访问规则。

注意

访问规则可以允许或拒绝对系统中所有服务的访问。必须在特定系统资源或域中设置更具体的访问规则。

3.4.1. 启用对域中用户的访问

本节论述了如何启用对域中用户的访问。

重要

仅允许访问特定用户或组比拒绝访问某些用户或组而允许访问其他所有用户或组要安全。因此，不建议默认允许访问所有用户，而只拒绝访问 realm 权限为 -x 的特定用户。反之，红帽建议为所有用户维护默认的 no access 策略，且只使用域允许为所选用户授予访问权限。

先决条件

- 您的 RHEL 系统是 Active Directory 域的成员。

流程

1. 授予对所有用户的访问权限：

```
# realm permit --all
```

2. 授予对特定用户的访问权限：

```
$ realm permit aduser01@example.com
$ realm permit 'AD.EXAMPLE.COM\aduser01'
```

目前，您只能允许访问主域中的用户，而不允许访问可信域中的用户。这是因为用户登录必须包含域名，SSSD 目前无法提供 **realmd** 可用子域的信息。

验证步骤

1. 使用 SSH 以 aduser01@example.com 用户身份登录到服务器：

```
$ ssh aduser01@example.com@server_name
[aduser01@example.com@server_name ~]$
```

2. 使用 ssh 命令第二次访问同一服务器，此时与 aduser02@example.com 用户身份进行以下操作：

```
$ ssh aduser02@example.com@server_name
Authentication failed.
```

请注意 **aduser02@example.com** 如何拒绝对该系统的访问。您只为 aduser01@example.com 用户授权可以登录到系统。由于指定的登录策略，来自该 Active Directory 域的所有其他用户都将被拒绝。

注意

如果在 **sssd.conf** 文件中将 **use_fully_qualified_names** 设置为 true，则所有请求都必须使用完全限定域名。但是，如果您将 **use_fully_qualified_names** 设置为 false，则可以在请求中使用完全限定名称，但输出中只会显示简化的版本。

其它资源

- 请查看 **realm(8)`** man page。

3.4.2. 拒绝对域中用户的访问

本节论述了如何拒绝对域内所有用户的访问。

重要

仅允许访问特定用户或组比拒绝访问某些用户或组而允许访问其他所有用户或组要安全。因此，不建议默认允许访问所有用户，而只拒绝访问 realm 权限为 -x 的特定用户。反之，红帽建议为所有用户维护默认的 no access 策略，且只使用域允许为所选用户授予访问权限。

先决条件

- 您的 RHEL 系统是 Active Directory 域的成员。

流程

1. 拒绝对域内所有用户的访问：

```
# realm deny --all
```

这个命令可防止 **realm** 帐户登录本地机器。使用 **realm permit** 来限制到特定帐户的登录。

2. 验证域用户的 **login-policy** 是否已设置为 **deny-any-login**：

```
[root@replica1 ~]# realm list
example.net
  type: kerberos
  realm-name: EXAMPLE.NET
  domain-name: example.net
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@example.net
  login-policy: deny-any-login
```

3. 使用 -x 选项拒绝对特定用户的访问：

```
$ realm permit -x 'AD.EXAMPLE.COM\aduser02'
```

验证步骤

- 使用 SSH 以 **aduser01@example.net** 用户身份登录到服务器。

```
$ ssh aduser01@example.net@server_name
Authentication failed.
```

注意

如果在 **sssd.conf** 文件中将 **use_fully_qualified_names** 设置为 true，则所有请求都必须使用完全限定域名。但是，如果您将 **use_fully_qualified_names** 设置为 false，则可以在请求中使用完全限定名称，但输出中只会显示简化的版本。

其它资源

- 请查看 **realm(8)`** man page。

3.5. 在 RHEL 中应用组策略对象访问控制

组策略对象(GPO)是存储在 Microsoft Active Directory(AD)中的访问控制设置集合,可应用于 AD 环境中的计算机和用户。通过在 AD 中指定 GPO,管理员可以定义加入 AD 的 Windows 客户端和 Red Hat Enterprise Linux(RHEL)主机都遵循的登录策略。

以下小节介绍了如何在您的环境中管理 GPO：

- 第 3.5.1 节 “SSSD 如何解释 GPO 访问控制规则”
- 第 3.5.2 节 “SSSD 支持的 GPO 设置列表”
- 第 3.5.3 节 “控制 GPO 强制的 SSSD 选项列表”

- 第 3.5.4 节 “更改 GPO 访问控制模式”
- 第 3.5.5 节 “在 AD GUI 中为 RHEL 主机创建和配置 GPO”

3.5.1. SSSD 如何解释 GPO 访问控制规则

默认情况下,SSSD 从 Active Directory(AD)域控制器检索组策略对象(GPOs),并评估它们以确定用户是否允许用户登录到 AD 加入的特定 RHEL 主机。

SSSD 将 AD *Windows 日志记录器映射* 到可插拔的身份验证模块(PAM)服务名称,以便在 GNU/Linux 环境中强制这些权限。

作为 AD 管理员,您可以将 GPO 规则的范围限制为特定用户、组或主机,方法是将它们列在 *安全过滤器中*。

3.5.1.1. 主机过滤的限制

旧版本的 SSSD 不评估 AD GPO 安全过滤器中的主机。

- **RHEL 8.3.0 和更新版本：** SSSD 支持安全过滤器中的用户、组和主机。
- **早于 8.3.0 的 RHEL 版本：** SSSD 忽略主机条目,且只在安全过滤器中支持用户和组。
  为确保 SSSD 将基于 GPO 的访问控制应用到特定主机,在 AD 域中创建一个新的机构单元(OU),将系统移到新的 OU,然后将 GPO 链接到这个 OU。

3.5.1.2. 按组过滤的限制

SSSD 目前不支持 Active Directory 的内置组,如带有安全标识符(SID) **S-1-5-32-544** 的 **Administrators**。红帽建议您在 AD GPOs 中针对 RHEL 主机使用 AD 内置组。

其它资源

- 有关 Windows GPO 选项及其对应的 SSSD 选项列表,请查看 SSSD 支持的 GPO 设置列表 。

3.5.2. SSSD 支持的 GPO 设置列表

下表显示了与 Windows 上 *组策略管理编辑器* 中指定的 Active Directory GPO 选项对应的 SSSD 选项。

表 3.1. SSSD 检索的 GPO 访问控制选项

GPO 选项	对应的 sssd.conf 选项
允许本地登录 拒绝在本地日志	**ad_gpo_map_interactive**
允许通过远程桌面服务登录 通过远程桌面服务登陆	**ad_gpo_map_remote_interactive**
从网络访问这个计算机 请从网络访问这台计算机。	**ad_gpo_map_network**
允许作为批处理任务登录 拒绝作为批处理作业登录	**ad_gpo_map_batch**

GPO 选项	对应的 sssd.conf 选项
允许作为服务登录 拒绝作为服务登录	**ad_gpo_map_service**

- 有关这些 **sssd.conf** 设置的详情,如映射到 GPO 选项的可插拔身份验证模块(PAM)服务,请查看 **sssd-ad(5)** 手册页条目。

3.5.3. 控制 GPO 强制的 SSSD 选项列表

3.5.3.1. ad_gpo_access_control 选项

您可以在 **/etc/sssd/sssd.conf** 文件中设置 **ad_gpo_access_control** 选项,在基于 GPO 的访问控制操作的三种不同模式间进行选择。

表 3.2. ad_gpo_access_control 值表

ad_gpo_access_control 的值	行为
enforcing	基于 GPO 的访问控制规则被评估并强制执行。 **这是 RHEL 8 中的默认设置。**
permissive	基于 GPO 的访问控制规则会被评估但 **不** 强制执行 ; 每次拒绝访问时都会记录 **syslog** 信息。这是 RHEL 7 中的默认设置。 这个模式是测试策略调整的理想模式,同时允许用户继续登录。
disabled	基于 GPO 的访问控制规则不会被评估,也不会强制实施。

3.5.3.2. ad_gpo_implicit_deny 选项

默认情况下，**ad_gpo_implicit_deny** 选项被设置为 **False**。在默认状态下,如果找不到 GPOs,则允许用户访问。如果将此选项设置为 **True**,您必须明确允许用户使用 GPO 规则访问。

您可以使用这个功能强化安全性,但不要意外地拒绝访问。红帽建议在 **ad_gpo_access_control** 设置为 **permissive** 时测试此功能。

以下两个表演示了用户根据 AD 服务器端定义的允许和拒绝登录权限以及 **ad_gpo_implicit_deny** 的值被允许或拒绝访问。

表 3.3. 将 ad_gpo_implicit_deny 设置为 False （默认）的登录行为

允许规则	拒绝规则	结果
缺少	缺少	允许所有用户
缺少	存在	仅允许没有拒绝规则的用户

允许规则	拒绝规则	结果
存在	缺少	只允许有允许规则的用户
存在	存在	只允许有允许规则而不在拒绝规则中的用户

表 3.4. ad_gpo_implicit_deny 设置为 True 的登录行为

允许规则	拒绝规则	结果
缺少	缺少	没有用户被允许
缺少	存在	没有用户被允许
存在	缺少	只允许有允许规则的用户
存在	存在	只允许有允许规则而不在拒绝规则中的用户

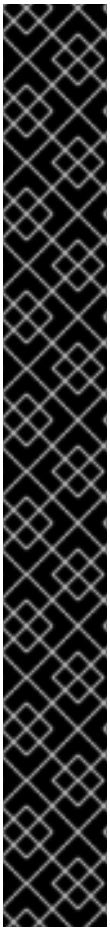
其它资源

- 有关在 SSSD 中更改 GPO 强制模式的步骤,请参阅 更改 GPO 访问控制模式。
- 有关每个 GPO 模式操作的详情,请查看 **sssd-ad(5)** Manual 页面中的 **ad_gpo_access_control** 条目。

3.5.4. 更改 GPO 访问控制模式

此流程更改了在加入 Active Directory(AD)环境的 RHEL 主机上如何评估并强制实施基于 GPO 的访问控制规则。

在本例中，您可以将 GPO 操作模式从 **enforcing** （默认）改为 **permissive**，以便进行测试。



重要

如果您看到以下错误, Active Directory 用户因为基于 GPO 的访问控制而无法登录：

- 在 **/var/log/secure**:

```
Oct 31 03:00:13 client1 sshd[124914]: pam_sss(sshd:account): Access denied for user aduser1: 6 (Permission denied)
Oct 31 03:00:13 client1 sshd[124914]: Failed password for aduser1 from 127.0.0.1 port 60509 ssh2
Oct 31 03:00:13 client1 sshd[124914]: fatal: Access denied for user aduser1 by PAM account configuration [preauth]
```

- 在 **/var/log/sssd/sssd__example.com_.log**:

```
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_perform_hbac_processing] (0x0040): GPO access check failed: [1432158236](Host Access Denied)
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_cse_done] (0x0040): HBAC processing failed: [1432158236](Host Access Denied}
(Sat Oct 31 03:00:13 2020) [sssd[be[example.com]]] [ad_gpo_access_done] (0x0040): GPO-based access control failed.
```

如果这不是正确的行为,您可以临时将 **ad_gpo_access_control** 设置为 **permissive**,如您在 AD 中故障排除正确的 GPO 设置时所述。

先决条件

- 已使用 SSSD 将 RHEL 主机加入到 AD 环境中。
- 编辑 **/etc/sssd/sssd.conf** 配置文件需要 **root** 权限。

流程

1. 停止 SSSD 服务。

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

2. 在文本编辑器中打开 **/etc/sssd/sssd.conf** 文件。
3. 为 AD 域在 **domain** 部分中将 **ad_gpo_access_control** 设置为 **permissive**。

```
[domain/example.com]
ad_gpo_access_control=permissive
...
```

4. 保存 **/etc/sssd/sssd.conf** 文件。
5. 重启 SSSD 服务以加载配置更改。

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

其它资源

- 有关不同 GPO 访问控制模式列表,请参阅控制 GPO 强制的 SSSD 选项列表。

3.5.5. 在 AD GUI 中为 RHEL 主机创建和配置 GPO

以下流程在 Active Directory(AD)图形用户界面(GUI)中创建组策略对象(GPO)以控制对 RHEL 主机的登录访问。

先决条件

- 已使用 SSSD 将 RHEL 主机加入到 AD 环境中。
- 您有 AD Administrator 特权才能使用 GUI 更改 AD。

流程

1. 在 **Active Directory Users and Computers** 中,创建一个机构单元(OU)与新的 GPO 关联：
   a. 右键点击域。
   b. 选择 **New**。
   c. 选择 **Organizational Unit**。
2. 点击代表 RHEL 主机（在它加入 Active Directory 时创建）的 Computer Object 名称,并将其拖动到新的 OU 中。通过在自己的 OU 中使用 RHEL 主机,GPO 以这个主机为目标。
3. 在 **Group Policy Management Editor** 中,为您创建的 OU 创建一个新的 GPO:
   a. 展开 **Forest**。
   b. 展开 **Domains**。
   c. 展开您的域。
   d. 右键点击新的 OU。
   e. 选择 **Create a GPO in this domain**。
4. 为新 GPO 指定名称，如 **Allow SSH access** 或 **Allow Console/GUI access**，并点 **OK**。
5. 编辑新的 GPO：
   a. 在 **Group Policy Management** 编辑器中选择 OU。
   b. 右击并选择 **Edit**。
   c. 选择 **User Rights Assignment**。
   d. 选择 **Computer Configuration**
   e. 选择 **Policies**。
   f. 选择 **Windows Settings**。
   g. 选择 **Security Settings**。
   h. 选择 **Local Policies**。

i. 选择 **User Rights Assignment**。

6. 分配登录权限：

   a. 双击 **Allow log on locally** 以授予本地控制台/GUI 访问权限。

   b. 双击 **Allow log on through Remote Desktop Services** 以授予 SSH 访问权限。

7. 在策略本身中添加您要访问这些策略的用户：

   a. 点 **Add User or Group**。

   b. 在空白字段中输入用户名。

   c. 点 **OK**。

其它资源

- 如需有关组策略对象的更多信息，请参阅 Microsoft 文档中的组策略对象。

3.5.6. 其它资源

- 有关将 RHEL 主机加入 Active Directory 环境的更多信息，请参阅使用 SSSD 将 RHEL 系统直接连接到 AD