Red Hat Enterprise Linux 9

配置和使用网络文件服务

在 Red Hat Enterprise Linux 9 中配置和使用网络文件服务的指南。

Last Updated: 2024-08-16

Red Hat Enterprise Linux 9 配置和使用网络文件服务

在 Red Hat Enterprise Linux 9 中配置和使用网络文件服务的指南。

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

本文档论述了如何在 Red Hat Enterprise Linux 9 上配置和运行网络文件服务，包括 Samba 服务器和 NFS 服务器。

目录

对红帽文档提供反馈 3

第 1 章 使用 SAMBA 作为服务器 4
1.1. 了解不同的 SAMBA 服务和模式 4
1.2. 使用 TESTPARM 工具验证 SMB.CONF 文件 6
1.3. 将 SAMBA 设置为独立服务器 7
1.4. 了解并配置 SAMBA ID 映射 9
1.5. 将 SAMBA 设置为 AD 域成员服务器 17
1.6. 在 IDM 域成员中设置 SAMBA 20
1.7. 设置使用 POSIX ACL 的 SAMBA 文件共享 25
1.8. 对使用 POSIX ACL 的共享设置权限 29
1.9. 设置使用 WINDOWS ACL 的共享 30
1.10. 使用 SMBCACLS 在 SMB 共享中管理 ACL 32
1.11. 允许用户在 SAMBA 服务器上共享目录 37
1.12. 配置共享以允许不进行身份验证的访问 40
1.13. 为 MACOS 客户端配置 SAMBA 41
1.14. 使用 SMBCLIENT 实用程序访问 SMB 共享 42
1.15. 将 SAMBA 设置为打印服务器 44
1.16. 在 SAMBA 打印服务器中为 WINDOWS 客户端设置自动打印机驱动程序下载 46
1.17. 在启用了 FIPS 模式的服务器上运行 SAMBA 52
1.18. 调整 SAMBA 服务器的性能 53
1.19. 将 SAMBA 配置为与需要 SMB 版本低于默认版本的客户端兼容 55
1.20. 经常使用 SAMBA 命令行工具 55
1.21. 其它资源 65

第 2 章 部署 NFS 服务器 66
2.1. 次 NFSV4 版本的主要功能 66
2.2. AUTH_SYS 身份验证方法 67
2.3. AUTH_GSS 身份验证方法 67
2.4. 导出的文件系统上的文件权限 68
2.5. NFS 服务器上需要的服务 68
2.6. /ETC/EXPORTS 配置文件 69
2.7. 配置只使用 NFSV4 的服务器 70
2.8. 配置一个具有可选的 NFSV4 支持的 NFSV3 服务器 72
2.9. 在 NFS 服务器上启用配额支持 74
2.10. 在 NFS 服务器上启用通过 RDMA 的 NFS 76
2.11. 在 RED HAT IDENTITY MANAGEMENT 域中使用 KERBEROS 建立一个 NFS 服务器 77

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 JIRA 提交反馈（需要帐户）

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

第 1 章 使用 SAMBA 作为服务器

Samba 在Red Hat Enterprise Linux中实现了服务器消息块(SMB)协议。SMB 协议用于访问服务器上的资源，如文件共享和共享打印机。此外，Samba 实现了Microsoft Windows 使用的分布式计算环境远程过程调用(DCE RPC)协议。

您可以以以下方式运行 Samba：

- Active Directory(AD)或 NT4 域成员
- 独立服务器
- NT4 主域控制器(PDC)或备份域控制器(BDC)

注意

红帽支持仅在支持 NT4 域的 Windows 版本的现有安装中支持 PDC 和 BDC 模式。红帽建议不要设置新的 Samba NT4 域，因为 Windows 7 和 Windows Server 2008 R2之后的Microsoft操作系不支持 NT4 域。

红帽不支持将 Samba 作为 AD 域控制器(DC)来运行。

有别于安装模式，您可以选择共享目录和打印机。这可让 Samba 充当文件和打印服务器。

1.1. 了解不同的 SAMBA 服务和模式

samba 软件包提供多个服务。根据您的环境和您要配置的场景，您需要一个或多个这些服务，并在不同的模式下配置 Samba。

1.1.1. Samba 服务

Samba 提供以下服务：

smbd

此服务使用 SMB 协议提供文件共享和打印服务。另外，该服务负责资源锁定和验证连接用户。对于身份验证域成员，**smbd** 需要 **winbindd**。**smb systemd**服务启动并停止**smbd**守护进程。
要使用**smbd**服务，请安装**samba**软件包。

nmbd

此服务通过 IPv4 协议使用 NetBIOS 提供主机名和 IP 解析。除了名字解析之外，**nmbd**服务还支持浏览 SMB 网络来查找域、工作组、主机、文件共享和打印机。为此，服务可将此信息直接报告给广播客户端，或者将其转发到本地或主浏览器。**nmb systemd**服务启动并停止**nmbd**守护进程。
请注意，现代 SMB 网络使用 DNS 来解析客户端和 IP 地址。对于 Kerberos，需要一个正常工作的 DNS 设置。

要使用**nmbd**服务，请安装 **samba**软件包。

winbindd

该服务为名字服务交换机(NSS)提供了一个接口，以便使用本地系统上的 AD 或 NT4 域用户和组。例如，这使域用户能够对在 Samba 服务器上托管的服务或其他本地服务进行身份验证。**winbind systemd**服务启动并停止**winbindd**守护进程。
如果将 Samba 设置为域成员，则必须在**smbd**服务运行之前启动**winbindd**。否则，本地系统将无法使用域用户和组。

要使用**winbindd**服务，请安装**samba-winbind**软件包。

重要

红帽仅支持将 Samba 作为带有**winbindd**服务的服务器运行，以便为本地系统提供域用户和组。由于某些限制，如缺少 Windows 访问控制列表(ACL)支持和 NT LAN Manager(NTLM)回退，目前不支持 SSSD。

1.1.2. Samba 安全服务

/etc/samba/smb.conf文件中的**[global]**部分中的**security**参数管理 Samba 如何验证连接到该服务的用户的身份。根据您在其中安装 Samba 的模式，参数必须设为不同的值：

对于 AD 域成员，设置security = ads

在这个模式中，Samba 使用 Kerberos 来验证 AD 用户。
有关将 Samba 设置为域成员的详情，请参考 将 Samba 设置为 AD 域成员服务器。

对于单独服务器，设置security = user

在这个模式中，Samba 使用本地数据库验证连接用户。
有关将 Samba 设置为独立服务器的详情，请参考 将 Samba 设置为独立服务器。

对于NT4 PDC 或 BDC，设置security = user

在此模式中，Samba 将用户身份验证到本地或 LDAP 数据库。

对于 NT4 域成员，设置security = domain

在此模式中，Samba 将连接的用户验证到 NT4 PDC 或 BDC。您不能在 AD 域成员中使用这个模式。
有关将 Samba 设置为域成员的详情，请参考 将 Samba 设置为 AD 域成员服务器。

其它资源

- **smb.conf(5)** 手册页中的 **security** 参数

1.1.3. Samba 服务和 Samba 客户端工具加载并重新载入其配置的情况

下面描述了 Samba 服务和工具加载并重新载入其配置：

- Samba 服务在以下情况下重新载入其配置：
  - 每 3 分钟自动进行
  - 在手动请求时，例如运行**smbcontrol all reload-config** 命令。
- Samba 客户端实用程序仅在启动时读取其配置。

请注意，某些参数（如**security** ）需要重启**smb**服务才能生效，而重新载入不足以生效。

其它资源

- **smb.conf(5)**手册页中的**如何应用配置更改** 部分
- **smbd(8)**、**nmbd(8)**和**winbindd(8)**手册页

1.1.4. 以安全的方式编辑 Samba 配置

Samba 服务每 3 分钟自动重新载入其配置。要防止服务在使用 **testparm** 工具验证配置前重新载入更改，您可以以安全的方式编辑 Samba 配置。

先决条件

- 已安装 Samba。

流程

1. 创建**/etc/samba/smb.conf**文件的副本：

```
# cp /etc/samba/smb.conf /etc/samba/samba.conf.copy
```

2. 编辑复制的文件并进行必要的更改。
3. 验证**/etc/samba/samba.conf.*copy***文件中的配置：

```
# testparm -s /etc/samba/samba.conf.copy
```

如果**testparm**报告错误，请修复这些错误，然后再次运行该命令。

4. 使用新配置覆盖**/etc/samba/smb.conf**文件：

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

5. 等待 Samba 服务自动重新载入其配置或手动重新载入配置：

```
# smbcontrol all reload-config
```

其它资源

- Samba 服务和 Samba 客户端工具加载并重新载入其配置的情况

1.2. 使用 TESTPARM 工具验证 SMB.CONF 文件

testparm工具验证**/etc/samba/smb.conf**文件中的 Samba 配置是否正确。该工具不但检测无效的参数和值，还检测不正确的设置，如 ID 映射。如果**testparm**报告没有问题，Samba 服务将成功加载**/etc/samba/smb.conf**文件。请注意，**testparm**无法验证配置的服务是否可用或按预期工作。

重要

红帽建议在每次修改此文件后，使用**testparm**来验证**/etc/samba/smb.conf**文件。

先决条件

- 已安装 Samba。
- 退出**/etc/samba/smb.conf**文件。

流程

1. 以**root**用户身份运行**testparm**工具：

```
# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Unknown parameter encountered: "log levell"
Processing section "[example_share]"
Loaded services file OK.
ERROR: The idmap range for the domain * (tdb) overlaps with the range of DOMAIN
(ad)!

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
 ...

[example_share]
 ...
```

前面的示例输出会报告不存在的参数以及不正确的 ID 映射配置。

2. 如果**testparm**报告了配置中不正确的参数、值或其他错误，请修复问题并再次运行该工具。

1.3. 将 SAMBA 设置为独立服务器

您可以将 Samba 设置为不是域成员的服务器。在此安装模式中，Samb身份验证到本地数据库，而不是中央DC。另外，您可以启用客户机访问，允许用户在没有身份验证的情况下连接到一个或多个服务。

1.3.1. 为独立服务器设置服务器配置

您可以为 Samba 独立服务器设置服务器配置。

流程

1. 安装**samba**软件包：

```
# dnf install samba
```

2. 编辑**/etc/samba/smb.conf**文件并设置以下参数：

```
[global]
 workgroup = Example-WG
 netbios name = Server
 security = user

 log file = /var/log/samba/%m.log
 log level = 1
```

此配置在**Example-learning**工作组里定义了一个名为**Server**的独立服务器。此外，此配置启用了最小级别(**1**)的日志记录，日志文件将存储在**/var/log/samba/**目录中。Samba 将把 **日志文件** 参数中的**%m** 宏扩展到连接客户端的 NetBIOS 名称。这可为每个客户端启用独立的日志文件。

3. （可选）配置文件或打印机共享。请参阅：
   - 设置使用 POSIX ACL 的共享
   - 设置使用 Windows ACL 的共享
   - 将 Samba 设置为打印服务器
4. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

5. 如果您设置了需要身份验证的共享，请创建用户帐户。
   详情请参阅 创建和启用本地用户帐户。
6. 打开所需的端口并使用**firewall-cmd**工具重新载入防火墙配置：

```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

7. 启用并启动**smb**服务：

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

其它资源

- **smb.conf(5)** 手册页

1.3.2. 创建并启用本地用户帐户

要让用户在连接到共享时进行身份验证，您必须在 Samba 主机上的操作系统和 Samba 数据库中创建帐户。Samba 要求操作系统帐户验证文件系统对象上的访问控制列表(ACL)和 Samba 帐户，来验证连接用户的身份。

如果您使用了**passdb backend = tdbsam** 默认设置，Samba 会将用户帐户存储在**/var/lib/samba/private/passdb.tdb**数据库中。

您可以创建一个名为 **example** 的本地 Samba 用户。

先决条件

- Samba 已安装，并配置为独立服务器。

流程

1. 创建操作系统帐户：

```
# useradd -M -s /sbin/nologin example
```

   此命令添加了**example**帐户，而不创建主目录如果帐户仅用于对 Samba 进行身份验证，请将**/sbin/nologin**命令指定为 shell，以防止帐户在本地登录。

2. 为操作系统帐户设置密码以启用它：

```
# passwd example
Enter new UNIX password: password
Retype new UNIX password: password
passwd: password updated successfully
```

Samba 不会使用操作系统帐户中的密码集进行身份验证。然而，您需要设置密码才能启用帐户。如果一个帐户被禁用，当这个用户连接时，Samba 会拒绝访问。

3. 将用户添加到 Samba 数据库，并为帐户设置密码：

```
# smbpasswd -a example
New SMB password: password
Retype new SMB password: password
Added user example.
```

当使用此帐户连接到 Samba 共享时，使用此密码进行验证。

4. 启用 Samba 帐户：

```
# smbpasswd -e example
Enabled user example.
```

1.4. 了解并配置 SAMBA ID 映射

Windows 域通过唯一安全标识符(SID)来区分用户和组。但是，Linux 需要为每个用户和组群有唯一的 UID 和 GID。如果您以域成员身份运行 Samba，**winbindd**服务负责向操作系统提供域用户和组的信息。

要启用**winbindd**服务来向 Linux提供唯一的用户和组ID，您必须在**/etc/samba/smb.conf**文件中为以下情况配置 ID 映射：

- 本地数据库（默认域）
- Samba 服务器所属的 AD 或 NT4 域
- 每个用户必须能够访问这个 Samba 服务器上的资源的可信域

Samba 为特定配置提供不同的 ID 映射后端。最常用的后端是：

后端	使用案例
tdb	*仅限默认域
ad	仅限 AD 域
rid	AD 和 NT4 域
autorid	AD、NT4 和 * 默认域

1.4.1. 规划 Samba ID 范围

无论您在 AD 中是否存储了 Linux UID 和 GID，还是将 Samba 配置为生成它们，每个域配置都需要一个唯一的 ID 范围，其不得与任何其他域重叠。

警告

如果您设置了重叠 ID 范围，Samba 无法正常工作。

例 1.1. 唯一的 ID 范围

以下显示了默认(*)、**AD-DOM**和**TRUST-DOM**域的非重叠 ID 映射范围。

```
[global]
...
idmap config * : backend = tdb
idmap config * : range = 10000-999999

idmap config AD-DOM:backend = rid
idmap config AD-DOM:range = 2000000-2999999

idmap config TRUST-DOM:backend = rid
idmap config TRUST-DOM:range = 4000000-4999999
```

重要

每个域只能分配一个范围。因此，在域范围之间有足够的空间。这可让您在域扩展后扩展范围。

如果您稍后给某个域分配了一个不同的范围，那么之前由这些用户和组创建的文件和目录的所有权将会丢失。

1.4.2. * 默认域

在域环境中，您可以为以下每个情况添加一个 ID 映射配置：

- Samba 服务器所属的域
- 每个可以访问 Samba 服务器的可信域

但是，对于所有其他对象，Samba 会从默认域分配 ID。这包括：

- 本地 Samba 用户和组
- Samba 内置帐户和组，如**BUILTIN\Administrators**

重要

您必须按描述的配置默认域，以使 Samba 正确运行。

默认域后端必须可写，才能永久存储分配的 ID。

对于默认域，您可以使用以下后端之一：

tdb

当您将默认域配置为使用**tdb**后端时，请设置一个足够大的 ID 范围，以包含将来要创建的对象，这些对象不属于已定义的域ID映射配置的一部分。
例如，在**/etc/samba/smb.conf**文件中的**[global]**部分中设置以下内容：

```
idmap config * : backend = tdb
idmap config * : range = 10000-999999
```

详情请查看 使用 TDB ID 映射后端。

autorid

当您将默认域配置为使用**autorid**后端时，为域添加额外的 ID 映射配置是可选的。
例如，在**/etc/samba/smb.conf**文件中的**[global]**部分中设置以下内容：

```
idmap config * : backend = autorid
idmap config * : range = 10000-999999
```

详情请查看 使用 autorid ID 映射后端。

1.4.3. 使用 tdb ID 映射后端

winbindd服务默认使用可写的**tdb** ID 映射后端来存储安全标识符(SID)、UID 以及 GID 映射表。这包括本地用户、组和内置主体。

仅将此后端用于*默认域。例如：

```
idmap config * : backend = tdb
idmap config * : range = 10000-999999
```

其它资源

- * 默认域。

1.4.4. 使用 ad ID 映射后端

您可以将 Samba AD 成员配置为使用 **ad** ID 映射后端。

ad ID 映射后端实现了一个只读 API，以便从 AD 读取帐户和组信息。它具有以下优点：

- 所有用户和组群设置都集中存储在 AD 中。
- 使用这个后端的所有 Samba 服务器中的用户和组群 ID 是一致的。
- ID 不会存储在本地数据库中（本地数据库可能会被损坏），因此文件所有者不会丢失。

注意

ad ID 映射后端不支持具有单向信任的Active Directory域。如果您使用单向信任在 Active Directory 中配置域成员，请使用以下一种 ID 映射后端：**tdb**、**delete** 或 **autorid**。

后端从 AD 读取以下属性：

AD 属性名称	对象类型	映射到
sAMAccountName	用户和组群	用户和组名称，取决于对象
uidNumber	User	用户 ID（UID）
gidNumber	组	组 ID（GID）
loginShell [a]	User	用户 shell 的路径
unixHomeDirectory [a]	User	用户主目录的路径
primaryGroupID [b]	User	主组群 ID

[a] 如果您设置了 **idmap config *DOMAIN*:unix_nss_info = yes**，则 Samba 只读取这个属性。

[b] 如果您设置了 **idmap config *DOMAIN*:unix_primary_group = yes**，则 Samba 只读取这个属性。

先决条件

- 用户和组必须在 AD 中设置唯一的 ID，并且 ID 必须在 **/etc/samba/smb.conf** 文件中配置的范围之内。其ID 不在范围之内的对象在 Samba 服务器上不可用。
- 用户和组必须在 AD 中设置所有必需的属性。如果缺少所需的属性，该用户或组将无法在 Samba 服务器中可用。所需的属性取决于您的配置。
- 已安装 Samba。
- Samba 配置（除了ID 映射）位于 **/etc/samba/smb.conf** 文件中。

流程

1. 编辑 **/etc/samba/smb.conf** 文件中的 **[global]** 部分：
   a. 如果默认域(*)不存在，请为其添加 ID 映射配置。例如：

   ```
   idmap config * : backend = tdb
   idmap config * : range = 10000-999999
   ```

   b. 为 AD 域启用 **ad** ID 映射后端：

   ```
   idmap config DOMAIN : backend = ad
   ```

   c. 设置分配给 AD 域中用户和组的 ID 范围。例如：

   ```
   idmap config DOMAIN : range = 2000000-2999999
   ```

重要

范围不得与这个服务器上的任何其他域配置重叠。此外，范围必须足够大，以便包含将来分配的所有 ID。详情请查看 规划 Samba ID 范围。

d. 当从AD读取属性时，使用RFC 2307模式来设置 Samba：

```
idmap config DOMAIN : schema_mode = rfc2307
```

e. 要让 Samba 从对应的 AD 属性读取登录 shell 和用户主目录的路径，请设置：

```
idmap config DOMAIN : unix_nss_info = yes
```

或者，您可以设置适用于所有用户的统一的域范围的主目录路径和登录 shell。例如：

```
template shell = /bin/bash
template homedir = /home/%U
```

f. 默认情况下，Samba 使用用户对象的 **primaryGroupID** 属性作为 Linux 上用户的主组。或者，您可以将 Samba 配置为使用**gidNumber**属性中设置的值：

```
idmap config DOMAIN : unix_primary_group = yes
```

2. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

3. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

其它资源

- * 默认域
- **smb.conf(5)** and **idmap_ad(8)** man pages
- **smb.conf(5)** 手册页中的 **VARIABLE SUBSTITUTIONS** 部分

1.4.5. 使用网格 ID 映射后端

您可以将 Samba 域成员配置为使用 **rid** ID 映射后端。

Samba 可以使用 Windows SID 的相对标识符(RID)，以便在 Red Hat Enterprise Linux 上生成 ID。

注意

RID 是 SID 的最后部分。例如，如果用户的 SID 是**S-1-5-21-5421822485-1151247151-421485315-30014**，那么**30014**是对应的 RID。

ridID映射后端实施了一个只读 API，以便根据 AD 和 NT4 域的算法映射方案计算帐户和组信息。当配置后端时，您必须在 **idmap config *DOMAIN* : *range***参数中设置最低和最高的 RID。Samba 不会映射比这个参数中设置低或更高 RID 的用户或组。

重要

作为只读后端，**rid**无法分配新的ID，例如为**BUILTIN**组。因此，请勿将此后端用于 * 默认域。

使用网格后端的好处

- 所有在配置范围内具有 RID 的域用户和组都会自动在域成员中可用。
- 您不需要手动分配 ID、主目录和登录 shell。

使用网格后端的缺陷

- 所有域用户可以获得相同的登录 shell 和主目录。但是，您可以使用变量。
- 如果它们都使用具有相同ID范围设置的**rid**后端，那么用户和组ID只在 Samba 域成员之间是相同的。
- 您不能阻止单独的用户或组在域成员中可用。只有超出配置范围以外的用户和组才会包括。
- 根据 **winbindd** 服务用于计算 ID 的公式，如果不同域中的对象有相同的 RID，那么在多域环境中可能会有重复ID的事情发生 。

先决条件

- 已安装 Samba。
- Samba 配置（除了ID 映射）位于 **/etc/samba/smb.conf** 文件中。

流程

1. 编辑 **/etc/samba/smb.conf** 文件中的 **[global]** 部分：

   a. 如果默认域(*)不存在，请为其添加 ID 映射配置。例如：

   ```
   idmap config * : backend = tdb
   idmap config * : range = 10000-999999
   ```

   b. 为域启用**rid**ID映射后端：

   ```
   idmap config DOMAIN : backend = rid
   ```

   c. 设置一个足够大的范围，以包括将来将要分配的所有RID。例如：

   ```
   idmap config DOMAIN : range = 2000000-2999999
   ```

   Samba 会忽略此域中其RID不在范围内的用户和组。

重要

范围不得与这个服务器上的任何其他域配置重叠。此外，范围必须足够大，以便包含将来分配的所有 ID。详情请查看 规划 Samba ID 范围。

d. 设置分配给所有映射用户的 shell 和主目录路径。例如：

```
template shell = /bin/bash
template homedir = /home/%U
```

2. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

3. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

其它资源

- * 默认域
- **smb.conf(5)** 手册页中的 **VARIABLE SUBSTITUTIONS** 部分
- RID 中本地 ID 的计算，请查看 **idmap_rid(8)** 手册页

1.4.6. 使用自动 ID 映射后端

您可以将 Samba 域成员配置为使用 **autorid** ID 映射后端。

autorid后端的工作方式与**rid**ID 映射后端类似，但可以为不同的域自动分配 ID。这可让您在以下情况下使用**autorid**后端：

- 仅用于*默认域
- 对于*默认域和附加域，不需要为每个附加域创建 ID 映射配置
- 只适用于特定域

注意

如果您对默认域使用**autorid**，为域添加额外的 ID 映射配置是可选的。

本节的部分内容来自在 Samba Wiki 中发布的 idmap config autorid 文档。许可证： CC BY 4.0。作者和贡献者：请参阅 Wiki页面上的历史选项卡。

使用自动扩展后端的好处

- 所有在配置范围内计算 UID 和 GID 的域用户和组都会在域成员中自动可用。
- 您不需要手动分配 ID、主目录和登录 shell。
- 没有重复的 ID，即使多域环境中的多个对象有相同的 RID。

缺陷

- 在 Samba 域成员中用户和组群 ID 不相同。
- 所有域用户可以获得相同的登录 shell 和主目录。但是，您可以使用变量。
- 您不能阻止单独的用户或组在域成员中可用。只有计算 UID 或 GID 不在配置范围内的用户和组才会包括。

先决条件

- 已安装 Samba。
- Samba 配置（除了ID 映射）位于 **/etc/samba/smb.conf** 文件中。

流程

1. 编辑 **/etc/samba/smb.conf** 文件中的 **[global]** 部分：

   a. 为 ***** 默认域启用**autorid**ID映射后端：

   ```
   idmap config * : backend = autorid
   ```

   b. 设置一个足够大的范围来为所有现有和将来的对象分配 ID。例如：

   ```
   idmap config * : range = 10000-999999
   ```

   Samba 忽略在此域中计算 ID 不在范围范围内的用户和组。

   > **警告**
   >
   > 设置范围并开始使用 Samba 后，您只能增加范围的上限。对范围的任何其他变化都可能会导致分配新的 ID，从而会丢失文件的所有者信息。

   c. 另外，还可设置范围大小。例如：

   ```
   idmap config * : rangesize = 200000
   ```

   Samba 会为每个域的对象分配这个连续的ID号，直到 **idmap config * : *range***参数中设置的范围内的所有ID分配完。

   > **注意**
   >
   > 如果设置 rangesize，则需要相应地调整范围。范围必须是 rangesize 的倍数。

   d. 设置分配给所有映射用户的 shell 和主目录路径。例如：

   ```
   template shell = /bin/bash
   template homedir = /home/%U
   ```

e. 另外，还可为域添加额外的 ID 映射配置。如果没有针对单个域的配置，Samba 则使用之前配置的 * 默认域中的 **autorid** 后端设置来计算 ID。

重要

范围不得与这个服务器上的任何其他域配置重叠。此外，范围必须足够大，以便包含将来分配的所有 ID。详情请查看 规划 Samba ID 范围。

2. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

3. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

其它资源

- **idmap_autorid(8)** 手册页中的 **THE MAPPING FORMULAS** 部分
- **idmap_autorid(8)** 手册页中的 **rangesize** 参数描述
- **smb.conf(5)** 手册页中的 **VARIABLE SUBSTITUTIONS** 部分

1.5. 将 SAMBA 设置为 AD 域成员服务器

如果您正在运行 AD 或 NT4 域，请使用 Samba 将 Red Hat Enterprise Linux 服务器添加为域的成员，以便可以：

- 访问其他域成员上的域资源
- 对本地服务（如 **sshd**）验证域用户
- 托管在服务器上的共享目录和打印机，以充当文件和打印服务器

1.5.1. 将 RHEL 系统添加到 AD 域中

Samba Winbind 是系统安全服务守护进程(SSSD)的一个替代方案，用于将活动目录(AD)与 Red Hat Enterprise Linux(RHEL)系统连接。您可以使用 **realmd** 将 RHEL 系统加入到 AD 域，来配置 Samba Winbind 。

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：

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

3. 要在域成员中共享目录或打印机，请安装**samba** 软件包：

```
# dnf 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
```

使用上面的命令，**realm**工具会自动：

- 为**ad.example.com**域中的成员创建**/etc/samba/smb.conf**文件
- 将用于用户和组查找的**winbind**模块添加到**/etc/nsswitch.conf**文件中
- 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，并使服务在系统引导时启动

6. 另外，在**/etc/samba/smb.conf**文件中设置备用的 ID 映射后端或自定义 ID 映射设置。

详情请参阅 了解和配置 Samba ID 映射。

1. 验证**winbind**服务是否运行：

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

重要

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

2. 如果您安装了**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
```

3. 另外，如果您要验证Active Directory的本地登录，请启用**winbind_krb5_localauth**插件。请参阅使用 MIT Kerberos 的本地授权插件。

验证

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**文件的所有者设置为**AD\administrator**，组设置为**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. 对于 AD 域成员，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。查看
- 使用 GPO 在 Active Directory 中启用 AES 加密类型
- **realm(8)** 手册页

1.5.2. 使用 MIT Kerberos 的本地授权插件

winbind服务向域成员提供Active Directory用户。在某些情况下，管理员希望域用户能够对域成员上运行的本地服务（如SSH服务器）启用身份验证。当使用 Kerberos 来验证域用户时，启用**winbind_krb5_localauth**插件，通过**winbind** 服务将 Kerberos 主体正确映射到Active Directory帐户。

例如，如果Active Directory用户的**sAMAccountName**属性设置为**EXAMPLE**，并且用户尝试使用小写的用户名进行日志记录，Kerberos将返回大写的用户名。因此，条目不匹配，身份验证失败。

使用**winbind_krb5_localauth**插件时，帐户名称会被正确映射。请注意，这只适用于 GSSAPI 身份验证，不适用于获取初始票据授权票据(TGT)。

先决条件

- Samba 配置为 Active Directory 的成员。
- Red Hat Enterprise Linux 对 Active Directory 进行身份验证。
- **winbind**服务在运行。

流程

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
}
```

其它资源

- **winbind_krb5_localauth(8)** 手册页。

1.6. 在 IDM 域成员中设置 SAMBA

您可以在加入到 Red Hat Identity Management (IdM)域的主机上设置 Samba。来自IdM的用户，以及来自受信任的 Active Directory(AD)域的用户(如果有的话)可以访问 Samba 提供的共享和打印机服务。

重要

对 IdM 域成员使用 Samba 是一种不受支持的技术预览特性，且包含了某些限制。例如，IdM 信任控制器不支持活动目录全局目录服务，并且不支持使用分布式计算环境/远程过程调用(DCE/RPC)协议解析 IdM 组。因此，AD 用户在登录到其他 IdM 客户端时只能访问托管在 IdM 客户端上的 Samba 共享和打印机;登录到 Windows 机器的 AD 用户无法访问托管在 IdM 域成员上的 Samba 共享。

我们鼓励在 IdM 域成员中部署 Samba 的用户向红帽提供反馈意见。

如果 AD 域中的用户需要访问 Samba 提供的共享和打印机服务，请确保在 AD 中启用了 AES 加密类型。如需更多信息，请参阅 使用 GPO 在活动目录中启用 AES 加密类型 。

先决条件

- 主机作为 IdM 域的客户端加入。
- IdM 服务器和客户端都必须运行在 RHEL 9.0 或更高版本上。

1.6.1. 准备 IdM 域以便在域成员中安装 Samba

在IdM客户端上设置Samba之前，必须在IdM服务器上使用**ipa-adtrust-install**工具来准备IdM域。

注意

运行**ipa-adtrust-install**命令的任何系统都会自动成为 AD 信任控制器。但是，您必须在 IdM 服务器上只运行一次 **ipa-adtrust-install** 。

先决条件

- IdM 服务器已安装。
- 您需要 root 权限才能安装软件包并重新启动 IdM 服务。

步骤

1. 安装所需的软件包：

```
[root@ipaserver ~]# dnf install ipa-server-trust-ad samba-client
```

2. 以 IdM 管理用户身份进行身份验证：

```
[root@ipaserver ~]# kinit admin
```

3. 运行 **ipa-adtrust-install** 工具：

```
[root@ipaserver ~]# ipa-adtrust-install
```

如果 IdM 安装了集成的 DNS 服务器，则会自动创建 DNS 服务记录。

如果您在没有集成 DNS 服务器的情况下安装了 IdM，**ipa-adtrust-install** 会打印一个服务记录列表，您必须手动将它们添加到 DNS，然后才能继续操作。

4. 该脚本提示您 **/etc/samba/smb.conf** 已存在，并将被重写：

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your existing
Samba configuration.

Do you wish to continue? [no]: yes
```

5. 该脚本提示您配置 **slapi-nis** 插件，这是一个兼容插件，允许旧的 Linux 客户端与受信任的用户一起工作：

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted users.

Enable trusted domains support in slapi-nis? [no]: yes
```

6. 系统会提示您运行 SID 生成任务，以便为任何现有用户创建 SID：

```
Do you want to run the ipa-sidgen task? [no]: yes
```

这是一个资源密集型任务，因此如果您有大量的用户，您可以在其他时间运行此操作。

7. **（可选）** 默认情况下，对于 Windows Server 2008 及更高版本，动态 RPC 端口范围定义为 **49152-65535**。如果需要为您的环境定义一个不同的动态 RPC 端口范围，请将 Samba 配置为使用不同的端口，并在防火墙设置中开放这些端口。以下示例将端口范围设置为**55000-65000**。

```
[root@ipaserver ~]# net conf setparm global 'rpc server dynamic port range' 55000-
65000
[root@ipaserver ~]# firewall-cmd --add-port=55000-65000/tcp
[root@ipaserver ~]# firewall-cmd --runtime-to-permanent
```

8. 重启**ipa**服务：

```
[root@ipaserver ~]# ipactl restart
```

9. 使用**smbclient**工具来验证 Samba 是否响应 IdM 端的 Kerberos 身份验证：

```
[root@ipaserver ~]# smbclient -L ipaserver.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
   Sharename       Type      Comment
   ---------       ----      -------
   IPC$            IPC       IPC Service (Samba 4.15.2)
...
```

1.6.2. 在 IdM 客户端中安装和配置 Samba 服务器

您可以在已在 IdM 域注册的客户端上安装和配置 Samba。

先决条件

- IdM 服务器和客户端都必须运行在 RHEL 9.0 或更高版本上。
- 已准备好 IdM 域，如 为在域成员上安装 Samba 准备 IdM 域 中所述。
- 如果 IdM 具有配置了 AD 的信任，请为 Kerberos 启用 AES 加密类型。例如，使用组策略对象(GPO)来启用 AES 加密类型。详情请参阅 使用 GPO 在活动目录中启用 AES 加密 。

流程

1. 安装**ipa-client-samba**软件包：

```
[root@idm_client]# dnf install ipa-client-samba
```

2. 使用**ipa-client-samba**工具准备客户端并创建初始 Samba 配置：

```
[root@idm_client]# ipa-client-samba
Searching for IPA server...
IPA server: DNS discovery
Chosen IPA master: idm_server.idm.example.com
SMB principal to be created: cifs/idm_client.idm.example.com@IDM.EXAMPLE.COM
NetBIOS name to be used: IDM_CLIENT
Discovered domains to use:

 Domain name: idm.example.com
NetBIOS name: IDM
        SID: S-1-5-21-525930803-952335037-206501584
   ID range: 212000000 - 212199999

 Domain name: ad.example.com
NetBIOS name: AD
        SID: None
   ID range: 1918400000 - 1918599999
```

```
Continue to configure the system with these values? [no]: yes
Samba domain member is configured. Please check configuration at /etc/samba/smb.conf
and start smb and winbind services
```

3. 默认情况下，**ipa-client-samba**会自动将**[homes]**部分添加到**/etc/samba/smb.conf**文件中，该文件在用户连接时动态共享用户的主目录。如果用户在这个服务器上没有主目录，或者您不想共享主目录，请从**/etc/samba/smb.conf**中删除以下行：

```
[homes]
    read only = no
```

4. 共享目录和打印机。详情请查看：
   - 设置使用 POSIX ACL 的 Samba 文件共享
   - 设置使用 Windows ACL 的共享
   - 将 Samba 设置为打印服务器
5. 在本地防火墙中打开 Samba 客户端所需的端口：

```
[root@idm_client]# firewall-cmd --permanent --add-service=samba-client
[root@idm_client]# firewall-cmd --reload
```

6. 启用并启动**smb**和**winbind**服务：

```
[root@idm_client]# systemctl enable --now smb winbind
```

验证

在安装了 **samba-client** 软件包的不同 IdM 域成员上运行以下验证步骤：

- 使用 Kerberos 身份验证列出 Samba 服务器中的共享：

```
$ smbclient -L idm_client.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry

    Sharename       Type      Comment
    ---------       ----      -------
    example         Disk
    IPC$            IPC       IPC Service (Samba 4.15.2)
...
```

其它资源

- **ipa-client-samba(1)** man page

1.6.3. 如果 IdM 信任新域，请手动添加 ID 映射配置

Samba 需要一个 ID 映射配置，用户可从该域访问资源。在 IdM 客户端上运行的现有 Samba 服务器上，在管理员向 Active Directory(AD)域添加了新的信任后，您必须手动添加 ID 映射配置。

先决条件

- 您在 IdM 客户端中配置了 Samba。之后，IdM 增加了一个新的信任。
- 在可信 AD 域中必须禁用 Kerberos 的 DES 和 RC4 加密类型。为了安全起见，RHEL 9 不支持这些弱加密类型。

步骤

1. 使用主机的 keytab 进行身份验证：

```
[root@idm_client]# kinit -k
```

2. 使用**ipa idrange-find**命令来显示新域的基本 ID 和 ID 范围大小。例如，以下命令显示了**ad.example.com**域的值：

```
[root@idm_client]# ipa idrange-find --name="AD.EXAMPLE.COM_id_range" --raw
---------------
1 range matched
---------------
  cn: AD.EXAMPLE.COM_id_range
  ipabaseid: 1918400000
  ipaidrangesize: 200000
  ipabaserid: 0
  ipanttrusteddomainsid: S-1-5-21-968346183-862388825-1738313271
  iparangetype: ipa-ad-trust
----------------------------
Number of entries returned 1
----------------------------
```

在后续步骤中，您需要**ipabaseid**和**ipaidrangesize**属性的值。

3. 要计算可用最高的 ID，请使用以下公式：

```
maximum_range = ipabaseid + ipaidrangesize - 1
```

使用上一步中的值，**ad.example.com**域的最大可用 ID 是**1918599999**(1918400000 + 200000 - 1)。

4. 编辑**/etc/samba/smb.conf**文件，并将域的 ID 映射配置添加到**[global]**部分：

```
idmap config AD : range = 1918400000 - 1918599999
idmap config AD : backend = sss
```

将**ipabaseid**属性的值指定为最小值，将上一步中的计算值指定为该范围的最大值。

5. 重启**smb**和**winbind**服务：

```
[root@idm_client]# systemctl restart smb winbind
```

验证

- 使用 Kerberos 身份验证列出 Samba 服务器中的共享：

```
$ smbclient -L idm_client.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
```

```
    Sharename       Type      Comment
    ---------       ----      -------
    example         Disk
    IPC$            IPC       IPC Service (Samba 4.15.2)
...
```

1.6.4. 其它资源

- 安装身份管理客户端

1.7. 设置使用 POSIX ACL 的 SAMBA 文件共享

作为 Linux 服务，Samba 支持与 POSIX ACL 的共享。它们允许您使用诸如**chmod**等工具在 Samba 服务器上本地管理权限。如果共享是存储在支持扩展属性的文件系统中，您可以使用多个用户和组定义 ACL。

注意

如果您需要使用精细的 Windows ACL，请参阅 设置使用 Windows ACL 的共享。

这个部分的内容基于 Samba Wiki 中发布的 Setting up a Share Using POSIX ACLs 文档。许可证： CC BY 4.0。作者和贡献者：请参阅 Wiki 页面上的历史选项卡。

1.7.1. 添加使用 POSIX ACL 的共享

您可以创建一个名为 **example** 的共享，它提供 **/srv/samba/example/** 目录的内容，并使用 POSIX ACL。

先决条件

Samba 采用以下模式之一设置：

- 独立服务器
- 域成员

流程

1. 如果不存在，请创建文件夹。例如：

```
# mkdir -p /srv/samba/example/
```

2. 如果您在**enforcing**模式下运行 SELinux，请在目录中设置**samba_share_t**上下文：

```
# semanage fcontext -a -t samba_share_t "/srv/samba/example(/.*)?"
# restorecon -Rv /srv/samba/example/
```

3. 在目录中设置文件系统 ACL。详情请查看：
   - 在使用 POSIX ACL 的 Samba 共享上设置标准 ACL
   - 在使用 POSIX ACL 的共享上设置扩展 ACL。
4. 将示例共享添加到**/etc/samba/smb.conf**文件中。例如，添加启用了共享的写操作：

```
[example]
 path = /srv/samba/example/
 read only = no
```

注意

无论文件系统 ACL 是什么；如果您没有设置**read only = no**，Samba 会以只读模式共享该目录。

5. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

6. 打开所需的端口，并使用**firewall-cmd**工具重新加载防火墙配置：

```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

7. 重启**smb**服务：

```
# systemctl restart smb
```

1.7.2. 在使用 POSIX ACL 的 Samba 共享中设置标准 Linux ACL

Linux 中的标准 ACL 支持为一个所有者、一个组和所有其他未定义用户设置权限。您可以使用**chown**、**chgrp**和**chmod**工具来更新 ACL。如果您需要精确控制，您需要使用更复杂的 POSIX ACL，请参阅

在使用 POSIX ACL 的 Samba 共享上设置扩展 ACL 。

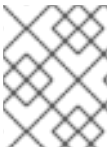
以下步骤将**/srv/samba/example/**目录的所有者设置为**root**用户，将读写权限赋予**Domain Users** 组，并拒绝所有其他用户的访问。

先决条件

- 存在要设置 ACL 的 Samba 共享。

流程

```
# chown root:"Domain Users" /srv/samba/example/
# chmod 2770 /srv/samba/example/
```



注意

对目录启用 set-group-ID(SGID)位会自动对目录组的所有新文件和子目录设置默认组，而不是通常的行为，将其设置为创建新目录条目的用户的主组。

其它资源

- **chown(1)** 和 **chmod(1)** 手册页

1.7.3. 在使用 POSIX ACL 的 Samba 共享中设置扩展的 ACL

如果文件系统中保存了共享目录的支持扩展 ACL，您可以使用它们设置复杂的权限。扩展 ACL 可以包含多个用户和组群的权限。

扩展 POSIX ACL 可让您使用多个用户和组配置复杂的 ACL。但是，您只能设置以下权限：

- 无权限
- 读权限
- 写权限
- 全控制

如果您需要更细粒度的 Windows 权限，如 **创建文件夹 / 追加数据**，请将共享配置为使用 Windows ACL。

请参阅 设置使用 Windows ACL 的共享 。

以下流程演示了如何在共享中启用扩展 ACL。另外，它还包含有关设置扩展 ACL 的示例。

先决条件

- 存在要设置 ACL 的 Samba 共享。

流程

1. 在**/etc/samba/smb.conf**文件中的共享部分启用以下参数，以启用扩展 ACL 的 ACL 继承：

   ```
   inherit acls = yes
   ```

   详情请查看 **smb.conf(5)**手册页中的参数描述。

2. 重启**smb**服务：

   ```
   # systemctl restart smb
   ```

3. 在目录中设置 ACL。例如：

   例 1.2. 设置扩展 ACL

   以下步骤为**Domain Admins**组设置读、写和执行权限，为**Domain Users**组设置读和执行权限，并拒绝其他人对**/srv/samba/example/**目录的访问：

   1. 为主用户帐户组禁用自动授予权限：

      ```
      # setfacl -m group::--- /srv/samba/example/
      # setfacl -m default:group::--- /srv/samba/example/
      ```

      目录的主组还被映射到动态**CREATOR GROUP**主体。当您对Samba 共享使用扩展 POSIX ACL 时，主体会被自动添加，您无法将其删除。

   2. 设置目录中的权限：

      a. 对**Domain Admins**组赋予读、写和执行权限：

```
# setfacl -m group:"DOMAIN\Domain Admins":rwx /srv/samba/example/
```

b. 对**Domain Users**组赋予读和执行权限：

```
# setfacl -m group:"DOMAIN\Domain Users":r-x /srv/samba/example/
```

c. **other** ACL条目设置权限，以拒绝与其他 ACL 条目不匹配的用户的访问：

```
# setfacl -R -m other::--- /srv/samba/example/
```

这些设置只适用于这个目录。在 Windows 中，这些 ACL 映射到仅**此文件**夹模式。

3. 要使上一步中设置的权限被在此目录中创建的新文件系统对象继承，请执行以下操作：

```
# setfacl -m default:group:"DOMAIN\Domain Admins":rwx /srv/samba/example/
# setfacl -m default:group:"DOMAIN\Domain Users":r-x /srv/samba/example/
# setfacl -m default:other::--- /srv/samba/example/
```

使用这些设置，现在将主体的仅**此文件**夹模式设置为**此文件**夹、**子文件**夹**和文件**模式。

Samba 将流程中设置的权限映射到以下 Windows ACL:

主体	权限	适用于
*domain**Domain*Admins	全控制	这个文件夹、子文件夹和文件
Domain\Domain Users	读和执行	这个文件夹、子文件夹和文件
每个人 [a]	无	这个文件夹、子文件夹和文件
所有者（Unix 用户\所有者） [b]	全控制	只限于这个文件夹
primary_group (Unix 用户\primary_group) [c]	无	只限于这个文件夹
创建者所有者 [d] [e]	全控制	只适用于子文件夹和文件
创建者组 [e] [f]	无	只适用于子文件夹和文件

[a] Samba从**othe** ACL 条目映射此主体的权限。

[b] Samba 将目录的所有者映射到此条目。

[c] Samba 将目录的主组群映射到这个条目。

[d] 在新文件系统对象中，创建者会自动继承这个主体的权限。

[e] 在使用 POSIX ACL 的共享中不支持从 ACL 配置或删除这些主体。

[f] 在新文件系统对象中，创建器的主组群自动继承这个主体的权限。

1.8. 对使用 POSIX ACL 的共享设置权限

另外，要限制或赋予对 Samba 共享的访问权限，您可以在**/etc/samba/smb.conf**文件的共享部分设置某些参数。

注意

如果用户、组或主机能够访问共享，则进行基于共享的权限管理。这些设置不会影响文件系统 ACL。

使用基于共享的设置来限制对共享的访问，例如拒绝特定主机的访问。

先决条件

- 与 POSIX ACL 的共享已被设置。

1.8.1. 配置基于用户和组群的共享访问权限

基于用户和组的访问控制，使您能够赋予或拒绝特定用户和组对共享的访问权限。

先决条件

- 已存在您要设置用户或组群访问的 Samba 共享。

流程

1. 例如，要在 **用户帐户** 访问时允许 **Domain Users** 组的所有成员访问共享，请在共享的配置中添加以下参数：

```
valid users = +DOMAIN\"Domain Users"
invalid users = DOMAIN\user
```

   invalid users 参数的优先级高于**valid users** 参数。例如，如果 **user**帐户是 **Domain Users** 组的成员，则在使用上例时会拒绝此帐户的访问。

2. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

其它资源

- **smb.conf(5)** 手册页

1.8.2. 配置基于主机的共享访问权限

基于主机的访问控制允许您根据客户端的主机名、IP 地址或 IP 范围授予或拒绝对共享的访问。

以下流程解释了如何启用 **127.0.0.1** IP 地址、 **192.0.2.0/24** IP 范围，以及**client1.example.com** 主机来访问共享，另外拒绝了对 **client2.example.com** 主机的访问：

先决条件

- 已存在您要设置基于主机的访问的 Samba 共享。

流程

1. 在 **/etc/samba/smb.conf** 文件的共享配置中添加以下参数：

```
hosts allow = 127.0.0.1 192.0.2.0/24 client1.example.com
hosts deny = client2.example.com
```

   hosts deny 参数的优先级高于 **hosts allow**。例如，如果 **client1.example.com** 解析为 **hosts allow** 参数中列出的 IP 地址，那么此主机的访问将被拒绝。

2. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

其它资源

- **smb.conf(5)** 手册页

1.9. 设置使用 WINDOWS ACL 的共享

Samba 支持在共享和文件系统对象中设置 Windows ACL。这可让您：

- 使用精细 Windows ACL
- 使用 Windows 管理共享权限和文件系统 ACL

或者，您可以将共享配置为使用 POSIX ACL。

详情请参阅 设置使用 POSIX ACL 的 Samba 文件共享 。

这个部分的内容基于 Samba Wiki 中发布的 Setting up a Share Using Windows ACLs 文档。许可证： CC BY 4.0。作者和贡献者：请参阅 Wiki 页面上的历史选项卡。

1.9.1. 授予 SeDiskOperatorPrivilege 特权

只有被赋予了 **SeDiskOperatorPrivilege** 特权的用户和组才能对使用了 Windows ACL 的共享配置权限。

流程

1. 例如，要对 ***DOMAIN*\Domain Admins** 组赋予 **SeDiskOperatorPrivilege** 特权：

```
# net rpc rights grant "DOMAIN\Domain Admins" SeDiskOperatorPrivilege -U
"DOMAIN\administrator"
Enter DOMAIN\administrator's password:
Successfully granted rights.
```

注意

在域环境中，对域组赋予 **SeDiskOperatorPrivilege**。这可让您通过更新用户的组成员资格来集中管理特权。

2. 列出所有被赋予了 **SeDiskOperatorPrivilege** 的用户和组：

```
# net rpc rights list privileges SeDiskOperatorPrivilege -U "DOMAIN\administrator"
Enter administrator's password:
SeDiskOperatorPrivilege:
  BUILTIN\Administrators
  DOMAIN\Domain Admins
```

1.9.2. 启用 Windows ACL 支持

要配置支持 Windows ACL 的共享，您必须在 Samba 中启用此功能。

先决条件

- 在 Samba 服务器中配置了一个用户共享。

流程

1. 要全局启用所有共享，请在 **/etc/samba/smb.conf** 文件的 **[global]** 部分添加以下设置：

```
vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes
```

   或者，您可以通过将相同的参数添加到共享部分来启用对单个共享的 Windows ACL 支持。

2. 重启**smb**服务：

```
# systemctl restart smb
```

1.9.3. 添加使用 Windows ACL 的共享

您可以创建一个名为 **example** 的共享，其共享 **/srv/samba/example/** 目录的内容，并使用 Windows ACL。

流程

1. 如果不存在，请创建文件夹。例如：

```
# mkdir -p /srv/samba/example/
```

2. 如果您在**enforcing**模式下运行 SELinux，请在目录中设置**samba_share_t**上下文：

```
# semanage fcontext -a -t samba_share_t "/srv/samba/example(/.)?"*
# restorecon -Rv /srv/samba/example/
```

3. 将示例共享添加到**/etc/samba/smb.conf**文件中。例如，添加启用了共享的写操作：

```
[example]
 path = /srv/samba/example/
 read only = no
```

注意

无论文件系统 ACL 是什么；如果您没有设置**read only = no**，Samba 会以只读模式共享该目录。

4. 如果您没有在**[global]** 部分中对所有共享启用 Windows ACL 支持，那么请在 **[example]** 部分中添加以下参数来为这个共享启用此特性：

```
vfs objects = acl_xattr
map acl inherit = yes
store dos attributes = yes
```

5. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

6. 打开所需的端口，并使用**firewall-cmd**工具重新加载防火墙配置：

```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

7. 重启**smb**服务：

```
# systemctl restart smb
```

1.9.4. 管理使用 Windows ACL 的共享的共享权限和文件系统 ACL

要在使用 Windows ACL 的 Samba 共享上管理共享权限和文件系统 ACL，请使用 Windows 应用程序，如**计算机管理**。详情请查看 Windows 文档。或者，使用 **smbcacls** 工具来管理 ACL。

注意

要从 Windows 修改文件系统权限，您必须使用赋予了 **SeDiskOperatorPrivilege** 特权的帐户。

其它资源

- 使用 smbcacls 在 SMB 共享中管理 ACL
- 授予 SeDiskOperatorPrivilege 特权

1.10. 使用 SMBCACLS 在 SMB 共享中管理 ACL

smbcacls 工具可以列出、设置和删除存储在 SMB 共享中的文件和目录的 ACL。您可以使用 **smbcacls** 来管理文件系统 ACL：

- 在使用高级 Windows ACL 或 POSIX ACL 的本地或远程 Samba 服务器中
- 在 Red Hat Enterprise Linux 上，远程管理在 Windows 上托管的共享的 ACL

1.10.1. 访问控制条目

文件系统对象的每个 ACL 条目都包含以下格式的访问控制条目(ACE)：

> *security_principal:access_right/inheritance_information/permissions*

> **例 1.3. 访问控制条目**
>
> 如果 **AD\Domain Users** 组对Windows 上的**此文件夹、子文件夹和文件**拥有**修改**权限，那么ACL 将包含以下 ACE：
>
> > AD\Domain Users:ALLOWED/OI|CI/CHANGE

ACE 包含以下部分：

安全主体
: 安全主体是 ACL 中权限的用户、组群或 SID。

访问权利
: 定义是否赋予或拒绝了对对象的访问权限。该值可以是 **ALLOWED** 或 **DENIED**。

继承信息
: 存在以下值：

表 1.1. 继承设置

值	描述	映射到
OI	对象实例	这个文件夹和文件
CI	容器继承	这个文件夹和子文件夹
IO	只继承	ACE 不适用于当前文件或目录
ID	继承	ACE 从父目录中继承

另外，这些值可以合并如下：

表 1.2. 继承设置组合

值组合	映射到 Windows 应用于 设置
OI|CI	这个文件夹、子文件夹和文件
OI|CI|IO	只适用于子文件夹和文件
CI|IO	只使用子文件夹
OI|IO	仅限文件

权限

这个值可以是代表一个或多个 Windows 权限的十六进制值，也可以是一个 **smbcacls** 别名：

- 代表一个或多个 Windows 权限的十六进制值。
  下表以十六进制格式显示了高级 Windows 权限及其对应的值：

表 1.3. 十六进制格式的Windows权限及其相应的smbcacls值

Windows 权限	十六进制值
全控制	**0x001F01FF**
遍历文件夹 / 执行文件	**0x00100020**
列出文件夹 / 读数据	**0x00100001**
读取属性	**0x00100080**
读取扩展属性	**0x00100008**
创建文件 / 写数据	**0x00100002**
创建文件夹/附加数据	**0x00100004**
写入属性	**0x00100100**
写扩展属性	**0x00100010**
删除子文件夹和文件	**0x00100040**
删除	**0x00110000**
读取权限	**0x00120000**
更改权限	**0x00140000**
获取所有权	**0x00180000**

可以使用位 **OR** 操作将多个权限组合为一个十六进制值。

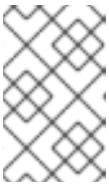
详情请参阅 ACE 掩码计算。

- **smbcacls** 别名。下表显示了可用的别名：

表 1.4. 现有 smbcacls 别名及其对应的 Windows 权限

smbcacls 别名	映射至 Windows 权限
R	读

smbcacls 别名	映射至 Windows 权限
READ	读和执行
W	特殊： ○ 创建文件 / 写数据 ○ 创建文件夹/附加数据 ○ 写入属性 ○ 写扩展属性 ○ 读取权限
D	删除
P	更改权限
O	获取所有权
X	遍历 / 执行
CHANGE	修改
FULL	全控制



注意

设置权限时，您可以组合单例别名。例如，您可以设置 **RD** 来应用 Windows 权限 **读** 和 **删除**。但是，您既不能组合多个非字母别名，也无法组合别名和十六进制值。

1.10.2. 使用 smbcacls 显示 ACL

要显示 SMB 共享的 ACL，请使用 **smbcacls** 工具。如果您运行不带任何操作参数的 **smbcacls**，如 **--add**，那么工具会显示文件系统对象的 ACL。

流程

例如，列出 //**server**/**example** 共享的根目录的 ACL：

```
# smbcacls //server/example / -U "DOMAIN\administrator"
Enter DOMAIN\administrator's password:
REVISION:1
CONTROL:SR|PD|DI|DP
OWNER:AD\Administrators
GROUP:AD\Domain Users
ACL:AD\Administrator:ALLOWED/OI|CI/FULL
ACL:AD\Domain Users:ALLOWED/OI|CI/CHANGE
ACL:AD\Domain Guests:ALLOWED/OI|CI/0x00100021
```

命令的输出会显示：

- **REVISION** ：安全描述符的内部 Windows NT ACL 修订版
- **CONTROL** ：安全描述符控制
- **OWNER** ：安全描述符所有者的名称或 SID
- **GROUP** ：安全描述符组的名称或 SID
- **ACL** 条目.详情请参阅 访问控制条目。

1.10.3. ACE 掩码计算

在大多数情况下，当添加或更新 ACE 时，您可以使用 现有的 smbcacls 别名及其相应的 Windows 权限 中列出的 **smbcacls** 别名。

但是，如果您要设置 Windows 权限及其相应的 smbcacls 值（十六进制格式） 中列出的高级 Windows 权限，则必须使用逐位 **OR** 操作来计算正确的值。您可以使用以下 shell 命令计算值：

```
# echo $(printf '0x%X' $(( hex_value_1 | hex_value_2 | ... )))
```

例 1.4. 计算 ACE 掩码

您需要设置以下权限：

- 遍历文件夹/执行文件(0x00100020)
- 列出文件夹/读数据(0x00100001)
- 读属性(0x00100080)

要计算上面权限的十六进制值，请输入：

```
# echo $(printf '0x%X' $(( 0x00100020 | 0x00100001 | 0x00100080 )))
0x1000A1
```

设置或更新 ACE 时使用返回的值。

1.10.4. 使用 smbcacls 添加、更新和删除 ACL

根据您传递给 **smbcacls** 工具的参数，您可以添加、更新和删除文件或目录的 ACL。

添加 ACL
要对 **//server/example** 共享的根添加ACL，该共享将**此文件夹、子文件夹和文件**的 **CHANGE** 权限赋予 **AD\Domain Users** 组：

```
# smbcacls //server/example / -U "DOMAIN\administrator --add ACL:"AD\Domain
Users":ALLOWED/OI|CI/CHANGE
```

更新 ACL

更新 ACL 与添加新的 ACL 类似。您可以使用 **--modify** 参数和现有的安全主体来覆盖 ACL，以便更新 ACL。如果 **smbcacls** 在 ACL 列表中找到了安全主体，那么工具会更新这些权限。否则，命令会失败并报错：

```
ACL for SID principal_name not found
```

例如，要更新 **AD\Domain Users** 组的权限，并将其设置为对 **此文件**夹、**子文件**夹**和文件**的**READ**权限，请执行以下操作：

```
# smbcacls //server/example / -U "DOMAIN\administrator --modify ACL:"AD\Domain
Users":ALLOWED/OI|CI/READ
```

删除 ACL
要删除 ACL，请将带有确切ACL的 **--delete** 参数传递给 **smbcacls** 工具。例如：

```
# smbcacls //server/example / -U "DOMAIN\administrator --delete ACL:"AD\Domain
Users":ALLOWED/OI|CI/READ
```

1.11. 允许用户在 SAMBA 服务器上共享目录

在 Samba 服务器上，你可以配置用户共享目录,而无需root权限。

1.11.1. 启用用户共享功能

在用户可以共享目录之前，管理员必须在 Samba 中启用用户共享。

例如，仅允许本地 **example** 组的成员创建用户共享：

流程

1. 如果本地 **example** 组不存在，请创建它：

```
# groupadd example
```

2. 为 Samba 准备目录以存储用户共享定义并正确设置其权限。例如：
   a. 创建目录：

```
# mkdir -p /var/lib/samba/usershares/
```

   b. 为 **example** 组设置写权限：

```
# chgrp example /var/lib/samba/usershares/
# chmod 1770 /var/lib/samba/usershares/
```

   c. 设置粘性位以防止用户重命名或删除此目录中其他用户存储的文件。

3. 编辑 **/etc/samba/smb.conf** 文件，并将以下内容添加到 **[global]** 部分：
   a. 设置您配置用来存储用户共享定义的目录的路径。例如：

```
usershare path = /var/lib/samba/usershares/
```

b. 设置允许在这个服务器上创建多少个用户共享 Samba。例如：

```
usershare max shares = 100
```

如果您对 **usershare max shares** 参数使用默认值 **0**，则用户共享将被禁用。

c. 另外，还可设置绝对目录路径列表。例如，要配置 Samba 只允许共享 **/data** 和 **/srv** 目录的子目录，请设置：

```
usershare prefix allow list = /data /srv
```

有关您可以设置的更多用户共享相关参数的列表，请参阅 **smb.conf(5)** 手册页中的 **用户共享** 部分。

4. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

5. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

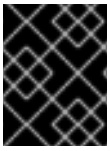
用户现在可以创建用户共享。

1.11.2. 添加用户共享

在 Samba 中启用了用户共享功能后，用户可以通过运行 **net usershare add** 命令在 Samba 服务器上共享目录，而无需 **root** 权限。

net usershare add 命令的说明：

net usershare add share_name path [[comment] | [ACL]] [guest_ok=y|n]



重要

如果在创建用户共享时设置了 ACL，您必须在 ACL 之前指定comment参数。要设置空的 comment，请在双引号中使用空字符串。

请注意，如果管理员在 **/etc/samba/smb.conf** 文件的 **[global]** 部分中设置了 **usershare allow guests = yes**，用户只能对用户共享启用 guest访问。

例 1.5. 添加用户共享

用户想要在 Samba 服务器上共享 **/srv/samba/** 目录。该共享应命名为 **example**，未设置任何 comment，应该可以被 guest 用户访问。此外，对 **AD\Domain Users** 组的共享权限应设置为可完全访问，对其他用户设置为读权限。要添加此共享，请以用户身份运行：

```
$ net usershare add example /srv/samba/ "" "AD\Domain Users":F,Everyone:R
guest_ok=yes
```

1.11.3. 更新用户共享的设置

要更新用户共享的设置，请使用具有相同共享名称和新设置的 **net usershare add** 命令覆盖共享。

请参阅 添加用户共享。

1.11.4. 显示现有用户共享的信息

用户可以在 Samba 服务器上输入 **net usershare info** 命令，来显示用户共享及其设置。

先决条件

- 在 Samba 服务器中配置了一个用户共享。

流程

1. 显示任意用户创建的所有用户共享：

```
$ net usershare info -l
[share_1]
path=/srv/samba/
comment=
usershare_acl=Everyone:R,host_name\user:F,
guest_ok=y
...
```

   若要只列出运行命令的用户所创建的共享，请省略 **-l** 参数。

2. 若要只显示关于特定共享的信息，请将共享名称或通配符传给命令。例如，显示名称以 **share_** 开头的共享的信息：

```
$ net usershare info -l share_*
```

1.11.5. 列出用户共享

如果您想只列出可用的用户共享，而不列出它们的设置，请使用 **net usershare list** 命令。

先决条件

- 在 Samba 服务器中配置了一个用户共享。

流程

1. 列出任意用户创建的共享：

```
$ net usershare list -l
share_1
share_2
...
```

   若要只列出运行命令的用户所创建的共享，请省略 **-l** 参数。

2. 若要只列出特定的共享，请将共享名称或通配符传给命令。例如，只列出名称以 **share_** 开头的共享 ：

```
$ net usershare list -l share_*
```

1.11.6. 删除用户共享

要删除用户共享，请以创建共享的用户身份或以 **root** 用户身份，使用**net usershare delete** 命令。

先决条件

- 在 Samba 服务器中配置了一个用户共享。

流程

```
$ net usershare delete share_name
```

1.12. 配置共享以允许不进行身份验证的访问

在某些情况下，您想要共享一个用户无需身份验证即可连接到的目录。若要对此进行配置，请对共享启用guest访问。

> **警告**
>
> 不需要身份验证的共享可能会造成安全隐患。

1.12.1. 启用对共享的客户机访问

如果对共享启用了 guest 访问，Samba 会将guest连接映射到**guest account**参数中设置的操作系统帐户。如果至少满足以下条件之一，Guest用户就可以访问此共享上的文件：

- 该帐户在文件系统 ACL 中列出
- **other** 用户的 POSIX 权限允许这样做

例 1.6. 客户端共享权限

如果您将 Samba 配置为将guest帐户映射到 **nobody** （这是默认值），那么以下示例中的 ACL：

- 允许 guest 用户读 **file1.txt**
- 允许 guest 用户读和修改 **file2.txt**
- 防止 guest 用户读或修改 **file3.txt**

```
-rw-r--r--. 1 root       root      1024 1. Sep 10:00 file1.txt
-rw-r-----. 1 nobody     root      1024 1. Sep 10:00 file2.txt
-rw-r-----. 1 root       root      1024 1. Sep 10:00 file3.txt
```

流程

1. 编辑 **/etc/samba/smb.conf** 文件：

   a. 如果这是您在这个服务器上设置的第一个客户机共享：

      i. 在 **[global]** 部分中设置**map to guest = Bad User** ：

      ```
      [global]
          ...
          map to guest = Bad User
      ```

      使用这个设置，Samba 将拒绝使用错误密码的登录尝试，除非用户名不存在。如果指定的用户名不存在，并且对共享启用了 guest 访问，那么 Samba 会将连接视为guest登录。

      ii. 默认情况下，Samba 将 guest 帐户映射到 Red Hat Enterprise Linux 上的 **nobody** 帐户。另外，您也可以设置另外一个帐户。例如：

      ```
      [global]
          ...
          guest account = user_name
      ```

      此参数中设置的帐户必须在 Samba 服务器中本地存在。出于安全考虑，红帽建议使用没有分配有效 shell 的帐户。

   b. 在 **[example]** 共享部分中添加 **guest ok = yes** 设置：

   ```
   [example]
       ...
       guest ok = yes
   ```

2. 验证**/etc/samba/smb.conf**文件：

   ```
   # testparm
   ```

3. 重新载入 Samba 配置：

   ```
   # smbcontrol all reload-config
   ```

1.13. 为 MACOS 客户端配置 SAMBA

fruit 虚拟文件系统(VFS)Samba 模块提供了与 Apple 服务器消息块(SMB)客户端增强了的兼容性。

1.13.1. 优化 Samba 配置，以便为 macOS 客户端提供文件共享

fruit 模块提供增强的 Samba 与 macOS 客户端的兼容性。您可以为托管在 Samba 服务器上的所有共享配置模块，以便为 macOS 客户端优化文件共享。

注意

全局启用 **fruit** 模块。当客户端建立到服务器的第一个连接时，使用 macOS 的客户端协商服务器消息块版本 2 (SMB2) Apple (AAPL)协议扩展。如果客户端第一次连接到未启用 AAPL 扩展的共享，那么客户端不会对服务器的任何共享使用扩展。

先决条件

- Samba 配置为文件服务器。

流程

1. 编辑 **/etc/samba/smb.conf** 文件，并在 **[global]** 部分启用 **fruit**和**streams_xattr** VFS 模块：

```
vfs objects = fruit streams_xattr
```

> **重要**
>
> 在启用 **streams_xattr** 之前，您必须启用 **fruit**模块。**fruit** 模块使用备用数据流 (ADS)。因此，您也必须启用 **streams_xattr** 模块。

2. 另外，要对共享提供 macOS Time Machine 支持，请在 **/etc/samba/smb.conf** 文件中的共享配置中添加以下设置：

```
fruit:time machine = yes
```

3. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

4. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

其它资源

- **vfs_fruit(8)** 手册页。
- 配置文件共享：
  - 设置使用 POSIX ACL 的 Samba 文件共享
  - 设置使用 Windows ACL 的共享。

1.14. 使用 SMBCLIENT 实用程序访问 SMB 共享

smbclient 工具可让您访问 SMB 服务器中的文件共享，类似于命令行 FTP 客户端。例如，您可以使用它来向共享上传文件和从共享下载文件。

先决条件

- **samba-client** 软件包已安装。

1.14.1. smbclient 互动模式如何工作

例如，使用 ***DOMAIN\user*** 帐户对在 **server** 上托管的**example**共享进行身份验证：

```
# smbclient -U "DOMAIN\user" //server/example
```

```
Enter domain\user's password:
Try "help" to get a list of possible commands.
smb: \>
```

在 **smbclient** 成功连接到共享后，工具进入互动模式并显示以下提示：

```
smb: \>
```

要在互动 shell 中显示所有可用命令，请输入：

```
smb: \> help
```

要显示特定命令的帮助信息，请输入：

```
smb: \> help command_name
```

其它资源

- **smbclient(1)** 手册页

1.14.2. 在互动模式中使用 smbclient

如果您使用不带 **-c** 参数的 **smbclient**，那么工具将进入交互模式。下面的步骤演示了如何连接到 SMB 共享并从子目录中下载文件。

流程

1. 连接到共享：

```
# smbclient -U "DOMAIN\user_name" //server_name/share_name
```

2. 进到 **/example/** 目录：

```
smb: \> d /example/
```

3. 列出目录中的文件：

```
smb: \example\> ls
  .                   D        0  Thu Nov 1 10:00:00 2018
  ..                  D        0  Thu Nov 1 10:00:00 2018
  example.txt         N  1048576  Thu Nov 1 10:00:00 2018

        9950208 blocks of size 1024. 8247144 blocks available
```

4. 下载 **example.txt** 文件：

```
smb: \example\> get example.txt
getting file \directory\subdirectory\example.txt of size 1048576 as example.txt (511975,0
KiloBytes/sec) (average 170666,7 KiloBytes/sec)
```

5. 从共享断开：

```
smb: \example\> exit
```

1.14.3. 在脚本模式中使用 smbclient

如果将 **-c** 参数传给 **smbclient**，那么你可对远程 SMB 共享自动执行命令。这可让您在脚本中使用 **smbclient**。

下面的步骤演示了如何连接到 SMB 共享并从子目录中下载文件。

流程

- 使用以下命令连接到共享，进到 **example** 目录，下载 **example.txt** 文件：

```
# smbclient -U DOMAIN\user_name //server_name/share_name -c "cd /example/ ; get example.txt ; exit"
```

1.15. 将 SAMBA 设置为打印服务器

如果您将 Samba 设置为打印服务器，那么网络中的客户端可以使用 Samba 进行打印。此外，如果进行了配置， Windows 客户端可以从 Samba 服务器下载驱动程序。

本节的部分内容摘自在 Samba Wiki 中发布的将Samba设置为打印服务器文档。许可证： CC BY 4.0。作者和贡献者：请参阅 Wiki 页面上的历史选项卡。

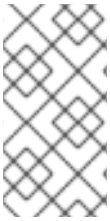
先决条件

Samba 采用以下模式之一设置：

- 独立服务器
- 域成员

1.15.1. 在 Samba 中启用打印服务器支持

默认情况下，在 Samba 中不启用打印服务器支持。要将 Samba 用作打印服务器，您必须相应地配置 Samba。



注意

打印作业和打印机操作需要远程过程调用(RPC)。默认情况下，Samba 根据需要启动 **rpcd_spools** 服务来管理 RPC。在第一个 RPC 调用过程中，或者当您更新了 CUPS 中的打印机列表时，Samba 会从 CUPS 检索打印机信息。每台打印机可能需要大约 1 秒。因此，如果您有超过 50 台打印机，请调优 **rpcd_spools** 设置。

先决条件

- 打印机在 CUPS 服务器中配置。
  有关在 CUPS 中配置打印机的详情，请查看打印服务器上 CUPS Web 控制台 (https://*printserver*:631/help)中提供的文档。

流程

1. 编辑 **/etc/samba/smb.conf** 文件：

a. 添加 **[printers]** 部分，以启用 Samba 中的打印后端：

```
[printers]
        comment = All Printers
        path = /var/tmp/
        printable = yes
        create mask = 0600
```

重要

[printers] 共享名称是写死的，不能更改。

b. 如果 CUPS 服务器运行在不同的主机或端口上，请在 **[printers]** 部分中指定设置：

```
cups server = printserver.example.com:631
```

c. 如果您有许多打印机，请将空闲秒数设置为比连接到 CUPS 的打印机数高的值。例如，如果您有 100 台打印机，请在 **[global]** 部分中设置：

```
rpcd_spoolss:idle_seconds = 200
```

如果这个设置在您的环境中没有缩放，请在 **[global]** 部分中增加 **rpcd_spools** worker 的数量：

```
rpcd_spoolss:num_workers = 10
```

默认情况下，**rpcd_spools** 启动 5 个 worker。

2. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

3. 打开所需的端口，并使用**firewall-cmd**工具重新加载防火墙配置：

```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

4. 重启**smb**服务：

```
# systemctl restart smb
```

重启服务后，Samba 会自动共享在 CUPS 后端中配置的所有打印机。如果想要仅手动共享特定打印机，请参阅 手动共享特定的打印机。

验证

- 提交打印作业。例如，要打印 PDF 文件，请输入：

```
# smbclient -Uuser //sambaserver.example.com/printer_name -c "print example.pdf"
```

1.15.2. 手动共享特定的打印机

如果您将 Samba 配置为打印服务器，默认情况下，Samba 会共享在 CUPS 后端中配置的所有打印机。以下流程解释了如何只共享特定的打印机。

先决条件

- Samba 被设置为打印服务器

流程

1. 编辑 **/etc/samba/smb.conf** 文件：

   a. 在 **[global]** 部分中，通过以下设置禁用自动打印机共享：

   ```
   load printers = no
   ```

   b. 为您要共享的每个打印机添加一段。例如，要在 Samba 中将 CUPS 后端中名为 **example** 的打印机共享为 **Example-Printer**，请添加以下部分：

   ```
   [Example-Printer]
        path = /var/tmp/
        printable = yes
        printer name = example
   ```

   您不需要为每个打印机单独设置 spool 目录。您可以在打印机的**path** 参数中设置与您在 **[printers]** 部分中设置的完全相同的 spool 目录。

2. 验证**/etc/samba/smb.conf**文件：

   ```
   # testparm
   ```

3. 重新载入 Samba 配置：

   ```
   # smbcontrol all reload-config
   ```

1.16. 在 SAMBA 打印服务器中为 WINDOWS 客户端设置自动打印机驱动程序下载

如果您在为 Windows 客户端运行 Samba 打印服务器，你可以上传驱动程序并预配置打印机。如果用户连接到打印机,Windows 会自动在客户端本地下载并安装驱动程序。用户不需要本地管理员权限进行安装。另外，Windows 应用预配置的驱动程序设置，如纸匣的数量。

本节的部分内容摘自 Samba Wiki 上发布的为 Windows 客户端设置自动打印机驱动程序下载文档。许可证： CC BY 4.0。作者和贡献者：请参阅 Wiki 页面上的历史选项卡。

先决条件

- Samba 被设置为打印服务器

1.16.1. 有关打印机驱动程序的基本信息

本节提供有关打印机驱动程序的一般信息。

支持的驱动程序模型版本

Samba 只支持 Windows 2000 及更高版本支持的，以及 Windows Server 2000 及更高版本支持的打印机驱动程序模型版本 3。Samba 不支持 Windows 8 和 Windows Server 2012 中引入的驱动程序模型版本 4。但是，这些及之后的 Windows 版本也支持版本 3 驱动程序。

包感知驱动程序
Samba 不支持包感知驱动程序。

准备上传的打印机驱动程序
在您将驱动程序上传到 Samba 打印服务器之前：

- 如果驱动程序采用压缩格式提供，请解包它。
- 有些驱动程序需要启动一个设置应用程序，以便在 Windows 主机上本地安装驱动程序。在某些情况下，安装程序会在设置运行期间将单个文件提取到操作系统的临时文件夹中。使用驱动程序文件上传：
  a. 启动安装程序。
  b. 将临时文件夹中的文件复制到新位置。
  c. 取消安装。

请您的打印机厂商提供支持上传到打印服务器的驱动程序。

为客户端提供 32 位和 64 位驱动
要为 32 位和 64 位 Windows 客户端提供打印机的驱动程序，您必须上传两个架构具有完全相同名称的驱动程序。例如，如果您上传名为**Example PostScript**的 32 位驱动程序和名为**Example PostScript (v1.0)**的 64 位驱动程序，则名称不匹配。因此，您只能为打印机分配其中一个驱动程序，且该驱动程序无法对这两个架构都适用。

1.16.2. 启用用户上传和预配置驱动程序

要上传和预配置打印机驱动程序，用户或组需要被赋予 **SePrintOperatorPrivilege** 特权。用户必须被添加到 **printadmin** 组中。在安装 **samba** 软件包时，Red Hat Enterprise Linux 会自动创建这个组。**printadmin** 组被分配了低于 1000 的最小可用动态系统 GID。

流程

1. 例如，要对 **printadmin** 组赋予 **SePrintOperatorPrivilege** 特权：

```
# net rpc rights grant "printadmin" SePrintOperatorPrivilege -U
"DOMAIN\administrator"
Enter DOMAIN\administrator's password:
Successfully granted rights.
```

注意

在域环境中，将 **SePrintOperatorPrivilege** 赋予域组。这可让您通过更新用户的组成员资格来集中管理特权。

2. 列出所有被赋予了 **SePrintOperatorPrivilege** 的用户和组：

```
# net rpc rights list privileges SePrintOperatorPrivilege -U "DOMAIN\administrator"
Enter administrator's password:
SePrintOperatorPrivilege:
```

```
BUILTIN\Administrators
DOMAIN\printadmin
```

1.16.3. 设置 print$ 共享

Windows 操作系统从打印服务器上名为 **print$** 的共享中下载打印机驱动程序。这个共享名称在 Windows 中硬编码，无法更改。

以下流程解释了如何将 **/var/lib/samba/drivers/** 目录共享为**print$**，并使本地 **printadmin** 组成员能够上传打印机驱动程序。

流程

1. 在 **/etc/samba/smb.conf** 文件中添加 **[print$]** 部分：

```
[print$]
        path = /var/lib/samba/drivers/
        read only = no
        write list = @printadmin
        force group = @printadmin
        create mask = 0664
        directory mask = 2775
```

   使用这些设置：

   - 只有 **printadmin** 组成员才能将打印机驱动程序上传到共享。
   - 新创建的文件和目录的组将被设为 **printadmin**。
   - 新文件的权限将被设置为 **664**。
   - 新目录的权限将被设置为 **2775**。

2. 要只为所有打印机上传 64 位驱动程序，请在 **/etc/samba/smb.conf** 文件的 **[global]** 部分包含此设置：

```
spoolss: architecture = Windows x64
```

   如果没有这个设置，Windows 只显示您上传的至少 32 位版本的驱动程序。

3. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

4. 重新载入 Samba 配置

```
# smbcontrol all reload-config
```

5. 如果 **printadmin** 组不存在，就创建它：

```
# groupadd printadmin
```

6. 将 **SePrintOperatorPrivilege** 特权赋予 **printadmin** 组。

```
# net rpc rights grant "printadmin" SePrintOperatorPrivilege -U
"DOMAIN\administrator"
Enter DOMAIN\administrator's password:
Successfully granted rights.
```

7. 如果您在**enforcing**模式下运行 SELinux，请在目录中设置**samba_share_t**上下文：

```
# semanage fcontext -a -t samba_share_t "/var/lib/samba/drivers(/.*)?"

# restorecon -Rv /var/lib/samba/drivers/
```

8. 对 **/var/lib/samba/drivers/** 目录设置权限：

   - 如果使用 POSIX ACL，请设置：

```
# chgrp -R "printadmin" /var/lib/samba/drivers/
# chmod -R 2775 /var/lib/samba/drivers/
```

   - 如果使用 Windows ACL，请设置：

主体	权限	适用于
创建者所有者	全控制	只适用于子文件夹和文件
通过身份验证的用户	读和执行、列出目录内容、读	这个文件夹、子文件夹和文件
printadmin	全控制	这个文件夹、子文件夹和文件

有关在 Windows 上设置 ACL 的详情，请查看 Windows 文档。

其它资源

- 使用户能够上传和预配置驱动程序。

1.16.4. 创建 GPO 以启用客户端信任 Samba 打印服务器

出于安全考虑，最近的 Windows 操作系统会阻止客户端从不受信任的服务器下载非包感知的打印机驱动程序。如果您的打印服务器是 AD 中的成员，您可以在域中创建一个组策略对象(GPO)来信任 Samba 服务器。

先决条件

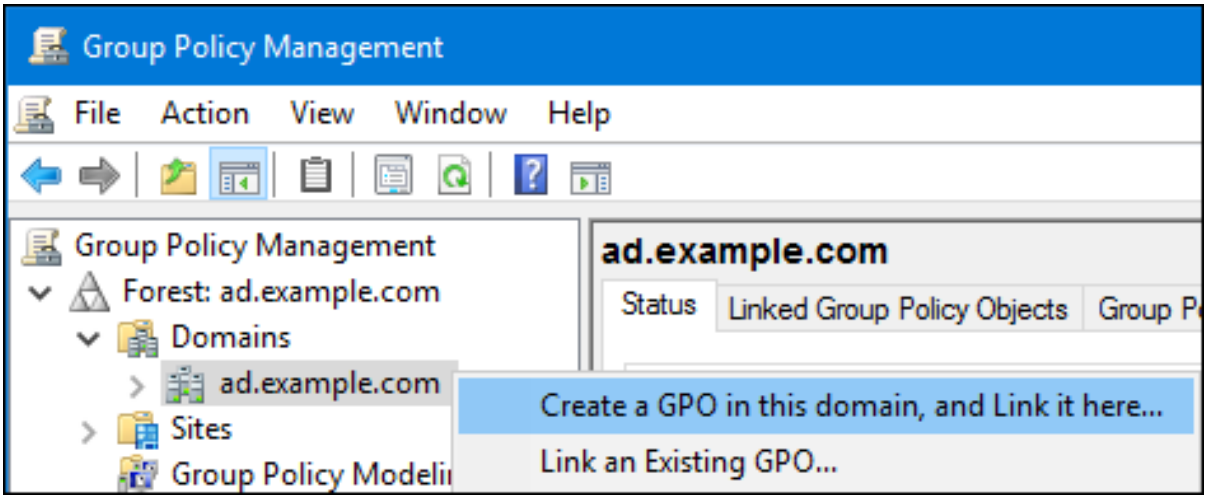
- Samba 打印服务器是 AD 域的成员。
- 您用来创建 GPO 的 Windows 计算机必须安装有 Windows 远程服务器管理工具(RSAT)。详情请查看 Windows 文档。

流程

1. 使用允许编辑组策略的帐户（如 AD 域 **Administrator** 用户）登录到 Windows 计算机。

2. 打开 组**策略管理控制台**。

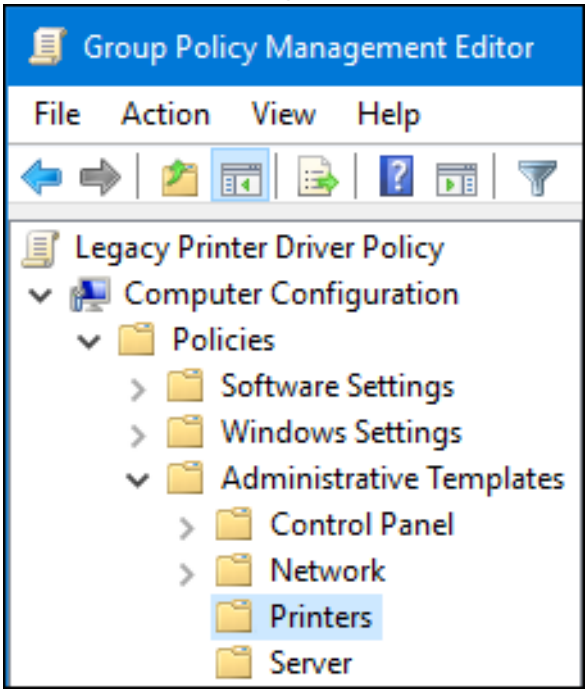
3. 右键单击 AD 域并选择 **创建此域中的 GPO，并链接到此处**。



4. 为 GPO 输入一个名称，如 **Legacy Printer Driver Policy**， 并点击 **OK**。新的 GPO 将在域条目下显示。

5. 右键单击新创建的 GPO，然后选择 **编辑** 以打开 组**策略管理编辑器**。

6. 进入 **Computer Configuration** → **Policies** → **Administrative Templates** → **Printers**。

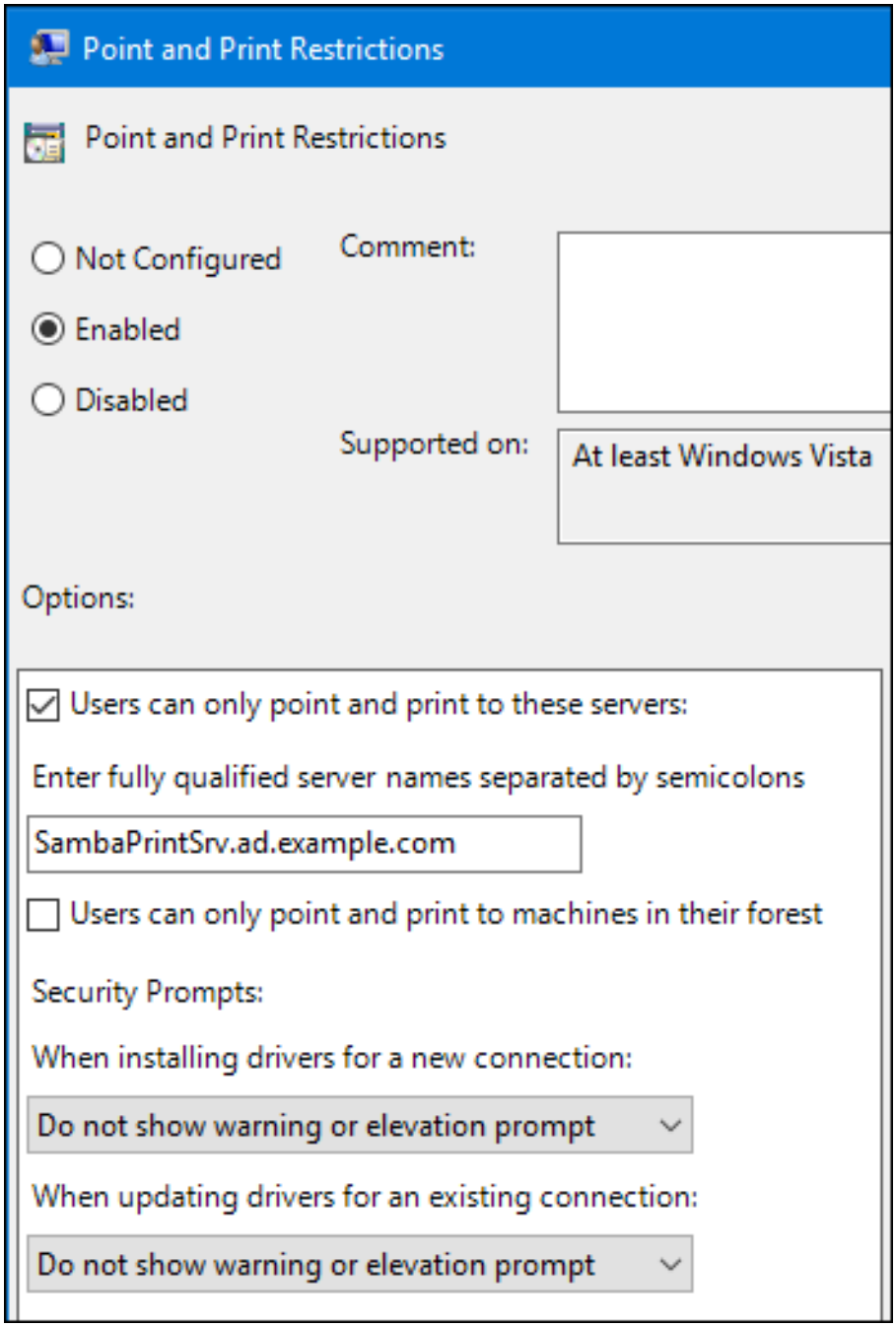


7. 在窗口的右侧，双击 **指向和打印限制** 来编辑策略：

   a. 启用策略并设置以下选项：

      i. 选择 **用户只能指向并打印到这些服务器**，再将 Samba 打印服务器的完全限定域名 (FQDN)输入到此选项旁边的字段。

      ii. 在 **安全提示** 下的两个复选框中，选择 **不显示警告 或 高程提示**。

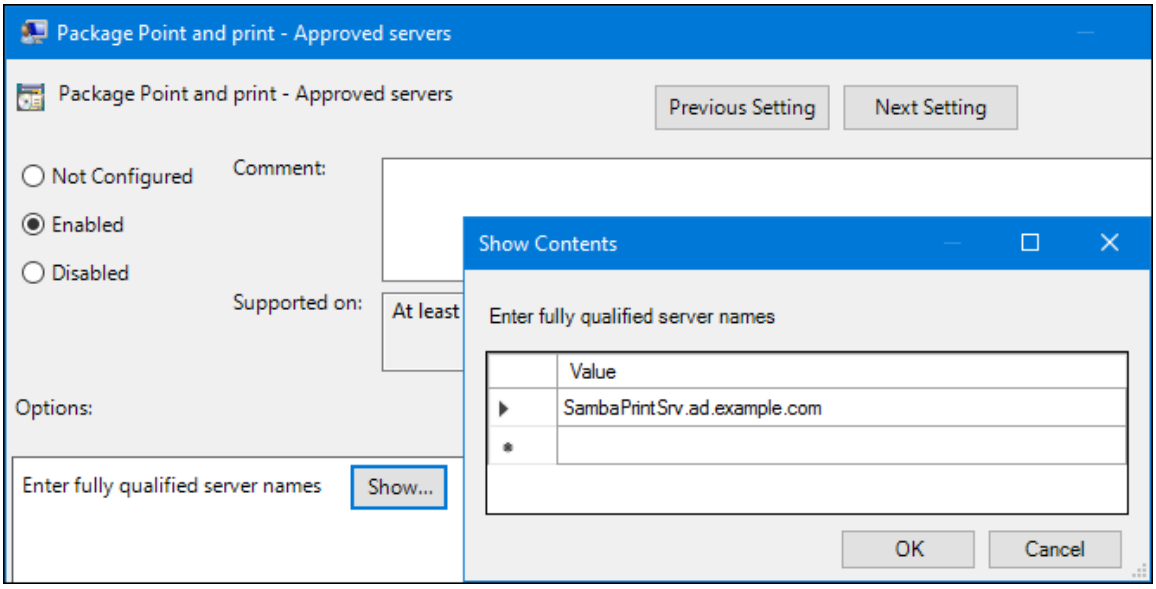


b. 点击确定。

8. 双击 **包指向和打印 - 已批准的服务器** 来编辑策略：

a. 启用策略并单击 **显示** 按钮。

b. 输入 Samba 打印服务器的 FQDN。



c. 单击 **OK**，关闭 **显示内容** 和策略的属性窗口。

9. 关闭 **组策略管理编辑器**。

10. 关闭 **组策略管理控制台**。

在 Windows 域成员应用了组策略后，用户连接到打印机时会自动从 Samba 服务器下载打印机驱动程序。

其它资源

- 有关使用组策略，请参阅 Windows 文档。

1.16.5. 上传驱动程序和预配置打印机

在 Windows 客户端使用 **打印管理** 应用程序上传托管在 Samba 打印服务器上的驱动程序和预配置打印机。详情请查看 Windows 文档。

1.17. 在启用了 FIPS 模式的服务器上运行 SAMBA

本节概述了在启用了 FIPS 模式的情况下运行 Samba 的限制。还提供了在运行 Samba 的 Red Hat Enterprise Linux 主机上启用 FIPS 模式的流程。

1.17.1. 在 FIPS 模式中使用 Samba 的限制

在指定条件下，以下 Samba 模式和功能在 FIPS 模式下工作：

- Samba 仅在 Active Directory(AD)或使用AES密码进行Kerberos身份验证的红帽身份管理(IdM)环境中作为域成员。
- Samba 作为 Active Directory 域成员上的文件服务器。但是，这需要客户端使用 Kerberos 向服务器进行身份验证。

由于 FIPS 的安全性增强，如果启用了 FIPS 模式，以下 Samba 特性和模式将无法正常工作：

- NT LAN Manager(NTLM)验证，因为 RC4 密码已被阻止
- 服务器消息块版本 1(SMB1)协议

- 独立文件服务器模式，因为它使用了 NTLM 身份验证
- NT4 风格的域控制器
- NT4 风格的域成员.请注意,红帽继续支持后台使用的主域控制器（PDC）功能 IdM。
- 针对Samba 服务器的密码修改.您只能对 Active Directory 域控制器使用 Kerberos 进行密码修改。

以下特性没有在 FIPS 模式下测试，因此红帽不支持：

- 将 Samba 作为打印服务器来运行

1.17.2. 在 FIPS 模式下使用 Samba

您可以在运行 Samba 的 RHEL 主机上启用 FIPS 模式。

先决条件

- 在 Red Hat Enterprise Linux 主机上配置了Samba 。
- Samba 以 FIPS 模式支持的模式运行。

流程

1. 在 RHEL 中启用 FIPS 模式：

```
# fips-mode-setup --enable
```

2. 重启服务器：

```
# reboot
```

3. 使用 **testparm** 工具来验证配置：

```
# testparm -s
```

如果命令显示任何错误或不兼容，请修复它们以确保 Samba 正常工作。

其它资源

- 第 1.17.1 节 “在 FIPS 模式中使用 Samba 的限制”

1.18. 调整 SAMBA 服务器的性能

了解在某些情况下，哪些设置可以提高 Samba 的性能，以及哪些设置可能会对性能有负面影响。

本节的部分内容来自在 Samba Wiki 中发布的 Performance Tuning 文档。许可证： CC BY 4.0。作者和贡献者：请参阅 Wiki 页面上的历史选项卡。

先决条件

- Samba 被设置为文件或打印服务器

1.18.1. 设置 SMB 协议版本

每个新的 SMB 版本都添加了特性并提高了协议的性能。最新的 Windows 和 Windows 服务器操作系统始终支持最新的协议版本。如果 Samba 也使用最新的协议版本，那么连接到 Samba 的 Windows 客户端将从性能改进中受益。在 Samba 中，server max protocol的默认值被设置为最新支持的稳定的 SMB 协议版本。

注意

要始终拥有最新的稳定的 SMB 协议版本，请不要设置 **server max protocol** 参数。如果手动设置参数，则需要修改 SMB 协议的每个新版本的设置，以便启用最新的协议版本。

以下流程解释了如何对 **server max protocol** 参数使用默认值。

步骤

1. 从 **/etc/samba/smb.conf** 文件的 **[global]** 部分中删除 **server max protocol** 参数。
2. 重新载入 Samba 配置

```
# smbcontrol all reload-config
```

1.18.2. 与包含大量文件的目录调整共享

Linux 支持区分大小写的文件名。因此，在搜索或访问文件时，Samba需要针对大小写文件名来扫描目录。您可以将共享配置为只以小写或大写来创建新文件，这可以提高性能。

先决条件

- Samba 配置为文件服务器

步骤

1. 将共享上的所有文件重命名为小写。

注意

使用这个过程中的设置，名称不为小写的文件将不再显示。

2. 在共享部分中设置以下参数：

```
case sensitive = true
default case = lower
preserve case = no
short preserve case = no
```

有关参数的详情，请查看 **smb.conf(5)** 手册页 中的描述。

3. 验证**/etc/samba/smb.conf**文件：

```
# testparm
```

4. 重新载入 Samba 配置：

```
# smbcontrol all reload-config
```

应用了这些设置后，此共享上所有新创建的文件的名称都使用小写。由于这些设置，Samba 不再需要针对大小写来扫描目录，这样可以提高性能。

1.18.3. 可能会对性能造成负面影响的设置

默认情况下，Red Hat Enterprise Linux 中的内核会根据高网络性能进行了微调。例如，内核对缓冲区大小使用自动轮询机制。在 **/etc/samba/smb.conf** 文件中设置 **socket options** 参数会覆盖这些内核设置。因此，设置此参数会在大多数情况下降低 Samba 网络性能。

要使用内核的优化的设置，请从 **/etc/samba/smb.conf** 中的 **[global]** 部分删除 **socket options** 参数。

1.19. 将 SAMBA 配置为与需要 SMB 版本低于默认版本的客户端兼容

Samba 对它支持的最小服务器消息块(SMB)版本使用合理的安全默认值。但是，如果您的客户端需要较旧的 SMB 版本，您可以配置 Samba 来支持它。

1.19.1. 设置 Samba 服务器支持的最小 SMB 协议版本

在 Samba 中，**/etc/samba/smb.conf** 文件中的 **server min protocol** 参数定义了 Samba 服务器支持的最小服务器消息块(SMB)协议版本。您可以更改最小 SMB 协议版本。

注意

默认情况下，RHEL 8.2 及之后版本上的 Samba 只支持 SMB2 和更新的协议版本。红帽建议不要使用已弃用的 SMB1 协议。但是，如果您的环境需要 SMB1，您可以手动将 **server min protocol** 参数设置为 **NT1** 来重新启用 SMB1。

先决条件

- 已安装并配置 Samba。

流程

1. 编辑 **/etc/samba/smb.conf** 文件，添加 **server min protocol** 参数，并将参数设置为服务器应支持的最小 SMB 协议版本。例如，要将 SMB 协议的最小版本设置为 **SMB3**，请添加：

```
server min protocol = SMB3
```

2. 重启**smb**服务：

```
# systemctl restart smb
```

其它资源

- **smb.conf(5)** 手册页

1.20. 经常使用 SAMBA 命令行工具

本章论述了使用 Samba 服务器时经常使用的命令。

1.20.1. 使用 net ads join 和 net rpc join 命令

使用 **net** 工具的 **join** 子命令，您可以将 Samba 加入到 AD 或 NT4 域。要加入域，您必须手动创建 **/etc/samba/smb.conf** 文件，并有选择地更新其他配置，如 PAM。

重要

红帽建议使用 **realm** 工具来加入域。**realm** 工具自动更新所有涉及的配置文件。

流程

1. 使用以下设置手动创建 **/etc/samba/smb.conf** 文件：
   - 对于 AD 域成员：

     ```
     [global]
     workgroup = domain_name
     security = ads
     passdb backend = tdbsam
     realm = AD_REALM
     ```

   - 对于 NT4 域成员：

     ```
     [global]
     workgroup = domain_name
     security = user
     passdb backend = tdbsam
     ```

2. 为 * 默认域和要加入到 **/etc/samba/smb.conf** 文件中 **[global]** 部分的域添加 ID 映射配置。
3. 验证**/etc/samba/smb.conf**文件：

   ```
   # testparm
   ```

4. 以域管理员身份加入域：
   - 加入 AD 域：

     ```
     # net ads join -U "DOMAIN\administrator"
     ```

   - 要加入 NT4 域：

     ```
     # net rpc join -U "DOMAIN\administrator"
     ```

5. 将 **winbind** 源追加到 **/etc/nsswitch.conf** 文件中的 **passwd** 和 **group** 数据库条目中：

   ```
   passwd:     files winbind
   group:      files winbind
   ```

6. 启用并启动 **winbind** 服务：

   ```
   # systemctl enable --now winbind
   ```

7. （可选）使用 **authselect** 工具来配置 PAM。
   详情请查看 **authselect(8)** 手册页。

8. 另外，对于 AD 环境，配置 Kerberos 客户端。
   详情请查看您的 Kerberos 客户端文档。

其它资源

- 将 Samba 加入到域。
- 了解并配置 Samba ID 映射。

1.20.2. 使用 net rpc right 命令

在 Windows 中，您可以为帐户和组分配特权来执行特殊操作，如对共享设置 ACL 或上传打印机驱动程序。在 Samba 服务器上，您可以使用 **net rpc permissions** 命令来管理特权。

列出您可以设置的权限
若要列出所有可用的特权及其所有者，可使用 **net rpc permissions list** 命令。例如：

```
# net rpc rights list -U "DOMAIN\administrator"
Enter DOMAIN\administrator's password:
    SeMachineAccountPrivilege  Add machines to domain
     SeTakeOwnershipPrivilege  Take ownership of files or other objects
           SeBackupPrivilege  Back up files and directories
          SeRestorePrivilege  Restore files and directories
    SeRemoteShutdownPrivilege  Force shutdown from a remote system
     SePrintOperatorPrivilege  Manage printers
         SeAddUsersPrivilege  Add users and groups to the domain
      SeDiskOperatorPrivilege  Manage disk shares
         SeSecurityPrivilege  System security
```

授予权限
若要为帐户或组赋予特权，可使用 **net rpc rights grant** 命令。

例如，将**SePrintOperatorPrivilege** 特权赋予 ***DOMAIN*\printadmin** 组 ：

```
# net rpc rights grant "DOMAIN\printadmin" SePrintOperatorPrivilege -U
"DOMAIN\administrator"
Enter DOMAIN\administrator's password:
Successfully granted rights.
```

撤销权限
若要从帐户或组撤销特权，可使用 **net rpc rights revoke** 命令。

例如，要对***DOMAIN*\printadmin** 组撤销 **SePrintOperatorPrivilege** 特权：

```
# net rpc rights remoke "DOMAIN\printadmin" SePrintOperatorPrivilege -U
"DOMAIN\administrator"
Enter DOMAIN\administrator's password:
Successfully revoked rights.
```

1.20.3. 使用 net rpc share 命令

net rpc share 命令提供了在本地或远程 Samba 或 Windows 服务器上列出、添加和删除共享的功能。

列出共享
若要列出 SMB 服务器上的共享，请使用 **net rpc share list** 命令。（可选）将 **-S** ***server_name*** 参数传给命令，以列出远程服务器的共享。例如：

```
# net rpc share list -U "DOMAIN\administrator" -S server_name
Enter DOMAIN\administrator's password:
IPC$
share_1
share_2
...
```

注意

在 **/etc/samba/smb.conf** 文件中设置了 **browseable = no** 的、托管在 Samba 服务器上的共享不会显示在输出中。

添加共享
net rpc share add 命令允许您向 SMB 服务器添加共享。

例如，要在共享 **C:\example** 目录的远程 Windows 服务器中添加一个名为 **example** 的共享：

```
# net rpc share add example="C:\example" -U "DOMAIN\administrator" -S server_name
```

注意

在指定 Windows 目录名称时，您必须省略路径中的结尾反斜杠。

使用命令在 Samba 服务器中添加共享：

- 在 **-U** 参数中指定的用户必须拥有在目标服务器上赋予了 **SeDiskOperatorPrivilege** 的特权。
- 您必须编写一个脚本，其在 **/etc/samba/smb.conf** 文件中添加共享部分，并重新加载 Samba 。该脚本必须在 **/etc/samba/smb.conf** 的 **[global]** 部分中的 **add share command** 参数中设置。详情请查看 **smb.conf(5)** 手册页中的 **add share command** 描述。

删除共享
net rpc share delete 命令允许您从 SMB 服务器中删除共享。

例如，要从远程 Windows 服务器中删除名为 example 的共享：

```
# net rpc share delete example -U "DOMAIN\administrator" -S server_name
```

使用命令从 Samba 服务器中删除共享：

- 在 **-U** 参数中指定的用户必须被赋予了 **SeDiskOperatorPrivilege** 特权。
- 您必须编写一个脚本，其从 **/etc/samba/smb.conf** 文件中删除共享的部分，并重新加载 Samba 。该脚本必须在 **/etc/samba/smb.conf** 的 **[global]** 部分中的 **delete share command** 参数中设置。详情请查看 **smb.conf(5)** 手册页中的 **delete share command** 描述。

1.20.4. 使用 net user 命令

net user 命令允许您在 AD DC 或 NT4 PDC 中执行以下操作：

- 列出所有用户帐户
- 添加用户
- 删除用户

注意

只有在列出域用户帐户时，才需要指定连接方法，如 AD 域的**ads** 或 NT4 域的 **rpc** 。其他用户相关的子命令可以自动探测连接方法。

将 **-U** ***user_name*** 参数传给命令，以指定允许执行所请求的操作的用户。

列出域用户帐户
列出 AD 域中的所有用户：

```
# net ads user -U "DOMAIN\administrator"
```

列出 NT4 域中的所有用户：

```
# net rpc user -U "DOMAIN\administrator"
```

在域中添加用户帐户
在 Samba 域成员中，您可以使用 **net user add** 命令将用户帐户添加到域。

例如，将 **user** 账户添加到域：

1. 添加帐户：

```
# net user add user password -U "DOMAIN\administrator"
User user added
```

2. （可选）使用远程过程调用(RPC)shell 来启用 AD DC 或 NT4 PDC 中的帐户。例如：

```
# net rpc shell -U DOMAIN\administrator -S DC_or_PDC_name
Talking to domain DOMAIN (S-1-5-21-1424831554-512457234-5642315751)

net rpc> user edit disabled user: no
Set user's disabled flag from [yes] to [no]

net rpc> exit
```

从域中删除用户帐户
对于 Samba 域成员，您可以使用 **net user delete** 命令从域中删除用户帐户。

例如，从域中删除 **user** 账户：

```
# net user delete user -U "DOMAIN\administrator"
User user deleted
```

1.20.5. 使用 rpcclient 工具

The **rpcclient** 工具可让您在本地或远程 SMB 服务器上手动执行客户端 Microsoft 远程过程调用(MS-RPC)功能。但是，大部分特性都已集成到 Samba 提供的单独工具中。使用 **rpcclient** 只用于测试 MS-PRC 功能。

先决条件

- **samba-client** 软件包已安装。

例子
例如，您可以使用 **rpcclient** 工具来：

- 管理打印机假脱机子系统(SPOOLSS)。

  例 1.7. 将驱动程序分配给打印机

  ```
  # rpcclient server_name -U "DOMAIN\administrator" -c 'setdriver "printer_name" "driver_name"'
  Enter DOMAIN\administrators password:
  Successfully set printer_name to driver driver_name.
  ```

- 检索有关 SMB 服务器的信息。

  例 1.8. 列出所有文件共享和共享的打印机

  ```
  # rpcclient server_name -U "DOMAIN\administrator" -c 'netshareenum'
  Enter DOMAIN\administrators password:
  netname: Example_Share
   remark:
   path:   C:\srv\samba\example_share\
   password:
  netname: Example_Printer
   remark:
   path:   C:\var\spool\samba\
   password:
  ```

- 使用安全帐户管理器远程(SAMR)协议来执行操作。

  例 1.9. 在 SMB 服务器中列出用户

  ```
  # rpcclient server_name -U "DOMAIN\administrator" -c 'enumdomusers'
  Enter DOMAIN\administrators password:
  user:[user1] rid:[0x3e8]
  user:[user2] rid:[0x3e9]
  ```

  如果您针对独立服务器或域成员运行命令，它将列出本地数据库中的用户。针对 AD DC 或 NT4 PDC 运行命令列出域用户。

其它资源

- **rpcclient(1)** 手册页

1.20.6. 使用 samba-regedit 应用程序

某些设置（如打印机配置）存储在 Samba 服务器上的注册表中。您可以使用基于 ncurses 的 **samba-regedit** 应用程序来编辑 Samba 服务器的注册表。

```
Path: ...AL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Print/Printers/
 Key                  Value
 Name                 Name              | Type       | Data
 +Example-Printer     Attributes        | REG_DWORD  | 0x00001848 (6216)
                      ChangeID          | REG_DWORD  | 0x00160374 (1442676)
                      Datatype          | REG_SZ     | RAW
                      Default Priority  | REG_DWORD  | 0x00000001 (1)
                      Description       | REG_SZ     |
                      Location          | REG_SZ     |
                      Name              | REG_SZ     | Example-Printer
                      Parameters        | REG_SZ     |
                      Port              | REG_SZ     | Samba Printer Port
                      Print Processor   | REG_SZ     | winprint
                      Printer Driver    | REG_SZ     | Example Printer Driver
                      Priority          | REG_DWORD  | 0x00000001 (1)
                      Security          | REG_BINARY | (248 bytes)
                      Separator File    | REG_SZ     |
                      Share Name        | REG_SZ     | Example-Printer
                      StartTime         | REG_DWORD  | 0x00000000 (0)
                      Status            | REG_DWORD  | 0x00000000 (0)
                      UntilTime         | REG_DWORD  | 0x00000000 (0)
[n] New Value [d] Del Value [ENTER] Edit [b] Edit binary                VALUES
[TAB] Switch sections [q] Quit [UP] List up [DOWN] List down [/] Search [x] Next
```

先决条件

- **samba-client** 软件包已安装。

流程

要启动应用程序，请输入：

```
# samba-regedit
```

使用以下键：

- 上键和下键：在注册表树和值中进行导航。
- **Enter**：打开关键字或编辑值。
- 选项卡 ：在 **Key** 和 **Value** 窗格间切换。
- **Ctrl+C**：关闭应用程序。

1.20.7. 使用 smbcontrol 工具

smbcontrol 工具允许您向 **smbd**、**nmbd**、**winbindd 或** 所有这些服务发送命令消息。这些控制消息指示服务重新载入其配置。

先决条件

- **samba-common-tools** 软件包已安装。

流程

- 通过将 **reload-config** 消息类型发送给 **所有** 目的地，来重新载入 **smbd**、**nmbd**、**winbindd** 服务的配置：

```
# smbcontrol all reload-config
```

其它资源

- **smbcontrol(1)** 手册页

1.20.8. 使用 smbpasswd 工具

smbpasswd 工具管理本地 Samba 数据库中的用户帐户和密码。

先决条件

- **samba-common-tools** 软件包已安装。

流程

1. 如果您以用户身份运行命令，**smbpasswd** 将修改运行命令的用户的 Samba 密码。例如：

```
[user@server ~]$ smbpasswd
New SMB password: password
Retype new SMB password: password
```

2. 如果以 **root** 用户身份运行 **smbpasswd**，例如，您可以使用该工具来：

   - 创建一个新用户：

```
[root@server ~]# smbpasswd -a user_name
New SMB password: password
Retype new SMB password: password
Added user user_name.
```

> **注意**
>
> 在将用户添加到 Samba 数据库之前，您必须先在本地操作系统中创建帐户。请参阅配置基本系统设置指南中的 从命令行添加新用户 部分。

   - 启用 Samba 用户：

```
[root@server ~]# smbpasswd -e user_name
Enabled user user_name.
```

   - 禁用 Samba 用户：

```
[root@server ~]# smbpasswd -x user_name
Disabled user user_name
```

   - 删除用户：

```
[root@server ~]# smbpasswd -x user_name
Deleted user user_name.
```

其它资源

- **smbpasswd(8)** 手册页

1.20.9. 使用 smbstatus 工具

smbstatus 工具报告，关于：

- 每个 **smbd** 守护进程的每个 PID 到 Samba 服务器的连接。此报告包括用户名、主组群、SMB 协议版本、加密和签名信息。
- 每个 Samba 共享的连接。此报告包括 **smbd** 守护进程的 PID、连接机器的 IP、连接建立的时间戳、加密和签名信息。
- 锁定文件列表。报告条目包括更多详情，如 Opportunistic lock(oplock)类型

先决条件

- **samba** 软件包已安装。
- **smbd** 服务在运行。

流程

```
# smbstatus

Samba version 4.15.2
PID  Username              Group               Machine                          Protocol Version  Encryption
Signing
----------------------------------------------------------------------------------------------------------------
-
963  DOMAIN\administrator  DOMAIN\domain users  client-pc  (ipv4:192.0.2.1:57786)  SMB3_02
-          AES-128-CMAC

Service  pid  Machine    Connected at                Encryption  Signing:
----------------------------------------------------------------------------
example  969  192.0.2.1  Thu Nov  1 10:00:00 2018 CEST  -          AES-128-CMAC

Locked files:
Pid  Uid    DenyMode   Access    R/W     Oplock      SharePath          Name      Time
--------------------------------------------------------------------------------------------------------
969  10000  DENY_WRITE 0x120089  RDONLY  LEASE(RWH)  /srv/samba/example  file.txt  Thu
Nov  1 10:00:00 2018
```

其它资源

- **smbstatus(1)** 手册页

1.20.10. 使用 smbtar 工具

smbtar 工具备份 SMB 共享的内容或其子目录，并将内容存储在 **tar** 存档中。或者，您可以将内容写入磁带设备。

先决条件

- **samba-client** 软件包已安装。

流程

- 使用以下命令备份 **//server/example/** 共享中 **demo** 目录的内容，并将内容存储在 **/root/example.tar** 归档中：

```
# smbtar -s server -x example -u user_name -p password -t /root/example.tar
```

其它资源

- **smbtar(1)** 手册页

1.20.11. 使用 wbinfo 工具

wbinfo 工具查询并返回 **winbindd** 服务创建和使用的信息。

先决条件

- **samba-winbind-clients** 软件包已安装。

流程

例如，您可以使用 **wbinfo** 来：

- 列出域用户：

```
# wbinfo -u
AD\administrator
AD\guest
...
```

- 列出域组：

```
# wbinfo -g
AD\domain computers
AD\domain admins
AD\domain users
...
```

- 显示用户的 SID：

```
# wbinfo --name-to-sid="AD\administrator"
S-1-5-21-1762709870-351891212-3141221786-500 SID_USER (1)
```

- 显示域和信任的信息：

```
# wbinfo --trusted-domains --verbose
Domain Name   DNS Domain          Trust Type  Transitive  In   Out
```

```
BUILTIN                    None       Yes        Yes  Yes
server                     None       Yes        Yes  Yes
DOMAIN1     domain1.example.com   None       Yes        Yes  Yes
DOMAIN2     domain2.example.com   External   No         Yes  Yes
```

其它资源

- **wbinfo(1)** 手册页

1.21. 其它资源

- **smb.conf(5)** 手册页
- **/usr/share/docs/samba-version/** 目录包含 Samba 项目提供的通用文档，脚本示例和 LDAP 架构文件
- 设置 Samba 和 Clustered Trivial Database (CDTB)以共享存储在 GlusterFS 卷上的目录
- 在 Red Hat Enterprise Linux 中挂载 SMB 共享

第 2 章 部署 NFS 服务器

通过使用网络文件系统(NFS)协议，远程用户可以通过网络挂载共享目录，并像它们是本地挂载的那样使用它们。这可让您将资源整合到网络的集中服务器中。

2.1. 次 NFSV4 版本的主要功能

每个次 NFSv4 版本均带来了旨在提高性能和安全的增强。使用这些改进来充分利用 NFSv4 的潜力，确保网络之间高效且可靠的文件共享。

NFSv4.2 的主要功能

服务器端复制

服务器端复制是 NFS 服务器在服务器上复制文件，而无需通过网络来回传输数据的一种能力。

稀疏文件

使文件有一个或多个空白或间隙，它们是仅由零组成的未分配或未初始化的数据块。这使应用程序可以在稀疏文件中映射出孔的位置。

保留空间

在写数据前，客户端可以在存储服务器上保留或分配空间。这防止服务器耗尽空间。

标记的 NFS

强制实施数据访问权限，并为 NFS 文件系统上的各个文件在客户端和服务器之间启用 SELinux 标签。

布局增强

提供了使并行 NFS (pNFS)服务器收集更好的性能统计信息的功能。

NFSv4.1 的主要功能

对 pNFS 的客户端支持

对集群服务器高速 I/O 的支持，可让您在多台机器上存储数据，来提供对数据的直接访问，以及对元数据的同步更新。

会话

会话维护相对于属于客户端连接的服务器的状态。这些会话通过减少与为每个远程过程调用(RPC)操作建立和终止连接关联的开销，提供了改进的性能和效率。

NFSv4.0 的主要功能

RPC 和安全性

RPCSEC_GSS 框架增强了 RPC 安全性。NFSv4 协议为带内安全协商引入了一个新操作。这可让客户端查询服务器策略，来安全地访问文件系统资源。

流程和操作结构

NFS 4.0 引入了 **COMPOUND** 流程，它允许客户端将多个操作合并为一个请求，来减少 RPC。

文件系统模型

NFS 4.0 保留分层的文件系统模型，将文件视为字节流，并使用 UTF-8 对名称进行编码以实现国际化。

- **文件处理类型**
  使用易失性文件句柄，服务器可以根据需要对文件系统更改进行调整，并使客户端能够适应，而无需永久的文件句柄。

- **属性类型**

文件属性结构包括 required, recommended, 和 named 属性，各自有不同的目的。从 NFSv3 派生的 required 属性对于区分文件类型至关重要，而 recommended 属性（如 ACL）提供增强的访问控制。

- **多服务器命名空间**
  命名空间跨多个服务器，根据属性、支持引用、冗余和无缝服务器迁移简化文件系统传输。

OPEN 和 CLOSE 操作

这些操作可在一个点上组合文件查找、创建和语义共享，并使文件访问管理更高效。

文件锁定

文件锁定是协议的一部分，消除了对 RPC 回调的需求。文件锁定状态由服务器在基于租期的模式下管理的，其中无法续订租期可能导致服务器释放状态。

客户端缓存和委托

缓存与之前的版本类似，具有客户端决定属性和目录缓存的超时。NFS 4.0 中的委派允许服务器将某些职责分配给客户端，保证特定的文件共享语义，并在没有立即服务器交互的情况下启用本地文件操作。

2.2. AUTH_SYS 身份验证方法

AUTH_SYS 方法（也称为 **AUTH_UNIX** ）是一种客户端身份验证机制。使用 **AUTH_SYS** ，客户端向服务器发送用户的用户 ID (UID)和组 ID (GID)，来在访问文件时验证其身份和权限。它被视为不太安全，因为它依赖于客户端提供的信息，使得在错误配置时容易受到未经授权的访问。

映射机制可确保 NFS 客户端在服务器上可以访问具有合适权限的文件，即使系统间的 UID 和 GID 分配有所不同。UID 和 GID 是使用以下机制在 NFS 客户端和服务器间进行映射的：

直接映射

UID 和 GID 直接由 NFS 服务器和本地及远程系统之间的客户端进行映射。这需要在所有参与 NFS 文件共享的系统上进行一致的 UID 和 GID 分配。例如，客户端上 UID 为 1000 的用户只能访问服务器上 UID 为 1000 的用户有权限访问的共享上的文件。
对于 NFS 环境中简化的 ID 管理，管理员通常依赖集中服务，如 LDAP 或网络信息服务(NIS)来管理跨多个系统的 UID 和 GID 映射。

用户和组 ID 映射

NFS 服务器和客户端可以使用 **idmapd** 服务在不同的系统间转换 UID 和 GID，以进行一致的识别和权限分配。

2.3. AUTH_GSS 身份验证方法

Kerberos 是一种网络身份验证协议，它允许通过非安全网络对客户端和服务器进行安全身份验证。它使用对称密钥加密，并需要一个可信密钥分发中心(KDC)来验证用户和服务。

与 **AUTH_SYS** 不同，使用 **RPCSEC_GSS** Kerberos 机制，服务器不依赖于客户端就可正确表示哪个用户正在访问文件。相反，加密用于向服务器验证用户的身份，这可防止恶意的客户端在没有用户的 Kerberos 凭据的情况下模拟该用户。

在 **/etc/exports** 文件中，**sec** 选项定义一个或多个共享应提供的 Kerberos 安全性的方法，并且客户端可以通过以下方法之一挂载共享。**sec** 选项支持以下值：

- **sys**: 无加密保护（默认）
- **krb5** ：仅用于验证

- **krb5i**: 身份验证和完整性保护
- **krb5p** ：身份验证、完整性检查和流量加密

请注意，方法提供的加密功能越多，性能越低。

2.4. 导出的文件系统上的文件权限

导出的文件系统上的文件权限决定了对客户端通过 NFS 访问它们的文件和目录的访问权限。

远程主机挂载了 NFS 文件系统后，每个共享文件所拥有的唯一保护是其文件系统权限。如果共享同一用户 ID (UID)值的两个用户在不同的客户端系统上挂载相同的 NFS 文件系统，则他们可以修改彼此的文件。

NFS 将客户端上的 **root** 用户视为与服务器上的 **root** 用户相同。但是，默认情况下，在访问 NFS 共享时，NFS 服务器将 **root** 映射为 **nobody** 帐户。**root_squash** 选项控制此行为。

其它资源

- **exports(5)** 手册页

2.5. NFS 服务器上需要的服务

Red Hat Enterprise Linux (RHEL)使用内核模块和用户空间进程的组合来提供 NFS 文件共享：

表 2.1. NFS 服务器上需要的服务

服务名称	NFS 版本	描述
nfsd	3, 4	为请求共享 NFS 文件系统提供服务的 NFS 内核模块。
rpcbind	3	这个进程接受来自本地远程过程调用(RPC)服务的端口保留，使其可用或被宣传出去，允许相应的远程 RPC 服务访问它们。**rpcbind** 服务响应请求，并建立到指定的 RPC 服务的连接。
rpc.mountd	3, 4	此服务处理来自 NFSv3 客户端的 **MOUNT** 请求，NFSv4 服务器使用此服务的内部功能。 它检查请求的 NFS 共享是否当前由 NFS 服务器导出，是否允许客户端访问它。
rpc.nfsd	3, 4	这个进程通告显式的 NFS 版本和服务器定义的协议。它与内核合作来满足 NFS 客户端的动态需求，例如在每次 NFS 客户端连接时提供服务器线程。 **nfs-server** 服务启动此进程。
lockd	3	这个内核模块实现 Network Lock Manager (NLM)协议，它允许客户端锁定服务器上的文件。当 NFS 服务器运行时，RHEL 自动加载模块。
rpc.rquotad	3, 4	此服务为远程用户提供用户配额信息。

服务名称	NFS 版本	描述
rpc.idmapd	4	这个进程提供 NFSv4 客户端和服务器的向上调用，其在 NFSv4 名称（*'user@domain'* 形式的字符串）和本地用户和组 ID 之间进行映射。
gssproxy	3, 4	此服务代表 **rpc.nfsd** 处理 **krb5** 身份验证。
nfsdcld	4	此服务提供 NFSv4 客户端跟踪守护进程，当其它客户端在网络分区与服务器重启结合期间获取冲突锁时，该守护进程防止服务器授予锁回收。
rpc.statd	3	此服务在本地主机重启时向其他 NFSv3 客户端提供通知，当在远程 NFSv3 主机重启时，向内核提供通知。

其它资源

- **rpcbind (8)**, **rpc.mountd (8)**, **rpc.nfsd (8)**, **rpc.statd (8)**, **rpc.rquotad (8)**, **rpc.idmapd (8)**, **gssproxy (8)**, **nfsdcld (8)**, **rpc.statd (8)** 手册页

2.6. /ETC/EXPORTS 配置文件

/etc/exports 文件控制服务器导出哪些目录。每行包含一个导出点、允许挂载目录的空格分开的客户端的列表，以及每个客户端的选项：

```
<directory> <host_or_network_1>(<options_1>) <host_or_network_n>(<options_n>)...
```

以下是 **/etc/exports** 条目的各个部分：

<export>
要导出的目录。

<host_or_network>
共享要导出到的主机或网络。例如，您可以指定主机名、IP 地址或 IP 网络。

<options>
主机或网络的选项。

在客户端和服务器选项之间添加一个空格，更改行为。例如，以下行没有同样的含义：

```
/projects client.example.com(rw)
/projects client.example.com (rw)
```

在第一行中，服务器只允许 **client.example.com** 以读写模式挂载 **/projects** 目录，而其他主机不能挂载共享。但是，由于第二行中 **client.example.com** 和 **(rw)** 之间的空格，服务器以只读模式（默认设置）将目录导出到 **client.example.com**，但所有其他主机可以以读写模式挂载共享。

NFS 服务器对每个导出的目录使用以下默认设置：

表 2.2. /etc/exports 中条目的默认选项

默认设置	描述
ro	以只读模式导出目录。
sync	在将之前请求所做的更改写入磁盘之前，NFS 服务器不会回复请求。
wdelay	如果服务器怀疑有另一个写请求待处理，则它会延迟写入到磁盘。
root_squash	防止客户端上的 **root** 用户对导出的目录有 **root** 权限。启用 **root_squash** 后，NFS 服务器将访问权限从 **root** 映射到用户 **nobody**。

2.7. 配置只使用 NFSV4 的服务器

如果您的网络中没有任何 NFSv3 客户端，则您可以配置 NFS 服务器，以只支持 NFSv4 或其特定的次协议版本。在服务器上仅使用 NFSv4 可减少向网络开放的端口数量。

流程

1. 安装 **nfs-utils** 软件包：

```
# dnf install nfs-utils
```

2. 编辑 **/etc/nfs.conf** 文件，并进行以下更改：

   a. 在 **[nfsd]** 部分中禁用 **vers3** 参数来禁用 NFSv3：

```
[nfsd]
vers3=n
```

   b. 可选：如果您只需要特定的 NFSv4 次版本，请取消所有 **vers4.<minor_version>** 参数的注释，并相应地设置它们，例如：

```
[nfsd]
vers3=n
# vers4=y
vers4.0=n
vers4.1=n
vers4.2=y
```

   使用这个配置，服务器仅提供 NFS 版本 4.2。

   重要

   如果您只需要特定的 NFSv4 次版本，则只为次版本设置参数。不要取消 **vers4** 参数的注释，以避免不可预测地激活或停用次版本。默认情况下，**vers4** 参数启用或禁用所有 NFSv4 次版本。但是，如果您将 **vers4** 与其他 **vers** 参数一起设置了，则此行为会改变。

3. 禁用所有与 NFSv3 相关的服务：

```
# systemctl mask --now rpc-statd.service rpcbind.service rpcbind.socket
```

4. 将 **rpc.mountd** 守护进程配置为不侦听 NFSv3 挂载请求。使用以下内容创建 **/etc/systemd/system/nfs-mountd.service.d/v4only.conf** 文件：

```
[Service]
ExecStart=
ExecStart=/usr/sbin/rpc.mountd --no-tcp --no-udp
```

5. 重新加载 **systemd** 管理器配置，并重启 **nfs-mountd** 服务：

```
# systemctl daemon-reload
# systemctl restart nfs-mountd
```

6. 可选：创建一个您要共享的目录，例如：

```
# mkdir -p /nfs/projects/
```

如果要共享一个现有的目录，请跳过这一步。

7. 对 **/nfs/projects/** 目录设置您需要的权限：

```
# chmod 2770 /nfs/projects/
# chgrp users /nfs/projects/
```

这些命令在 **/nfs/projects/** 目录上为 **users** 组设置写权限，并确保对此目录中创建的新条目自动设置同样的组。

8. 对您要共享的每个目录添加一个到 **/etc/exports** 文件的导出点：

```
/nfs/projects/     192.0.2.0/24(rw) 2001:db8::/32(rw)
```

此条目共享 **/nfs/projects/** 目录，以使 **192.0.2.0/24** 和 **2001:db8::/32** 子网中的客户端具有读和写访问权限。

9. 在 **firewalld** 中打开相关端口：

```
# firewall-cmd --permanent --add-service nfs
# firewall-cmd --reload
```

10. 启用并启动 NFS 服务器：

```
# systemctl enable --now nfs-server
```

验证

- 在服务器上，验证服务器是否只提供您配置的 NFS 版本：

```
# cat /proc/fs/nfsd/versions
-3 +4 -4.0 -4.1 +4.2
```

- 在客户端上，执行以下步骤：

  1. 安装 **nfs-utils** 软件包：

```
# dnf install nfs-utils
```

2. 挂载一个导出的 NFS 共享：

```
# mount server.example.com:/nfs/projects/ /mnt/
```

3. 以是 **users** 组成员的用户身份，在 **/mnt/** 中创建一个文件：

```
# touch /mnt/file
```

4. 列出目录，以验证该文件是否被创建：

```
# ls -l /mnt/
total 0
-rw-r--r--. 1 demo users 0 Jan 16 14:18 file
```

2.8. 配置一个具有可选的 NFSV4 支持的 NFSV3 服务器

在仍然使用 NFSv3 客户端的网络中，将服务器配置为使用 NFSv3 协议提供共享。如果您的网络中还有较新的客户端，您还可以启用 NFSv4。默认情况下，Red Hat Enterprise Linux NFS 客户端使用服务器提供的最新 NFS 版本。

流程

1. 安装 **nfs-utils** 软件包：

```
# dnf install nfs-utils
```

2. 可选：默认启用 NFSv3 和 NFSv4。如果您不需要 NFSv4 或只需要特定的次版本，取消所有 **vers4.<minor_version>** 参数的注释，并相应地设置它们：

```
[nfsd]
# vers3=y
# vers4=y
vers4.0=n
vers4.1=n
vers4.2=y
```

使用这个配置，服务器仅提供 NFS 版本 3 和 4.2。

重要

如果您只需要特定的 NFSv4 次版本，则只为次版本设置参数。不要取消 **vers4** 参数的注释，以避免不可预测地激活或停用次版本。默认情况下，**vers4** 参数启用或禁用所有 NFSv4 次版本。但是，如果您将 **vers4** 与其他 **vers** 参数一起设置了，则此行为会改变。

3. 默认情况下，NFSv3 RPC 服务使用随机端口。要启用防火墙配置，请在 **/etc/nfs.conf** 文件中配置固定的端口号：

   a. 在 **[lockd]** 部分中，为 **nlockmgr** RPC 服务设置固定的端口号，例如：

```
[lockd]
port=5555
```

使用这个设置，服务自动对 UDP 和 TCP 协议使用此端口号。

b. 在 **[statd]** 部分中，为 **rpc.statd** 服务设置固定的端口号，例如：

```
[statd]
port=6666
```

使用这个设置，服务自动对 UDP 和 TCP 协议使用此端口号。

4. 可选：创建一个您要共享的目录，例如：

```
# mkdir -p /nfs/projects/
```

如果要共享一个现有的目录，请跳过这一步。

5. 对 **/nfs/projects/** 目录设置您需要的权限：

```
# chmod 2770 /nfs/projects/
# chgrp users /nfs/projects/
```

这些命令在 **/nfs/projects/** 目录上为 **users** 组设置写权限，并确保对此目录中创建的新条目自动设置同样的组。

6. 对您要共享的每个目录添加一个到 **/etc/exports** 文件的导出点：

```
/nfs/projects/     192.0.2.0/24(rw) 2001:db8::/32(rw)
```

此条目共享 **/nfs/projects/** 目录，以使 **192.0.2.0/24** 和 **2001:db8::/32** 子网中的客户端具有读和写访问权限。

7. 在 **firewalld** 中打开相关端口：

```
# firewall-cmd --permanent --add-service={nfs,rpc-bind,mountd}
# firewall-cmd --permanent --add-port={5555/tcp,5555/udp,6666/tcp,6666/udp}
# firewall-cmd --reload
```

8. 启用并启动 NFS 服务器：

```
# systemctl enable --now rpc-statd nfs-server
```

验证

- 在服务器上，验证服务器是否只提供您配置的 NFS 版本：

```
# cat /proc/fs/nfsd/versions
+3 +4 -4.0 -4.1 +4.2
```

- 在客户端上，执行以下步骤：

  1. 安装 **nfs-utils** 软件包：

```
# dnf install nfs-utils
```

2. 挂载一个导出的 NFS 共享：

```
# mount -o vers=<version> server.example.com:/nfs/projects/ /mnt/
```

3. 验证是否使用指定的 NFS 版本挂载了共享：

```
# mount | grep "/mnt"
server.example.com:/nfs/projects/ on /mnt type nfs (rw,relatime,vers=3,...
```

4. 以是 **users** 组成员的用户身份，在 **/mnt/** 中创建一个文件：

```
# touch /mnt/file
```

5. 列出目录，以验证该文件是否被创建：

```
# ls -l /mnt/
total 0
-rw-r--r--. 1 demo users 0 Jan 16 14:18 file
```

2.9. 在 NFS 服务器上启用配额支持

如果要限制用户或组群可以存储的数据量，您可以在文件系统上配置配额。在 NFS 服务器上，**rpc-rquotad** 服务确保配额也应用于 NFS 客户端上的用户。

先决条件

- NFS 服务器正在运行并已配置。
- 已在 ext 或 XFS 文件系统上配置了配额。

流程

1. 验证是否已在您导出的目录上启用了配额：
   - 对于 ext 文件系统，请输入：

```
# quotaon -p /nfs/projects/
group quota on /nfs/projects (/dev/sdb1) is on
user quota on /nfs/projects (/dev/sdb1) is on
project quota on /nfs/projects (/dev/sdb1) is off
```

   - 对于 XFS 文件系统，请输入：

```
# findmnt /nfs/projects
TARGET     SOURCE FSTYPE OPTIONS
/nfs/projects /dev/sdb1 xfs
rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,usrquota,grpquota
```

2. 安装 **quota-rpc** 软件包：

```
# dnf install quota-rpc
```

3. 可选。默认情况下，配额 RPC 服务在端口 875 上运行。如果要在不同的端口上运行服务，请将 **-p <port_number>** 附加到 **/etc/sysconfig/rpc-rquotad** 文件中的 **RPCRQUOTADOPTS** 变量中：

```
RPCRQUOTADOPTS="-p __<port_number>__"
```

4. 可选：默认情况下，远程主机只能读取配额。要允许客户端设置配额，请将 **-S** 选项附加到 **/etc/sysconfig/rpc-rquotad** 文件中的 **RPCRQUOTADOPTS** 变量中：

```
RPCRQUOTADOPTS="-S"
```

5. 在 **firewalld** 中打开端口：

```
# firewall-cmd --permanent --add-port=875/udp
# firewall-cmd --reload
```

6. 启用并启动 **rpc-rquotad** 服务：

```
# systemctl enable --now rpc-rquotad
```

验证

1. 在客户端中：

   a. 挂载导出的共享：

   ```
   # mount server.example.com:/nfs/projects/ /mnt/
   ```

   b. 显示配额。命令取决于导出的目录的文件系统。例如：

   - 要显示所有挂载的 ext 文件系统上特定用户的配额，请输入：

   ```
   # quota -u <user_name>
   Disk quotas for user demo (uid 1000):
       Filesystem    space    quota    limit    grace    files    quota    limit    grace
   server.example.com:/nfs/projects
               0K      100M     200M                0        0        0
   ```

   - 要显示 XFS 文件系统上用户和组配额，请输入：

   ```
   # xfs_quota -x -c "report -h" /mnt/
   User quota on /nfs/projects (/dev/vdb1)
             Blocks
   User ID     Used     Soft     Hard     Warn/Grace
   ---------- ---------------------------------
   root        0        0        0        00 [------]
   demo        0        100M     200M     00 [------]
   ```

其它资源

- **quota (1)** 手册页
- **xfs_quota(8)** 手册页

2.10. 在 NFS 服务器上启用通过 RDMA 的 NFS

远程直接内存访问(RDMA)是一种协议，它允许客户端系统将数据直接从存储服务器的内存传输到其自己的内存中。这提高了存储吞吐量，减少了服务器和客户端之间数据传输的延迟，并降低了两端的 CPU 负载。如果 NFS 服务器和客户端是通过 RDMA 连接的，则客户端可以使用 NFSoRDMA 挂载导出的目录。

先决条件

- NFS 服务正在运行且已配置
- InfiniBand 或 RDMA over Converged Ethernet (RoCE)设备已安装在服务器上。
- IP over InfiniBand (IPoIB)已在服务器上配置，InfiniBand 设备分配了一个 IP 地址。

流程

1. 安装 **rdma-core** 软件包：

```
# dnf install rdma-core
```

2. 如果软件包已安装，请验证 **/etc/rdma/modules/rdma.conf** 文件中的 **xprtrdma** 和 **svcrdma** 模块是否已取消注释：

```
# NFS over RDMA client support
xprtrdma
# NFS over RDMA server support
svcrdma
```

3. 可选。默认情况下，RDMA 上的 NFS 使用端口 20049。如果要使用不同的端口，请在 **/etc/nfs.conf** 文件的 **[nfsd]** 部分中设置 **rdma-port** 设置：

```
rdma-port=<port>
```

4. 在 **firewalld** 中打开 NFSoRDMA 端口：

```
# firewall-cmd --permanent --add-port={20049/tcp,20049/udp}
# firewall-cmd --reload
```

   如果您设置了与 20049 不同的端口，请调整端口号。

5. 重启 **nfs-server** 服务：

```
# systemctl restart nfs-server
```

验证

1. 在带有 InfiniBand 硬件的客户端上执行以下步骤：
   a. 安装以下软件包：
      -

```
# dnf install nfs-utils rdma-core
```

b. 通过 RDMA 挂载导出的 NFS 共享：

```
# mount -o rdma server.example.com:/nfs/projects/ /mnt/
```

如果您设置了与默认端口号(20049)不同的端口，请将 **port=<*port_number*>** 传给命令：

```
# mount -o rdma,port=<port_number> server.example.com:/nfs/projects/ /mnt/
```

c. 验证共享是否已使用 **rdma** 选项挂载了：

```
# mount | grep "/mnt"
server.example.com:/nfs/projects/ on /mnt type nfs (...,proto=rdma,...)
```

其它资源

- 配置 InfiniBand 和 RDMA 网络

2.11. 在 RED HAT IDENTITY MANAGEMENT 域中使用 KERBEROS 建立一个 NFS 服务器

如果您使用 Red Hat Identity Management (IdM)，您可以将 NFS 服务器加入到 IdM 域中。这可让您集中管理用户和组，并使用 Kerberos 进行身份验证、完整性保护和流量加密。

先决条件

- NFS 服务器在 Red Hat Identity Management (IdM)域中 已注册。
- NFS 服务器正在运行并已配置。

流程

1. 以 IdM 管理员身份获取 kerberos 票据：

```
# kinit admin
```

2. 创建一个 **nfs/<FQDN>** 服务主体：

```
# ipa service-add nfs/nfs_server.idm.example.com
```

3. 从 IdM 检索 **nfs** 服务主体，并将其存储在 **/etc/krb5.keytab** 文件中：

```
# ipa-getkeytab -s idm_server.idm.example.com -p nfs/nfs_server.idm.example.com -k
/etc/krb5.keytab
```

4. 可选：显示 **/etc/krb5.keytab** 文件中的主体：

```
# klist -k /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
```

```
---- ------------------------------------------------------------------------
   1 nfs/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   1 nfs/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   1 nfs/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   1 nfs/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   7 host/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   7 host/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   7 host/nfs_server.idm.example.com@IDM.EXAMPLE.COM
   7 host/nfs_server.idm.example.com@IDM.EXAMPLE.COM
```

默认情况下，当您将主机加入到 IdM 域时，IdM 客户端会将主机主体添加到 **/etc/krb5.keytab** 文件中。如果缺少主机主体，请使用 **ipa-getkeytab -s** ***idm_server.idm.example.com*** **-p** ***host/nfs_server.idm.example.com*** **-k /etc/krb5.keytab** 命令添加它。

5. 使用 **ipa-client-automount** 工具配置 IdM ID 的映射：

```
# ipa-client-automount
Searching for IPA server...
IPA server: DNS discovery
Location: default
Continue to configure the system with these values? [no]: yes
Configured /etc/idmapd.conf
Restarting sssd, waiting for it to become available.
Started autofs
```

6. 更新 **/etc/exports** 文件，并将 Kerberos 安全方法添加到客户端选项中。例如：

```
/nfs/projects/      192.0.2.0/24(rw,sec=krb5i)
```

如果您希望客户端可以从多个安全方法中选择，请使用冒号分割它们：

```
/nfs/projects/      192.0.2.0/24(rw,sec=krb5:krb5i:krb5p)
```

7. 重新载入导出的文件系统：

```
# exportfs -r
```