



Red Hat Enterprise Linux 9

ネットワークファイルサービスの設定および使用

Red Hat Enterprise Linux 9 でネットワークファイルサービスを設定して使用するガイド

Red Hat Enterprise Linux 9 ネットワークファイルサービスの設定および使用

Red Hat Enterprise Linux 9 でネットワークファイルサービスを設定して使用するガイド

法律上の通知

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.

概要

本書は、Samba サーバーおよび NFS サーバーを含む、Red Hat Enterprise Linux 9 でネットワーク ファイルサービスを設定し、実行する方法を説明します。

目次

多様性を受け入れるオープンソースの強化	3
RED HAT ドキュメントへのフィードバック (英語のみ)	4
第1章 SAMBA をサーバーとして使用	5
1.1. さまざまな SAMBA サービスおよびモードについて	5
1.2. TESTPARM ユーティリティを使用した SMB.CONF ファイルの検証	8
1.3. SAMBA をスタンドアロンサーバーとして設定	8
1.4. SAMBA ID マッピングの理解および設定	11
1.5. SAMBA を AD ドメインメンバーサーバーとして設定	20
1.6. IDM ドメインメンバーでの SAMBA の設定	23
1.7. POSIX ACL を使用した SAMBA ファイル共有の設定	28
1.8. POSIX ACL を使用する共有への権限の設定	32
1.9. WINDOWS ACL で共有の設定	34
1.10. SMBCACLS で SMB 共有上の ACL の管理	37
1.11. ユーザーが SAMBA サーバーのディレクトリーを共有できるようにする	41
1.12. 認証なしでアクセスを許可する共有の設定	45
1.13. MACOS クライアント向けの SAMBA の設定	46
1.14. SMBCLIENT ユーティリティを使用した SMB 共有へのアクセス	47
1.15. プリントサーバーとしての SAMBA の設定	49
1.16. SAMBA プリントサーバーでの WINDOWS クライアント用の自動プリンタードライバダウンロードの設定	52
1.17. FIPS モードが有効なサーバーでの SAMBA の実行	58
1.18. SAMBA サーバーのパフォーマンスチューニング	59
1.19. SAMBA がデフォルトの SMB バージョンよりも前のバージョンのクライアントと互換対応するような設定	61
1.20. 頻繁に使用される SAMBA コマンドラインユーティリティ	62
1.21. 関連情報	72
第2章 NFS サーバーのデプロイ	73
2.1. NFSV4 のマイナーバージョンの主な機能	73
2.2. AUTH_SYS 認証方式	74
2.3. AUTH_GSS 認証方式	75
2.4. エクスポートされたファイルシステムのファイル権限	75
2.5. NFS サーバーに必要なサービス	75
2.6. /ETC/EXPORTS 設定ファイル	77
2.7. NFSV4 専用サーバーの設定	78
2.8. オプションの NFSV4 サポートを備えた NFSV3 サーバーの設定	80
2.9. NFS サーバーでクォータサポートを有効にする	82
2.10. NFS サーバーで NFS OVER RDMA を有効にする	84
2.11. RED HAT IDENTITY MANAGEMENT ドメインで KERBEROS を使用する NFS サーバーを設定する	85

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[Red Hat CTO である Chris Wright のメッセージ](#) をご覧ください。

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. [Jira](#) の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. ダイアログの下部にある **Create** をクリックします。

第1章 SAMBA をサーバーとして使用

Samba は、Red Hat Enterprise Linux にサーバーメッセージブロック (SMB) プロトコルを実装します。SMB プロトコルは、ファイル共有、共有プリンターなど、サーバーのリソースにアクセスするのに使用されます。また、Samba は、Microsoft Windows が使用する分散コンピューティング環境のリモートプロシージャコール (DCE RPC) のプロトコルを実装します。

Samba は以下のように実行できます。

- Active Directory (AD) または NT4 ドメインメンバー
- スタンドアロンサーバー
- NT4 プライマリドメインコントローラー (PDC) またはバックアップドメインコントローラー (BDC)



注記

Red Hat は、NT4 ドメインに対応する Windows バージョンの既存のインストールでのみ、PDC モードおよび BDC モードをサポートします。Red Hat では、新しい Samba NT4 ドメインを設定しないことを推奨します。これは、Windows 7 および Windows Server 2008 R2 以降の Microsoft オペレーティングシステムが NT4 ドメインに対応していないためです。

Red Hat は、Samba を AD ドメインコントローラー (DC) として実行することはサポートしていません。

インストールモードとは関係なく、必要に応じてディレクトリーやプリンターを共有できます。これにより、Samba がファイルサーバーおよびプリントサーバーとして機能できるようになります。

1.1. さまざまな SAMBA サービスおよびモードについて

samba パッケージは複数のサービスを提供します。環境と設定するシナリオに応じて、これらのサービスが1つ以上必要となり、Samba をさまざまなモードで設定します。

1.1.1. Samba サービス

Samba は以下のサービスを提供します。

smbd

このサービスは、SMB プロトコルを使用してファイル共有およびプリントサービスを提供します。また、サービスは、リソースのロックと、接続ユーザーの認証を担当します。ドメインメンバーを認証するには、**smbd** に **winbindd** が必要です。**smb systemd** サービスが起動し、**smbd** デーモンが停止します。

smbd サービスを使用するには、**samba** パッケージをインストールします。

nmbd

このサービスは、NetBIOS over IPv4 プロトコルを使用してホスト名および IP 解決を提供します。名前解決に加え、**nmbd** サービスで SMB ネットワークを参照して、ドメイン、作業グループ、ホスト、ファイル共有、およびプリンターを探すことができます。このため、サービスはこの情報をブロードキャストクライアントに直接報告するか、ローカルまたはマスターのブラウザーに転送します。**nmb systemd** サービスは、**nmbd** デーモンを起動し、停止します。

最近の SMB ネットワークは、クライアントおよび IP アドレスの解決に DNS を使用することに注意してください。Kerberos の場合は、稼働中の DNS 設定が必要です。

nmbd サービスを使用するには、**samba** パッケージをインストールします。

winbindd

このサービスは、ローカルシステムの AD または NT4 のドメインユーザーおよびグループを使用する Name Service Switch (NSS) のインターフェイスを提供します。これにより、たとえばドメインユーザーを、Samba サーバーにホストされるサービスや他のローカルサービスに認証できます。**winbind systemd** サービスは、**winbindd** デモンを開始および停止します。

Samba をドメインメンバーとして設定する場合は、**smbd** サービスの前に **winbindd** を起動する必要があります。そうしないと、ドメインユーザーおよびグループはローカルシステムで使用できなくなります。

winbindd サービスを使用するには、**samba-winbind** パッケージをインストールします。



重要

Red Hat は、ドメインユーザーおよびグループをローカルシステムに提供するために、Samba を、**winbindd** サービスを使用するサーバーとして実行することのみをサポートします。Windows アクセス制御リスト (ACL) のサポート、NT LAN Manager (NTLM) のフォールバックがないなど、特定の制限により、SSSD に対応しません。

1.1.2. Samba セキュリティーサービス

`/etc/samba/smb.conf` ファイルの **[global]** セクションの **security** パラメーターは、Samba がサービスに接続しているユーザーを認証する方法を管理します。Samba をインストールするモードに応じて、パラメーターは異なる値に設定する必要があります。

AD ドメインメンバーに、**security = ads** を設定する。

このモードでは、Samba は Kerberos を使用して AD ユーザーを認証します。

Samba をドメインメンバーとして設定する方法の詳細については、[Samba を AD ドメインメンバーサーバーとして設定](#) を参照してください。

スタンドアロンサーバーで、**security = user** を設定する。

このモードでは、Samba がローカルデータベースを使用して接続ユーザーを認証します。

Samba をスタンドアロンサーバーとしてセットアップする方法の詳細については、[スタンドアロンサーバーとしての Samba の設定](#) を参照してください。

NT4 PDC または BDC に **security = user** を設定する。

Samba は、このモードでは、ユーザーをローカルまたは LDAP データベースに認証します。

NT4 ドメインメンバーで、**security = domain** を設定する。

Samba は、このモードでは、NT4 PDC または BDC にユーザーを接続する認証を行います。このモードは、AD ドメインメンバーには使用できません。

Samba をドメインメンバーとして設定する方法の詳細については、[Samba を AD ドメインメンバーサーバーとして設定](#) を参照してください。

関連情報

- **smb.conf(5)** man ページの **security** パラメーター

1.1.3. Samba サービスおよび Samba クライアントユーティリティーが設定を読み込み、再読み込みするシナリオ

以下は、Samba サービスおよびユーティリティーによる設定の読み込み、再読み込み時について説明します。

- Samba サービスは、設定を再読み込みする時:
 - 3分ごとに自動更新
 - 手動要求の場合に **smbcontrol all reload-config** コマンドを実行するとします。
- Samba クライアントユーティリティーは、起動時にのみ設定を読み取ります。

security などの特定のパラメーターの適用には、**smb** サービスの再起動が必要です。再読み込みだけでは十分ではないことに注意してください。

関連情報

- **smb.conf(5)** man ページの **How configuration changes are apply** セクション
- **smbd(8)**、**nmbd(8)**、および **winbindd(8)** man ページ

1.1.4. 安全な方法での Samba 設定の編集

Samba サービスは、3分ごとに設定を自動的に再読み込みします。**testparm** ユーティリティーでの設定の検証前にサービスが変更を再読み込みしないように、安全な方法で Samba 設定を編集できます。

前提条件

- Samba がインストールされている。

手順

1. **/etc/samba/smb.conf** ファイルのコピーを作成します。

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

2. コピーして作成したファイルを編集し、必要な変更を加えます。
3. **/etc/samba/samba.conf.copy** ファイルの設定を確認します。

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

testparm がエラーを報告した場合は、修正してもう一度コマンドを実行します。

4. **/etc/samba/smb.conf** ファイルを新しい設定に上書きします。

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

5. Samba サービスが設定を自動的に再読み込みするか、手動で設定を再読み込みするまで待ちます。

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

関連情報

- [Samba サービスおよび Samba クライアントユーティリティーが設定を読み込み、再読み込みするシナリオ](#)

1.2. TESTPARM ユーティリティーを使用した SMB.CONF ファイルの検証

`testparm` ユーティリティーは、`/etc/samba/smb.conf` ファイルの Samba 設定が正しいことを確認します。このユーティリティーは、無効なパラメーターおよび値を検出しますが、ID マッピングなどの間違った設定も検出します。`testparm` が問題を報告しないと、Samba サービスは `/etc/samba/smb.conf` ファイルを正常に読み込みます。`testparm` は、設定されたサービスが利用可能であること、または期待通りに機能するかを確認できないことに注意してください。



重要

Red Hat では、このファイルの変更後に毎回 `testparm` を使用して、`/etc/samba/smb.conf` ファイルを検証することが推奨されます。

前提条件

- Samba をインストールしている。
- `/etc/samba/smb.conf` ファイルが存在する。

手順

1. `root` ユーザーで `testparm` ユーティリティーを実行します。

```
# 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 level"
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]
...
```

上記の出力例では、存在しないパラメーターと間違っ ID マッピングの設定が報告されます。

2. `testparm` が設定内の間違っパラメーター、値、またはその他のエラーを報告する場合は、問題を修正してから再度ユーティリティーを実行してください。

1.3. SAMBA をスタンドアロンサーバーとして設定

Samba は、ドメインのメンバーではないサーバーとして設定できます。このインストールモードでは、Samba はユーザーを中央 DC ではなくローカルデータベースに認証します。また、ゲストアクセスを有効にして、ユーザーが、認証なしで1つまたは複数のサービスに接続できるようにすることもできます。

1.3.1. スタンドアロンサーバーのサーバー設定の設定

Samba スタンドアロンサーバーのサーバー設定を設定できます。

手順

1. **samba** パッケージをインストールします。

```
# dnf install samba
```

2. `/etc/samba/smb.conf` ファイルを編集して、以下のパラメーターを設定します。

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

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

この設定では、**Example-WG** ワークグループに、スタンドアロンサーバー (**Server**) を定義します。また、この設定により最小レベル (1) でのログ記録が可能になり、ログファイルは `/var/log/samba/` ディレクトリーに保存されます。Samba は、**log file** パラメーターの `%m` マクロを、接続しているクライアントの NetBIOS 名までデプロイメントします。これにより、クライアントごとに個別のログファイルが有効になります。

3. オプションで、ファイルまたはプリンターの共有を設定します。参照:

- [POSIX ACL で共有の設定](#)
- [Windows ACL で共有の設定](#)
- [プリントサーバーとしての Samba の設定](#)

4. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

5. 認証が必要な共有を設定する場合は、ユーザーアカウントを作成します。詳細は [ローカルユーザーアカウントの作成および有効化](#) を参照してください。
6. **firewall-cmd** ユーティリティーを使用して必要なポートを開き、ファイアウォール設定を再読み込みします。

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

7. **smb** サービスを有効にして起動します。

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

関連情報

- **smb.conf(5)** man ページ

1.3.2. ローカルユーザーアカウントの作成および有効化

共有への接続時にユーザーが認証を行えるようにするには、オペレーティングシステムと Samba データベースの両方で Samba ホストにアカウントを作成する必要があります。Samba では、ファイルシステムオブジェクトでアクセス制御リスト (ACL) を検証するオペレーティングシステムアカウントと、接続ユーザーの認証を行う Samba アカウントが必要です。

passdb backend = tdbsam のデフォルト設定を使用すると、Samba はユーザーアカウントを **/var/lib/samba/private/passdb.tdb** データベースに保存します。

example という名前のローカル Samba ユーザーを作成できます。

前提条件

- Samba が、スタンドアロンサーバーとしてインストールされている。

手順

1. オペレーティングシステムアカウントを作成します。

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

このコマンドは、ホームディレクトリーを作成せずに、**example** アカウントを追加します。アカウントが Samba への認証のみに使用される場合は、**/sbin/nologin** コマンドをシェルとして割り当て、アカウントがローカルでログインしないようにします。

2. オペレーティングシステムのアカウントにパスワードを設定して、これを有効にします。

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

Samba は、オペレーティングシステムのアカウントに設定されたパスワードを使用して認証を行いません。ただし、アカウントを有効にするには、パスワードを設定する必要があります。アカウントが無効になると、そのユーザーが接続した時に Samba がアクセスを拒否します。

3. Samba データベースにユーザーを追加し、そのアカウントにパスワードを設定します。

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

このアカウントを使用して Samba 共有に接続する場合に、このパスワードを使用して認証を行います。

4. Samba アカウントを有効にします。

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

1.4. SAMBA ID マッピングの理解および設定

Windows ドメインは、ユーザーおよびグループを一意的セキュリティ識別子 (SID) で区別します。ただし、Linux では、ユーザーおよびグループごとに一意の UID と GID が必要です。Samba をドメインメンバーとして実行する場合は、**winbindd** サービスが、ドメインユーザーおよびグループに関する情報をオペレーティングシステムに提供します。

winbindd サービスが、ユーザーおよびグループの一意的 ID を Linux に提供するようにするには、`/etc/samba/smb.conf` ファイルで ID マッピングを設定する必要があります。

- ローカルデータベース (デフォルトドメイン)
- Samba サーバーがメンバーになっている AD または NT4 のドメイン
- ユーザーがこの Samba サーバーのリソースにアクセスする必要のある信頼ドメイン

Samba は、特定の設定に対して異なる ID マッピングバックエンドを提供します。最も頻繁に使用されるバックエンドは、以下の通りです。

バックエンド	ユースケース
tdb	* デフォルトドメインのみ
ad	AD ドメインのみ
rid	AD ドメインおよび NT4 ドメイン
autorid	AD、NT4、および * デフォルトのドメイン

1.4.1. Samba ID 範囲の計画

Linux の UID および GID を AD に保存するか、Samba がそれを生成するように設定するかに関係なく、各ドメイン設定には、他のドメインと重複しない一意の ID 範囲が必要です。



警告

重複する ID 範囲を設定すると、Samba が正常に機能しなくなります。

例1.1 一意の ID 範囲

以下は、デフォルト (*)、**AD-DOM**、および **TRUST-DOM** のドメインの非オーバーラッピングの ID マッピング範囲を示しています。

```
[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

1つのドメインに割り当てられるのは1つの範囲だけです。したがって、ドメイン範囲間で十分な容量を残しておきます。これにより、ドメインが拡大した場合に、後で範囲を拡張できます。

後で別の範囲をドメインに割り当てると、このユーザーおよびグループが作成したファイルおよびディレクトリーの所有権が失われます。

1.4.2. * デフォルトドメイン

ドメイン環境では、以下の各 ID マッピング設定を追加します。

- Samba サーバーがメンバーとなっているドメイン
- Samba サーバーにアクセスできる信頼された各ドメイン

ただし、Samba が、その他のすべてのオブジェクトに、デフォルトドメインから ID を割り当てます。これには以下が含まれます。

- ローカルの Samba ユーザーおよびグループ
- Samba の組み込みアカウントおよびグループ (**BUILTIN\Administrators** など)

重要

Samba が正常に機能できるようにするには、説明に従ってデフォルトのドメインを設定する必要があります。

割り当てられた ID を永続的に格納するには、デフォルトのドメインバックエンドを書き込み可能にする必要があります。

デフォルトドメインには、以下のいずれかのバックエンドを使用できます。

tdb

デフォルトのドメインを、**tdb** バックエンドを使用するように設定する場合は、ID 範囲を設定します。この ID 範囲には、将来作成されるオブジェクトや、定義されたドメイン ID マッピング設定には含まれないオブジェクトを追加できます。

たとえば、`/etc/samba/smb.conf` ファイルの **[global]** セクションで以下を設定します。

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

■
詳細は、[TDB ID マッピングバックエンドの使用](#) を参照してください。

autorid

autorid バックエンドを使用するように、デフォルトのドメインを設定する場合、ドメイン用の ID マッピング設定を追加するかどうかは任意になります。

たとえば、`/etc/samba/smb.conf` ファイルの **[global]** セクションで以下を設定します。

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

詳細は、[autorid ID マッピングバックエンドの使用](#) を参照してください。

1.4.3. tdb ID マッピングバックエンドの使用

winbindd サービスは、デフォルトで書き込み可能な **tdb** ID マッピングバックエンドを使用して、セキュリティ識別子 (SID)、UID、および GID のマッピングテーブルを格納します。これには、ローカルユーザー、グループ、組み込みプリンシパルが含まれます。

このバックエンドは、* デフォルトドメインにのみ使用してください。以下に例を示します。

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

関連情報

- [* デフォルトドメイン](#)

1.4.4. ad ID マッピングバックエンドの使用

ad ID マッピングバックエンドを使用するように Samba AD メンバーを設定できます。

ad ID マッピングバックエンドは、読み取り専用 API を実装し、AD からアカウントおよびグループの情報を読み取ります。これには、以下の利点があります。

- ユーザーとグループの全設定は、AD に集中的に保存されます。
- ユーザーおよびグループの ID は、このバックエンドを使用するすべての Samba サーバーで一貫しています。
- ID は、破損する可能性のあるローカルデータベースには保存されないため、ファイルの所有権は失われません。



注記

ad ID マッピングバックエンドは、一方向の信頼を使用する Active Directory ドメインに対応していません。一方向の信頼で Active Directory のドメインメンバーを設定する場合は、**tdb**、**rid**、または **autorid** のいずれかの ID マッピングバックエンドを使用します。

ad バックエンドは、AD から以下の属性を読み込みます。

AD 属性名	オブジェクトの種類	マッピング先
sAMAccountName	ユーザーおよびグループ	オブジェクトのユーザー名またはグループ名
uidNumber	ユーザー	ユーザー ID (UID)
gidNumber	グループ	グループ ID (GID)
loginShell ^[a]	ユーザー	ユーザーのシェルのパス
unixHomeDirectory ^[a]	ユーザー	ユーザーのホームディレクトリーのパス
primaryGroupID ^[b]	ユーザー	プライマリーグループ ID

^[a] **idmap config DOMAIN:unix_nss_info = yes** を設定している場合に限り、Samba がこの属性を読み込みます。

^[b] **idmap config DOMAIN:unix_primary_group = yes** を設定している場合に限り、Samba がこの属性を読み込みます。

前提条件

- ユーザーおよびグループはいずれも、AD で一意の ID が設定され、ID が、**/etc/samba/smb.conf** ファイルで設定されている範囲内にある。ID が範囲外にあるオブジェクトは、Samba サーバーでは利用できません。
- ユーザーおよびグループには、AD ですべての必須属性が設定されている。必要な属性がないと、ユーザーまたはグループは Samba サーバーで使用できなくなります。必要な属性は、設定によって異なります。前提条件:
- Samba をインストールしている。
- ID マッピングを除く Samba 設定が **/etc/samba/smb.conf** ファイルにある。

手順

1. **/etc/samba/smb.conf** ファイルの **[global]** セクションを編集します。
 - a. デフォルトドメイン (*) に ID マッピング設定が存在しない場合は追加します。以下に例を示します。

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

- b. AD ドメインの **ad** ID マッピングバックエンドを有効にします。

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

- c. AD ドメインのユーザーおよびグループに割り当てられている ID の範囲を設定します。以下に例を示します。

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



重要

この範囲は、このサーバーの他のドメイン設定と重複させることはできません。また、この範囲には、今後割り当てられる ID がすべて収まる大きさを設定する必要があります。詳細は、[Samba ID 範囲の計画](#) を参照してください。

- d. Samba が AD から属性を読み取る際に [RFC 2307](#) スキーマを使用するように設定します。

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

- e. Samba が、対応する AD 属性からログインシェルおよびユーザーホームディレクトリーのパスを読み取るようにする場合は、以下を設定します。

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

または、すべてのユーザーに適用される、ドメイン全体のホームディレクトリーのパスおよびログインシェルを統一して設定できます。以下に例を示します。

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

- f. デフォルトでは、Samba は、ユーザーオブジェクトの **primaryGroupID** 属性を、Linux のユーザーのプライマリーグループとして使用します。または、代わりに **gidNumber** 属性に設定されている値を使用するように Samba を設定できます。

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

2. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

3. Samba 設定を再読み込みします。

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

関連情報

- [* デフォルトドメイン](#)
- [smb.conf\(5\)](#) および [idmap_ad\(8\)](#) man ページ
- [smb.conf\(5\)](#) man ページの **VARIABLE SUBSTITUTIONS** セクション

1.4.5. rid ID マッピングバックエンドの使用

rid ID マッピングバックエンドを使用するように Samba ドメインメンバーを設定できます。

Samba は、Windows SID の相対識別子 (RID) を使用して、Red Hat Enterprise Linux で ID を生成できます。



注記

RID は、SID の最後の部分です。たとえば、ユーザーの SID が **S-1-5-21-5421822485-1151247151-421485315-30014** の場合、対応する RID は **30014** になります。

rid ID マッピングバックエンドは、AD ドメインおよび NT4 ドメインのアルゴリズムマッピングスキームに基づいてアカウントおよびグループの情報を計算する読み取り専用 API を実装します。バックエンドを設定する場合は、**idmap config DOMAIN : range** パラメーターで、RID の最小値および最大値を設定する必要があります。Samba は、このパラメーターで設定される RID の最小値および最大値を超えるユーザーまたはグループをマッピングしません。



重要

読み取り専用のバックエンドとして、**rid** は、**BUILTIN** グループなど、新しい ID を割り当てることができません。したがって、*デフォルトドメインにはこのバックエンドを使用しないでください。

rid バックエンドを使用した利点

- 設定された範囲内の RID があるドメインユーザーとグループはすべて、自動的にドメインメンバーで利用可能になります。
- ID、ホームディレクトリー、およびログインシェルを手動で割り当てる必要はありません。

rid バックエンドを使用した場合の短所

- すべてのドメインユーザーは、割り当てられた同じログインシェルとホームディレクトリーを取得します。ただし、変数を使用できません。
- 同じ ID 範囲設定で **rid** バックエンドを使用している Samba ドメインメンバーでは、ユーザー ID とグループ ID が同じになります。
- ドメインメンバーで個々のユーザーまたはグループを除外して、利用できないようにすることはできません。設定されている範囲外にあるユーザーとグループのみが除外されます。
- 異なるドメインのオブジェクトの RID が同じ場合は、**winbindd** サービスが ID の計算に使用する式に基づき、複数ドメインの環境で重複する ID が発生する場合があります。

前提条件

- Samba をインストールしている。
- ID マッピングを除く Samba 設定が **/etc/samba/smb.conf** ファイルにある。

手順

1. **/etc/samba/smb.conf** ファイルの **[global]** セクションを編集します。
 - a. デフォルトドメイン (*) に ID マッピング設定が存在しない場合は追加します。以下に例を示します。

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

- b. ドメインの **rid** ID マッピングバックエンドを有効にします。

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

- c. 今後割り当てられるすべての RID が収まる大きさの範囲を設定します。以下に例を示します。

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

Samba は、そのドメインの RID がその範囲内がないユーザーおよびグループを無視します。



重要

この範囲は、このサーバーの他のドメイン設定と重複させることはできません。また、この範囲には、今後割り当てられる ID がすべて収まる大きさを設定する必要があります。詳細は、[Samba ID 範囲の計画](#) を参照してください。

- d. すべてのマッピングユーザーに割り当てられるシェルおよびホームディレクトリーのパスを設定します。以下に例を示します。

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

2. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

3. Samba 設定を再読み込みします。

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

関連情報

- [* デフォルトドメイン](#)
- `smb.conf(5)` man ページの **VARIABLE SUBSTITUTIONS** セクション
- RID からのローカル ID の計算については、`idmap_rid(8)` man ページを参照してください。

1.4.6. autorid ID マッピングバックエンドの使用

`autorid` ID マッピングバックエンドを使用するように Samba ドメインメンバーを設定できます。

`autorid` バックエンドは、`rid` ID マッピングバックエンドと同様の動作をしますが、異なるドメインに対して自動的に ID を割り当てることができます。これにより、以下の状況で `autorid` バックエンドを使用できます。

- * デフォルトドメインのみ
- * デフォルトドメインと追加のドメインでは、追加のドメインごとに ID マッピング設定を作成する必要はありません。
- 特定のドメインのみ



注記

デフォルトドメインに **autorid** を使用する場合は、ドメイン用の ID マッピング設定を追加するかどうかは任意です。

このセクションの一部は、Samba Wiki に公開されているドキュメント [idmap config autorid](#) に掲載されています。ライセンスは、[CC BY 4.0](#) にあります。著者および貢献者は、Wiki ページの [history](#) タブを参照してください。

autorid バックエンドを使用した利点

- 設定された範囲内に計算した UID と GID があるすべてのドメインユーザーおよびグループは、ドメインメンバーで自動的に利用可能になります。
- ID、ホームディレクトリー、およびログインシェルを手動で割り当てる必要はありません。
- 複数ドメイン環境内の複数のオブジェクトが同じ RID を持つ場合でも、重複する ID はありません。

短所

- Samba ドメインメンバー間では、ユーザー ID とグループ ID は同じではありません。
- すべてのドメインユーザーは、割り当てられた同じログインシェルとホームディレクトリーを取得します。ただし、変数を使用できます。
- ドメインメンバーで個々のユーザーまたはグループを除外して、利用できないようにすることはできません。計算された UID または GID が、設定された範囲外にあるユーザーとグループのみが除外されます。

前提条件

- Samba をインストールしている。
- ID マッピングを除く Samba 設定が **/etc/samba/smb.conf** ファイルにある。

手順

1. **/etc/samba/smb.conf** ファイルの **[global]** セクションを編集します。
 - a. *デフォルトドメインの **autorid** ID マッピングバックエンドを有効にします。

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

- b. 既存および将来の全オブジェクトに ID を割り当てられる大きさの範囲を設定します。以下に例を示します。

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

Samba は、このドメインで計算した ID が範囲内でないユーザーおよびグループを無視します。



警告

範囲を設定し、Samba がそれを使用して開始してからは、範囲の上限を小さくすることはできません。範囲にその他の変更を加えると、新しい ID 割り当てが発生し、ファイルの所有権が失われる可能性があります。

- c. 必要に応じて、範囲サイズを設定します。以下に例を示します。

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

Samba は、**idmap config * : range** パラメーターに設定されている範囲からすべての ID を取得するまで、各ドメインのオブジェクトにこの数の連続 ID を割り当てます。



注記

rangesize を設定する場合は、適宜範囲を調整する必要があります。この範囲は rangesize の倍数である必要があります。

- d. すべてのマッピングユーザーに割り当てられるシェルおよびホームディレクトリーのパスを設定します。以下に例を示します。

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

- e. 必要に応じて、ドメイン用の ID マッピング設定を追加します。個別のドメインの設定が利用できない場合、Samba は以前に設定した * デフォルトドメインの **autorid** バックエンド設定を使用して ID を計算します。



重要

この範囲は、このサーバーの他のドメイン設定と重複させることはできません。また、この範囲には、今後割り当てられる ID がすべて収まる大きさを設定する必要があります。詳細は、[Samba ID 範囲の計画](#) を参照してください。

2. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

3. Samba 設定を再読み込みします。

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

関連情報

- `idmap_autorid(8)` man ページの **THE MAPPING FORMULAS** セクション

- `idmap_autorid(8)` man ページの `rangesize` パラメーターの説明
- `smb.conf(5)` man ページの `VARIABLE SUBSTITUTIONS` セクション

1.5. SAMBA を AD ドメインメンバーサーバーとして設定

AD または NT4 のドメインを実行している場合は、Samba を使用して Red Hat Enterprise Linux サーバーをメンバーとしてドメインに追加し、以下を取得します。

- その他のドメインメンバーのドメインリソースにアクセスする
- `sshd` などのローカルサービスに対してドメインユーザーを認証する
- サーバーにホストされているディレクトリーおよびプリンターを共有して、ファイルサーバーおよびプリントサーバーとして動作する

1.5.1. RHEL システムの AD ドメインへの参加

Samba Winbind は、Red Hat Enterprise Linux (RHEL) システムを Active Directory (AD) に接続するための System Security Services Daemon (SSSD) の代替手段です。`realmd` を使用して Samba Winbind を設定することで、RHEL システムを AD ドメインに参加させることができます。

手順

1. AD で Kerberos 認証に非推奨の RC4 暗号化タイプが必要な場合は、RHEL でこの暗号のサポートを有効にします。

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

2. 以下のパッケージをインストールします。

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

3. ドメインメンバーでディレクトリーまたはプリンターを共有するには、`samba` パッケージをインストールします。

```
# dnf install samba
```

4. 既存の Samba 設定ファイル `/etc/samba/smb.conf` をバックアップします。

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

5. ドメインに参加します。たとえば、ドメイン `ad.example.com` に参加するには、以下のコマンドを実行します。

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

上記のコマンドを使用すると、`realm` ユーティリティーが自動的に以下を実行します。

- `ad.example.com` ドメインのメンバーシップに `/etc/samba/smb.conf` ファイルを作成します。

- ユーザーおよびグループの検索用の **winbind** モジュールを、**/etc/nsswitch.conf** ファイルに追加します。
 - **/etc/pam.d/** ディレクトリーの PAM (プラグ可能な認証モジュール) 設定ファイルを更新します。
 - **winbind** サービスを起動し、システムの起動時にサービスを起動できるようにします。
6. 必要に応じて、**/etc/samba/smb.conf** ファイルの別の ID マッピングバックエンド、またはカスタマイズした ID マッピングを設定します。

詳細は、[SambaID マッピングの理解と設定](#) を参照してください。

1. **winbind** サービスが稼働していることを確認します。

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



重要

Samba がドメインのユーザーおよびグループの情報をクエリーできるようにするには、**smb** を起動する前に **winbind** サービスを実行する必要があります。

2. **samba** パッケージをインストールしてディレクトリーおよびプリンターを共有している場合は、**smb** サービスを有効化して開始します。

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

3. 必要に応じて、Active Directory へのローカルログインを認証する場合は、**winbind_krb5_localauth** プラグインを有効にします。[MIT Kerberos 用のローカル承認プラグインの使用](#)

検証手順

1. AD ドメインの AD 管理者アカウントなど、AD ユーザーの詳細を表示します。

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

2. AD ドメイン内のドメインユーザーグループのメンバーをクエリーします。

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

3. オプションで、ファイルやディレクトリーに権限を設定する際に、ドメインのユーザーおよびグループを使用できることを確認します。たとえば、**/srv/samba/example.txt** ファイルの所有者を **AD\administrator** に設定し、グループを **AD\Domain Users** に設定するには、以下のコマンドを実行します。

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

4. Kerberos 認証が期待どおりに機能することを確認します。

- a. AD ドメインメンバーで、**administrator@AD.EXAMPLE.COM** プリンシパルのチケットを取得します。

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

- b. キャッシュされた Kerberos チケットを表示します。

```
# 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. 利用可能なドメインの表示:

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

関連情報

- 非推奨の RC4 暗号化を使用しない場合は、AD で AES 暗号化タイプを有効にすることができます。詳細は、
- [GPO を使用した Active Directory で AES 暗号化タイプの有効化](#)
- [realm\(8\) man ページ](#)

1.5.2. MIT Kerberos 用のローカル承認プラグインの使用

winbind サービスは、Active Directory ユーザーをドメインメンバーに提供します。特定の状況では、管理者が、ドメインメンバーで実行している SSH サーバーなどのローカルサービスに対して、ドメインユーザーが認証を行えるようにします。Kerberos を使用してドメインユーザーを認証している場合は、**winbind** サービスを介して、**winbind_krb5_localauth** プラグインが Kerberos プリンシパルを Active Directory アカウントに正しくマッピングできるようにします。

たとえば、Active Directory ユーザーの **sAMAccountName** 属性を **EXAMPLE** に設定し、小文字のユーザー名でユーザーがログインしようとするすると、Kerberos はユーザー名を大文字で返します。その結果、エントリーは認証の失敗に一致しません。

winbind_krb5_localauth プラグインを使用すると、アカウント名が正しくマッピングされます。これは GSSAPI 認証にのみ適用され、初期のチケット付与チケット (TGT) の取得には該当しません。

前提条件

- Samba が Active Directory のメンバーとして設定されている。
- Red Hat Enterprise Linux が、Active Directory に対してログイン試行を認証している。
- **winbind** サービスが実行している。

手順

/etc/krb5.conf ファイルを編集し、以下のセクションを追加します。

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

関連情報

- [winbind_krb5_localauth\(8\) man ページ](#).

1.6. IDM ドメインメンバーでの SAMBA の設定

Red Hat Identity Management (IdM) ドメインに参加しているホスト上で Samba をセットアップできます。IdM のユーザー、および可能であれば、信頼された Active Directory (AD) ドメインのユーザーは、Samba が提供する共有およびプリンターサービスにアクセスできます。

重要

IdM ドメインメンバーで Samba を使用する機能は、テクノロジープレビュー機能で、特定の制限が含まれています。たとえば、IdM 信頼コントローラーは Active Directory グローバルカタログサービスをサポートしておらず、分散コンピューティング環境/リモートプロシージャコール (DCE/RPC) プロトコルを使用した IdM グループの解決をサポートしていません。結果として、AD ユーザーは、他の IdM クライアントにログインしている場合、IdM クライアントでホストされている Samba 共有とプリンターにのみアクセスできます。Windows マシンにログインしている AD ユーザーは、IdM ドメインメンバーでホストされている Samba 共有にアクセスできません。

IdM ドメインメンバーに Samba をデプロイしているお客様は、ぜひ Red Hat にフィードバックをお寄せください。

AD ドメインのユーザーが Samba によって提供される共有およびプリンターサービスにアクセスする必要がある場合は、AES 暗号化タイプが AD になっていることを確認してください。詳細は、[GPO を使用した Active Directory での AES 暗号化タイプの有効化](#) を参照してください。

前提条件

- ホストは、クライアントとして IdM ドメインに参加している。
- IdM サーバーとクライアントの両方が RHEL 9.0 以降で実行されている必要がある。

1.6.1. Samba をドメインメンバーにインストールするための IdM ドメインの準備

IdM クライアントに Samba を設定する前に、IdM サーバーで `ipa-adtrust-install` ユーティリティーを使用して IdM ドメインを準備する必要があります。



注記

ipa-adtrust-install コマンドを自動的に実行するシステムは、AD 信頼コントローラーになります。ただし、**ipa-adtrust-install** は、IdM サーバーで1回のみ実行する必要があります。

前提条件

- IdM サーバーがインストールされている。
- パッケージをインストールし、IdM サービスを再起動するには、root 権限が必要です。

手順

1. 必要なパッケージをインストールします。

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

2. IdM 管理ユーザーとして認証します。

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

3. **ipa-adtrust-install** ユーティリティーを実行します。

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

統合 DNS サーバーとともに IdM がインストールされていると、DNS サービスレコードが自動的に作成されます。

IdM が統合 DNS サーバーなしで IdM をインストールすると、**ipa-adtrust-install** は、続行する前に DNS に手動で追加する必要があるサービスレコードのリストを出力します。

4. スクリプトにより、**/etc/samba/smb.conf** がすでに存在し、書き換えられることが求められます。

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

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

5. このスクリプトは、従来の Linux クライアントが信頼できるユーザーと連携できるようにする互換性プラグインである **slapi-nis** プラグインを設定するように求めるプロンプトを表示します。

```
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. SID 生成タスクを実行して、既存ユーザーに SID を作成するように求められます。

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

これはリソースを集中的に使用するタスクであるため、ユーザー数が多い場合は別のタイミングで実行できます。

7. (必要に応じて) デフォルトでは、Windows Server 2008 以降での動的 RPC ポートの範囲は **49152-65535** として定義されます。ご使用の環境に異なる動的 RPC ポート範囲を定義する必要がある場合は、Samba が異なるポートを使用するように設定し、ファイアウォール設定でそのポートを開くように設定します。以下の例では、ポート範囲を **55000-65000** に設定します。

```
[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. ipa サービスを再起動します。

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

9. smbclient ユーティリティーを使用して、Samba が IdM からの Kerberos 認証に応答することを確認します。

```
[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. IdM クライアントでの Samba サーバーのインストールおよび設定

IdM ドメインに登録されたクライアントに Samba をインストールして設定できます。

前提条件

- IdM サーバーとクライアントの両方が RHEL 9.0 以降で実行されている必要がある。
- IdM ドメインは、[ドメインメンバーに Samba をインストールするための IdM ドメインの準備](#)の説明に従って準備されます。
- IdM に AD で設定された信頼がある場合は、Kerberos の AES 暗号化タイプを有効にします。たとえば、[グループポリシーオブジェクト \(GPO\) を使用して、AES 暗号化の種類を有効にします](#)。詳細は、[GPO を使用した Active Directory での AES 暗号化の有効化](#) を参照してください。

手順

1. ipa-client-samba パッケージをインストールします。

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

2. ipa-client-samba ユーティリティーを使用して、クライアントを準備し、初期 Samba 設定を作成します。

```
[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

```

- デフォルトでは、**ipa-client-samba** は、ユーザーが接続したときにそのユーザーのホームディレクトリーを動的に共有するために、**/etc/samba/smb.conf** ファイルに **[homes]** セクションが自動的に追加されます。ユーザーがこのサーバーにホームディレクトリーがない場合、または共有したくない場合は、**/etc/samba/smb.conf** から次の行を削除します。

```

[homes]
read only = no

```

- ディレクトリーとプリンターを共有します。詳細は、以下を参照してください。
 - [POSIX ACL を使用した Samba ファイル共有の設定](#)
 - [Windows ACL で共有の設定](#)
 - [プリントサーバーとしての Samba の設定](#)
- ローカルファイアウォールで Samba クライアントに必要なポートを開きます。

```

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

```

- smb** サービスおよび **winbind** サービスを有効にして開始します。

```

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

```

検証手順

samba-client パッケージがインストールされている別の IdM ドメインメンバーで次の検証手順を実行します。

- Kerberos 認証を使用して、Samba サーバー上の共有をリスト表示します。

```

$ 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)
...

```

関連情報

- `ipa-client-samba(1)` の man ページ

1.6.3. IdM が新しいドメインを信頼する場合は、ID マッピング設定を手動で追加

Samba では、ユーザーがリソースにアクセスする各ドメインの ID マッピング設定が必要です。IdM クライアントで実行している既存の Samba サーバーでは、管理者が Active Directory (AD) ドメインに新しい信頼を追加した後、ID マッピング設定を手動で追加する必要があります。

前提条件

- IdM クライアントで Samba を設定している。その後、IdM に新しい信頼が追加されている。
- Kerberos の暗号化タイプ DES および RC4 は、信頼できる AD ドメインで無効にしている。セキュリティ上の理由から、RHEL 9 はこのような弱い暗号化タイプに対応していません。

手順

1. ホストのキータブを使用して認証します。

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

2. `ipa idrange-find` コマンドを使用して、新しいドメインのベース ID と ID 範囲のサイズの両方を表示します。たとえば、次のコマンドは `ad.example.com` ドメインの値を表示します。

```

[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
-----

```

次の手順で、`ipabaseid` 属性および `ipaidrangesize` 属性の値が必要です。

3. 使用可能な最高の ID を計算するには、次の式を使用します。

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

前の手順の値を使用すると、**ad.example.com** ドメインで使用可能な最大 ID は **1918599999** (1918400000 + 200000 - 1) です。

4. **/etc/samba/smb.conf** ファイルを編集し、ドメインの ID マッピング設定を **[global]** セクションに追加します。

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

ipabaseid 属性の値を最小値として指定し、前の手順で計算された値を範囲の最大値として指定します。

5. **smb** サービスおよび **winbind** サービスを再起動します。

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

検証手順

- Kerberos 認証を使用して、Samba サーバー上の共有をリスト表示します。

```
$ 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. 関連情報

- [Installing an Identity Management client](#)

1.7. POSIX ACL を使用した SAMBA ファイル共有の設定

Samba は、Linux サービスとして、POSIX ACL との共有に対応します。**chmod** などのユーティリティーを使用して、Samba サーバーの権限をローカルに管理できます。拡張属性に対応するファイルシステムに共有が保存されている場合は、複数のユーザーおよびグループで ACL を定義できます。



注記

代わりにきめ細かい Windows ACL を使用する必要がある場合は、[Windows ACL を使用する共有の設定](#) を参照してください。

このセクションの一部は、Samba Wiki に公開されているドキュメント [Setting up a Share Using POSIX ACLs](#) に掲載されています。ライセンスは、[CC BY 4.0](#) にあります。著者および貢献者は、Wiki ページの [history](#) タブを参照してください。

1.7.1. POSIX ACL を使用する共有の追加

/srv/samba/example/ ディレクトリーのコンテンツを提供し、POSIX ACL を使用する **example** という名前の共有を作成できます。

前提条件

Samba が、以下のいずれかのモードで設定されている。

- [スタンドアロンサーバー](#)
- [ドメインメンバー](#)

手順

1. ディレクトリが存在しない場合は作成します。以下に例を示します。

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

2. SELinux を、**enforcing** モードで実行する場合は、そのディレクトリに **samba_share_t** コンテキストを設定します。

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

3. ディレクトリにファイルシステムの ACL を設定します。詳細は、以下を参照してください。

- [POSIX ACL を使用する Samba 共有での標準的な ACL の設定](#)
- [POSIX ACL を使用する Samba 共有で拡張 ACL の設定](#)

4. **/etc/samba/smb.conf** ファイルにサンプル共有を追加します。たとえば、共有の write-enabled を追加するには、次のコマンドを実行します。

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



注記

ファイルシステムの ACL に関係なく、**read only = no** を設定しないと、Samba がディレクトリを読み取り専用モードで共有します。

5. **/etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

6. **firewall-cmd** ユーティリティーを使用して必要なポートを開き、ファイアウォール設定を再読み込みします。

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

7. **smb** サービスを再起動します。

```
# systemctl restart smb
```

1.7.2. POSIX ACL を使用する Samba 共有での標準的な Linux ACL の設定

Linux の標準 ACL は、所有者、グループ、その他の未定義ユーザーの権限の設定に対応します。ユーティリティの **chown**、**chgrp**、および **chmod** を使用して ACL を更新できます。正確な制御が必要な場合は、より複雑な POSIX ACL を使用します。以下を参照してください。

[Setting extended ACLs on a Samba share that uses POSIX ACLs](#) .

以下の手順では、**/srv/samba/example/** ディレクトリーの所有者を **root** ユーザーに設定し、**Domain Users** グループに読み取りおよび書き込みの権限を付与して、他のすべてのユーザーのアクセスを拒否します。

前提条件

- ACL を設定する Samba 共有がある。

手順

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



注記

ディレクトリーで set-group-ID (SGID) ビットを有効にすると、新しいディレクトリーエントリーを作成したユーザーのプライマリーグループに設定する通常の動作の代わりに、すべての新しいファイルとサブディレクトリーのデフォルトグループが、そのディレクトリーグループのデフォルトグループに自動的に設定されます。

関連情報

- **chown(1)** および **chmod(1)** の man ページ

1.7.3. POSIX ACL を使用する Samba 共有での拡張 ACL の設定

共有ディレクトリーが保存されているファイルシステムが拡張 ACL に対応している場合は、それを使用して複雑な権限を設定できます。拡張 ACL には、複数のユーザーおよびグループの権限を指定できます。

拡張 POSIX ACL を使用すると、複数のユーザーおよびグループで複雑な ACL を設定できます。ただし、設定できるのは以下の権限のみです。

- アクセスなし
- 読み取りアクセス
- 書き込みアクセス
- 完全な制御

フォルダーの作成やデータの追加 など、詳細な Windows 権限が必要な場合は、Windows ACL を使用するように共有を設定します。

Windows ACL で共有の設定

以下の手順では、共有で拡張 ACL を有効にする方法を説明します。また、拡張 ACL の設定例も含まれています。

前提条件

- ACL を設定する Samba 共有がある。

手順

1. `/etc/samba/smb.conf` ファイルの共有セクションで以下のパラメーターを有効にして、拡張 ACL の ACL 継承を有効にします。

```
inherit acls = yes
```

詳細は、man ページの `smb.conf(5)` のパラメーターの説明を参照してください。

2. `smb` サービスを再起動します。

```
# systemctl restart smb
```

3. ディレクトリーの ACL を設定します。以下に例を示します。

例1.2 拡張 ACL の設定

以下の手順は、`/srv/samba/example/` ディレクトリーに対して、**Domain Admins** グループに読み取り、書き込み、および実行の権限、**Domain Users** グループに対する読み取りおよび実行の権限を設定し、その他の全員のアクセスを拒否します。

1. ユーザーアカウントのプライマリーグループへの自動許可権限を無効にします。

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

ディレクトリーのプライマリーグループは、さらに動的な **CREATOR GROUP** プリンシパルにマッピングされます。Samba 共有で拡張 POSIX ACL を使用すると、このプリンシパルは自動的に追加され、削除できません。

2. ディレクトリーに権限を設定します。

- a. **Domain Admins** グループに読み取り、書き込み、および実行の権限を付与します。

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

- b. **Domain Users** グループに読み取りおよび実行の権限を付与します。

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

- c. **その他** の ACL エントリーに権限を設定し、その他の ACL エントリーに一致しないユーザーへのアクセスを拒否します。

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

この設定は、このディレクトリーにのみ適用されます。Windows では、これらの ACL は **このフォルダーのみ** のモードにマッピングされます。

3. 前の手順で設定した権限を、このディレクトリーに作成した新規ファイルシステムのオブジェクトから継承できるようにするには、以下のコマンドを実行します。

```
# 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/
```

この設定では、プリンシパルのこのフォルダーのみモードが、このフォルダー、サブフォルダー、およびファイルに設定されます。

Samba は、手順に設定されている権限を、以下の Windows ACL にマッピングします。

プリンシパル	アクセス	適用先
Domain\Domain Admins	完全な制御	このフォルダー、サブフォルダー、およびファイル
Domain\Domain Users	読み取りおよび実行	このフォルダー、サブフォルダー、およびファイル
Everyone ^[a]	なし	このフォルダー、サブフォルダー、およびファイル
owner (Unix User\owner) ^[b]	完全な制御	このフォルダーのみ
primary_group (Unix User\primary_group) ^[c]	なし	このフォルダーのみ
CREATOR OWNER ^{[d][e]}	完全な制御	サブフォルダーおよびファイルのみ
CREATOR GROUP ^{[e][f]}	なし	サブフォルダーおよびファイルのみ

[a] Samba は、このプリンシパルの権限を **その他** の ACL エントリーからマッピングします。

[b] Samba は、ディレクトリーの所有者をこのエントリーにマッピングします。

[c] Samba は、ディレクトリーのプライマリーグループをこのエントリーにマッピングします。

[d] 新規ファイルシステムオブジェクトでは、作成者はこのプリンシパルの権限を自動的に継承します。

[e] POSIX ACL を使用する共有では、このプリンシパルの設定または削除には対応していません。

[f] 新規ファイルシステムオブジェクトの場合、作成者のプライマリーグループは、自動的にこのプリンシパルの権限を継承します。

1.8. POSIX ACL を使用する共有への権限の設定

必要に応じて、Samba 共有へのアクセスを制限または許可するには、`/etc/samba/smb.conf` ファイルの共有のセクションに特定のパラメーターを設定します。



注記

共有ベースの権限は、ユーザー、グループ、またはホストが共有にアクセスできるかどうかを管理します。この設定は、ファイルシステムの ACL には影響しません。

共有ベースの設定を使用して共有へのアクセスを制限します。たとえば、特定のホストからのアクセスを拒否します。

前提条件

- POSIX ACL との共有が設定されている。

1.8.1. ユーザーおよびグループに基づいた共有アクセスの設定

ユーザーおよびグループに基づいたアクセス制御により、特定のユーザーおよびグループの共有へのアクセスを許可または拒否できます。

前提条件

- ユーザーまたはグループベースのアクセスを設定する Samba 共有がある。

手順

1. たとえば、**Domain Users** グループの全メンバーが、**ユーザー** アカウントのアクセスが拒否されている時に共有にアクセスできるようにするには、共有の設定に以下のパラメーターを追加します。

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

無効なユーザー パラメーターの優先度は、**有効なユーザー** パラメーターよりも高くなります。たとえば、**ユーザー** アカウントが **Domain Users** グループのメンバーである場合に上述の例を使用すると、このアカウントへのアクセスは拒否されます。

2. Samba 設定を再読み込みします。

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

関連情報

- **smb.conf(5)** man ページ

1.8.2. ホストベースの共有アクセスの設定

ホストベースのアクセス制御により、クライアントのホスト名、IP アドレス、または IP 範囲に基づいて、共有へのアクセスを許可または拒否できます。

以下の手順では、IP アドレスの **127.0.0.1**、IP 範囲の **192.0.2.0/24**、およびホストの **client1.example.com** を有効にして共有にアクセスする方法と、**client2.example.com** ホストへのアクセスを拒否する方法を説明します。

前提条件

- ホストベースのアクセスを設定する Samba 共有がある。

手順

1. 以下のパラメーターを、`/etc/samba/smb.conf` ファイルの共有の設定に追加します。

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

hosts deny パラメーターは、**hosts allow** よりも優先順位が高くなります。たとえば、**client1.example.com** が **hosts allow** パラメーターにリスト表示されている IP アドレスに解決すると、このホストへのアクセスは拒否されます。

2. Samba 設定を再読み込みします。

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

関連情報

- [smb.conf\(5\) man ページ](#)

1.9. WINDOWS ACL で共有の設定

Samba は、共有およびファイルシステムオブジェクトへの Windows ACL の設定に対応します。これを使用すると、以下が可能になります。

- きめ細かな Windows ACL を使用する
- Windows を使用して共有権限およびファイルシステムの ACL を管理する

または、POSIX ACL を使用するよう共有を設定することもできます。

詳細は、[POSIX ACL を使用する Samba ファイル共有の設定](#) を参照してください。

このセクションの一部は、Samba Wiki に公開されているドキュメント [Setting up a Share Using Windows ACLs](#) に掲載されています。ライセンスは、[CC BY 4.0](#) にあります。著者および貢献者は、Wiki ページの [history](#) タブを参照してください。

1.9.1. SeDiskPrivilege 特権の付与

Windows ACL を使用する共有に対する権限を設定できるのは、**SeDiskOperatorPrivilege** 特権が付与されているユーザーおよびグループのみです。

手順

1. たとえば、**SeDiskOperatorPrivilege** 特権を **DOMAIN\Domain Admins** グループに付与するには、以下のコマンドを実行します。

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



注記

ドメイン環境では、**SeDiskOperatorPrivilege** をドメイングループに付与します。これにより、ユーザーのグループメンバーシップを更新し、権限を集中的に管理できます。

2. **SeDiskOperatorPrivilege** が付与されているすべてのユーザーおよびグループをリスト表示するには、以下のコマンドを実行します。

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

1.9.2. Windows ACL サポートの有効化

Windows ACL に対応する共有を設定するには、Samba でこの機能を有効にする必要があります。

前提条件

- ユーザー共有が Samba サーバーに設定されている。

手順

1. すべての共有に対してグローバルに有効にするには、次の設定を `/etc/samba/smb.conf` ファイルの `[global]` セクションに追加します。

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

または、共有のセクションに同じパラメーターを追加して、個別の共有に対して Windows ACL サポートを有効にできます。

2. **smb** サービスを再起動します。

```
# systemctl restart smb
```

1.9.3. Windows ACL を使用する共有の追加

`/srv/samba/example/` ディレクトリーのコンテンツを共有し、Windows ACL を使用する **example** という名前の共有を作成できます。

手順

1. ディレクトリーが存在しない場合は作成します。以下に例を示します。

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

2. SELinux を、**enforcing** モードで実行する場合は、そのディレクトリーに **samba_share_t** コンテキストを設定します。

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

3. `/etc/samba/smb.conf` ファイルにサンプル共有を追加します。たとえば、共有の `write-enabled` を追加するには、次のコマンドを実行します。

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



注記

ファイルシステムの ACL に関係なく、**read only = no** を設定しないと、Samba がディレクトリーを読み取り専用モードで共有します。

4. すべての共有の **[global]** セクションで Windows ACL サポートを有効にしていない場合は、以下のパラメーターを **[example]** セクションに追加して、この共有に対してこの機能を有効にします。

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

5. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

6. `firewall-cmd` ユーティリティーを使用して必要なポートを開き、ファイアウォール設定を再読み込みします。

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

7. `smb` サービスを再起動します。

```
# systemctl restart smb
```

1.9.4. Windows ACL を使用する共有の共有権限とファイルシステム ACL の管理

Windows ACL を使用する Samba 共有で共有権限およびファイルシステムの ACL を管理するには、**コンピューターの管理** などの Windows アプリケーションを使用します。詳細は、Windows のドキュメントを参照してください。または、**smbcacls** ユーティリティーを使用して ACL を管理します。



注記

Windows からファイルシステムの権限を変更するには、**SeDiskOperatorPrivilege** 権限が付与されたアカウントを使用する必要があります。

関連情報

- [smbcacls で SMB 共有上の ACL の管理](#)

- [SeDiskOperatorPrivilege 特権の付与](#)

1.10. SMBCACLS で SMB 共有上の ACL の管理

smbcacls ユーティリティは、SMB 共有に保存されたファイルおよびディレクトリーの ACL をリスト表示、設定、および削除できます。**smbcacls** を使用して、ファイルシステムの ACL を管理できます。

- 高度な Windows ACL または POSIX ACL を使用するローカルまたはリモートの Samba サーバー
- Red Hat Enterprise Linux で、Windows でホストされる共有の ACL をリモートで管理

1.10.1. アクセス制御エントリー

ファイルシステムオブジェクトの各 ACL エントリーには、以下の形式のアクセス制御エントリー (ACE) が含まれます。

```
security_principal:access_right/inheritance_information/permissions
```

例1.3 アクセス制御エントリー

AD\Domain Users グループに、Windows 上の **このフォルダー、サブフォルダー、およびファイル** に適用される **変更** 権限がある場合、ACL には以下の ACE が含まれます。

```
AD\Domain Users:ALLOWED/OI|CI/CHANGE
```

ACE には、以下が含まれます。

セキュリティープリンシパル

セキュリティープリンシパルは、ACL の権限が適用されるユーザー、グループ、または SID です。

アクセス権

オブジェクトへのアクセスが許可または拒否されるかどうかを定義します。値は **ALLOWED** または **DENIED** です。

継承情報

次の値を取ります。

表1.1 継承の設定

値	詳細	マップ先
OI	オブジェクトの継承	このフォルダーおよびファイル
CI	コンテナの継承	このフォルダーおよびサブフォルダー
IO	継承のみ	ACE は、現在のファイルまたはディレクトリーには適用されません。
ID	継承済	親ディレクトリーから ACE が継承されました。

また、値は以下のように組み合わせることができます。

表1.2 継承設定の組み合わせ

値の組み合わせ	Windows の適用先 設定にマップします。
O C I	このフォルダー、サブフォルダー、およびファイル
O C I IO	サブフォルダーおよびファイルのみ
C I IO	サブディレクトリーのみ
O I IO	ファイルのみ

権限

この値は、Windows の権限または **smbcacls** エイリアスを表す 16 進値になります。

- 1つ以上の Windows の権限を表す 16 進値。
次の表に、Windows の高度な権限とそれに対応する値を 16 進法で表示します。

表1.3 Windows の権限とそれに対応する smbcacls 値を 16 進法で設定

Windows の権限	16 進値
完全な制御	0x001F01FF
フォルダーのスキャンおよびファイルの実行	0x00100020
フォルダーのリスト表示 / データの読み取り	0x00100001
属性の読み取り	0x00100080
拡張属性の読み取り	0x00100008
ファイルの作成/データの書き込み	0x00100002
フォルダーの作成/データの追加	0x00100004
属性の書き込み	0x00100100
拡張属性の書き込み	0x00100010
サブフォルダーおよびファイルの削除	0x00100040
削除	0x00110000
権限の読み取り	0x00120000

Windows の権限	16 進値
権限の変更	0x00140000
所有権の取得	0x00180000

ビット単位の **OR** 演算を使用すると、複数の権限を1つの16進値として組み合わせることができます。

詳細は、[ACE マスク計算](#) を参照してください。

- **smbcacls** エイリアス。以下の表には、利用可能なエイリアスが表示されます。

表1.4 既存の smbcacls エイリアスとそれに対応する Windows の権限

smbcacls エイリアス	Windows の権限へのマッピング
-R	読み取り
READ	読み取りおよび実行
W	主な機能: <ul style="list-style-type: none"> ○ ファイルの作成/データの書き込み ○ フォルダーの作成/データの追加 ○ 属性の書き込み ○ 拡張属性の書き込み ○ 権限の読み取り
D	削除
%P	権限の変更
O	所有権の取得
X	スキャン / 実行
CHANGE	修正
FULL	完全な制御



注記

権限を設定する際に、1文字のエイリアスを組み合わせることができます。たとえば、Windows の権限の **Read** および **Delete** を適用するように **RD** を設定できます。ただし、1文字以外のエイリアスを複数組み合わせたり、エイリアスと 16 進値を組み合わせることはできません。

1.10.2. smbcacls を使用した ACL の表示

SMB 共有で ACL を表示するには、**smbcacls** ユーティリティを使用します。**--add** などの操作パラメーターを付けずに **smbcacls** を実行すると、ユーティリティは、ファイルシステムオブジェクトの ACL を表示します。

手順

たとえば、**//server/example** 共有のルートディレクトリーの ACL をリスト表示するには、以下のコマンドを実行します。

```
# 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
```

コマンドの出力は以下のようになります。

- **REVISION** - セキュリティー記述子の内部 Windows NT ACL リビジョン
- **CONTROL** - セキュリティー記述子の制御
- **OWNER** - セキュリティー記述子の所有者の名前または SID
- **GROUP** - セキュリティー記述子のグループの名前または SID
- **ACL** エントリー。詳細は、[アクセス制御エントリー](#) を参照してください。

1.10.3. ACE マスク計算

ほとんどの場合、ACE を追加または更新するときは、[既存の smbcacls エイリアスとそれに対応する Windows アクセス許可](#)に リストされている **smbcacls** エイリアスを使用します。

ただし、Windows の権限と [それに対応する smbcacls 値](#)を 16 進法でリストしたように高度な Windows の権限を設定する場合は、ビット単位の **OR** 操作を使用して正しい値を計算する必要があります。以下のシェルコマンドを使用して値を計算できます。

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

例1.4 ACE マスクの計算

以下の権限を設定します。

- フォルダースキャン / ファイルの実行 (0x00100020)
- フォルダースキャン / データの読み取り (0x00100001)
- 属性の読み取り (0x00100080)

以前の権限の 16 進値を計算するには、以下を入力します。

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

ACE を設定または更新する場合は、戻り値を使用します。

1.10.4. smbcacls を使用した ACL の追加、更新、および削除

smbcacls ユーティリティに渡すパラメーターに応じて、ファイルまたはディレクトリーから ACL を追加、更新、および削除できます。

ACL の追加

このフォルダー、サブフォルダー、およびファイルの **CHANGE** 権限を **AD\Domain Users** グループに付与する **//server/example** 共有のルートに ACL を追加するには、以下のコマンドを実行します。

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

ACL の更新

ACL の更新は、新しい ACL の追加に似ています。ACL を更新する場合は、**--modify** パラメーターと既存のセキュリティプリンシパルを使用して ACL を上書きします。**smbcacls** が ACL リスト内でセキュリティプリンシパルを検出すると、ユーティリティは権限を更新します。これを行わないと、以下のエラーでコマンドが失敗します。

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

たとえば、**AD\Domain Users** グループの権限を更新し、このフォルダー、サブフォルダー、およびファイルの **READ** に設定するには、以下のコマンドを実行します。

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

ACL の削除

ACL を削除するには、正確な ACL を持つ **--delete** パラメーターを **smbcacls** ユーティリティに渡します。以下に例を示します。

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

1.11. ユーザーが SAMBA サーバーのディレクトリーを共有できるようにする

Samba サーバーでは、root 権限なしでユーザーがディレクトリーを共有できるように設定できます。

1.11.1. ユーザーの共有機能の有効化

ユーザーがディレクトリーを共有できるようにするには、管理者が Samba でユーザー共有を有効にする必要があります。

たとえば、ローカルの **example** グループのメンバーのみがユーザー共有を作成できるようにするには、以下を実行します。

手順

1. ローカルの **example** グループが存在しない場合は作成します。

```
# groupadd example
```

2. ユーザー共有の定義を保存し、その権限を正しく設定するために、Samba 用のディレクトリーを準備します。以下に例を示します。

- a. ディレクトリーを作成します。

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

- b. **example** グループの書き込み権限を設定します。

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

- c. このディレクトリーの他のユーザーが保存したファイルの名前変更や削除を禁止するように sticky ビットを設定します。

3. **/etc/samba/smb.conf** ファイルを編集し、以下を **[global]** セクションに追加します。

- a. ユーザー共有の定義を保存するように設定したディレクトリーのパスを設定します。以下に例を示します。

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

- b. このサーバーで Samba を作成できるユーザー共有の数を設定します。以下に例を示します。

```
usershare max shares = 100
```

usershare max shares パラメーターにデフォルトの **0** を使用すると、ユーザー共有が無効になります。

- c. 必要に応じて、ディレクトリーの絶対パスのリストを設定します。たとえば、Samba が **/data** ディレクトリーおよび **/srv** ディレクトリーのサブディレクトリーの共有のみを許可するように設定するには、以下を設定します。

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

設定可能なユーザー共有関連のパラメーターのリストは、man ページの **smb.conf(5)** の **USERSHARES** セクションを参照してください。

4. **/etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

5. Samba 設定を再読み込みします。

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

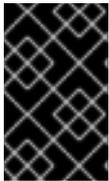
これで、ユーザーが、ユーザー共有を作成できるようになりました。

1.11.2. ユーザー共有の追加

Samba でユーザー共有機能を有効にすると、ユーザーは **net usershare add** コマンドを実行して、**root** 権限なしで Samba サーバーのディレクトリーを共有できます。

net usershare add コマンドの構文:

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



重要

ユーザー共有の作成時に ACL を設定する場合は、ACL の前に comment パラメーターを指定する必要があります。空のコメントを設定するには、空の文字列を二重引用符で囲みます。

管理者が、**/etc/samba/smb.conf** ファイルの **[global]** セクションで **usershare allow guests = yes** に設定すると、ユーザーはユーザー共有上でのみゲストアクセスを有効にできることに注意してください。

例1.5 ユーザー共有の追加

ユーザーが、Samba サーバーで **/srv/samba/** ディレクトリーを共有する場合があります。共有には、**example** という名前を付け、コメントを設定しないようにし、ゲストユーザーがアクセスできるようにします。また、共有権限は、**AD\Domain Users** グループへのフルアクセスと、その他のユーザーへの読み取り権限を設定する必要があります。この共有を追加するには、そのユーザーで以下を実行します。

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

1.11.3. ユーザー共有の設定の更新

ユーザー共有の設定を更新するには、同じ共有名と新しい設定で **net usershare add** コマンドを使用して共有を上書きします。

[ユーザー共有の追加](#) を参照します。

1.11.4. 既存のユーザー共有に関する情報の表示

ユーザーは、Samba サーバーで **net usershare info** コマンドを実行して、ユーザーの共有および設定を表示できます。

前提条件

- ユーザー共有が Samba サーバーに設定されている。

手順

1. 任意のユーザーが作成したすべてのユーザー共有を表示するには、以下のコマンドを実行します。

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

コマンドを実行するユーザーが作成した共有のみをリスト表示するには、**-l** パラメーターを省略します。

2. 特定の共有に関する情報のみを表示するには、共有名またはワイルドカードをコマンドに渡します。たとえば、名前が **share_** で始まる共有の情報を表示する場合は、以下のコマンドを実行します。

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

1.11.5. ユーザー共有のリスト表示

Samba サーバーで設定を行わずに利用可能なユーザー共有のみをリスト表示するには、**net usershare list** コマンドを使用します。

前提条件

- ユーザー共有が Samba サーバーに設定されている。

手順

1. 任意のユーザーが作成した共有をリスト表示するには、以下のコマンドを実行します。

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

コマンドを実行するユーザーが作成した共有のみをリスト表示するには、**-l** パラメーターを省略します。

2. 特定の共有のみをリスト表示するには、共有名またはワイルドカードをコマンドに渡します。たとえば、名前が **share_** で始まる共有のみをリスト表示するには、以下のコマンドを実行します。

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

1.11.6. ユーザー共有の削除

ユーザー共有を削除するには、共有を作成したユーザーまたは **root** ユーザーで、**net usershare delete** コマンドを実行します。

前提条件

- ユーザー共有が Samba サーバーに設定されている。

手順

```
$ net usershare delete share_name
```

1.12. 認証なしでアクセスを許可する共有の設定

特定の状況では、認証なしでユーザーが接続できるディレクトリーを共有します。これを設定するには、共有でゲストアクセスを有効にします。



警告

共有に認証を使用しないと、セキュリティリスクとなる場合があります。

1.12.1. 共有へのゲストアクセスの有効化

共有でゲストアクセスが有効になっている場合、Samba はゲスト接続を、**guest account** パラメーターで設定したオペレーティングシステムアカウントにマッピングします。少なくとも以下のいずれかの条件が満たされると、ゲストユーザーはこの共有のファイルにアクセスできます。

- アカウントがファイルシステムの ACL にリスト表示されます。
- その他 のユーザーの POSIX 権限はこれを許可します。

例1.6 ゲスト共有の権限

ゲストアカウントを **nobody** (デフォルト) にマッピングするように Samba を設定している場合は、下記の例の ACL が、以下を行うようになります。

- ゲストユーザーが **file1.txt** の読み込みを許可する
- ゲストユーザーによる **file2.txt** の読み込みおよび修正を許可する
- ゲストユーザーが **file3.txt** を読み込んだり修正しないようにする

```
-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
```

手順

1. **/etc/samba/smb.conf** ファイルを編集します。
 - a. これが、このサーバーで設定した最初のゲスト共有である場合は、以下を行います。

- i. **[global]** セクションに **map to guest = Bad User** を設定します。

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

この設定により、ユーザー名が存在しない限り、Samba は間違ったパスワードを使用したログイン試行を拒否します。指定したユーザー名がなく、ゲストアクセスが共有で有効になっている場合、Samba は接続をゲストのログインとして処理します。

- ii. デフォルトでは、Samba は、Red Hat Enterprise Linux の **nobody** アカウントにゲストアカウントをマッピングします。または、別のアカウントを設定することもできます。以下に例を示します。

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

このパラメーターに設定するアカウントは、Samba サーバーにローカルに存在する必要があります。セキュリティ上の理由から、Red Hat は有効なシェルを割り当てていないアカウントを使用することを推奨しています。

- b. **guest ok = yes** の設定を、**[example]** 共有セクションに追加します。

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

2. **/etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

3. Samba 設定を再読み込みします。

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

1.13. MACOS クライアント向けの SAMBA の設定

fruit 仮想ファイルシステム (VFS) の Samba モジュールは、Apple サーバーメッセージブロック (SMB) クライアントとの互換性を強化します。

1.13.1. MacOS クライアントにファイル共有を提供する Samba 設定の最適化

fruit モジュールは、Samba の MacOS クライアントとの互換性を強化します。Samba サーバーでホストされているすべての共有に対してモジュールを設定して、MacOS クライアント向けにファイル共有を最適化できます。



注記

fruit モジュールをシステム全体で有効にします。MacOS を使用するクライアントは、クライアントがサーバーへの最初の接続を確立する時に、サーバーメッセージブロックバージョン 2 (SMB2) Apple (AAPL) プロトコル拡張をネゴシエートします。クライアントが最初に AAPL 拡張機能を有効にせずに共有に接続すると、クライアントはサーバーの共有に拡張機能を使用しません。

前提条件

- Samba が、ファイルサーバーとして設定されている。

手順

1. `/etc/samba/smb.conf` ファイルを編集し、**[global]** セクションの VFS モジュール **fruit** および **streams_xattr** を有効にします。

```
vfs objects = fruit streams_xattr
```



重要

streams_xattr を有効にする前に、**fruit** モジュールを有効にする必要があります。**fruit** モジュールは、別のデータストリーム (ADS) を使用します。このため、**streams_xattr** モジュールも有効にする必要があります。

2. 必要に応じて、共有で macOS Time Machine のサポートを提供する場合は、`/etc/samba/smb.conf` ファイルの共有設定に次の設定を追加します。

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

3. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

4. Samba 設定を再読み込みします。

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

関連情報

- [vfs_fruit\(8\) の man ページ](#)
- ファイル共有の設定
 - [POSIX ACL を使用した Samba ファイル共有の設定](#)
 - [Windows ACL を使用する共有の設定](#)

1.14. SMBCLIENT ユーティリティーを使用した SMB 共有へのアクセス

smbclient ユーティリティーを使用すると、コマンドラインの FTP クライアントと同様に、SMB サーバーのファイル共有にアクセスできます。たとえば、ファイルを共有にアップロードしたり、共有からダウンロードしたりできます。

前提条件

- **samba-client** パッケージがインストールされている。

1.14.1. smbclient 対話モードの動作

たとえば、**DOMAIN\user** アカウントを使用して **サーバー** でホストされる **example** 共有に認証するには、以下のコマンドを実行します。

```
# smbclient -U "DOMAIN\user" //server/example
Enter domain\user's password:
Try "help" to get a list of possible commands.
smb: \>
```

smbclient が共有に正常に接続すると、ユーティリティーはインタラクティブモードになり、以下のプロンプトが表示されます。

```
smb: \>
```

対話式シェルで利用可能なすべてのコマンドを表示するには、以下のコマンドを実行します。

```
smb: \> help
```

特定のコマンドのヘルプを表示するには、以下のコマンドを実行します。

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

関連情報

- **smbclient(1)** man ページ

1.14.2. 対話モードでの smbclient の使用

-c パラメーターを指定せずに **smbclient** を使用すると、ユーティリティーは対話モードを開始します。以下の手順では、SMB 共有に接続し、サブディレクトリーからファイルをダウンロードする方法を説明します。

手順

1. 共有に接続します。

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

2. **/example/** ディレクトリーに移動します。

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

3. ディレクトリー内のファイルをリスト表示します。

```
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. **example.txt** ファイルをダウンロードします。

```
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. 共有から切断します。

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

1.14.3. スクリプトモードでの **smbclient** の使用

-c パラメーターを **smbclient** に渡すと、リモートの SMB 共有でコマンドを自動的に実行できます。これにより、スクリプトで **smbclient** を使用できます。

以下の手順では、SMB 共有に接続し、サブディレクトリーからファイルをダウンロードする方法を説明します。

手順

- 以下のコマンドで共有に接続して **example** ディレクトリーに移動し、**example.txt** ファイルをダウンロードします。

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

1.15. プリントサーバーとしての SAMBA の設定

Samba をプリントサーバーとして設定すると、ネットワーク上のクライアントが Samba を使用して印刷できます。さらに、Windows クライアントは、(Samba サーバーが設定されている場合は) Samba サーバーからドライバーをダウンロードすることもできます。

このセクションの一部は、Samba Wiki に公開されているドキュメント [Setting up Samba as a Print Server](#) に掲載されています。ライセンスは、[CC BY 4.0](#) にあります。著者および貢献者は、Wiki ページの [history](#) タブを参照してください。

前提条件

Samba が、以下のいずれかのモードで設定されている。

- [スタンドアロンサーバー](#)
- [ドメインメンバー](#)

1.15.1. Samba でのプリントサーバーのサポートの有効化

デフォルトでは、プリントサーバーサポートは Samba で有効になっていません。Samba をプリントサーバーとして使用するには、Samba を適切に設定する必要があります。



注記

印刷ジョブとプリンター操作には、リモートプロシージャコール (RPC) が必要です。デフォルトでは、Samba は RPC を管理するためにオンデマンドで **rpcd_spoolss** サービスを開始します。最初の RPC 呼び出し中、または CUPS でプリンターリストを更新するときに、Samba は CUPS からプリンター情報を取得します。これには、プリンターごとに約 1 秒かかる場合があります。そのため、プリンターが 50 台を超える場合は、**rpcd_spoolss** 設定を調整してください。

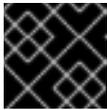
前提条件

- プリンターが CUPS サーバーで設定されている。
CUPS でプリンターを設定する方法は、プリントサーバーの CUPS Web コンソール (https://print_server_host_name:631/help) で提供されているドキュメントを参照してください。

手順

1. **/etc/samba/smb.conf** ファイルを編集します。
 - a. **[printers]** セクションを追加して、Samba で印刷バックエンドを有効にします。

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



重要

[printers] 共有名はハードコーディングされており、変更はできません。

- b. CUPS サーバーが別のホストまたはポートで実行されている場合は、**printers** セクションで設定を指定します。

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

- c. 多数のプリンターがある場合は、待機秒数を CUPS に接続されているプリンターの数よりも大きい値に設定します。たとえば、100 台のプリンターがある場合は、**[global]** セクションに次のように設定します。

```
rpcd_spoolss:idle_seconds = 200
```

この設定が環境内でスケーリングされない場合は、**[global]** セクションで **rpcd_spoolss** ワーカーの数も増やします。

```
rpcd_spoolss:num_workers = 10
```

デフォルトでは、**rpcd_spoolss** は 5 つのワーカーを開始します。

2. **/etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

3. **firewall-cmd** ユーティリティーを使用して必要なポートを開き、ファイアウォール設定を再読み込みします。

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

4. **smb** サービスを再起動します。

```
# systemctl restart smb
```

サービスを再起動すると、Samba は CUPS バックエンドに設定したすべてのプリンターを自動的に共有します。特定のプリンターのみを手動で共有する場合は、[特定のプリンターの手動共有](#) を参照してください。

検証

- 印刷ジョブを送信します。たとえば、PDF ファイルを印刷するには、次のように入力します。

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

1.15.2. 特定のプリンターの手動共有

Samba をプリントサーバーとして設定している場合、Samba は、デフォルトで CUPS バックエンドで設定されたプリンターをすべて共有します。以下の手順では、特定のプリンターのみを共有する方法を説明します。

前提条件

- Samba がプリントサーバーとして設定されている。

手順

1. **/etc/samba/smb.conf** ファイルを編集します。
 - a. **[global]** セクションで、以下の設定で自動プリンター共有を無効にします。

```
load printers = no
```

- b. 共有するプリンターごとにセクションを追加します。たとえば、Samba で CUPS バックエンドで **example** という名前のプリンターを **Example-Printer** として共有するには、以下のセクションを追加します。

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

各プリンターに個別のプールディレクトリーは必要ありません。**[printers]** セクションに設定したのと同じ spool ディレクトリーを、プリンターの **path** パラメーターに設定できます。

2. **/etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

3. Samba 設定を再読み込みします。

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

1.16. SAMBA プリントサーバーでの WINDOWS クライアント用の自動プリンタードライバーダウンロードの設定

Windows クライアント用に Samba プリントサーバーを実行している場合は、ドライバーをアップロードし、プリンターを事前設定できます。ユーザーがプリンターに接続すると、Windows により、ドライバーが自動的にクライアントにダウンロードされ、インストールされます。ユーザーがインストールするのに、ローカル管理者の権限を必要としません。また、Windows は、トレイの数などの事前設定済みのドライバー設定を適用します。

このセクションの一部は、Samba Wiki で公開されているドキュメント [Setting up Automatic Printer Driver Downloads for Windows Clients](#) に掲載されています。ライセンスは、[CC BY 4.0](#) にあります。著者および貢献者は、Wiki ページの [history](#) タブを参照してください。

前提条件

- Samba がプリントサーバーとして設定されている。

1.16.1. プリンタードライバーに関する基本情報

本セクションでは、プリンタードライバーに関する一般的な情報を説明します。

対応しているドライバーモデルのバージョン

Samba は、Windows 2000 以降および Windows Server 2000 以降でサポートされているプリンタードライバーのモデルバージョン 3 のみに対応します。Samba は、Windows 8 および Windows Server 2012 で導入されたドライバーモデルのバージョン 4 には対応していません。ただし、これ以降の Windows バージョンは、バージョン 3 のドライバーにも対応しています。

パッケージ対応ドライバー

Samba は、パッケージ対応ドライバーに対応していません。

アップロードするプリンタードライバーの準備

Samba プリントサーバーにドライバーをアップロードする場合は、以下を行います。

- ドライバーが圧縮形式で提供されている場合は、ドライバーをデプロイメントします。
- 一部のドライバーでは、Windows ホストにドライバーをローカルにインストールするセットアップアプリケーションを起動する必要があります。特定の状況では、インストーラーはセットアップの実行中にオペレーティングシステムの一時フォルダーに個別のファイルを抽出します。アップロードにドライバーファイルを使用するには、以下のコマンドを実行します。
 - a. インストーラーを起動します。
 - b. 一時フォルダーから新しい場所にファイルをコピーします。
 - c. インストールをキャンセルします。

プリントサーバーへのアップロードをサポートするドライバーは、プリンターの製造元にお問い合わせください。

クライアントに 32 ビットおよび 64 ビットのプリンター用ドライバーを提供

32 ビットと 64 ビットの両方の Windows クライアントのプリンターにドライバーを提供するには、両方のアーキテクチャーに対して、同じ名前のドライバーをアップロードする必要があります。たとえば、32 ビットのドライバー **Example PostScript** および 64 ビットのドライバー **Example PostScript (v1.0)** をアップロードする場合は、その名前が一致しません。その結果、ドライバーのいずれかをプリンターに割り当てることしかできなくなり、両方のアーキテクチャーでそのドライバーが使用できなくなります。

1.16.2. ユーザーがドライバーをアップロードおよび事前設定できるようにする

プリンタードライバーをアップロードおよび事前設定できるようにするには、ユーザーまたはグループに **SePrintOperatorPrivilege** 特権が付与されている必要があります。 **printadmin** グループにユーザーを追加する必要があります。Red Hat Enterprise Linux に **samba** パッケージをインストールすると、このグループが自動的に作成されます。 **printadmin** グループには、1000 未満で利用可能な一番小さい動的システムの GID が割り当てられます。

手順

- たとえば、**SePrintOperatorPrivilege** 権限を **printadmin** グループに付与するには、以下のコマンドを実行します。

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



注記

ドメイン環境では、**SePrintOperatorPrivilege** をドメイングループに付与します。これにより、ユーザーのグループメンバーシップを更新し、権限を集中的に管理できます。

- SePrintOperatorPrivilege** が付与されているユーザーとグループのリストを表示するには、以下を実行します。

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

1.16.3. print\$ 共有の設定

Windows のオペレーティングシステムは、プリントサーバーの共有 **print\$** から、プリンタードライバーをダウンロードします。この共有名は Windows でハードコーディングされており、変更はできません。

以下の手順は、**/var/lib/samba/drivers/** ディレクトリーを **print\$** として共有し、ローカルの **printadmin** グループのメンバーがプリンタードライバーをアップロードすることを有効にする方法を説明します。

手順

1. **[print\$]** セクションを **/etc/samba/smb.conf** ファイルに追加します。

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

以下の設定を使用します。

- **printadmin** グループのメンバーだけがプリンタードライバーを共有にアップロードできません。
 - 新規に作成されたファイルおよびディレクトリーのグループは **printadmin** に設定されます。
 - 新規ファイルの権限は **664** に設定されます。
 - 新しいディレクトリーの権限は、**2775** に設定されます。
2. 全プリンター向けに 64 ビットドライバーのみをアップロードするには、**/etc/samba/smb.conf** ファイルの **[global]** セクションに以下の設定を含めます。

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

この設定がないと、少なくとも 32 ビットバージョンでアップロードしたドライバーのみが表示されます。

3. **/etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

4. Samba 設定を再読み込みします。

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

5. **printadmin** グループが存在しない場合は作成します。

```
# groupadd printadmin
```

6. **SePrintOperatorPrivilege** 権限を、**printadmin** グループに付与します。

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

7. SELinux を、**enforcing** モードで実行する場合は、そのディレクトリーに **samba_share_t** コンテキストを設定します。

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

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

8. `/var/lib/samba/drivers/` ディレクトリーに権限を設定します。

- POSIX ACL を使用する場合は、以下を設定します。

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

- Windows ACL を使用する場合は、以下を設定します。

プリンシパル	アクセス	適用先
CREATOR OWNER	完全な制御	サブフォルダーおよびファイルのみ
認証されたユーザー	読み取りおよび実行、フォルダーのコンテンツのリスト表示、読み取り	このフォルダー、サブフォルダー、およびファイル
printadmin	完全な制御	このフォルダー、サブフォルダー、およびファイル

Windows での ACL の設定に関する詳細は、Windows のドキュメントを参照してください。

関連情報

- [ユーザーがドライバーをアップロードおよび事前設定できるようにする手順](#)

1.16.4. クライアントが Samba プリントサーバーを信頼できるようにする GPO の作成

セキュリティ上の理由から、最新の Windows オペレーティングシステムでは、クライアントが、信頼できないサーバーから、パッケージ対応ではないプリンタードライバーをダウンロードできないようにします。プリントサーバーが AD のメンバーである場合は、Samba サーバーを信頼するために、ドメインに Group Policy Object (GPO) を作成できます。

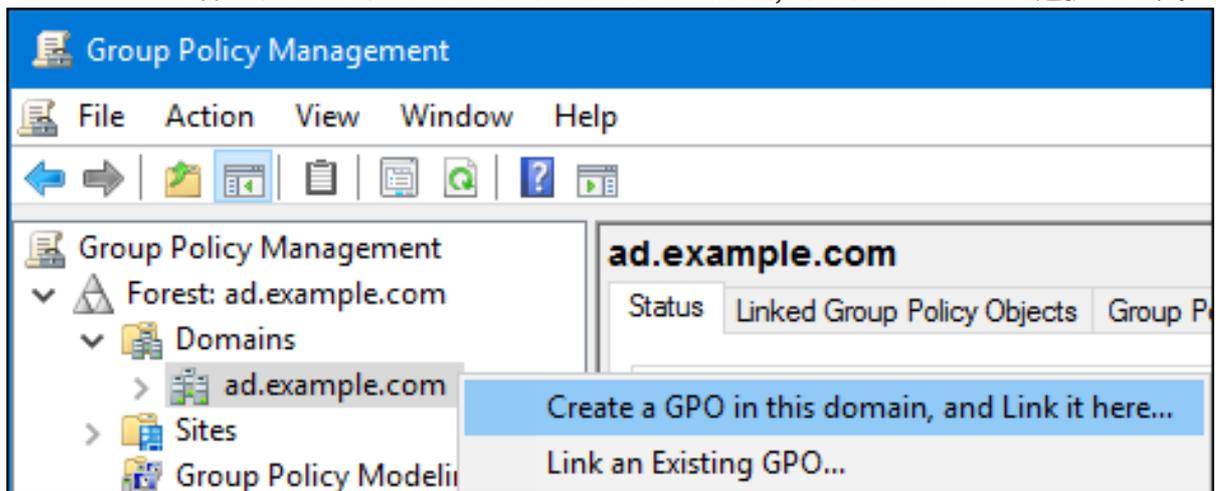
前提条件

- Samba プリントサーバーが、AD ドメインのメンバーである。
- GPO の作成に使用する Windows コンピューターに、RSAT (Windows Remote Server Administration Tools) がインストールされている。詳細は、Windows のドキュメントを参照してください。

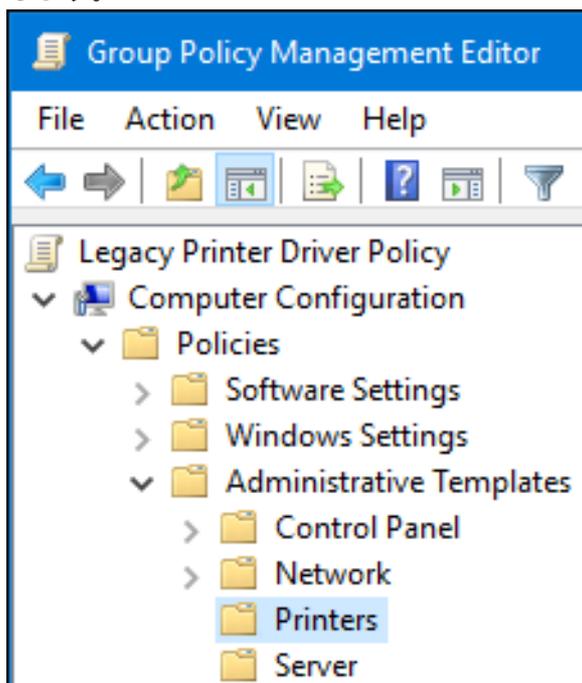
手順

1. AD ドメインの **管理者** ユーザーなど、グループポリシーの編集が可能なアカウントを使用して、Windows コンピューターにログインします。
2. **Group Policy Management Console** を開きます。

3. AD ドメインを右クリックし、**Create a GPO in this domain, and Link it here** を選択します。



4. **Legacy Printer Driver Policy** などの GPO の名前を入力して、**OK** をクリックします。新しい GPO がドメインエントリーの下に表示されます。
5. 新たに作成した GPO を右クリックして **Edit** を選択し、**Group Policy Management Editor** を開きます。
6. **Computer Configuration** → **Policies** → **Administrative Templates** → **Printers** の順にクリックします。



7. ウィンドウの右側で、**Point and Print Restriction** をダブルクリックして、ポリシーを編集します。
- a. ポリシーを有効にし、以下のオプションを設定します。
 - i. **Users can only point and print to these servers** を選択し、このオプションの横にあるフィールドに、Samba プリントサーバーの完全修飾ドメイン名 (FQDN) を入力します。
 - ii. **Security Prompts** の両チェックボックスで、**Do not show warning or elevation prompt** を選択します。

Point and Print Restrictions

Point and Print Restrictions

Not Configured Comment:

Enabled

Disabled

Supported on:

Options:

Users can only point and print to these servers:
Enter fully qualified server names separated by semicolons

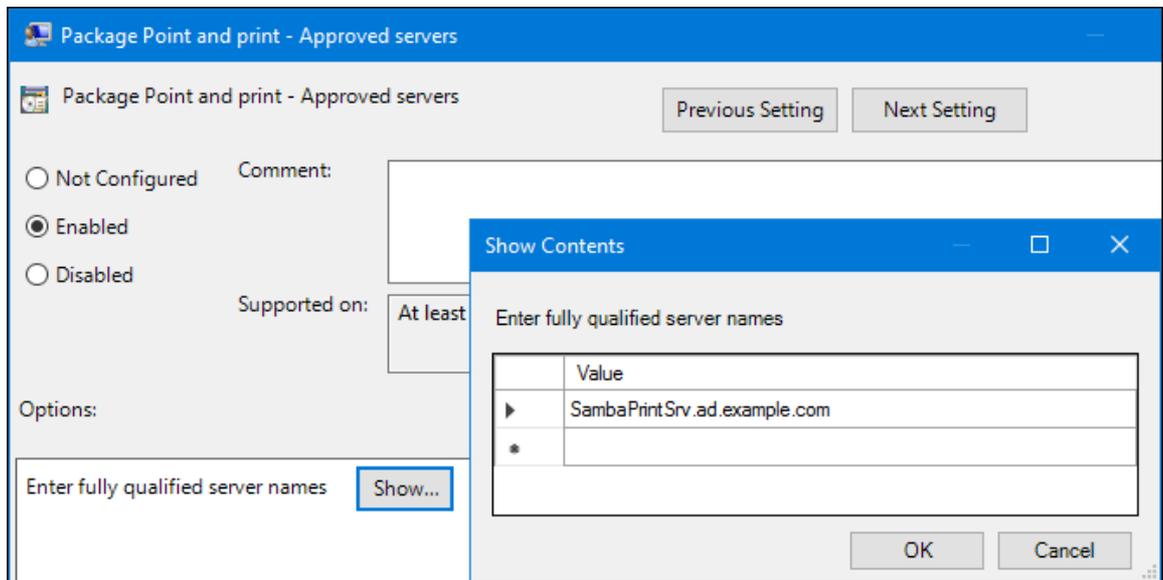
Users can only point and print to machines in their forest

Security Prompts:

When installing drivers for a new connection:

When updating drivers for an existing connection:

- b. OK をクリックします。
8. **Package Point and Print - Approved servers** をダブルクリックして、ポリシーを編集します。
- a. ポリシーを有効にして、**Show** ボタンをクリックします。
- b. Samba プリントサーバーの FQDN を入力します。



- c. **OK** をクリックして、**Show Contents** ウィンドウとポリシーのプロパティウィンドウの両方を閉じます。

9. **Group Policy Management Editor** を閉じます。

10. **Group Policy Management Console** を閉じます。

Windows ドメインメンバーがこのグループポリシーを適用すると、ユーザーがプリンターに接続する際に、プリンタードライバーが Samba サーバーから自動的にダウンロードされます。

関連情報

- グループポリシーの使用については、Windows のドキュメントを参照してください。

1.16.5. ドライバーのアップロードおよびプリンターの事前設定

Windows クライアントで **Print Management** アプリケーションを使用してドライバーをアップロードし、Samba プリントサーバーでホストされるプリンターを事前設定します。詳細は、Windows のドキュメントを参照してください。

1.17. FIPS モードが有効なサーバーでの SAMBA の実行

本セクションでは、FIPS モードが有効な状態で Samba を実行する制限の概要を説明します。また、Samba を実行している Red Hat Enterprise Linux ホストで FIPS モードを有効にする手順も提供します。

1.17.1. FIPS モードでの Samba の使用制限

以下の Samba モードと機能は、指定された条件下で FIPS モードで動作します。

- Samba は、AES 暗号化を使用する Kerberos 認証を使用する Active Directory (AD) または Red Hat Identity Management (IdM) 環境でのみ、ドメインメンバーとして使用できます。
- Active Directory ドメインメンバーのファイルサーバーとして Samba を使用する。ただし、クライアントは Kerberos を使用してサーバーに対して認証する必要があります。

FIPS のセキュリティが強化されているため、FIPS モードが有効な場合は、以下の Samba 機能およびモードは機能しません。

- RC4 暗号がブロックされていることによる NT LAN Manager (NTLM) 認証
- サーバーメッセージブロックバージョン 1 (SMB1) プロトコル
- NTLM 認証を使用することによるスタンドアロンファイルサーバーモード
- NT4- スタイルのドメインコントローラー
- NT4- スタイルのドメインメンバー Red Hat は、IdM がバックグラウンドで使用するプライマリドメインコントローラー (PDC) 機能のサポートを継続することに留意してください。
- Samba サーバーに対するパスワード変更 Active Directory ドメインコントローラーに対して Kerberos を使用してパスワードの変更のみを実行できます。

以下の機能は FIPS モードでテストされていないため、Red Hat ではサポートされていません。

- プリントサーバーとしての Samba の実行

1.17.2. FIPS モードでの Samba の使用

Samba を実行する RHEL ホストで FIPS モードを有効にすることができます。

前提条件

- Samba が Red Hat Enterprise Linux ホストに設定されている。
- Samba は、FIPS モードでサポートされるモードで実行する。

手順

1. RHEL で FIPS モードを有効にします。

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

2. サーバーを再起動します。

```
# reboot
```

3. `testparm` ユーティリティーを使用して、設定を確認します。

```
# testparm -s
```

コマンドがエラーや非互換性を表示する場合は、Samba が正常に機能するように修正してください。

関連情報

- [「FIPS モードでの Samba の使用制限」](#)

1.18. SAMBA サーバーのパフォーマンスチューニング

特定の状況で Samba のパフォーマンスを向上させることができる設定と、パフォーマンスに悪影響を与える可能性がある設定について説明します。

このセクションの一部は、Samba Wiki に公開されているドキュメント [Performance Tuning](#) に掲載されています。ライセンスは、[CC BY 4.0](#) にあります。著者および貢献者は、Wiki ページの [history](#) タブを参照してください。

前提条件

- Samba が、ファイルサーバーまたはプリントサーバーとして設定されている。

1.18.1. SMB プロトコルバージョンの設定

新しい SMB バージョンごとに機能が追加され、プロトコルのパフォーマンスが向上します。最新の Windows および Windows Server オペレーティングシステムは、常に最新のプロトコルバージョンに対応しています。Samba がプロトコルの最新バージョンも使用している場合は、Samba に接続する Windows クライアントで、このパフォーマンス改善を活用できます。Samba では、`server max protocol` のデフォルト値が、対応している安定した SMB プロトコルの最新バージョンに設定されます。



注記

常に最新の安定した SMB プロトコルバージョンを有効にするには、**server max protocol** パラメーターを設定しないでください。このパラメーターを手動で設定する場合は、最新のプロトコルバージョンを有効にするために、それぞれ新しいバージョンの SMB プロトコルで設定を変更する必要があります。

次の手順では、**server max protocol** パラメーターでデフォルト値を使用する方法を説明します。

手順

1. `/etc/samba/smb.conf` ファイルの **[global]** セクションから、**server max protocol** パラメーターを削除します。
2. Samba 設定を再読み込みします。

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

1.18.2. 大量のファイルを含むディレクトリーとの共有の調整

Linux は、大文字と小文字を区別するファイル名に対応しています。このため、Samba はファイルの検索時またはアクセス時に、大文字と小文字のファイル名のディレクトリーをスキャンする必要があります。小文字または大文字のいずれかでのみ新しいファイルを作成するように共有を設定すると、パフォーマンスが向上します。

前提条件

- Samba が、ファイルサーバーとして設定されている。

手順

1. 共有の全ファイルの名前を小文字に変更します。



注記

この手順の設定を使用すると、小文字以外の名前が付けられたファイルは表示されなくなります。

- 共有のセクションに、以下のパラメーターを設定します。

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

パラメーターの詳細は、man ページの **smb.conf(5)** を参照してください。

- /etc/samba/smb.conf** ファイルを検証します。

```
# testparm
```

- Samba 設定を再読み込みします。

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

この設定が適用されると、この共有に新たに作成されるすべてのファイルの名前が小文字になります。この設定により、Samba はディレクトリーを大文字と小文字で分けたスキャンが不要になり、パフォーマンスが向上します。

1.18.3. パフォーマンスが低下する可能性のある設定

デフォルトでは、Red Hat Enterprise Linux のカーネルは、ネットワークパフォーマンスが高くなるように調整されています。たとえば、カーネルはバッファサイズに自動チューニングメカニズムを使用しています。**/etc/samba/smb.conf** ファイルに **socket options** パラメーターを設定すると、このカーネル設定が上書きされます。その結果、このパラメーターの設定により、ほとんどの場合は、Samba ネットワークのパフォーマンスが低下します。

カーネルの最適化された設定を使用するには、**/etc/samba/smb.conf** の **[global]** セクションから **socket options** パラメーターを削除します。

1.19. SAMBA がデフォルトの SMB バージョンよりも前のバージョンのクライアントと互換対応するような設定

Samba は、サポート対象の最小サーバーメッセージブロック (SMB) バージョンに妥当で安全なデフォルト値を使用します。ただし、以前の SMB バージョンを必要とするクライアントがある場合は、Samba を設定してサポートできます。

1.19.1. Samba サーバーで対応している最小 SMB プロトコルバージョンの設定

Samba では、**/etc/samba/smb.conf** ファイルの **server min protocol** パラメーターは、Samba サーバーが対応する SMB (server message block) プロトコルの最小バージョンを定義します。SMB プロトコルの最小バージョンを変更できます。



注記

デフォルトでは、RHEL 8.2 以降の Samba では、SMB2 以降のプロトコルバージョンのみに対応します。Red Hat は、非推奨の SMB1 プロトコルを使用することは推奨されません。ただし、お使いの環境で SMB1 が必要な場合は、**server min protocol** パラメーターを手動で **NT1** に設定して、SMB1 を再度有効にできます。

前提条件

- Samba がインストールされ、設定されている。

手順

1. **/etc/samba/smb.conf** ファイルを編集し、**server min protocol** パラメーターを追加して、そのサーバーが対応する最小 SMB プロトコルバージョンに設定できます。たとえば、最小の SMB プロトコルバージョンを **SMB3** に設定するには、以下を追加します。

```
server min protocol = SMB3
```

2. **smb** サービスを再起動します。

```
# systemctl restart smb
```

関連情報

- **smb.conf(5)** man ページ

1.20. 頻繁に使用される SAMBA コマンドラインユーティリティー

本章では、Samba サーバーで作業する場合によく使用されるコマンドを説明します。

1.20.1. net ads join コマンドおよび net rpc join コマンドの使用

net ユーティリティーの **join** サブコマンドを使用すると、Samba を AD ドメインまたは NT4 ドメインに参加させることができます。ドメインに参加するには、**/etc/samba/smb.conf** ファイルを手動で作成し、必要に応じて PAM などの追加設定を更新する必要があります。



重要

Red Hat は、**realm** ユーティリティーを使用してドメインに参加させることを推奨します。**realm** ユーティリティーは、関連するすべての設定ファイルを自動的に更新します。

手順

1. 以下の設定で **/etc/samba/smb.conf** ファイルを手動で作成します。
 - AD ドメインメンバーの場合:

```
[global]
workgroup = domain_name
security = ads
```

```
passdb backend = tdbsam
realm = AD_REALM
```

- NT4 ドメインメンバーの場合:

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

2. `/etc/samba/smb.conf` ファイルの `[global]` セクションに、* デフォルトドメインおよび参加するドメイン用の ID マッピング設定を追加します。
3. `/etc/samba/smb.conf` ファイルを検証します。

```
# testparm
```

4. ドメイン管理者としてドメインに参加します。
 - AD ドメインに参加するには、以下のコマンドを実行します。

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

- NT4 ドメインに参加するには、以下のコマンドを実行します。

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

5. `/etc/nsswitch.conf` ファイルのデータベースエントリ `passwd` および `group` に `winbind` ソースを追加します。

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

6. `winbind` サービスを有効にして起動します。

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

7. 必要に応じて、`authselect` ユーティリティーを使用して PAM を設定します。詳細は、man ページの `authselect(8)` を参照してください。
8. AD 環境では、必要に応じて Kerberos クライアントを設定します。詳細は、Kerberos クライアントのドキュメントを参照してください。

関連情報

- [Samba のドメインへの参加](#)
- [Samba ID マッピングの理解および設定](#)

1.20.2. net rpc rights コマンドの使用

Windows では、アカウントおよびグループに特権を割り当て、共有での ACL の設定やプリンタードライバのアップロードなどの特別な操作を実行できます。Samba サーバーでは、**net rpc rights** コマンドを使用して権限を管理できます。

設定可能な権限のリスト表示

利用可能な特権とその所有者をすべて表示するには、**net rpc rights list** コマンドを使用します。以下に例を示します。

```
# 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
```

特権の付与

アカウントまたはグループへの特権を付与するには、**net rpc rights grant** コマンドを使用します。

たとえば、**SePrintOperatorPrivilege** 権限を、**DOMAIN\printadmin** グループに付与します。

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

特権の取り消し

アカウントまたはグループから特権を取り消すには、**net rpc rights revoke** コマンドを使用します。

たとえば、**DOMAIN\printadmin** グループから **SePrintOperatorPrivilege** 権限を取り消すには、以下のコマンドを実行します。

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

1.20.3. net rpc share コマンドの使用

net rpc share コマンドは、ローカルまたはリモートの Samba または Windows サーバーの共有のリスト表示、追加、および削除を行う機能を提供します。

共有のリスト表示

SMB サーバーの共有をリスト表示するには、**net rpc share list** コマンドを使用します。必要に応じて、**-S server_name** パラメーターをコマンドに渡して、リモートサーバーの共有をリスト表示します。以下に例を示します。

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

```
share_1
share_2
...
```



注記

`/etc/samba/smb.conf` ファイルのセクション内に `browseable = no` が設定されている Samba サーバーでホストされている共有は、出力には表示されません。

共有の追加

`net rpc share add` コマンドを使用すると、SMB サーバーに共有を追加できます。

たとえば、`C:\example\` ディレクトリーを共有するリモートの Windows サーバーに、共有 `example` を追加するには、以下のコマンドを実行します。

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



注記

Windows のディレクトリー名を指定する際は、パスの末尾のバックスラッシュを省略する必要があります。

このコマンドを使用して Samba サーバーに共有を追加するには、以下を行います。

- `-U` パラメーターで指定したユーザーは、出力先サーバーで `SeDiskOperatorPrivilege` 特権が付与されている必要があります。
- 共有セクションを、`/etc/samba/smb.conf` ファイルに追加し、Samba を再読み込みするスクリプトを記述する必要があります。スクリプトは、`/etc/samba/smb.conf` の `[global]` セクションの `add share command` パラメーターで設定する必要があります。詳細は、man ページの `smb.conf(5)` の `add share` コマンドの説明を参照してください。

共有の削除

`net rpc share delete` コマンドを使用すると、SMB サーバーから共有を削除できます。

たとえば、`example` という名前の共有を、リモートの Windows サーバーから削除するには、以下のコマンドを実行します。

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

このコマンドを使用して Samba サーバーから共有を削除するには、以下のコマンドを実行します。

- `-U` パラメーターで指定したユーザーは、`SeDiskOperatorPrivilege` 特権が付与されている必要があります。
- `/etc/samba/smb.conf` ファイルから共有のセクションを削除し、Samba を再読み込みするスクリプトを記述する必要があります。スクリプトは、`/etc/samba/smb.conf` の `[global]` セクションの `delete share command` パラメーターで設定する必要があります。詳細は、man ページの `smb.conf(5)` の `delete share` コマンドの説明を参照してください。

1.20.4. net user コマンドの使用

`net user` コマンドを使用すると、AD DC または NT4 PDC で以下の操作を実行できます。

- すべてのユーザーアカウントのリストを表示
- ユーザーの追加
- ユーザーの削除



注記

AD ドメイン用の **ads**、NT4 ドメイン用の **rpc** などの接続方法の指定は、ドメインユーザーアカウントをリスト表示する場合にのみ必要です。その他のユーザー関連のサブコマンドは、接続メソッドを自動検出できます。

-U user_name パラメーターをコマンドに渡して、要求されたアクションを実行できるユーザーを指定します。

ドメインユーザーアカウントのリスト表示

AD ドメイン内のユーザーをリスト表示するには、以下を実行します。

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

NT4 ドメインのユーザーをリスト表示するには、以下を実行します。

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

ユーザーアカウントのドメインへの追加

Samba ドメインメンバーの場合は、**net user add** コマンドを使用して、ユーザーアカウントをドメインに追加できます。

たとえば、**user** アカウントをドメインに追加します。

1. 以下のアカウントを追加します。

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

2. 必要に応じて、リモートプロシージャコール (RPC) シェルを使用して、AD DC または NT4 PDC でアカウントを有効にします。以下に例を示します。

```
# 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
```

ドメインからのユーザーアカウントの削除

Samba ドメインメンバーの場合は、**net user delete** コマンドを使用して、ドメインからユーザーアカウントを削除できます。

たとえば、ドメインから **user** アカウントを削除するには、以下のコマンドを実行します。

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

1.20.5. rpcclient ユーティリティーの使用

rpcclient ユーティリティーを使用すると、ローカルまたはリモートの SMB サーバーでクライアント側の Microsoft Remote Procedure Call (MS-RPC) 機能を手動で実行できます。ただし、ほとんどの機能は、Samba が提供する個別のユーティリティーに統合されています。**rpcclient** は、MS-PRC 関数のテストにのみ使用します。

前提条件

- **samba-client** パッケージがインストールされている。

例

たとえば、**rpcclient** ユーティリティーを使用して以下を行うことができます。

- プリンターのスプールサブシステム (SPOOLSS) を管理します。

例1.7 プリンターへのドライバーの割り当て

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

- SMB サーバーに関する情報を取得します。

例1.8 すべてのファイル共有および共有プリンターのリスト表示

```
# 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:
```

- Security Account Manager Remote (SAMR) プロトコルを使用して操作を実行します。

例1.9 SMB サーバー上のユーザーのリスト表示

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

スタンドアロンサーバーまたはドメインメンバーに対してコマンドを実行すると、ローカルデータベースのユーザーのリストが表示されます。ADDC または NT4 PDC に対してコマンドを実行すると、ドメインユーザーのリストが表示されます。

関連情報

- `rpcclient(1)` man ページ

1.20.6. samba-regedit アプリケーションの使用

プリンター設定などの特定の設定は、Samba サーバーのレジストリーに保存されます。ncurses ベースの `samba-regedit` アプリケーションを使用して、Samba サーバーのレジストリーを編集できます。

```
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
```

前提条件

- `samba-client` パッケージがインストールされている。

手順

アプリケーションを起動するには、次のコマンドを入力します。

```
# samba-regedit
```

次のキーを使用します。

- カーソルを上下に動かして、レジストリーツリーと値の間を移動します。
- **Enter** - キーを開くか、値を編集します。
- **Tab - Key** ペインと **Value** ペインを切り替えます。
- **Ctrl+C** - アプリケーションを閉じます。

1.20.7. smbcontrol ユーティリティーの使用

`smbcontrol` ユーティリティーを使用すると、`smbd`、`nmbd`、`winbindd`、またはこのすべてのサービスにコマンドメッセージを送信できます。この制御メッセージは、設定の再読み込みなどのサービスを指示します。

前提条件

- **samba-common-tools** パッケージがインストールされている。

手順

- **reload-config** メッセージタイプを **all** 宛に送信して、**smbd**、**nmbd**、**winbindd** サービスの設定をリロードします。

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

関連情報

- **smbcontrol(1)** man ページ

1.20.8. smbpasswd ユーティリティーの使用

smbpasswd ユーティリティーは、ローカルの Samba データベースでユーザーアカウントおよびパスワードを管理します。

前提条件

- **samba-common-tools** パッケージがインストールされている。

手順

1. ユーザーとしてコマンドを実行すると、**smbpasswd** はコマンドを実行するユーザーの Samba パスワードを変更します。以下に例を示します。

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

2. **root** で **smbpasswd** を実行すると、たとえば以下のようにユーティリティーを使用できます。

- 新しいユーザーを作成します。

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



注記

Samba データベースにユーザーを追加する前に、ローカルのオペレーティングシステムにアカウントを作成する必要があります。基本的なシステム設定の設定の [コマンドラインでの新規ユーザーの追加](#) セクションを参照してください。

- Samba ユーザーを有効にします。

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

- Samba ユーザーを無効にします。

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

- ユーザーを削除します。

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

関連情報

- **smbpasswd(8)** man ページ

1.20.9. smbstatus ユーティリティーの使用

smbstatus ユーティリティーは以下について報告します。

- 各 **smbd** デーモンの PID ごとの接続を Samba サーバーに接続します。このレポートには、ユーザー名、プライマリグループ、SMB プロトコルのバージョン、暗号、および署名の情報が含まれます。
- Samba 共有ごとの接続このレポートには、**smbd** デーモンの PID、接続しているマシンの IP、接続が確立された時点のタイムスタンプ、暗号、および署名情報が含まれます。
- ロックされたファイルのリスト。レポートエントリーには、日和見ロック (oplock) タイプなどの詳細が含まれます。

前提条件

- **samba** パッケージがインストールされている。
- **smbd** サービスが実行している。

手順

```
# 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
```

関連情報

- **smbstatus(1)** man ページ

1.20.10. smbtar ユーティリティーの使用

smbtar ユーティリティーは、SMB 共有またはそのサブディレクトリーのコンテンツのバックアップを作成し、そのコンテンツを **tar** アーカイブに保存します。または、コンテンツをテープデバイスに書き込むこともできます。

前提条件

- **samba-client** パッケージがインストールされている。

手順

- 以下のコマンドを使用して、**//server/example/** 共有上の **demo** ディレクトリーのコンテンツをバックアップして、**/root/example.tar** アーカイブにコンテンツを保存するには、以下を実行します。

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

関連情報

- **smbtar(1)** の man ページ

1.20.11. wbinfo ユーティリティーの使用

wbinfo ユーティリティーは、**winbindd** サービスが作成および使用する情報をクエリーし、返します。

前提条件

- **samba-winbind-clients** パッケージがインストールされている。

手順

たとえば、以下のように、**wbinfo** を使用できます。

- ドメインユーザーのリストを表示します。

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

- ドメイングループのリストを表示します。

```
# wbinfo -g
AD\domain computers
```

```
AD\domain admins
AD\domain users
...
```

- ユーザーの SID を表示します。

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

- ドメインおよび信頼に関する情報を表示します。

```
# 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
```

関連情報

- [wbinfo\(1\) man ページ](#)

1.21. 関連情報

- [smb.conf\(5\) man ページ](#)
- [/usr/share/docs/samba-version/](#) ディレクトリーには、Samba プロジェクトが提供する一般的なドキュメント、サンプルスクリプト、および LDAP スキーマファイルが含まれています。
- [Setting up Samba and the Clustered Trivial Database \(CTDB\) to share directories stored on an GlusterFS volume](#)
- [Red Hat Enterprise Linux での SMB 共有のマウント](#)

第2章 NFS サーバーのデプロイ

ネットワークファイルシステム (NFS) プロトコルを使用すると、リモートユーザーはネットワーク経由で共有ディレクトリーをマウントし、ローカルにマウントされたディレクトリーと同じように使用できます。また、リソースを、ネットワークの集中化サーバーに統合できるようになります。

2.1. NFSv4 のマイナーバージョンの主な機能

NFSv4 の各マイナーバージョンでは、パフォーマンスとセキュリティーの向上を目的とした機能強化が導入されます。この強化を利用して NFSv4 の可能性を最大限に活用すれば、ネットワーク全体で効率的かつ信頼性の高いファイル共有を実現できます。

NFSv4.2 の主な機能

サーバー側コピー

サーバー側コピーは、ネットワーク経由でデータを転送せずにサーバー上のファイルをコピーする NFS サーバーの機能です。

スパーズファイル

ファイルに1つ以上の空きスペース、つまりギャップを持たせることができます。ギャップとは、ゼロのみで構成される未割り当てまたは未初期化データブロックです。これにより、アプリケーションがスパーズファイル内のホールの位置を計画できるようになります。

領域の予約

クライアントが、データを書き込む前にストレージサーバー上の領域を予約または確保できます。これにより、サーバーの領域不足が防止されます。

ラベル付き NFS

データアクセス権を強制し、NFS ファイルシステム上の個々のファイルに対して、クライアントとサーバーとの間の SELinux ラベルを有効にします。

レイアウトの機能強化

Parallel NFS (pNFS) サーバーがより優れたパフォーマンス統計情報を収集できるようにする機能を提供します。

NFSv4.1 の主な機能

pNFS のクライアント側サポート

クラスター化されたサーバーへの高速 I/O のサポートにより、複数のマシンへのデータ保存、データへの直接アクセス、メタデータの更新の同期が可能になります。

セッション

セッションは、クライアントに属する接続に関連するサーバーの状態を維持します。この種類のセッションは、各リモートプロシーチャーコール (RPC) 操作の接続の確立と終了に関連するオーバーヘッドを削減し、パフォーマンスと効率を向上させます。

NFSv4.0 の主な機能

RPC とセキュリティー

RPCSEC_GSS フレームワークにより、RPC のセキュリティーが強化されます。NFSv4 プロトコルで、インバンドセキュリティーネゴシエーション用の新しい操作が導入されました。これにより、クライアントがファイルシステムリソースにセキュアにアクセスするためのサーバーポリシーをクエリーできるようになります。

プロシーチャーと操作の構造

NFS 4.0 で、**COMPOUND** プロシージャラーが導入されました。これにより、クライアントが複数の操作を1つの要求にマージして RPC を削減できるようになりました。

ファイルシステムモデル

NFS 4.0 は、階層型ファイルシステムモデルを保持し、ファイルをバイトストリームとして扱い、国際化のために名前を UTF-8 でエンコードします。

- **ファイルハンドルの種類**
揮発性のファイルハンドルにより、サーバーがファイルシステムの変更に適応できます。また、クライアントが、永続的なファイルハンドルを必要とせずに、必要に応じて適応できます。
- **属性タイプ**
ファイル属性構造には、必須属性、推奨属性、および名前付き属性が含まれています。各属性は異なる目的を果たします。NFSv3 から派生した必須属性は、ファイルタイプを区別するために必要です。一方、ACL などの推奨属性は、アクセス制御を強化します。
- **マルチサーバー名前空間**
名前空間は、複数のサーバー全体を対象に、属性に基づいてファイルシステム転送を簡素化します。また、参照、冗長性、シームレスなサーバー移行をサポートします。

OPEN および CLOSE 操作

これらの操作により、ファイルの検索、作成、セマンティック共有を1カ所で組み合わせて、ファイルアクセス管理を効率化できます。

ファイルロック

ファイルロックがプロトコルに含まれているため、RPC コールバックが不要になります。ファイルロックの状態は、リースベースのモデルに基づいてサーバーによって管理されます。リースの更新に失敗すると、サーバーによって状態が解放されることがあります。

クライアントのキャッシュと委譲

キャッシュは以前のバージョンと似ています。属性とディレクトリーのキャッシュのタイムアウトが、クライアントによって決定されます。NFS 4.0 の委譲により、サーバーがクライアントに特定の役割を割り当てることができます。これにより、特定のファイル共有セマンティクスが確保され、サーバーとの直接のやり取りなしでローカルファイル操作が可能になります。

2.2. AUTH_SYS 認証方式

AUTH_SYS 方式 (**AUTH_UNIX** と呼ばれます) は、クライアント認証メカニズムです。**AUTH_SYS** を使用すると、クライアントがファイルにアクセスするときに、ユーザーのアイデンティティーと権限を確認するために、ユーザーのユーザー ID (UID) とグループ ID (GID) をサーバーに送信します。**AUTH_SYS** は、クライアントが提供する情報に依存するため、誤って設定された場合に不正アクセスを受ける可能性があり、セキュリティが低いと考えられています。

マッピングメカニズムにより、UID と GID の割り当てがシステム間で異なる場合でも、NFS クライアントが適切な権限でサーバー上のファイルにアクセスできます。UID と GID は、次のメカニズムによって NFS クライアントとサーバーの間でマッピングされます。

直接マッピング

UID と GID は、NFS サーバーとクライアントによってローカルシステムとリモートシステム間で直接マッピングされます。これを行うには、NFS ファイル共有に参加しているすべてのシステム間で一貫した UID と GID の割り当てが必要です。たとえば、クライアント上の UID 1000 のユーザーは、サーバー上の UID 1000 のユーザーがアクセスできる共有上のファイルにのみアクセスできません。

管理者は、NFS 環境での ID 管理を簡素化するために、多くの場合、LDAP やネットワーク情報サービス (NIS) などの集中型サービスを利用して、複数のシステムにわたる UID と GID のマッピングを管理します。

ユーザー ID とグループ ID のマッピング

NFS サーバーおよびクライアントは、**idmapd** サービスを使用して、異なるシステム間で UID と GID を変換し、一貫した ID 識別と権限の割り当てを実現できます。

2.3. AUTH_GSS 認証方式

Kerberos は、セキュアでないネットワーク上でクライアントとサーバーのセキュアな認証を可能にするネットワーク認証プロトコルです。対称鍵暗号を使用し、ユーザーとサービスを認証するために、信頼できる Key Distribution Center (KDC) を必要とします。

AUTH_SYS とは異なり、**RPCSEC_GSS** Kerberos メカニズムでは、ファイルにアクセスしているユーザーを正しく表すために、サーバーがクライアントに依存することがありません。代わりに、暗号を使用してサーバーにユーザーを認証し、悪意のあるクライアントがそのユーザーの Kerberos 認証情報を持たずにユーザーになりすますことがないようにします。

`/etc/exports` ファイルの **sec** オプションで、共有が提供する Kerberos セキュリティ方式を1つ以上定義します。クライアントはこれらの方法のいずれかを使用して共有をマウントできます。**sec** オプションは次の値をサポートします。

- **sys**: 暗号化保護なし (デフォルト)
- **krb5** - 認証のみ
- **krb5i**: 認証と整合性保護
- **krb5p**: 認証、整合性チェック、およびトラフィック暗号化

方式が提供する暗号化機能が多いほど、パフォーマンスが低下することに注意してください。

2.4. エクスポートされたファイルシステムのファイル権限

エクスポートされたファイルシステムのファイル権限によって、NFS 経由でファイルとディレクトリーにアクセスするクライアントのアクセス権が決まります。

NFS ファイルシステムがリモートホストによってマウントされると、各共有ファイルに対する保護がファイルシステムの権限だけになります。同じユーザー ID (UID) の値を共有する2つのユーザーが、異なるクライアントシステムに同じ NFS ファイルシステムをマウントした場合、そのユーザーはお互いのファイルを変更できます。

NFS は、クライアント上の **root** ユーザーをサーバー上の **root** ユーザーと同等のものとして扱います。ただし、NFS サーバーは、NFS 共有にアクセスするときに、デフォルトで **root** を **nobody** アカウントにマップします。この動作は **root_squash** オプションにより制御します。

関連情報

- **exports(5)** man ページ

2.5. NFS サーバーに必要なサービス

Red Hat Enterprise Linux (RHEL) は、NFS ファイル共有を提供するのに、カーネルモジュールとユーザー空間プロセスの組み合わせを使用します。

表2.1 NFS サーバーに必要なサービス

サービス名	NFS バージョン	詳細
nfsd	3, 4	共有 NFS ファイルシステムに対する要求を処理する NFS カーネルモジュール。
rpcbind	3	このプロセスは、ローカルのリモートプロシージャコール (RPC) サービスからのポート予約を受け入れ、それを使用可能にするかアダプタイズして、対応するリモート RPC サービスがポート予約にアクセスできるようにします。 rpcbind サービスは、要求に応答し、指定された RPC サービスへの接続を設定します。
rpc.mountd	3, 4	このサービスは NFSv3 クライアントからの MOUNT 要求を処理します。NFSv4 サーバーはこのサービスの内部機能を使用します。 要求されている NFS 共有が現在 NFS サーバーによりエクスポートされているか、またその共有へのクライアントのアクセスが許可されているかを確認します。
rpc.nfsd	3, 4	このプロセスは、サーバーが定義する明示的な NFS バージョンとプロトコルをアダプタイズします。NFS クライアントが接続するたびにサーバーレッドを提供するなど、NFS クライアントの動的な要求に対応するために、カーネルと連携して動作します。 nfs-server サービスがこのプロセスを起動します。
lockd	3	このカーネルモジュールは、Network Lock Manager (NLM) プロトコルを実装します。これにより、クライアントがサーバー上のファイルをロックできるようになります。RHEL は、NFS サーバーの実行時にこのモジュールを自動的にロードします。
rpc.rquotad	3, 4	このサービスは、リモートユーザーのユーザークォータ情報を提供します。
rpc.idmapd	4	このプロセスは、NFSv4 名 (`user@domain` 形式の文字列) とローカルのユーザー ID およびグループ ID をマッピングする NFSv4 クライアントおよびサーバーのアップコールを提供します。
gssproxy	3, 4	このサービスは、 rpc.nfsd に代わって krb5 認証を処理します。
nfsdclid	4	このサービスは、NFSv4 クライアント追跡デーモンを提供します。このデーモンは、ネットワークパーティションとサーバーの再起動中に他のクライアントが競合するロックを取得したときに、サーバーがロックの回収を許可するのを防止します。

サービス名	NFS バージョン	詳細
rpc.statd	3	このサービスは、ローカルホストが再起動したときに他の NFSv3 クライアントに通知し、リモート NFSv3 ホストが再起動したときにカーネルに通知します。

関連情報

- `rpcbind(8)`、`rpc.mountd(8)`、`rpc.nfsd(8)`、`rpc.statd(8)`、`rpc.rquotad(8)`、`rpc.idmapd(8)`、`nsd(8)` `man` ページ

2.6. /ETC/EXPORTS 設定ファイル

`/etc/exports` ファイルは、サーバーがエクスポートするディレクトリーを制御します。各行に、エクスポートポイント、ディレクトリーのマウントが許可されているクライアントの空白区切りのリスト、および各クライアントのオプションが含まれています。

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

以下は `/etc/exports` のエントリーの各部分です。

<export>

エクスポートするディレクトリー。

<host_or_network>

エクスポートを共有するホストまたはネットワーク。たとえば、ホスト名、IP アドレス、または IP ネットワークを指定できます。

<options>

ホストまたはネットワークのオプション。

クライアントとオプションの間にスペースを追加すると、動作が変わります。たとえば、次の行はそれぞれ意味が異なります。

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

最初の行では、サーバーは `client.example.com` にのみ、`/projects` ディレクトリーを読み取り/書き込みモードでマウントすることを許可します。他のホストは共有をマウントできません。一方、2 番目の行では、`client.example.com` と `(rw)` の間にスペースがあるため、サーバーはディレクトリーを読み取り専用モード (デフォルト設定) で `client.example.com` にエクスポートします。他のすべてのホストは、読み取り/書き込みモードで共有をマウントできます。

NFS サーバーは、エクスポートされた各ディレクトリーに対して次のデフォルト設定を使用します。

表2.2 /etc/exports のエントリーのデフォルトオプション

デフォルト設定	詳細
ro	ディレクトリーを読み取り専用モードでエクスポートします。

デフォルト設定	詳細
sync	NFS サーバーは、以前の要求で発生した変更がディスクに書き込まれるまで、要求に応答しません。
wdelay	別の書き込み要求が保留中であると疑われる場合、サーバーはディスクへの書き込みを遅延します。
root_squash	クライアントの root ユーザーがエクスポートされたディレクトリーに対して root 権限を持つことを防ぎます。 root_squash を有効にすると、NFS サーバーは root からのアクセスをユーザー nobody にマッピングします。

2.7. NFSV4 専用サーバーの設定

ネットワーク内に NFSv3 クライアントが存在しない場合は、NFSv4 またはその特定のマイナープロトコルバージョンのみをサポートするように NFS サーバーを設定できます。サーバー上で NFSv4 のみを使用すると、ネットワークに開放されるポートの数が減ります。

手順

1. **nfs-utils** パッケージをインストールします。

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

2. **/etc/nfs.conf** ファイルを編集し、次の変更を加えます。

- a. NFSv3 を無効にするには、**[nfsd]** セクションの **vers3** パラメーターを無効にします。

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

- b. オプション: 特定の NFSv4 マイナーバージョンのみが必要な場合は、すべての **vers4.<minor_version>** パラメーターのコメントを解除し、各パラメーターを適切に設定します。次に例を示します。

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

この設定では、サーバーは NFS バージョン 4.2 のみを提供します。



重要

特定の NFSv4 マイナーバージョンのみが必要な場合は、そのマイナーバージョンのパラメーターのみを設定してください。予期しないマイナーバージョンのアクティブ化や非アクティブ化を回避するために、**vers4** パラメーターのコメントは解除しないでください。**vers4** パラメーターは、デフォルトですべての NFSv4 マイナーバージョンを有効または無効にします。ただし、**vers4** を他の **vers** パラメーターと組み合わせると、この動作は変わります。

3. NFSv3 関連のすべてのサービスを無効にします。

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

4. オプション: 共有するディレクトリーを作成します。以下に例を示します。

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

既存のディレクトリーを共有する場合は、このステップをスキップしてください。

5. **/nfs/projects/** ディレクトリーに必要な権限を設定します。

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

これらのコマンドは、**/nfs/projects/** ディレクトリーの **users** グループの書き込み権限を設定し、このディレクトリーに作成される新しいエントリーに対して同じグループを自動的に設定します。

6. 共有する各ディレクトリーについて、**/etc/exports** ファイルにエクスポートポイントを追加します。

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

このエントリーは、**/nfs/projects/** ディレクトリーを共有し、**192.0.2.0/24** および **2001:db8::/32** サブネット内のクライアントに読み取りおよび書き込みアクセスを許可します。

7. **firewalld** で適切なポートを開きます。

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

8. NFS サーバーを有効にして起動します。

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

検証

- サーバー上で、設定した NFS バージョンのみがサーバーから提供されていることを確認します。

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

- クライアントで次の手順を実行します。

1. **nfs-utils** パッケージをインストールします。

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

2. エクスポートされた NFS 共有をマウントします。

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

3. **users** グループのメンバーであるユーザーとして、**/mnt/** にファイルを作成します。

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

4. ファイルが作成されたことを確認するためにディレクトリーの内容をリスト表示します。

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

2.8. オプションの NFSV4 サポートを備えた NFSV3 サーバーの設定

NFSv3 クライアントを現在も使用しているネットワークでは、NFSv3 プロトコルを使用して共有を提供するようにサーバーを設定します。ネットワーク内に新しいクライアントもある場合は、さらに NFSv4 を有効にできます。デフォルトでは、Red Hat Enterprise Linux の NFS クライアントは、サーバーが提供する最新の NFS バージョンを使用します。

手順

1. **nfs-utils** パッケージをインストールします。

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

2. オプション: デフォルトでは、NFSv3 と NFSv4 が有効になっています。NFSv4 が必要ない場合、または特定のマイナーバージョンのみが必要な場合は、すべての **vers4.<minor_version>** パラメーターのコメントを解除し、各パラメーターを適切に設定します。

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

この設定では、サーバーは NFS バージョン 3 と 4.2 のみを提供します。



重要

特定の NFSv4 マイナーバージョンのみが必要な場合は、そのマイナーバージョンのパラメーターのみを設定してください。予期しないマイナーバージョンのアクティブ化や非アクティブ化を回避するために、**vers4** パラメーターのコメントは解除しないでください。**vers4** パラメーターは、デフォルトですべての NFSv4 マイナーバージョンを有効または無効にします。ただし、**vers4** を他の **vers** パラメーターと組み合わせて設定すると、この動作は変わります。

3. デフォルトでは、NFSv3 の RPC サービスはランダムなポートを使用します。ファイアウォール設定を有効にするには、**/etc/nfs.conf** ファイルで固定ポート番号を設定します。
 - a. **[lockd]** セクションで、**nlockmgr** RPC サービスの固定ポート番号を設定します。以下に例を示します。

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

この設定により、サービスが UDP プロトコルと TCP プロトコルの両方にこのポート番号を自動的に使用するようになります。

- b. **[statd]** セクションで、**rpc.statd** サービスの固定ポート番号を設定します。以下に例を示します。

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

この設定により、サービスが UDP プロトコルと TCP プロトコルの両方にこのポート番号を自動的に使用するようになります。

4. オプション: 共有するディレクトリーを作成します。以下に例を示します。

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

既存のディレクトリーを共有する場合は、このステップをスキップしてください。

5. **/nfs/projects/** ディレクトリーに必要な権限を設定します。

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

これらのコマンドは、**/nfs/projects/** ディレクトリーの **users** グループの書き込み権限を設定し、このディレクトリーに作成される新しいエントリーに対して同じグループを自動的に設定します。

6. 共有する各ディレクトリーについて、**/etc/exports** ファイルにエクスポートポイントを追加します。

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

このエントリーは、**/nfs/projects/** ディレクトリーを共有し、**192.0.2.0/24** および **2001:db8::/32** サブネット内のクライアントに読み取りおよび書き込みアクセスを許可します。

7. **firewalld** で適切なポートを開きます。

```
# 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
```

- NFS サーバーを有効にして起動します。

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

検証

- サーバー上で、設定した NFS バージョンのみがサーバーから提供されていることを確認します。

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

- クライアントで次の手順を実行します。
 - nfs-utils** パッケージをインストールします。

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

- エクスポートされた NFS 共有をマウントします。

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

- 指定した NFS バージョンを使用して共有がマウントされたことを確認します。

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

- users** グループのメンバーであるユーザーとして、**/mnt/** にファイルを作成します。

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

- ファイルが作成されたことを確認するためにディレクトリーの内容をリスト表示します。

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

2.9. NFS サーバーでクォータサポートを有効にする

ユーザーまたはグループが保存できるデータの量を制限する場合は、ファイルシステムにクォータを設定できます。クォータは、NFS サーバー上の **rpc-rquotad** サービスにより、NFS クライアント上のユーザーにも適用されます。

前提条件

- NFS サーバーが実行および設定されている。
- [ext](#) または [XFS](#) ファイルシステムにクォータが設定されている。

手順

1. エクスポートするディレクトリーでクォータが有効になっていることを確認します。

- ext ファイルシステムの場合は、次のように入力します。

```
# 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
```

- XFS ファイルシステムの場合は、次のように入力します。

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

2. **quota-rpc** パッケージをインストールします。

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

3. オプション: デフォルトでは、クォータ RPC サービスはポート 875 で実行されます。別のポートでサービスを実行する場合は、**/etc/sysconfig/rpc-rquotad** ファイルの **RPCRQUOTADOPTS** 変数に **-p <port_number>** を追加します。

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

4. オプション: デフォルトでは、リモートホストはクォータの読み取りのみが可能です。クライアントにクォータの設定を許可するには、**/etc/sysconfig/rpc-rquotad** ファイルの **RPCRQUOTADOPTS** 変数に **-S** オプションを追加します。

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

5. **firewalld** でポートを開きます。

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

6. **rpc-quotad** サービスを有効にして起動します。

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

検証

1. クライアントで以下を実行します。
 - a. エクスポートされた共有をマウントします。

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

- b. クォータを表示します。コマンドは、エクスポートされたディレクトリーのファイルシステムによって異なります。以下に例を示します。

- マウントした全 ext ファイルシステムの特定ユーザーのクォータを表示するには、次のように入力します。

```
# 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
      OK    100M   200M           0    0    0
```

- XFS ファイルシステムのユーザーおよびグループのクォータを表示するには、次のように入力します。

```
# 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 [-----]
```

関連情報

- [quota\(1\) man ページ](#)
- [xfs_quota\(8\) man ページ](#)

2.10. NFS サーバーで NFS OVER RDMA を有効にする

Remote Direct Memory Access (RDMA) は、クライアントシステムがストレージサーバーのメモリーから自身のメモリーにデータを直接転送できるようにするプロトコルです。これにより、ストレージのスループットが向上し、サーバーとクライアント間のデータ転送の遅延が減少し、両側の CPU 負荷が軽減されます。NFS サーバーとクライアントの両方が RDMA 経由で接続されている場合、クライアントは NFS over RDMA (NFS over RDMA) を使用してエクスポートされたディレクトリーをマウントできます。

前提条件

- NFS サービスが実行および設定されている。
- InfiniBand または RDMA over Converged Ethernet (RoCE) デバイスがサーバーにインストールされている。
- サーバーに IP over InfiniBand (IPoIB) が設定され、InfiniBand デバイスに IP アドレスが割り当てられている。

手順

- rdma-core** パッケージをインストールします。

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

- パッケージがすでにインストールされている場合は、**/etc/rdma/modules/rdma.conf** ファイル内の **xprtrdma** および **svcrdma** モジュールのコメントが解除されていることを確認します。

```
# NFS over RDMA client support
```

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

3. オプション: デフォルトでは、NFS over RDMA はポート 20049 を使用します。別のポートを使用する場合は、`/etc/nfs.conf` ファイルの `[nfsd]` セクションで `rdma-port` 設定を指定します。

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

4. `firewalld` で NFSoRDMA ポートを開きます。

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

20049 以外のポートを設定する場合は、ポート番号を変更します。

5. `nfs-server` サービスを再起動します。

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

検証

1. InfiniBand ハードウェアを搭載したクライアントで、次の手順を実行します。
 - a. 以下のパッケージをインストールします。

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

- b. エクスポートされた NFS 共有を RDMA 経由でマウントします。

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

デフォルト (20049) 以外のポート番号を設定する場合は、コマンドに `port=<port_number>` を渡します。

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

- c. `rdma` オプションを使用して共有がマウントされたことを確認します。

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

関連情報

- [InfiniBand ネットワークおよび RDMA ネットワークの設定](#)

2.11. RED HAT IDENTITY MANAGEMENT ドメインで KERBEROS を使用する NFS サーバーを設定する

Red Hat Identity Management (IdM) を使用すると、NFS サーバーを IdM ドメインに参加させることができます。これにより、ユーザーとグループを一元管理し、認証、整合性保護、トラフィック暗号化に Kerberos を使用できるようになります。

前提条件

- NFS サーバーが Red Hat Identity Management (IdM) ドメインに [登録](#) されている。
- NFS サーバーが実行および設定されている。

手順

1. IdM 管理者として Kerberos チケットを取得します。

```
# kinit admin
```

2. `nfs/<FQDN>` サービスプリンシパルを作成します。

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

3. IdM から `nfs` サービスプリンシパルを取得し、`/etc/krb5.keytab` ファイルに保存します。

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

4. オプション: `/etc/krb5.keytab` ファイル内のプリンシパルを表示します。

```
# 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
```

デフォルトでは、ホストを IdM ドメインに参加させると、IdM クライアントがホストプリンシパルを `/etc/krb5.keytab` ファイルに追加します。ホストプリンシパルがない場合は、`ipa-getkeytab -s idm_server.idm.example.com -p host/nfs_server.idm.example.com -k /etc/krb5.keytab` コマンドを使用して追加します。

5. `ipa-client-automount` ユーティリティを使用して、IdM ID のマッピングを設定します。

```
# 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. `/etc/exports` ファイルを更新し、クライアントオプションに Kerberos セキュリティ方式を追加します。以下に例を示します。

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

クライアントが複数のセキュリティー方式を選択できるようにするには、それらをコロンで区切って指定します。

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

7. エクスポートされたファイルシステムを再ロードします。

```
| # exportfs -r
```