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

Last Updated: 2022-07-19

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

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

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 5

RED HAT ドキュメントへのフィードバックの提供 6

第1章 SAMBA をサーバーとして使用 7
1.1. さまざまな SAMBA サービスおよびモードについて 7
1.1.1. Samba サービス 7
1.1.2. Samba セキュリティーサービス 8
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 9
1.1.4. 安全な方法での Samba 設定の編集 9
1.2. SAMBA 設定の確認 10
1.2.1. testparm ユーティリティーを使用した smb.conf ファイルの検証 10
1.3. SAMBA をスタンドアロンサーバーとして設定 11
1.3.1. スタンドアロンサーバーのサーバー構成の設定 11
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 12
1.4. SAMBA ID マッピングの理解および設定 13
1.4.1. Samba ID 範囲の計画 13
1.4.2. * デフォルトドメイン 14
1.4.3. tdb ID マッピングバックエンドの使用 15
1.4.4. ad ID マッピングバックエンドの使用 15
1.4.5. rid ID マッピングバックエンドの使用 18
1.4.6. autorid ID マッピングバックエンドの使用 20
1.5. SAMBA を AD ドメインメンバーサーバーとして設定 22
1.5.1. RHEL システムの AD ドメインへの参加 22
1.5.2. MIT Kerberos 用のローカル承認プラグインの使用 24
1.6. IDM ドメインメンバーでの SAMBA の設定 25
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 26
1.6.2. GPO を使用した Active Directory で AES 暗号化タイプの有効化 27
1.6.3. 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 28
1.6.4. IdM が新しいドメインを信頼する場合は、IDマッピング構成を手動で追加 30
1.6.5. 関連情報 31
1.7. POSIX ACL を使用した SAMBA ファイル共有の設定 31
1.7.1. POSIX ACL を使用する共有の追加 31
1.7.2. POSIX ACL を使用する Samba 共有での標準的な Linux ACL の設定 33
1.7.3. POSIX ACL を使用する Samba 共有で拡張 ACL の設定 33
1.8. POSIX ACL を使用する共有への権限の設定 35
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 36
1.8.2. ホストベースの共有アクセスの設定 36
1.9. WINDOWS ACL で共有の設定 37
1.9.1. SeDiskPrivilege 特権の付与 37
1.9.2. Windows ACL サポートの有効化 38
1.9.3. Windows ACL を使用する共有の追加 38
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 39
1.10. SMBCACLS で SMB 共有上の ACL の管理 40
1.10.1. アクセス制御エントリー 40
1.10.2. smbcacls を使用した ACL の表示 43
1.10.3. ACE マスク計算 43
1.10.4. smbcacls を使用した ACL の追加、更新、および削除 44
ACL の追加 44
ACL の更新 44
ACL の削除 44

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 44
1.11.1. ユーザーの共有機能の有効化 44
1.11.2. ユーザー共有の追加 46
1.11.3. ユーザー共有の設定の更新 46
1.11.4. 既存のユーザー共有に関する情報の表示 46
1.11.5. ユーザー共有の一覧表示 47
1.11.6. ユーザー共有の削除 47
1.12. 認証なしでアクセスを許可する共有の設定 48
1.12.1. 共有へのゲストアクセスの有効化 48
1.13. MACOS クライアント向けの SAMBA の設定 49
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 49
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 50
1.14.1. smbclient 対話モードの動作 50
1.14.2. 対話モードでの smbclient の使用 51
1.14.3. スクリプトモードでの smbclient の使用 52
1.15. プリントサーバーとしての SAMBA の設定 52
1.15.1. Samba の spoolssd サービス 52
1.15.2. Samba でのプリントサーバーのサポートの有効化 54
1.15.3. 特定のプリンターの手動共有 55
1.16. 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 55
1.16.1. プリンタードライバーに関する基本情報 56
対応しているドライバーモデルのバージョン 56
パッケージ対応ドライバー 56
アップロードするプリンタードライバーの準備 56
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 56
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 56
1.16.3. print$ 共有の設定 57
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 59
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 62
1.17. FIPS モードが有効なサーバーでの SAMBA の実行 62
1.17.1. FIPS モードでの Samba の使用制限 62
1.17.2. FIPS モードでの Samba の使用 63
1.18. SAMBA サーバーのパフォーマンスチューニング 63
1.18.1. SMB プロトコルバージョンの設定 64
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 64
1.18.3. パフォーマンスが低下する可能性のある設定 65
1.19. SAMBA が、SMB バージョンがデフォルトよりも低いクライアントと互換性するように設定 65
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 65
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 66
1.20.1. net ads join コマンドおよび net rpc join コマンドの使用 66
1.20.2. net rpc rights コマンドの使用 67
設定可能な権限の一覧表示 68
特権の付与 68
特権の取り消し 68
1.20.3. net rpc share コマンドの使用 68
共有の一覧表示 68
共有の追加 69
共有の削除 69
1.20.4. net user コマンドの使用 69
ドメインユーザーアカウントの一覧表示 70
ユーザーアカウントのドメインへの追加 70
ドメインからのユーザーアカウントの削除 70
1.20.5. rpcclient ユーティリティーの使用 71

例 71
1.20.6. samba-regedit アプリケーションの使用 72
1.20.7. smbcontrol ユーティリティーの使用 72
1.20.8. smbpasswd ユーティリティーの使用 73
1.20.9. smbstatus ユーティリティーの使用 74
1.20.10. smbtar ユーティリティーの使用 75
1.20.11. wbinfo ユーティリティーの使用 75
1.21. 関連情報 76

第2章 NFS 共有のエクスポート 77
2.1. NFS の概要 77
2.2. 対応している NFS バージョン 77
デフォルトの NFS バージョン 77
NFS のマイナーバージョンの機能 77
2.3. NFSV3 と NFSV4 の TCP プロトコルと UDP プロトコル 78
2.4. NFS が必要とするサービス 78
NFSv4 を使用する RPC サービス 79
2.5. NFS ホスト名の形式 79
2.6. NFS サーバーの設定 80
2.6.1. /etc/exports 設定ファイル 80
エクスポートエントリー 80
デフォルトのオプション 81
デフォルトオプションと上書きオプション 82
2.6.2. exportfs ユーティリティー 82
一般的な exportfs オプション 82
2.7. NFS および RPCBIND 83
2.8. NFS のインストール 84
2.9. NFS サーバーの起動 84
2.10. NFS と RPCBIND のトラブルシューティング 84
2.11. ファイアウォールの背後で動作するように NFS サーバーを設定する 85
2.11.1. ファイアウォールの内側で動作するように NFSv3 対応サーバーを設定 86
2.11.2. ファイアウォールの内側で実行されるように NFSv4 専用サーバーを設定する手順 87
2.11.3. ファイアウォールの内側で動作するように NFSv3 クライアントを設定する手順 87
2.11.4. ファイアウォールの内側で動作するように NFSv4 クライアントを設定する 89
2.12. ファイアウォールからの RPC クォータのエクスポート 89
2.13. NFS OVER RDMA の有効化 (NFSORDMA) 90
2.14. 関連情報 90

第3章 NFS のセキュア化 91
3.1. AUTH_SYS とエクスポート制御による NFS 保護 91
3.2. AUTH_GSSを使用した NFS セキュリティー 91
3.3. KERBEROS を使用するために NFS サーバーおよびクライアントを設定 92
3.4. NFSV4 セキュリティーオプション 93
3.5. マウントされた NFS エクスポートに対するファイル権限 93

第4章 NFS での PNFS SCSI レイアウトの有効化 94
4.1. PNFS テクノロジー 94
4.2. PNFS SCSI レイアウト 94
クライアントとサーバーとの間の操作 94
デバイスの予約 94
4.3. PNFS と互換性がある SCSI デバイスの確認 95
4.4. サーバーで PNFS SCSI の設定 96
4.5. クライアントで PNFS SCSI の設定 96
4.6. サーバーでの PNFS SCSI 予約の解放 97

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 プロパティー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、弊社の CTO、Chris Wright のメッセージ を参照してください。

RED HAT ドキュメントへのフィードバックの提供

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。

- 特定の部分についての簡単なコメントをお寄せいただく場合は、以下をご確認ください。
  1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上隅に **Feedback** ボタンがあることを確認してください。
  2. マウスカーソルで、コメントを追加する部分を強調表示します。
  3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
  4. 表示される手順に従ってください。
- Bugzilla を介してフィードバックを送信するには、新しいチケットを作成します。
  1. Bugzilla の Web サイトに移動します。
  2. Component で **Documentation** を選択します。
  3. **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記入してください。
  4. **Submit Bug** 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

本セクションでは、Samba に含まれるさまざまなサービスと設定可能なさまざまなモードを説明します。

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) のインターフェースを提供します。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** デー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設定する方法は、「Samba をスタンドアロンサーバー として設定」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が設定を読み込み、再読み込みするときの方法を説明します。

- Samba サービスは、設定を再読み込みします。
  - 3 分ごとに自動更新
  - 手動要求では、たとえば、**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。リロードに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。この手順では、**testparm** ユーティリティーを使用して設定を検証する前に、サービスが変更をリロードしないように Samba 設定を編集する方法を説明します。

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. コピーされ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で上書きします。

```
# 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、または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

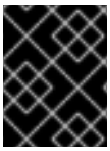
- Samba サービスおよび Samba クライアントユーティリティーが設定を読み込み、再読み込みするシナリオ

1.2. SAMBA 設定の確認

Red Hat は、**/etc/samba/smb.conf** ファイルを更新するたびに Samba 設定を確認することを推奨します。本セクションでは、その詳細を説明します。

1.2.1. 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** ファイルは存在します。

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 levell"
Processing section "[example_share]"
Loaded services file OK.
ERROR: The idmap range for the domain * (tdb) overlaps with the range of DOMAIN (ad)!

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
 ...

[example_share]
 ...
```

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

2. **testparm** が設定内の間違ったパラメーター、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構成の設定

本セクションでは、Samba スタンドアロンサーバーにサーバー構成を設定する方法を説明します。

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
```

この構成では、**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 名まで展開します。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構成します。参照:

- POSIX ACL で共有の設定
- Windows ACL で共有の設定
- Samba をプリントサーバーとして設定

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 page

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。

このセクションの手順では、ローカル Samba ユーザー (**example**) を作成する方法を説明します。

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、設定されている。

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の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の 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ンディングの 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。

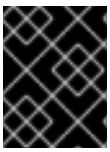
1.4.2. * デフォルトドメイン

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、このセクションで説明されている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、セキュリティー識別子 (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

本セクションでは、**ad** ID マッピングバックエンドを使用するように Samba AD メンバーを設定する方法を説明します。

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。

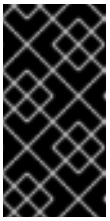
   ```
   idmap config * : backend = tdb
   idmap config * : range = 10000-999999
   ```

   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構成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)** and **idmap_ad(8)** man pages
- **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

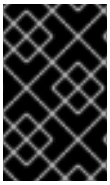
本セクションでは、**rid** ID マッピングバックエンドを使用するように Samba ドメインメンバーを設定する方法を説明します。

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、変数を使用できます。
- 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 がその範囲内に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構成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

本セクションでは、Samba ドメインメンバーを設定して、**autorid** ID マッピングバックエンドを使用する方法を説明します。

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 が範囲内にないユーザーおよびグループを無視します。

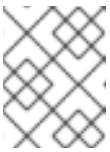
   警告

   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構成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
- man ページの **idmap_autorid(8)** 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。本セクションでは、**realmd** を使用して Samba Winbind を設定して、RHEL システムを AD ドメインに参加させる方法を説明します。

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。

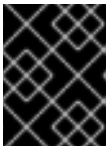
- **ad.example.com** ドメインのメンバーシップに **/etc/samba/smb.conf** ファイルを作成します。
- ユーザーおよびグループの検索用の **winbind** モジュールを、**/etc/nsswitch.conf** ファイルに追加します。
- **/etc/pam.d/** ディレクトリーの PAM (プラグ可能な認証モジュール) 設定ファイルを更新します。
- **winbind** サービスを起動し、システムの起動時にサービスを起動できるようにします。

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「Samba ID マッピングの概要」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。「Using the local authorization plug-in for MIT Kerberos」を参照してください。

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。GPO を使用した Active Directory で AES 暗号化タイプの有効化について参照し てください。これは、AD の他のサービスに影響を及ぼす可能性があることに注意してください。
- man ページの **realm(8)**

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)** の man ページ

1.6. IDM ドメインメンバーでの SAMBA の設定

本セクションでは、Red Hat Identity Management (IdM) ドメインに参加しているホストで Samba を設定する方法を説明します。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の Samba の使用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 Global Catalog サービスをサポートしません。DCE/RPC(Distributed Computing Environment / Remote Procedure Calls)プロトコルを使用した IdM グループの解決には対応していません。これにより、AD ユーザーは、他の IdM クライアントにログインする際に、IdM クライアントでホストされる Samba 共有および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 をデプロイする場合は、Red Hat にフィードバックをお寄せください。

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。

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. プロンプトが表示されたら、IdM ドメインの NetBIOS 名を入力するか、**Enter** を押して提案された名前を使用します。

```
Trust is configured but no NetBIOS domain name found, setting it now.
Enter the NetBIOS name for the IPA domain.
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
Example: EXAMPLE.

NetBIOS domain name [IDM]:
```

7. 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。

8. **(必要に応じて)** デフォルトでは、Windows Server 2008 以降では、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
```

9. **ipa** サービスを再起動します。

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

10. **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 server.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. GPO を使用した Active Directory で AES 暗号化タイプの有効化

本セクションでは、グループポリシーオブジェクト (GPO) を使用して、Active Directory (AD) で AES 暗号化タイプを有効にする方法を説明します。IdM クライアントで Samba サーバーを実行するなど、RHEL の特定の機能には、この暗号化タイプが必要です。

RHEL は、弱い DES および RC4 の暗号化タイプをサポートしなくなった点に注意してください。

前提条件

- グループポリシーを編集できるユーザーとして AD にログインしている。
- **Group Policy Management Console** がコンピューターにインストールされている。

手順

1. **Group Policy Management Console** を開きます。
2. **デフォルトドメインポリシー** を右クリックして、**編集** を選択します。**Group Policy Management Editor** を閉じます。
3. **コンピューターの設定 → ポリシー → Windows の設定 → セキュリティの設定 → ローカルポリシー → セキュリティーオプション** に移動します。
4. **ネットワーク セキュリティ: Kerberos で許可する暗号化の種類を構成する** をダブルクリックします。
5. **AES256_HMAC_SHA1** を選択し、必要に応じて、**将来の暗号化タイプ** を選択します。
6. **OK** をクリックします。
7. **Group Policy Management Editor** を閉じます。
8. **既定のドメインコントローラーポリシー** に対して手順を繰り返します。
9. Windows ドメインコントローラー (DC) がグループポリシーを自動的に適用するまで待ちます。または、GPO を DC に手動で適用するには、管理者権限を持つアカウントを使用して次のコマンドを入力します。

```
C:\> gpupdate /force /target:computer
```

1.6.3. 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

本セクションでは、IdM ドメインに登録されたクライアントに Samba をインストールおよび設定する方法を説明します。

前提条件

- IdM サーバーとクライアントは、RHEL 9.0 以降で実行する必要があります。
- 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 構成を作成します。

```
[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
```

3. 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
```

4. ディレクトリーとプリンターを共有します。詳細は、次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

5. 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
```

6. **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一覧表示します。

```
$ 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

1.6.4. IdM が新しいドメインを信頼する場合は、IDマッピング構成を手動で追加

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 に新しい信頼を追加されています。
- 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。セキュリティー上の理由から、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 マッピング構成を **[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一覧表示します。

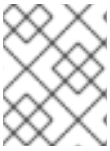
```
$ smbclient -L idm_client.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry

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

1.6.5. 関連情報

- 「Identity Management クライアントのインストール」を参照してください。

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

代わりに詳細な 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

本セクションでは、**/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する方法を説明します。

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. ディレクトリーにファイルシステムの ACL を設定します。詳細は、次を参照してください。
   - POSIX ACL を使用する Samba 共有での標準 ACL の設定
   - POSIX ACL を使用する共有での拡張 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 がディレクトリー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。ユーティリティーの **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。を参照してください。

POSIX ACL を使用する Samba 共有に拡張 ACL を設定 する。

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 を使用した共有の設定 」を参照してください。

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ました。

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 page

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** パラメーターに一覧表示されている 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 page

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 を使用するように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一覧表示するには、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

本セクションでは、**/srv/samba/example/** ディレクトリーのコンテンツを共有する **example** という名前の共有を作成し、Windows ACL を使用する方法を説明します。

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 ユーティリティーは、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 を一覧表示、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	コンテナーの継承	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。
OI|CI	このフォルダー、サブフォルダー、およびファイル
OI|CI|IO	サブフォルダーおよびファイルのみ
CI|IO	サブディレクトリーのみ
OI|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**
フォルダーの一覧表示 / 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: ○ 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** ユーティリティーを使用します。**--add** などの操作パラメーターを付けずに **smbcacls** を実行すると、ユーティリティーは、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 を一覧表示するには、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場合は、既存の **smbcacls** エイリアス とそれに対応する Windows パーミッション に記載されている 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。

- フォルダーのスキャン / ファイルの実行 (0x00100020)
- フォルダーの一覧表示 / 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 ユーティリティー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ープリンシパルを使用して ACL を上書きします。**smbcacls** が ACL 一覧内でセキュリティープリンシパルを検出すると、ユーティリティー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** ユーティリティーに渡します。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一覧を設定します。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一覧は、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
```

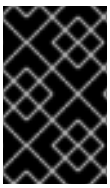
これで、ユーザーが、ユーザー共有を作成できるようになりました。

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 参照してください。

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一覧表示するには、**-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. ユーザー共有の一覧表示

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一覧表示するには、**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一覧表示するには、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一覧表示するには、**-l** パラメーターを省略します。

2. 特定の共有のみを一覧表示するには、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一覧表示するには、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、セキュリティー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 に一覧表示されます。
- **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。セキュリティー上の理由から、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

本セクションでは、サーバーでホストされるすべての Samba 共有に **fruit** モジュールを設定し、macOS クライアントの Samba ファイル共有を最適化する方法を説明します。

注記

Red Hat は、**fruit** モジュールをグローバルに有効にすることを推奨します。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際に、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 で共有の 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)** の 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一覧表示します。

   ```
   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

- 以下のコマンドを使用して共有に接続し **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 の spoolssd サービス

Samba の **spoolssd** は、**smbd** サービスに統合されるサービスです。Samba 設定の **spoolssd** を有効にすると、大量のジョブまたはプリンターがあるプリントサーバーのパフォーマンスが大幅に向上します。

spoolssd がないと、Samba は **smbd** プロセスをフォークし、各プリントジョブの **printcap** キャッシュを初期化します。プリンターが多数あると、キャッシュの初期化中に **smbd** サービスが数秒間応答しなくなることがあります。**spoolssd** サービスを使用すると、遅延なしでプリントジョブを処理している、プレフォークされた **smbd** プロセスを開始することができます。主な **spoolssd smbd** プロセスは、少ないメモリーを使用し、子プロセスをフォークして終了します。

以下の手順では、**spoolssd** サービスを有効にする方法を説明します。

手順

1. **/etc/samba/smb.conf** ファイルの **[global]** セクションを編集します。
   a. 以下のパラメーターを追加します。

```
rpc_server:spoolss = external
rpc_daemon:spoolssd = fork
```

   b. 必要に応じて、以下のパラメーターを設定できます。

パラメーター	デフォルト	説明
spoolssd:prefork_min_children	5	子プロセスの最小数
spoolssd:prefork_max_children	25	子プロセスの最大数
spoolssd:prefork_spawn_rate	5	新しい接続が確立されると、Samba は、このパラメーターに設定した新しい子プロセスの数を、**spoolssd:prefork_max_children** に設定された値までフォークします。
spoolssd:prefork_max_allowed_clients	100	子プロセスが処理するクライアントの数
spoolssd:prefork_child_min_life	60	子プロセスの最小有効期間 (秒単位)。最小は 60 秒です。

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

```
# testparm
```

3. **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 が自動的に **smbd** 子プロセスを開始します。

```
# ps axf
...
30903 smbd
30912  \_ smbd
30913      \_ smbd
30914      \_ smbd
30915      \_ smbd
...
```

1.15.2. Samba でのプリントサーバーのサポートの有効化

本セクションでは、Samba でプリントサーバーのサポートを有効にする方法を説明します。

手順

1. Samba サーバーで CUPS を設定し、そのプリンターを CUPS バックエンドに追加します。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。

注記

Samba は、CUPS が Samba プリントサーバーにローカルにインストールされている場合に限り、CUPS に印刷ジョブを転送できます。

2. **/etc/samba/smb.conf** ファイルを編集します。

   a. **spoolssd** サービスを有効にする場合は、以下のパラメーターを **[global]** セクションに追加します。

```
rpc_server:spoolss = external
rpc_daemon:spoolssd = fork
```

   b. 印刷バックエンドを設定するには、**[printers]** セクションを追加します。

```
[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。

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

```
# testparm
```

4. **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
```

5. **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。

1.15.3. 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ス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. 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、ドライバーを展開します。
- 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

1. 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。

2. **SePrintOperatorPrivilege** が付与されているユーザーとグループの一覧を表示するには、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す。
- 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. プリンターの 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]** セクションにこの設定を含めます。

```
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一覧表示、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

プリンシパル	アクセス	適用先
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。

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

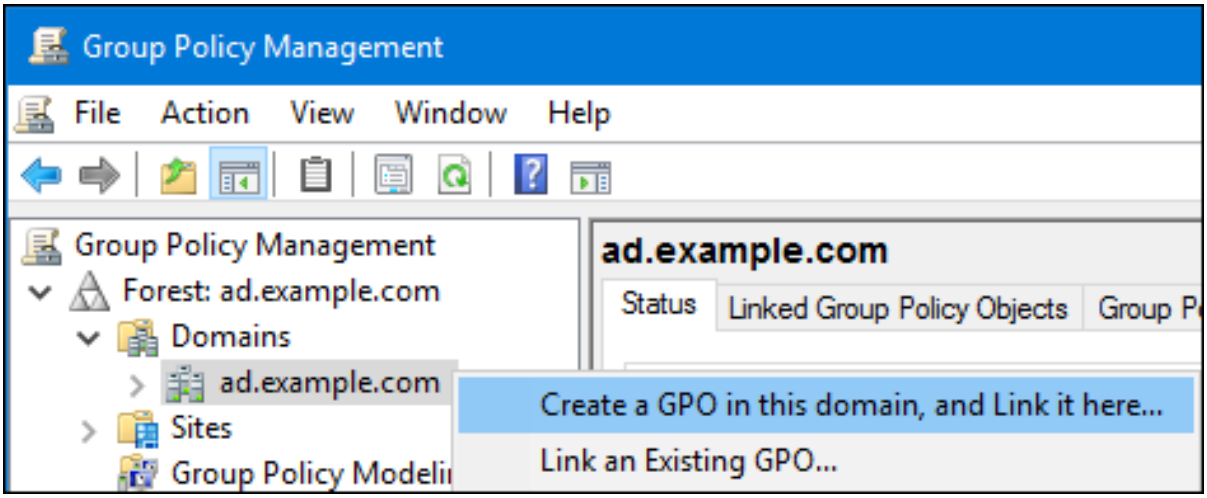
セキュリティー上の理由から、最新の Windows オペレーティングシステムでは、クライアントが、信頼できないサーバーから、パッケージ対応ではないプリンタードライバーをダウンロードできないようにします。プリントサーバーが AD のメンバーである場合は、Samba サーバーを信頼するために、ドメインに Group Policy Object (GPO) を作成できます。

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

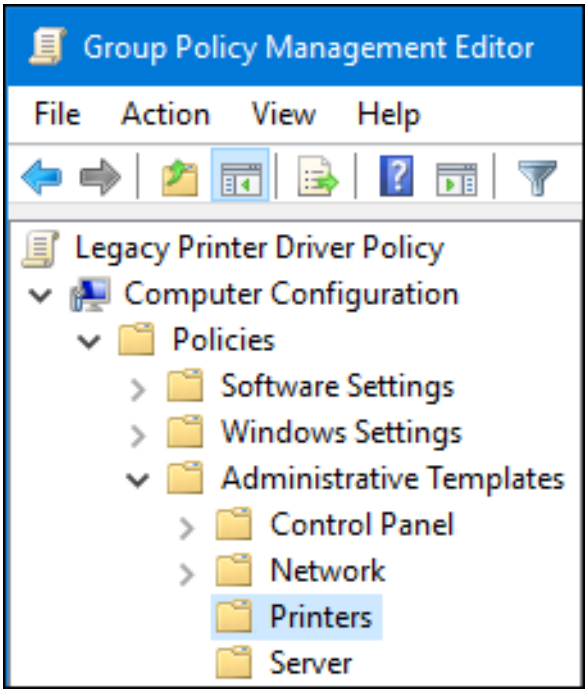
1. AD ドメインの **管理者** ユーザーなど、グループポリシーの編集が可能なアカウントを使用して、Windows コンピューターにログインします。
2. **Group Policy Management Console** を開きます。
3. AD ドメインを右クリックし、**Create a GPO in this domain, and Link it here** を選択します。



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。

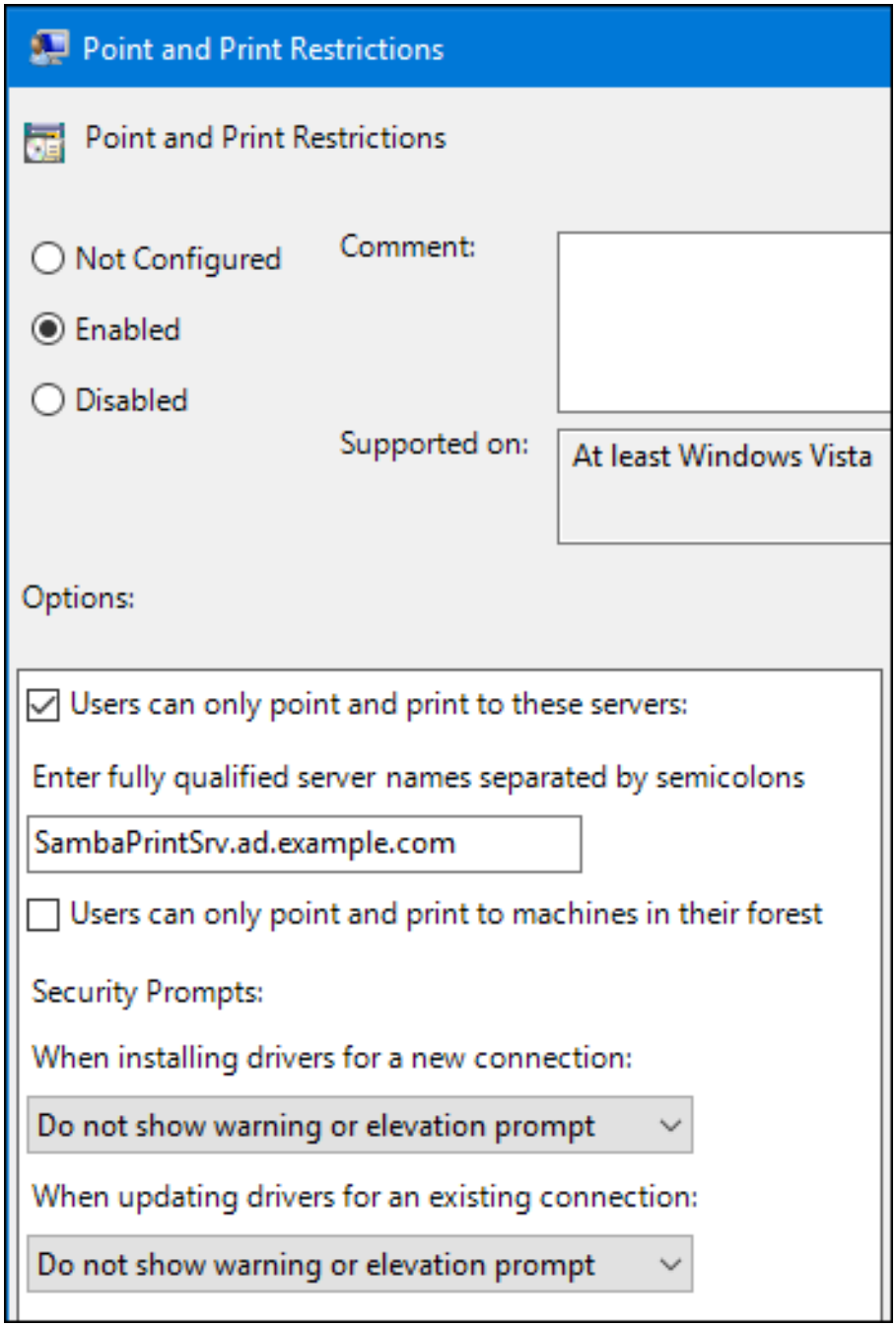


7. ウィンドウの右側で、**Point and Print Restriction** をダブルクリックして、ポリシーを編集します。

   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。

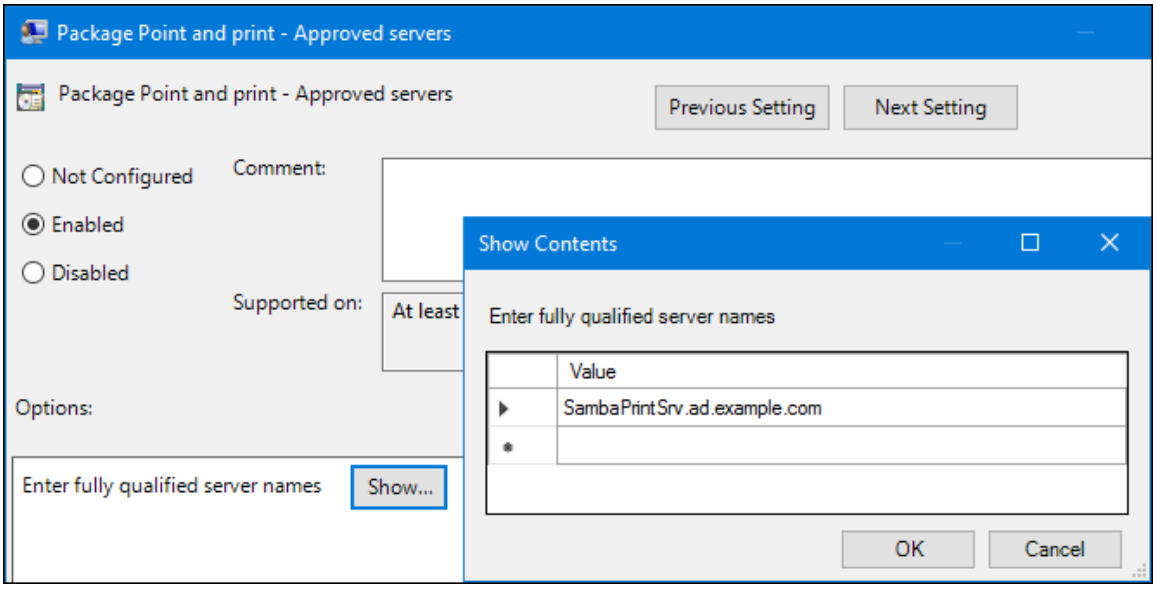


b. OK をクリックします。

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ー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 のセキュリティー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ー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

本セクションでは、Samba を実行する RHEL ホストで FIPS モードを有効にする方法を説明します。

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

本章では、特定の状況で Samba のパフォーマンスを改善できる設定と、パフォーマンスが低下する可能性のある設定を説明します。

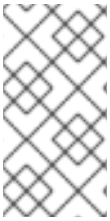
このセクションの一部は、Samba Wiki に公開されているドキュメント「Performance Tuning」に掲載されています。ライセンスは、CC BY 4.0 にあります。著者および貢献者は、Wiki ページの history タブを参照してください。

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。

2. 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。

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
```

この設定が適用されと、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ー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。

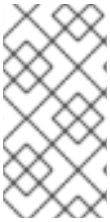
カーネルの最適化された設定を使用するには、**/etc/samba/smb.conf** の **[global]** セクションから **socket options** パラメーターを削除します。

1.19. SAMBA が、SMB バージョンがデフォルトよりも低いクライアントと互換性するように設定

Samba は、サポートしている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、古い 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。本セクションでは、SMB プロトコルの最小バージョンを変更する方法を説明します。



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 page

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ー **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 をドメインに参加させる。
- 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ー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。

設定可能な権限の一覧表示
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.
```

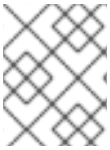
1.20.3. net rpc share コマンドの使用

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 サーバーの共有の一覧表示、追加、および削除を行う機能を提供します。

共有の一覧表示
SMB サーバーの共有を一覧表示するには、**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一覧表示します。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
...
```



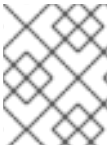
注記

/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
```

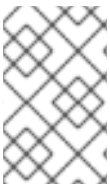
このコマンドを使用して Samba サーバーから共有を削除するには、以下のコマンドを実行します。

- **-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一覧を表示
- 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一覧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一覧表示
AD ドメイン内のユーザーを一覧表示するには、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一覧表示するには、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一覧表示

  ```
  # 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一覧表示

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

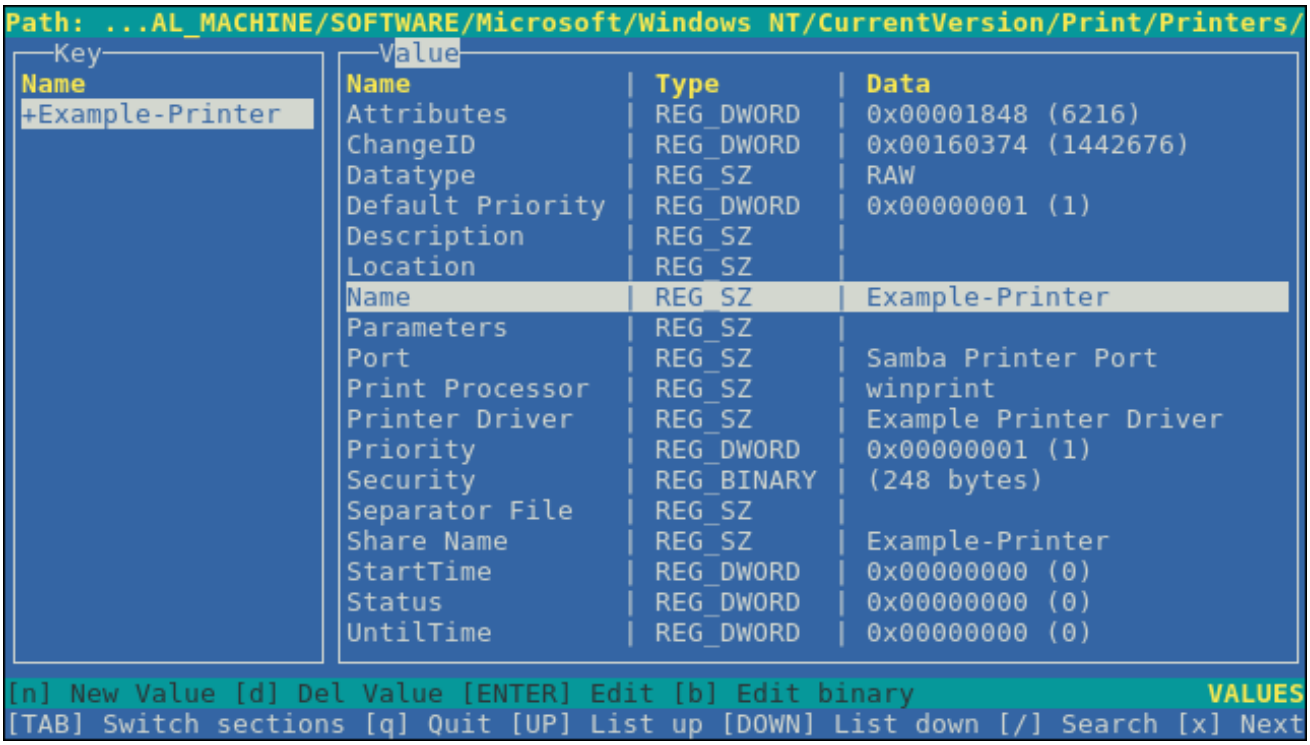
  スタンドアロンサーバーまたはドメインメンバーに対してコマンドを実行すると、ローカルデータベースのユーザーの一覧が表示されます。ADDC または NT4 PDC に対してコマンドを実行すると、ドメインユーザーの一覧が表示されます。

関連情報

- **rpcclient(1)** の 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。



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。

本セクションの手順では、**reload-config** メッセージタイプを **すべて** の宛先に送信することで、**smbd**、**nmbd**、**winbindd** のサービスの設定を再読み込みする方法を示します。

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

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

関連情報

- **smbcontrol(1)** の 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

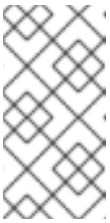
1. ユーザーとしてコマンドを実行すると、**smbpasswd** はコマンドを実行するユーザーの Samba パスワードを変更します。以下に例を示します。

```
[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構成』 の「コマンドラインから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一覧。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一覧を表示します。

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

- ドメイングループの一覧を表示します。

```
# 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

- Red Hat Samba パッケージには、パッケージがインストールするすべての Samba コマンドおよび設定ファイルの man ページが含まれています。たとえば、**/etc/samba/smb.conf** ファイルの man ページを表示して、このファイルに設定できる設定パラメーターをすべて説明します。

```
# man smb.conf
```

- **/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。

- 『Red Hat Cluster Storage Administration Guide』 - Samba と Clustered Trivial Database (CDTB) の設定に関する情報を提供し、GlusterFS ボリュームに保存されているディレクトリーを共有します。

- Red Hat Enterprise Linux での SMB 共有のマウント

第2章 NFS 共有のエクスポート

システム管理者は、NFS サーバーを使用して、ネットワーク上のシステムのディレクトリーを共有できます。

2.1. NFS の概要

本セクションでは、NFS サービスの基本概念を説明します。

ネットワークファイルシステム (NFS) を利用すると、リモートのホストがネットワーク経由でファイルシステムをマウントし、そのファイルシステムを、ローカルにマウントしているファイルシステムと同じように操作できるようになります。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。

NFS サーバーは、**/etc/exports** 設定ファイルを参照して、そのクライアントがエクスポート済みファイルシステムにアクセスできるかどうかを確認します。アクセスが可能なことが確認されると、そのユーザーは、ファイルおよびディレクトリーへの全操作を行えるようになります。

2.2. 対応している NFS バージョン

本セクションでは、Red Hat Enterprise Linux でサポートされている NFS のバージョンと、その機能の一覧を紹介します。

現在、Red Hat Enterprise Linux 9 は、以下の NFS のメジャーバージョンに対応しています。

- NFS バージョン 3 (NFSv3) は安全な非同期書き込みに対応しており、以前の NFSv2 よりもエラー処理において安定しています。64 ビットのファイルサイズとオフセットにも対応しているため、クライアントは 2 GB を超えるファイルデータにアクセスできます。
- NFS バージョン 4 (NFSv4) は、ファイアウォールやインターネットを介して動作し、**rpcbind** サービスを必要とせず、アクセス制御リスト (ACL) に対応し、ステートフルな操作を利用します。

NFS バージョン 2 (NFSv2) は、Red Hat のサポート対象外になりました。

デフォルトの NFS バージョン

Red Hat Enterprise Linux 9 のデフォルトの NFS バージョンは 4.2 です。NFS クライアントは、デフォルトで NFSv4.2 を使用してマウントを試行し、サーバーが NFSv4.2 に対応していない場合は NFSv4.1 にフォールバックします。マウントは後で NFSv4.0 に戻り、次に NFSv3 に戻ります。

NFS のマイナーバージョンの機能

以下は、Red Hat Enterprise Linux 9 における NFSv4.2 の機能です。

サーバー側コピー

NFS クライアントが **copy_file_range()** システムコールを使用してネットワークリソースを無駄にすることなく、データを効率的にコピーできるようにします。

スパースファイル

ファイルに 1 つ以上の **ホール** を持たせることができます。ホールとは、割り当てられていない、またはゼロのみで構成される未初期化データブロックです。NFSv4.2 の **lseek()** 操作は **seek_hole()** と **seek_data()** に対応しています。これにより、アプリケーションはスパースファイルのホールの場所をマップできます。

領域の予約

ストレージサーバーが空き領域を予約することを許可します。これにより、サーバーで領域が不足

することがなくなります。NFSv4.2 は、領域を予約するための **allocate()** 操作、領域の予約を解除するための **deallocate()** 操作、およびファイル内の領域の事前割り当てまたは割り当て解除を行う **fallocate()** 操作に対応しています。

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

一部の Parallel NFS (pNFS) サーバーがより良いパフォーマンス統計を収集できるようにする **layoutstats()** 操作が提供されます。

NFSv4.1 の機能は次のとおりです。

- ネットワークのパフォーマンスおよびセキュリティーを強化し、pNFS のクライアント側サポートも含みます。
- コールバックに個別の TCP 接続を必要としなくなりました。これにより、NAT やファイアウォールが干渉した場合など、クライアントと通信できない場合でも NFS サーバーは委任を許可できます。
- 応答が失われ、操作が 2 回送信された場合に特定の操作が不正確な結果を返すことがあるという以前の問題を防ぐために、1 回限りのセマンティクスを提供します (再起動操作を除く)。

2.3. NFSV3 と NFSV4 の TCP プロトコルと UDP プロトコル

NFSv4 は、IP ネットワークで TCP (Transmission Control Protocol) の実行が必要です。

NFSv3 は、Red Hat Enterprise Linux の以前のバージョンで User Datagram Protocol (UDP) を使用することもできます。Red Hat Enterprise Linux 9 では、NFS over UDP に対応しなくなりました。デフォルトでは、UDP は、NFS サーバーで無効になります。

2.4. NFS が必要とするサービス

本セクションでは、NFS サーバーの実行または NFS 共有のマウントに必要なシステムサービスの一覧を紹介します。Red Hat Enterprise Linux は、このサービスを自動的に開始します。

Red Hat Enterprise Linux では、NFS ファイル共有を提供するのに、カーネルレベルのサポートとサービスのプロセスの組み合わせを使用します。NFS のすべてのバージョンは、クライアントとサーバーとの間の RPC (Remote Procedure Call) に依存します。NFS ファイルシステムの共有やマウントには、実装されている NFS のバージョンに応じて、次のようなサービスが連携して動作することになります。

nfsd

共有 NFS ファイルシステムに対する要求を処理する NFS サーバーカーネルモジュールです。

rpcbind

ローカルの RPC サービスからポート予約を受け取ります。その後、これらのポートは、対応するリモートの RPC サービスによりアクセス可能であることが公開されます。**rpcbind** サービスは、RPC サービスへの要求に応答し、要求された RPC サービスへの接続を設定します。このプロセスは NFSv4 では使用されません。

rpc.mountd

NFS サーバーは、このプロセスを使用して NFSv3 クライアントの **MOUNT** 要求を処理します。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。マウントの要求が許可されると、**nfs-**

mountd サービスは Success ステータスで応答し、この NFS 共有用の File-Handle を NFS クライアントに戻します。

rpc.nfsd

このプロセスでは、サーバーが公開している明示的な NFS のバージョンとプロトコルを定義できます。NFS クライアントが接続するたびにサーバース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、Linux カーネルと連携して動作します。このプロセスは、**nfs-server** サービスに対応します。

lockd

クライアントとサーバーの両方で実行するカーネルスレッドです。Network Lock Manager (NLM) プロトコルを実装し、NFSv3 のクライアントが、サーバーでファイルのロックを行えるようにします。NFS サーバーが実行中で、NFS ファイルシステムがマウントされていれば、このプロセスは常に自動的に起動します。

rpc.statd

このプロセスは、Network Status Monitor (NSM) RPC プロトコルを実装します。NFS サーバーが正常にシャットダウンされずに再起動すると、NFS クライアントに通知します。**rpc-statd** サービスは、**nfs-server** サービスにより自動的に起動されるため、ユーザー設定は必要ありません。このプロセスは NFSv4 では使用されません。

rpc.rquotad

このプロセスは、リモートユーザーのユーザークォーター情報を提供します。**quota-rpc** パッケージが提供する **rpc-rquotad** サービスは、**nfs-server** の起動時にユーザーが起動する必要があります。

rpc.idmapd

このプロセスは、ネットワークの NFSv4 の名前 (**user@domain** 形式の文字列) と、ローカルの UID および GID のマッピングを行う NFSv4 の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。**idmapd** を NFSv4 で正常に動作させるには、**/etc/idmapd.conf** ファイルを設定する必要があります。少なくとも、NFSv4 マッピングドメインを定義する **Domain** パラメーターを指定する必要があります。NFSv4 マッピングドメインが DNS ドメイン名と同じ場合は、このパラメーターは必要ありません。クライアントとサーバーが ID マッピングの NFSv4 マッピングドメインに合意しないと、適切に動作しません。

rpc.idmapd を使用するのは NFSv4 サーバーだけで、**nfs-idmapd** サービスにより起動します。NFSv4 クライアントは、キーリングベースの **nfsidmap** ユーティリティーを使用します。これはカーネルによりオンデマンドで呼び出され、ID マッピングを実行します。**nfsidmap** に問題がある場合は、クライアントが **rpc.idmapd** の使用にフォールバックします。

NFSv4 を使用する RPC サービス

NFSv4 プロトコルには、マウントとロックのプロトコルが組み込まれています。サーバーは、既知の TCP ポート 2049 もリッスンします。そのため、NFSv4 は **rpcbind** サービス、**lockd** サービス、および **rpc-statd** サービスと対話する必要はありません。**nfs-mountd** サービスは、エクスポートを設定するために NFS サーバーで引き続き必要となりますが、ネットワーク上の操作には関与しません。

関連情報

- **rpcbind**を使用しないサーバーのみ NFSv4 を設定する。

2.5. NFS ホスト名の形式

本セクションでは、NFS 共有をマウントまたはエクスポートするときにホストの指定に使用するさまざまな形式を説明します。

次の形式でホストを指定できます。

単独のマシン

次のいずれかになります。

- 完全修飾ドメイン名 (サーバーにより解決)
- ホスト名 (サーバーにより解決)
- IP アドレス

IP ネットワーク

以下のいずれかの形式が有効です。

- **a.b.c.d/z** - **a.b.c.d** がネットワークで、**z** がネットマスクのビット数になります (例: **192.168.0.0/24**)。
- **a.b.c.d/netmask** - **a.b.c.d** がネットワークで、**netmask** がネットマスクになります (例: **192.168.100.8/255.255.255.0**)。

Netgroup

@group-name 形式 - **group-name** は NIS netgroup 名です。

2.6. NFS サーバーの設定

本セクションでは、NFS サーバーでエクスポートを構成する 2 種類の構文およびオプションを説明します。

- 設定ファイル **/etc/exports** を手動で編集する方法
- コマンドラインで **exportfs** ユーティリティーを使用する方法

2.6.1. /etc/exports 設定ファイル

/etc/exports ファイルは、リモートホストにどのファイルシステムをエクスポートするかを制御し、オプションを指定します。以下の構文ルールに従います。

- 空白行は無視する。
- コメント行は、ハッシュ記号 (**#**) で始める。
- 長い行は、バックスラッシュ (\) で改行できる。
- エクスポートするファイルシステムは、それぞれ 1 行で指定する。
- 許可するホストの一覧は、エクスポートするファイルシステムの後に空白文字を追加し、その後に追加する。
- 各ホストのオプションは、ホストの識別子の直後に括弧を追加し、その中に指定する。ホストと最初の括弧の間には空白を使用しない。

エクスポートエントリー
エクスポートするファイルシステムの各エントリーは、以下のように指定します。

```
export host(options)
```

各ホストにそれぞれオプションを付けて、複数のホストを 1 行で指定することもできます。この場合は、以下のように、各ホスト名の後に、そのホストに対するオプションを括弧を付けて追加します。ホストは空白文字で区切ります。

```
export host1(options1) host2(options2) host3(options3)
```

この構造では、次のようになります。

export
エクスポートするディレクトリー

host
エクスポートを共有するホストまたはネットワーク

options
ホストに使用されるオプション

例2.1 簡潔な /etc/exports ファイル

最も簡単な方法は、**/etc/exports** ファイルに、エクスポートするディレクトリーと、そのディレクトリーへのアクセスを許可するホストを指定することです。

```
/exported/directory bob.example.com
```

ここで、**bob.example.com** は、NFS サーバーから **/exported/directory/** をマウントできます。この例ではオプションが指定されていないため、NFS はデフォルトのオプションを使用します。

重要

/etc/exports ファイルの形式では、特に空白文字の使用が非常に厳しく扱われます。ホストからエクスポートするファイルシステムの間、そしてホスト同士の間には、必ず空白文字を挿入してください。また、それ以外の場所 (コメント行を除く) には、空白文字を追加しないでください。

たとえば、以下の 2 つの行は意味が異なります。

```
/home bob.example.com(rw)
/home bob.example.com (rw)
```

最初の行は、**bob.example.com** からのユーザーにのみ、**/home** ディレクトリーへの読み取り/書き込みアクセスを許可します。2 番目の行では、**bob.example.com** からのユーザーにディレクトリーを読み取り専用 (デフォルト) でマウントすることを許可し、その他のユーザーに読み取り/書き込みでマウントすることを許可します。

デフォルトのオプション
エクスポートエントリーのデフォルトオプションは次のとおりです。

ro
エクスポートするファイルシステムは読み取り専用です。リモートホストは、このファイルシステムで共有されているデータを変更できません。このファイルシステムで変更 (読み取り/書き込み) を可能にするには、rw オプションを指定します。

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。代わりに非同期書き込みを有効にするには、**async** オプションを指定します。

wdelay

NFS サーバーは、別の書き込み要求が差し迫っていると判断すると、ディスクへの書き込みを遅らせます。これにより、複数の書き込みコマンドが同じディスクにアクセスする回数を減らすことができるため、書き込みのオーバーヘッドが低下し、パフォーマンスが向上します。これを無効にするには、**no_wdelay** オプションを指定します。これは、デフォルトの sync オプションが指定されている場合に限り利用できます。

root_squash

(ローカルからではなく) リモートから接続している root ユーザーが root 権限を持つことを阻止します。代わりに、そのユーザーには、NFS サーバーにより、ユーザー ID **nobody** が割り当てられます。これにより、リモートの root ユーザーの権限を、最も低いローカルユーザーレベルにまで下げて (squash)、高い確率でリモートサーバーへの書き込む権限を与えないようにすることができます。この root squashing を無効にするには、**no_root_squash** オプションを指定します。
(root を含む) すべてのリモートユーザーの権限を下げるには、**all_squash** オプションを使用します。特定ホストのリモートユーザーに対して、NFS サーバーが割り当てるユーザー ID とグループ ID を指定するには、**anonuid** オプションと **anongid** オプションを以下のように使用します。

```
export host(anonuid=uid,anongid=gid)
```

uid と **gid** は、それぞれユーザー ID とグループ ID の番号になります。 **anonuid** オプションと **anongid** オプションにより、共有するリモート NFS ユーザー用に、特別なユーザーアカウントおよびグループアカウントを作成できます。

Red Hat Enterprise Linux の NFS では、デフォルトでアクセス制御リスト (ACL) に対応しています。この機能を無効にするには、ファイルシステムをエクスポートする際に **no_acl** オプションを指定します。

デフォルトオプションと上書きオプション
エクスポートするすべてのファイルシステムの各デフォルトは、明示的に上書きする必要があります。たとえば、**rw** オプションを指定しないと、エクスポートするファイルシステムが読み取り専用として共有されます。以下は、**/etc/exports** の例になりますが、ここでは 2 つのデフォルトオプションを上書きします。

```
/another/exported/directory 192.168.0.3(rw,async)
```

この例では、**192.168.0.3** は **/another/exported/directory/** の読み書きをマウントでき、ディスクへの書き込みはすべて非同期になります。

2.6.2. exportfs ユーティリティー

root ユーザーは、**exportfs** ユーティリティーを使用すると、NFS サービスを再起動せずにディレクトリーを選択してエクスポートまたはアンエクスポートできます。適切なオプションが指定されると、**exportfs** ユーティリティーは、エクスポートされたファイルシステムを **/var/lib/nfs/xtab** に書き込みます。ファイルシステムへのアクセス権を決定する際には、**nfs-mountd** サービスが **xtab** ファイルを参照するため、エクスポートしたファイルシステムのリストの変更が直ちに反映されます。

一般的な exportfs オプション
exportfs で利用できる一般的なオプションの一覧は以下のようになります。

-r

/var/lib/nfs/etab に新しいエクスポート一覧を作成して、**/etc/exports** に一覧表示されているディレクトリーをすべてエクスポートします。このオプションにより、**/etc/exports** に変更が加えられると、エクスポート一覧が効果的に更新されます。

-a

exportfs に渡されるその他のオプションに応じて、すべてのディレクトリーをエクスポートするかどうかを判断します。その他のオプションが指定されていないと、**exportfs** は、**/etc/exports** で指定されたすべてのファイルシステムをエクスポートします。

-o file-systems

/etc/exports 内に記載されていない、エクスポートされるディレクトリーを指定します。**file-systems** の部分を、エクスポートされる追加のファイルシステムに置き換えます。これらのファイルシステムは、**/etc/exports** で指定されたものと同じフォーマットでなければなりません。このオプションは、多くの場合、エクスポートされるファイルシステムの一覧に永続的に追加する前に、エクスポートされるファイルシステムをテストするために使用されます。

-i

/etc/exports を無視します。コマンドラインで指定されたオプションのみが、エクスポート用ファイルシステムの定義に使用されます。

-u

すべての共有ディレクトリーをエクスポートしなくなります。**exportfs -ua** コマンドは、すべての NFS サービスを稼働状態に維持しながら、NFS ファイル共有を保留します。NFS 共有を再度有効にするには、**exportfs -r** を使用します。

-v

詳細な表示です。**exportfs** コマンドを実行するときに表示されるエクスポート、または非エクスポートのファイルシステムの情報が、より詳細に表示されます。

exportfs ユーティリティーにオプションが渡されていない場合は、現在エクスポートされているファイルシステムのリストが表示されます。

関連情報

- NFS ホスト名の形式。

2.7. NFS および RPCBIND

本セクションでは、NFSv3 で必要とされる **rpcbind** サービスの目的を説明します。

rpcbind サービスは、RPC (Remote Procedure Call) サービスを、そのサービスがリッスンするポートにマッピングします。RPC のプロセスが開始すると、その開始が **rpcbind** に通知され、そのプロセスがリッスンしているポートと、そのプロセスが処理することが予想される RPC プログラム番号が登録されます。クライアントシステムは、特定の RPC プログラム番号でサーバーの **rpcbind** と通信します。**rpcbind** サービスは、クライアントを適切なポート番号にリダイレクトし、要求されたサービスと通信できるようにします。

RPC ベースのサービスは、**rpcbind** を使用して、クライアントの受信要求で接続を確立します。したがって、RPC ベースのサービスが起動する前に、**rpcbind** を利用可能な状態にする必要があります。

rpcbind のアクセス制御ルールは、すべての RPC ベースのサービスに影響します。あるいは、NFS RPC デーモンごとにアクセス制御ルールを指定することもできます。

関連情報

- **rpc.mountd(8)** man page

- **rpc.statd(8)** man page

2.8. NFS のインストール

この手順では、NFS 共有のマウントまたはエクスポートに必要なすべてのパッケージをインストールします。

手順

- **nfs-utils** パッケージをインストールします。

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

2.9. NFS サーバーの起動

この手順では、NFS 共有をエクスポートするために必要な NFS サーバーの起動方法を説明します。

前提条件

- NFSv3 の接続に対応しているサーバーで、**rpcbind** サービスを実行している。**rpcbind** がアクティブであることを確認するには、次のコマンドを実行します。

```
$ systemctl status rpcbind
```

サービスが停止している場合は、起動して有効にします。

```
$ systemctl enable --now rpcbind
```

手順

- システムの起動時に、NFS サーバーを起動して自動的に起動するようにするには、次のコマンドを使用します。

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

関連情報

- NFSv4 専用サーバーの 設定

2.10. NFS と RPCBIND のトラブルシューティング

rpcbind サービスでは通信に使用するポート番号と RPC サービス間の調整を行うため、トラブルシューティングを行う際は、**rpcbind** を使用して現在の RPC サービスの状態を表示させると便利です。**rpcinfo** ユーティリティーは、RPC ベースの各サービスとそのポート番号、RPC プログラム番号、バージョン番号、および IP プロトコルタイプ (TCP または UDP) が表示されます。

手順

1. **rpcbind** に対して適切な RPC ベースの NFS サービスが有効になっていることを確認するには、次のコマンドを実行します。

```
# rpcinfo -p
```

例2.2 rpcinfo -p コマンドの出力

以下に、上記コマンドの出力例を示します。

```
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp  20048  mountd
    100005    1   tcp  20048  mountd
    100005    2   udp  20048  mountd
    100005    2   tcp  20048  mountd
    100005    3   udp  20048  mountd
    100005    3   tcp  20048  mountd
    100024    1   udp  37769  status
    100024    1   tcp  49349  status
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    3   tcp   2049  nfs_acl
    100021    1   udp  56691  nlockmgr
    100021    3   udp  56691  nlockmgr
    100021    4   udp  56691  nlockmgr
    100021    1   tcp  46193  nlockmgr
    100021    3   tcp  46193  nlockmgr
    100021    4   tcp  46193  nlockmgr
```

NFS サービスの 1 つが正しく起動しないと、**rpcbind** は、そのサービスに対するクライアントからの RPC 要求を、正しいポートにマッピングできません。

2. 多くの場合は、NFSが **rpcinfo** の出力に表示されていない時に NFS を再起動すると、サービスが **rpcbind** に正しく登録され、動作を開始します。

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

関連情報

- NFSv4 専用サーバーの 設定

2.11. ファイアウォールの背後で動作するように NFS サーバーを設定する

NFS には **rpcbind** サービスが必要です。このサービスは RPC サービスのポートを動的に割り当て、ファイアウォールルールの設定で問題が発生する可能性があります。以下のセクションでは、サポートが必要な場合に、ファイアウォールの内側で機能するように NFS バージョンを設定する方法を説明します。

- NFSv3
  これには、NFSv3 をサポートするサーバーがすべて含まれます。

- NFSv3 専用サーバー
- NFSv3 と NFSv4 の両方に対応するサーバー

- NFSv4-only

2.11.1. ファイアウォールの内側で動作するように NFSv3 対応サーバーを設定

次の手順では、NFSv3 に対応するサーバーを設定し、ファイアウォールの内側で実行する方法を説明します。これには、NFSv3 と NFSv4 の両方に対応する NFSv3 専用サーバーとサーバーが含まれます。

手順

1. クライアントがファイアウォールの背後にある NFS 共有にアクセスできるようにするには、NFS サーバーで次のコマンドを実行してファイアウォールを構成します。

```
firewall-cmd --permanent --add-service mountd
firewall-cmd --permanent --add-service rpc-bind
firewall-cmd --permanent --add-service nfs
```

2. 以下のように、**/etc/nfs.conf** ファイルの RPC サービスの **nlockmgr** が使用するポートを指定します。

```
[lockd]

port=tcp-port-number
udp-port=udp-port-number
```

   または、**/etc/modprobe.d/lockd.conf** ファイルで、**nlm_tcpport** および **nlm_udpport** を指定することもできます。

3. NFS サーバーで以下のコマンドを実行して、ファイアウォールで指定したポートを開きます。

```
firewall-cmd --permanent --add-port=<lockd-tcp-port>/tcp
firewall-cmd --permanent --add-port=<lockd-udp-port>/udp
```

4. 以下のように、**/etc/nfs.conf** ファイルの **[statd]** セクションを編集して、**rpc.statd** の静的ポートを追加します。

```
[statd]

port=port-number
```

5. NFS サーバーで以下のコマンドを実行して、ファイアウォールに追加したポートを開きます。

```
firewall-cmd --permanent --add-port=<statd-tcp-port>/tcp
firewall-cmd --permanent --add-port=<statd-udp-port>/udp
```

6. ファイアウォール設定を再読み込みします。

```
firewall-cmd --reload
```

7. **rpc-statd** サービスを最初に再起動してから、**nfs-server** サービスを再起動します。

```
# systemctl restart rpc-statd.service
# systemctl restart nfs-server.service
```

または、**/etc/modprobe.d/ lockd.conf** ファイルにロックされたポートを指定した場合は、次のコマンドを実行します。

a. **/proc/sys/fs/nfs/nlm_tcpport** と **/proc/sys/fs/nfs/nlm_udpport** の現在の値を更新します。

```
# sysctl -w fs.nfs.nlm_tcpport=<tcp-port>
# sysctl -w fs.nfs.nlm_udpport=<udp-port>
```

b. **rpc-statd** サービスおよび **nfs-server** サービスを再起動します。

```
# systemctl restart rpc-statd.service
# systemctl restart nfs-server.service
```

2.11.2. ファイアウォールの内側で実行されるように NFSv4 専用サーバーを設定する手順

次の手順では、NFSv4 専用サーバーをファイアウォールの内側で実行するように設定する方法を説明します。

手順

1. クライアントがファイアウォールの内側にある NFS 共有にアクセスできるようにするには、NFS サーバーで以下のコマンドを実行してファイアウォールを設定します。

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

2. ファイアウォール設定を再読み込みします。

```
firewall-cmd --reload
```

3. nfs-server を再起動します。

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

2.11.3. ファイアウォールの内側で動作するように NFSv3 クライアントを設定する手順

ファイアウォールの内側で実行するように NFSv3 クライアントを設定する手順は、ファイアウォールの内側で実行するように NFSv3 サーバーを設定する手順と似ています。

設定するマシンが NFS クライアントとサーバーの両方である場合、「NFSv3 対応サーバーがファイアウォールの内側で実行されるように設定」で説明されている手順に 従います。

以下の手順では、ファイアウォールの内側でのみ NFS クライアントであるマシンを設定する方法を説明します。

手順

1. クライアントがファイアウォールの内側で NFS クライアントにコールバックを実行できるようにするには、NFS クライアントで以下のコマンドを実行して **rpc-bind** サービスをファイアウォールに追加します。

```
firewall-cmd --permanent --add-service rpc-bind
```

2. 以下のように、**/etc/nfs.conf** ファイルの RPC サービスの **nlockmgr** が使用するポートを指定します。

```
[lockd]

port=port-number
udp-port=upd-port-number
```

   または、**/etc/modprobe.d/lockd.conf** ファイルで、**nlm_tcpport** および **nlm_udpport** を指定することもできます。

3. NFS クライアントで以下のコマンドを実行して、ファイアウォールで指定したポートを開きます。

```
firewall-cmd --permanent --add-port=<lockd-tcp-port>/tcp
firewall-cmd --permanent --add-port=<lockd-udp-port>/udp
```

4. 以下のように、**/etc/nfs.conf** ファイルの **[statd]** セクションを編集して、**rpc.statd** の静的ポートを追加します。

```
[statd]

port=port-number
```

5. NFS クライアントで以下のコマンドを実行して、ファイアウォールに追加したポートを開きます。

```
firewall-cmd --permanent --add-port=<statd-tcp-port>/tcp
firewall-cmd --permanent --add-port=<statd-udp-port>/udp
```

6. ファイアウォール設定を再読み込みします。

```
firewall-cmd --reload
```

7. **rpc-statd** サービスを再起動します。

```
# systemctl restart rpc-statd.service
```

   または、**/etc/modprobe.d/ lockd.conf** ファイルにロックされたポートを指定した場合は、次のコマンドを実行します。

   a. **/proc/sys/fs/nfs/nlm_tcpport** と **/proc/sys/fs/nfs/nlm_udpport** の現在の値を更新します。

```
# sysctl -w fs.nfs.nlm_tcpport=<tcp-port>
# sysctl -w fs.nfs.nlm_udpport=<udp-port>
```

b. **rpc-statd** サービスを再起動します。

```
# systemctl restart rpc-statd.service
```

2.11.4. ファイアウォールの内側で動作するように NFSv4 クライアントを設定する

この手順は、クライアントが NFSv4.0 を使用している場合に限り行います。その場合は、NFSv4.0 コールバックのポートを開く必要があります。

それ以降のプロトコルバージョンでは、クライアントが開始した同じ接続でコールバックを実行するため、この手順は NFSv4.1 以降には必要ありません。

手順

1. NFSv4.0 コールバックがファイアウォールを通過できるようにするには、**/proc/sys/fs/nfs/nfs_callback_tcpport** を設定し、以下のようにサーバーがクライアントのそのポートに接続できるようにします。

```
# echo "fs.nfs.nfs_callback_tcpport = <callback-port>" >/etc/sysctl.d/90-nfs-callback-port.conf
# sysctl -p /etc/sysctl.d/90-nfs-callback-port.conf
```

2. NFS クライアントで以下のコマンドを実行して、ファイアウォールの指定のポートを開きます。

```
firewall-cmd --permanent --add-port=<callback-port>/tcp
```

3. ファイアウォール設定を再読み込みします。

```
firewall-cmd --reload
```

2.12. ファイアウォールからの RPC クォータのエクスポート

ディスククォータを使用するファイルシステムをエクスポートする場合は、クォータの RPC (Remote Procedure Call) サービスを使用して、NFS クライアントにディスククォータデータを提供できます。

手順

1. **rpc-rquotad** サービスを有効にして起動します。

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

注記

rpc-rquotad サービスが有効になっている場合は、nfs-server サービスが起動した後に自動的に起動されます。

2. ファイアウォールの内側で、クォータの RPC サービスにアクセスできるようにするには、TCP (UDP が可能な場合は UDP) の 875 ポートを開く必要があります。デフォルトのポート番号は **/etc/services** ファイルで定義します。
デフォルトのポート番号は、**/etc/sysconfig/rpc-rquotad** ファイルの **RPCRQUOTADOPTS** 変数に **-p port-number** を追加すると上書きできます。

3. デフォルトで、リモートホストはクォータのみを読み取ることができます。クライアントにクォータの設定を許可したい場合は、**/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。

4. **rpc-rquotad** を再起動して、**/etc/sysconfig/rpc-rquotad** ファイルの変更を反映します。

```
# systemctl restart rpc-rquotad
```

2.13. NFS OVER RDMA の有効化 (NFSORDMA)

Remote Direct Memory Access(RDMA)サービスは、Red Hat Enterprise Linux 9 の RDMA 対応ハードウェアで自動的に機能します。

手順

1. **rdma-core** パッケージをインストールします。

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

2. **xprtrdma** および **svcrdma** の行が **/etc/rdma/modules/rdma.conf** ファイルでコメントアウト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. NFS サーバーで、**/mnt/nfsordma** ディレクトリーを作成し、**/etc/exports** にエクスポートします。

```
# mkdir /mnt/nfsordma
# echo "/mnt/nfsordma *(fsid=0,rw,async,insecure,no_root_squash)" >> /etc/exports
```

4. NFS クライアントで、nfs-share をサーバーの IP アドレスでマウントします（例：**172.31.0.186** ）。

```
# mount -o rdma,port=20049 172.31.0.186:/mnt/nfs-share /mnt/nfs
```

5. **nfs-server** サービスを再起動します。

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

関連情報

- RFC 5667 標準

2.14. 関連情報

- Linux NFS wiki

第3章 NFS のセキュア化

サーバーで NFS ファイルシステムをエクスポートする場合や、クライアントにマウントする際に、NFS セキュリティーリスクを最小限に抑え、サーバーのデータを保護するには、以下のセクションを検討してください。

3.1. AUTH_SYS とエクスポート制御による NFS 保護

NFS は、エクスポートしたファイルへのアクセスを制御するために、以下の従来のオプションを提供します。

- サーバーは、IP アドレスまたはホスト名を使用して、どのホストにどのファイルシステムのマウントを許可するかをサーバー側で制限します。
- サーバーは、ローカルユーザーの場合と同じ方法で、NFS クライアントのユーザーに対してファイルシステムの権限を強制します。従来は、NFS は **AUTH_SYS** コールメッセージ (**AUTH_UNIX** とも呼ばれます) を使用してこれを実行していました。このメッセージは、クライアントが、ユーザーの UID と GID を提示します。これは、悪意のあるクライアントや誤って設定されたクライアントが簡単にこの間違いを招き、ユーザーがアクセスすべきではないファイルにアクセスできる可能性があることを意味します。

潜在的なリスクを制限するため、多くの場合、管理者は、共通のユーザー ID およびグループ ID に対して、ユーザー権限を読み取り専用にするか、権限を下げてアクセスを制限します。ただし、このソリューションにより、NFS 共有が元々想定されている方法では使用されなくなります。

さらに、攻撃者が、NFS ファイルシステムをエクスポートするシステムが使用する DNS サーバーを制御できた場合は、特定のホスト名または完全修飾ドメイン名に関連付けられたシステムを、承認されていないマシンに指定できます。これで、認証されていないマシンは、NFS 共有のマウントを許可するシステムに**なります**。これは、ユーザー名やパスワードの情報が交換されず、NFS マウントに追加のセキュリティーが提供されるためです。

NFS 経由でディレクトリーのエクスポートを行う際にワイルドカードを使用する場合は慎重に行ってください。ワイルドカードの対象が予定よりも広い範囲のシステムを対象とする可能性があります。

関連情報

- NFS および **rpcbind** のセキュリティーを保護するには、**nftables**、**firewalld** などを使用します。
- **nft(8)** man ページ
- man ページの **firewalld-cmd(1)**

3.2. AUTH_GSSを使用した NFS セキュリティー

NFS の全バージョンは、RPCSEC_GSS および Kerberos のメカニズムに対応します。

AUTH_SYS とは異なり、RPCSEC_GSS Kerberos メカニズムでは、サーバーは、どのユーザーがそのファイルにアクセスしているかを正確に表すことをクライアントに依存しません。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。RPCSEC_GSS Kerberos メカニズムを使用することが、マウントを保護する最も簡単な方法になります。Kerberos の設定後は、追加の設定が不要になるためです。

3.3. KERBEROS を使用するために NFS サーバーおよびクライアントを設定

Kerberos はネットワーク認証システムであり、対称暗号化と、信頼できるサードパーティー (KDC) を使用してクライアントとサーバーが相互に認証できるようにします。Red Hat では、Kerberos の設定に Identity Management (IdM) を使用することを推奨します。

前提条件

- Kerberos Key Distribution Centre (**KDC**) がインストールされ、設定されている。

手順

1. - NFS サーバー側で、**nfs/hostname.domain@REALM** プリンシパルを作成します。
   - サーバーとクライアントに、**host/hostname.domain@REALM** を作成します。
   - クライアントとサーバーのキータブに、対応する鍵を追加します。
2. サーバーで、**sec=** オプションを使用して、希望するセキュリティーフレーバーを有効にします。すべてのセキュリティーフレーバーと非暗号化マウントを有効にするには、以下のコマンドを実行します。

   ```
   /export *(sec=sys:krb5:krb5i:krb5p)
   ```

   sec= オプションを使用するのに有効なセキュリティーフレーバーは、以下のようになります。

   - **sys** - 暗号化の保護なし (デフォルト)
   - **krb5** - 認証のみ
   - **krb5i** - インテグリティー保護
     - ユーザー認証に Kerberos V5 を使用し、データの改ざんを防ぐために安全なチェックサムを使用して NFS 操作の整合性チェックを実行します。
   - **krb5p** - プライバシー保護
     - ユーザー認証、整合性チェックに Kerberos V5 を使用し、トラフィックの傍受を防ぐため NFS トラフィックの暗号化を行います。これが最も安全な設定になりますが、パフォーマンスのオーバーヘッドも最も高くなります。
3. クライアントで、**sec=krb5** (もしくは設定に応じて **sec=krb5i** または **sec=krb5p**) をマウントオプションに追加します。

   ```
   # mount -o sec=krb5 server:/export /mnt
   ```

関連情報

- krb5 セキュアな NFS で root としてファイルの作成 推奨されません。
- **exports(5)** man ページ
- **nfs(5)** man ページ

3.4. NFSV4 セキュリティーオプション

NFSv4 には、Microsoft Windows NT モデルの機能や幅広い導入の経緯があるため、POSIX モデルではなく、Microsoft Windows NT モデルをベースとした ACL サポートが含まれます。

NFSv4 のもう 1 つの重要なセキュリティー機能は、ファイルシステムのマウントに **MOUNT** プロトコルを使用しなくなることです。**MOUNT** プロトコルは、プロトコルがファイルを処理する方法により、セキュリティー上のリスクが発生します。

3.5. マウントされた NFS エクスポートに対するファイル権限

リモートホストにより NFS ファイルシステムを読み取りまたは読み書きとしてマウントした場合は、パーティションが、各共有ファイルに対する唯一の保護となります。同じユーザー ID 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すると、そのユーザーは互いのファイルを修正できるようになります。また、クライアントシステムで root としてログインした場合は、**su -** コマンドを使用して、NFS 共有が設定されたファイルにアクセスできます。

デフォルトでは、アクセス制御リスト (ACL) は、Red Hat Enterprise Linux では NFS が対応しています。Red Hat では、この機能を有効にしておくことを推奨します。

デフォルトでは、NFS がファイルシステムをエクスポートする際に、**root squashing** を使用します。これにより、NFS 共有にアクセスするユーザーのユーザー ID が、ローカルマシンの root ユーザーとして **nobody** に設定されます。Root squashing は、デフォルトのオプション **root_squash** で制御されます。このオプションの詳細は、「 NFS サーバーの設定 」を参照してください。

NFS 共有を読み取り専用としてエクスポートする場合は、**all_squash** オプションの使用を検討してください。このオプションでは、エクスポートしたファイルシステムにアクセスするすべてのユーザーが、**nobody** ユーザーのユーザー ID を取得します。

第4章 NFS での PNFS SCSI レイアウトの有効化

データのアクセスに pNFS SCSI レイアウトを使用するように、NFS サーバーおよびクライアントを設定できます。pNFS SCSI は、ファイルへの長期接続のシングルクライアントアクセスに伴うユースケースで利点があります。

前提条件

- クライアントとサーバーの両方で、SCSI コマンドを同じブロックデバイスに送信する必要があります。つまり、ブロックデバイスは共有 SCSI バス上になければなりません。
- ブロックデバイスに XFS ファイルシステムが含まれている必要があります。
- SCSI デバイスは、 SCSI-3 Primary Commands 仕様で説明されているように、SCSI Persistent Reservation に対応している必要があります。

4.1. PNFS テクノロジー

pNFS アーキテクチャーでは、NFS のスケーラビリティーが改善されます。サーバーに pNFS が実装されると、クライアントは複数のサーバーで同時にデータにアクセスできるようになります。これにより、パフォーマンスが向上します。

pNFS は、RHEL では以下のストレージプロトコルまたはレイアウトに対応しています。

- ファイル
- Flexfiles
- SCSI

4.2. PNFS SCSI レイアウト

SCSI レイアウトは、pNFS ブロックレイアウトの作業に基づいています。このレイアウトは、SCSI デバイス全体に定義されます。これには、SCSI 永続予約に対応する必要がある論理ユニット (lUS) として、固定サイズのブロックが連続的に含まれています。LU デバイスは、SCSI デバイスの識別子で識別されます。

pNFS SCSI は、ファイルへの長期接続のシングルクライアントアクセスのユースケースで適切に実行されます。例として、メールサーバーまたはクラスターを格納している仮想マシンなどが挙げられます。

クライアントとサーバーとの間の操作
NFS クライアントが、ファイルからの読み取り、またはファイルへの書き込みを行うと、クライアントは **LAYOUTGET** 操作を実行します。サーバーは、SCSI デバイスのファイルの場所に反応します。このクライアントは、使用する SCSI デバイスを判断するために、**GETDEVICEINFO** の追加操作が必要になる場合があります。正しく動作するのであれば、クライアントは、**READ** 操作および **WRITE** 操作をサーバーに送信する代わりに、SCSI デバイスに直接 I/O 要求を発行することができます。

クライアント間のエラーまたは競合により、サーバーがレイアウトを再び呼び出したり、クライアントにレイアウトを発行しなくなることがあります。この場合、クライアントは SCSI デバイスに I/O 要求を直接送信するのではなく、サーバーへの **READ** 操作および **WRITE** 操作の発行にフォールバックします。

操作を監視するには、「 pNFS SCSI レイアウトの監視」を参照して ください。

デバイスの予約

pNFS SCSI は、予約の割り当てを通じてフェンシングを処理します。サーバーがレイアウトをクライアントに発行する前に、SCSI デバイスを予約して、登録したクライアントのみがデバイスにアクセスできるようにします。クライアントが、その SCSI デバイスに対してコマンドを実行できても、そのデバイスに登録されていない場合は、クライアントからの多くの操作が、そのデバイス上で失敗します。たとえば、サーバーが、そのデバイスのレイアウトをクライアントに送信していないと、クライアントの **blkid** コマンドは、XFS ファイルシステムの UUID を表示できません。

サーバーは、独自の永続予約を削除しません。これにより、クライアントやサーバーの再起動時に、デバイスのファイルシステム内のデータが保護されます。SCSI デバイスを他の目的で使用するには、NFS サーバーで、手動で永続予約を削除する必要があります。

4.3. PNFS と互換性がある SCSI デバイスの確認

この手順では、SCSI デバイスが pNFS SCSI レイアウトに対応しているかどうかを確認します。

前提条件

- 以下のコマンドで、**sg3-utils** パッケージがインストールされている。

```
# dnf install sg3_utils
```

手順

- サーバーおよびクライアントの両方で、適切な SCSI デバイスサポートを確認します。

```
# sg_persist --in --report-capabilities --verbose path-to-scsi-device
```

Persist Through Power Loss Active (**PTPL_A**) ビットが設定されるようにします。

例4.1 pNFS SCSI をサポートする SCSI デバイス

以下は、pNFS SCSI に対応する SCSI デバイスにおける **sg_persist** 出力の例になります。PTPL **_A** ビットが **1** を報告します。

```
    inquiry cdb: 12 00 00 00 24 00
    Persistent Reservation In cmd: 5e 02 00 00 00 00 00 20 00 00
  LIO-ORG   block11          4.0
  Peripheral device type: disk
Report capabilities response:
  Compatible Reservation Handling(CRH): 1
  Specify Initiator Ports Capable(SIP_C): 1
  All Target Ports Capable(ATP_C): 1
  Persist Through Power Loss Capable(PTPL_C): 1
  Type Mask Valid(TMV): 1
  Allow Commands: 1
  Persist Through Power Loss Active(PTPL_A): 1
    Support indicated in Type mask:
      Write Exclusive, all registrants: 1
      Exclusive Access, registrants only: 1
      Write Exclusive, registrants only: 1
      Exclusive Access: 1
      Write Exclusive: 1
      Exclusive Access, all registrants: 1
```

関連情報

- **sg_persist(8)** man page

4.4. サーバーで PNFS SCSI の設定

この手順では、NFS サーバーが pNFS SCSI レイアウトをエクスポートするように設定します。

手順

1. サーバーで、SCSI デバイスで作成した XFS ファイルシステムをマウントします。
2. NFS バージョン 4.1 以降をエクスポートするように NFS サーバーを設定します。**/etc/nfs.conf** ファイルの **[nfsd]** セクションに、以下のオプションを設定します。

```
[nfsd]

vers4.1=y
```

3. **pnfs** オプションを指定して、NFS で XFS ファイルシステムをエクスポートするように NFS サーバーを設定します。

例4.2 pNFS SCSI をエクスポートする /etc/exports のエントリー

/etc/exports 設定ファイルの以下のエントリーにより、**/exported/directory/** にマウントされているファイルシステムを、pNFS SCSI レイアウトとして **allowed.example.com** クライアントにエクスポートします。

```
/exported/directory allowed.example.com(pnfs)
```

関連情報

- NFS 共有 のエクスポート

4.5. クライアントで PNFS SCSI の設定

この手順では、pNFS SCSI レイアウトをマウントするように NFS クライアントを設定します。

前提条件

- NFS サーバーは、pNFS SCSI で XFS ファイルシステムをエクスポートするように設定されています。「サーバーでの pNFS SCSI の設定」を参照して ください。

手順

- クライアントで、NFS バージョン 4.1 以降を使用して、エクスポートした XFS ファイルシステムをマウントします。

```
# mount -t nfs -o nfsvers=4.1 host:/remote/export /local/directory
```

NFS なしで XFS ファイルシステムを直接マウントしないでください。

関連情報

- NFS 共有 のマウント

4.6. サーバーでの PNFS SCSI 予約の解放

この手順では、NFS サーバーが SCSI デバイスを維持している永続的な予約を解放します。これにより、pNFS SCSI をエクスポートする必要がなくなったら、SCSI デバイスを別の目的で使用できるようになります。

サーバーから予約を削除する必要があります。別の IT Nexus から削除することはできません。

前提条件

- 以下のコマンドで、**sg3-utils** パッケージがインストールされている。

```
# dnf install sg3_utils
```

手順

1. サーバーで、既存の予約をクエリーします。

```
# sg_persist --read-reservation path-to-scsi-device
```

例4.3 /dev/sda での予約のクエリー

```
# *sg_persist --read-reservation /dev/sda*

  LIO-ORG   block_1          4.0
  Peripheral device type: disk
  PR generation=0x8, Reservation follows:
    Key=0x100000000000000
    scope: LU_SCOPE,  type: Exclusive Access, registrants only
```

2. サーバーにある既存の登録を削除します。

```
# sg_persist --out \
            --release \
            --param-rk=reservation-key \
            --prout-type=6 \
            path-to-scsi-device
```

例4.4 /dev/sda にある予約の削除

```
# sg_persist --out \
              --release \
              --param-rk=0x100000000000000 \
              --prout-type=6 \
              /dev/sda

  LIO-ORG   block_1          4.0
  Peripheral device type: disk
```

関連情報

- **sg_persist(8)** man page