Red Hat Enterprise Linux 9

Configuration et utilisation des services de fichiers en réseau

Un guide pour la configuration et l'utilisation des services de fichiers réseau dans Red Hat Enterprise Linux 9.

Last Updated: 2024-02-13

Red Hat Enterprise Linux 9 Configuration et utilisation des services de fichiers en réseau

Un guide pour la configuration et l'utilisation des services de fichiers réseau dans Red Hat Enterprise Linux 9.

Notice légale

Résumé

Ce document décrit comment configurer et exécuter des services de fichiers réseau sur Red Hat Enterprise Linux 9, y compris le serveur Samba et le serveur NFS.

Table des matières

RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le message de notre directeur technique Chris Wright.

FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de Bugzilla.
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.

CHAPITRE 1. UTILISATION DE SAMBA EN TANT QUE SERVEUR

Samba implémente le protocole Server Message Block (SMB) dans Red Hat Enterprise Linux. Le protocole SMB est utilisé pour accéder aux ressources d'un serveur, telles que les partages de fichiers et les imprimantes partagées. En outre, Samba met en œuvre le protocole Distributed Computing Environment Remote Procedure Call (DCE RPC) utilisé par Microsoft Windows.

Vous pouvez exécuter Samba en tant que :

- Membre d'un domaine Active Directory (AD) ou NT4
- Un serveur autonome
- Un contrôleur de domaine primaire (PDC) ou un contrôleur de domaine de secours (BDC) NT4

NOTE

Red Hat prend en charge les modes PDC et BDC uniquement dans les installations existantes avec des versions de Windows qui prennent en charge les domaines NT4. Red Hat recommande de ne pas configurer un nouveau domaine Samba NT4, car les systèmes d'exploitation Microsoft postérieurs à Windows 7 et Windows Server 2008 R2 ne prennent pas en charge les domaines NT4.

Red Hat ne prend pas en charge l'exécution de Samba en tant que contrôleur de domaine AD (DC).

Indépendamment du mode d'installation, vous pouvez optionnellement partager des répertoires et des imprimantes. Cela permet à Samba d'agir en tant que serveur de fichiers et d'impression.

1.1. COMPRENDRE LES DIFFÉRENTS SERVICES ET MODES DE SAMBA

Cette section décrit les différents services inclus dans Samba et les différents modes que vous pouvez configurer.

1.1.1. Les services Samba

Samba fournit les services suivants :

smbd

Ce service fournit des services de partage de fichiers et d'impression en utilisant le protocole SMB. En outre, le service est responsable du verrouillage des ressources et de l'authentification des utilisateurs connectés. Pour l'authentification des membres du domaine, **smbd** nécessite **winbindd**. Le service **smb systemd** démarre et arrête le démon **smbd**.
Pour utiliser le service **smbd**, installez le paquet **samba**.

nmbd

Ce service assure la résolution des noms d'hôtes et des adresses IP à l'aide du protocole NetBIOS sur IPv4. En plus de la résolution des noms, le service **nmbd** permet de naviguer dans le réseau SMB pour localiser les domaines, les groupes de travail, les hôtes, les partages de fichiers et les imprimantes. Pour ce faire, le service rapporte ces informations directement au client de diffusion ou les transmet à un navigateur local ou principal. Le service **nmb systemd** démarre et arrête le démon **nmbd**.

Notez que les réseaux SMB modernes utilisent le DNS pour résoudre les clients et les adresses IP. Pour Kerberos, une configuration DNS fonctionnelle est nécessaire.

Pour utiliser le service **nmbd**, installez le paquet **samba**.

winbindd

Ce service fournit une interface permettant au commutateur de service de noms (NSS) d'utiliser les utilisateurs et les groupes du domaine AD ou NT4 sur le système local. Cela permet, par exemple, aux utilisateurs du domaine de s'authentifier auprès des services hébergés sur un serveur Samba ou auprès d'autres services locaux. Le service **winbind systemd** démarre et arrête le démon **winbindd**. Si vous configurez Samba en tant que membre d'un domaine, **winbindd** doit être démarré avant le service **smbd**. Sinon, les utilisateurs et les groupes du domaine ne sont pas disponibles pour le système local...

Pour utiliser le service **winbindd**, installez le paquet **samba-winbind**.

IMPORTANT

Red Hat prend uniquement en charge l'exécution de Samba en tant que serveur avec le service **winbindd** pour fournir des utilisateurs et des groupes de domaine au système local. En raison de certaines limitations, telles que l'absence de prise en charge de la liste de contrôle d'accès (ACL) de Windows et du système de secours NT LAN Manager (NTLM), SSSD n'est pas pris en charge.

1.1.2. Les services de sécurité Samba

Le paramètre **security** dans la section **[global]** du fichier **/etc/samba/smb.conf** gère la façon dont Samba authentifie les utilisateurs qui se connectent au service. Selon le mode dans lequel vous installez Samba, le paramètre doit être défini avec des valeurs différentes :

Sur un membre du domaine AD, définir security = ads

Dans ce mode, Samba utilise Kerberos pour authentifier les utilisateurs AD.
Pour plus de détails sur la configuration de Samba en tant que membre de domaine, voir Configuration de Samba en tant que serveur membre de domaine AD .

Sur un serveur autonome, définissez security = user

Dans ce mode, Samba utilise une base de données locale pour authentifier les utilisateurs qui se connectent.
Pour plus de détails sur la configuration de Samba en tant que serveur autonome, voir Configuration de Samba en tant que serveur autonome.

Sur un PDC ou un BDC NT4, définissez security = user

Dans ce mode, Samba authentifie les utilisateurs auprès d'une base de données locale ou LDAP.

Sur un membre du domaine NT4, définir security = domain

Dans ce mode, Samba authentifie les utilisateurs qui se connectent à un PDC ou BDC NT4. Vous ne pouvez pas utiliser ce mode sur les membres du domaine AD.
Pour plus de détails sur la configuration de Samba en tant que membre de domaine, voir Configuration de Samba en tant que serveur membre de domaine AD .

Ressources supplémentaires

- **security** dans la page de manuel **smb.conf(5)**

1.1.3. Scénarios lorsque les services Samba et les utilitaires clients Samba chargent et rechargent leur configuration

Ce qui suit décrit quand les services et utilitaires Samba chargent et rechargent leur configuration :

- Les services Samba rechargent leur configuration :
  - Automatiquement toutes les 3 minutes
  - Sur demande manuelle, par exemple lorsque vous exécutez la commande **smbcontrol all reload-config**.
- Les utilitaires du client Samba ne lisent leur configuration que lorsque vous les démarrez.

Notez que certains paramètres, tels que **security**, nécessitent un redémarrage du service **smb** pour être pris en compte et qu'un rechargement n'est pas suffisant.

Ressources supplémentaires

- La section **How configuration changes are applied** dans la page de manuel **smb.conf(5)**
- Les pages de manuel **smbd(8)**, **nmbd(8)**, et **winbindd(8)**

1.1.4. Modifier la configuration de Samba en toute sécurité

Les services Samba rechargent automatiquement leur configuration toutes les 3 minutes. Cette procédure décrit comment modifier la configuration de Samba de manière à empêcher les services de recharger les modifications avant que vous n'ayez vérifié la configuration à l'aide de l'utilitaire **testparm**.

Conditions préalables

- Samba est installé.

Procédure

1. Créer une copie du fichier **/etc/samba/smb.conf**:

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

2. Modifiez le fichier copié et apportez les changements souhaités.
3. Vérifiez la configuration dans le fichier **/etc/samba/samba.conf.*copy*** dans le fichier

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

   Si **testparm** signale des erreurs, corrigez-les et exécutez à nouveau la commande.

4. Remplacer le fichier **/etc/samba/smb.conf** par la nouvelle configuration :

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

5. Attendez que les services Samba rechargent automatiquement leur configuration ou qu'ils la rechargent manuellement :

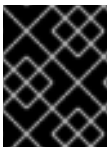
```
# smbcontrol all reload-config
```

Ressources supplémentaires

- Scénarios lorsque les services Samba et les utilitaires clients Samba chargent et rechargent leur configuration

1.2. VÉRIFICATION DU FICHIER SMB.CONF À L'AIDE DE L'UTILITAIRE TESTPARM

L'utilitaire **testparm** vérifie que la configuration de Samba dans le fichier **/etc/samba/smb.conf** est correcte. L'utilitaire détecte les paramètres et les valeurs invalides, mais aussi les paramètres incorrects, par exemple pour le mappage des identifiants. Si **testparm** ne signale aucun problème, les services Samba chargeront avec succès le fichier **/etc/samba/smb.conf**. Notez que **testparm** ne peut pas vérifier que les services configurés seront disponibles ou fonctionneront comme prévu.



IMPORTANT

Red Hat vous recommande de vérifier le fichier **/etc/samba/smb.conf** en utilisant **testparm** après chaque modification de ce fichier.

Conditions préalables

- Vous avez installé Samba.
- Le fichier **/etc/samba/smb.conf** se termine.

Procédure

1. Exécutez l'utilitaire **testparm** en tant qu'utilisateur **root**:

```
# 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]
 ...
```

L'exemple précédent fait état d'un paramètre inexistant et d'une configuration de mappage d'ID incorrecte.

2. Si **testparm** signale des paramètres ou des valeurs incorrects ou d'autres erreurs dans la configuration, corrigez le problème et exécutez à nouveau l'utilitaire.

1.3. CONFIGURATION DE SAMBA EN TANT QUE SERVEUR AUTONOME

Vous pouvez configurer Samba comme un serveur qui n'est pas membre d'un domaine. Dans ce mode d'installation, Samba authentifie les utilisateurs auprès d'une base de données locale plutôt qu'auprès d'un DC central. En outre, vous pouvez activer l'accès invité pour permettre aux utilisateurs de se connecter à un ou plusieurs services sans authentification.

1.3.1. Mise en place de la configuration du serveur pour le serveur autonome

Cette section décrit comment établir la configuration du serveur pour un serveur autonome Samba.

Procédure

1. Installez le paquetage **samba**:

```
# dnf install samba
```

2. Modifiez le fichier **/etc/samba/smb.conf** et définissez les paramètres suivants :

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

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

Cette configuration définit un serveur autonome nommé **Server** au sein du groupe de travail **Example-WG**. En outre, cette configuration active la journalisation à un niveau minimal (**1**) et les fichiers de journalisation seront stockés dans le répertoire **/var/log/samba/**. Samba étend la macro **%m** dans le paramètre **log file** au nom NetBIOS des clients qui se connectent. Cela permet de créer des fichiers journaux individuels pour chaque client.

3. En option, configurez le partage de fichiers ou d'imprimantes. Voir :

- Configuration d'un partage utilisant des ACL POSIX
- Configuration d'un partage utilisant les ACL de Windows
- Configurer Samba en tant que serveur d'impression

4. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

5. Si vous configurez des partages nécessitant une authentification, créez les comptes d'utilisateur.
Pour plus d'informations, voir Création et activation des comptes d'utilisateurs locaux .

6. Ouvrez les ports requis et rechargez la configuration du pare-feu à l'aide de l'utilitaire **firewall-cmd**:

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

7. Activez et démarrez le service **smb**:

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

Ressources supplémentaires

- **smb.conf(5)** page de manuel

1.3.2. Création et activation de comptes d'utilisateurs locaux

Pour permettre aux utilisateurs de s'authentifier lorsqu'ils se connectent à un partage, vous devez créer les comptes sur l'hôte Samba à la fois dans le système d'exploitation et dans la base de données Samba. Samba a besoin du compte du système d'exploitation pour valider les listes de contrôle d'accès (ACL) sur les objets du système de fichiers et du compte Samba pour authentifier les utilisateurs qui se connectent.

Si vous utilisez le paramètre par défaut **passdb backend = tdbsam**, Samba stocke les comptes d'utilisateurs dans la base de données **/var/lib/samba/private/passdb.tdb**.

La procédure décrite dans cette section explique comment créer un utilisateur local Samba nommé **example**.

Conditions préalables

- Samba est installé et configuré comme un serveur autonome.

Procédure

1. Créer le compte du système d'exploitation :

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

Cette commande ajoute le compte **example** sans créer de répertoire personnel. Si le compte n'est utilisé que pour s'authentifier auprès de Samba, attribuez à la commande **/sbin/nologin** le statut de shell afin d'empêcher le compte de se connecter localement.

2. Définissez un mot de passe pour le compte du système d'exploitation afin de l'activer :

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

Samba n'utilise pas le mot de passe défini sur le compte du système d'exploitation pour s'authentifier. Cependant, vous devez définir un mot de passe pour activer le compte. Si un compte est désactivé, Samba refuse l'accès si cet utilisateur se connecte.

3. Ajoutez l'utilisateur à la base de données Samba et définissez un mot de passe pour le compte :

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

Utilisez ce mot de passe pour vous authentifier lorsque vous utilisez ce compte pour vous connecter à un partage Samba.

4. Activer le compte Samba :

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

1.4. COMPRENDRE ET CONFIGURER LE MAPPAGE DES IDENTIFIANTS SAMBA

Les domaines Windows distinguent les utilisateurs et les groupes par des identifiants de sécurité (SID) uniques. Cependant, Linux exige des UID et des GID uniques pour chaque utilisateur et chaque groupe. Si vous exécutez Samba en tant que membre d'un domaine, le service **winbindd** est chargé de fournir au système d'exploitation des informations sur les utilisateurs et les groupes du domaine.

Pour permettre au service **winbindd** de fournir à Linux des identifiants uniques pour les utilisateurs et les groupes, vous devez configurer le mappage des identifiants dans le fichier **/etc/samba/smb.conf** pour :

- La base de données locale (domaine par défaut)
- Le domaine AD ou NT4 dont le serveur Samba est membre
- Chaque domaine de confiance à partir duquel les utilisateurs doivent pouvoir accéder aux ressources de ce serveur Samba

Samba fournit différents back ends de mappage d'ID pour des configurations spécifiques. Les back ends les plus fréquemment utilisés sont les suivants :

Retour à la case départ	Use case
tdb	Le domaine par défaut ***** uniquement
ad	Domaines AD uniquement
rid	Domaines AD et NT4
autorid	AD, NT4 et le domaine par défaut *****

1.4.1. Planification des plages d'ID Samba

Que vous stockiez les UID et GID Linux dans AD ou que vous configuriez Samba pour les générer, chaque configuration de domaine nécessite une plage d'ID unique qui ne doit pas se chevaucher avec d'autres domaines.

AVERTISSEMENT

Si vous définissez des plages d'identifiants qui se chevauchent, Samba ne fonctionnera pas correctement.

Exemple 1.1. Plages d'identifiants uniques

Le tableau suivant montre les plages de mappage d'ID qui ne se chevauchent pas pour les domaines par défaut (*), **AD-DOM** et **TRUST-DOM**.

```
[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
```

IMPORTANT

Vous ne pouvez attribuer qu'une seule plage par domaine. Par conséquent, laissez suffisamment d'espace entre les plages des domaines. Cela vous permettra d'étendre la plage ultérieurement si votre domaine s'agrandit.

Si vous attribuez ultérieurement une plage différente à un domaine, la propriété des fichiers et des répertoires créés précédemment par ces utilisateurs et ces groupes sera perdue.

1.4.2. The * default domain

Dans un environnement de domaine, vous ajoutez une configuration de mappage d'ID pour chacun des éléments suivants :

- Le domaine dont le serveur Samba est membre
- Chaque domaine de confiance qui doit pouvoir accéder au serveur Samba

Cependant, pour tous les autres objets, Samba attribue des identifiants du domaine par défaut. Ceci inclut :

- Utilisateurs et groupes locaux de Samba
- Comptes et groupes intégrés à Samba, tels que **BUILTIN\Administrators**

IMPORTANT

Vous devez configurer le domaine par défaut comme décrit dans cette section pour permettre à Samba de fonctionner correctement.

Le back-end du domaine par défaut doit être accessible en écriture pour stocker en permanence les identifiants attribués.

Pour le domaine par défaut, vous pouvez utiliser l'un des back ends suivants :

tdb

Lorsque vous configurez le domaine par défaut pour utiliser le back-end **tdb**, définissez une plage d'ID suffisamment large pour inclure les objets qui seront créés à l'avenir et qui ne font pas partie d'une configuration définie de mappage d'ID de domaine.
Par exemple, dans la section **[global]** du fichier **/etc/samba/smb.conf**, vous pouvez définir ce qui suit :

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

Pour plus de détails, voir Utilisation du back-end de mappage des ID TDB .

autorid

Lorsque vous configurez le domaine par défaut pour utiliser le back-end **autorid**, l'ajout de configurations supplémentaires de mappage d'ID pour les domaines est facultatif.
Par exemple, dans la section **[global]** du fichier **/etc/samba/smb.conf**, vous pouvez définir ce qui suit :

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

Pour plus de détails, voir Utilisation du back-end de mappage de l'identifiant autorid .

1.4.3. Utilisation du back-end de mappage de l'ID de la tdb

Le service **winbindd** utilise par défaut le back-end de mappage d'ID inscriptible **tdb** pour stocker les tables de mappage d'identifiants de sécurité (SID), d'identifiants d'utilisateur (UID) et d'identifiants d'utilisateur (GID). Cela inclut les utilisateurs locaux, les groupes et les mandants intégrés.

Utilisez ce back-end uniquement pour le domaine par défaut *****. Par exemple :

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

Ressources supplémentaires

- The * default domain.

1.4.4. Utilisation du back-end de mappage des identifiants publicitaires

Cette section décrit comment configurer un membre Samba AD pour utiliser le back-end de mappage d'ID **ad**.

Le back-end de mappage d'ID **ad** met en œuvre une API en lecture seule pour lire les informations sur les comptes et les groupes à partir d'AD. Cela présente les avantages suivants :

- Tous les paramètres des utilisateurs et des groupes sont stockés de manière centralisée dans AD.
- Les ID d'utilisateur et de groupe sont cohérents sur tous les serveurs Samba qui utilisent ce back-end.
- Les identifiants ne sont pas stockés dans une base de données locale susceptible d'être corrompue, et les propriétaires des fichiers ne peuvent donc pas être perdus.

NOTE

Le back-end de mappage d'ID **ad** ne prend pas en charge les domaines Active Directory avec des trusts à sens unique. Si vous configurez un membre de domaine dans un Active Directory avec des trusts à sens unique, utilisez à la place l'un des backends de mappage d'ID suivants : **tdb**, **rid**, ou **autorid**.

Le back-end de l'annonce lit les attributs suivants de l'annonce :

Nom de l'attribut AD	Type d'objet	Mises en correspondance avec
sAMAccountName	Utilisateur et groupe	Nom de l'utilisateur ou du groupe, en fonction de l'objet
uidNumber	User	Identifiant de l'utilisateur (UID)
gidNumber	Groupe	ID du groupe (GID)
loginShell [a]	User	Chemin d'accès à l'interpréteur de commandes de l'utilisateur
unixHomeDirectory [a]	User	Chemin d'accès au répertoire personnel de l'utilisateur
primaryGroupID [b]	User	ID du groupe primaire

[a] Samba ne lit cet attribut que si vous avez défini **idmap config *DOMAIN*:unix_nss_info = yes**.

[b] Samba ne lit cet attribut que si vous avez défini **idmap config *DOMAIN*:unix_primary_group = yes**.

Conditions préalables

- Les utilisateurs et les groupes doivent avoir des identifiants uniques définis dans AD, et les identifiants doivent être compris dans la plage configurée dans le fichier **/etc/samba/smb.conf**. Les objets dont les ID sont en dehors de cette plage ne seront pas disponibles sur le serveur Samba.

- Les utilisateurs et les groupes doivent avoir tous les attributs requis définis dans AD. Si les attributs requis sont manquants, l'utilisateur ou le groupe ne sera pas disponible sur le serveur Samba. Les attributs requis dépendent de votre configuration. conditions préalables
- Vous avez installé Samba.
- La configuration de Samba, à l'exception du mappage des identifiants, existe dans le fichier **/etc/samba/smb.conf**.

Procédure

1. Modifiez la section **[global]** dans le fichier **/etc/samba/smb.conf**:
   a. Ajoutez une configuration de mappage d'ID pour le domaine par défaut (*) s'il n'existe pas. Par exemple :

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

   b. Activer le back-end de mappage de **ad** ID pour le domaine AD :

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

   c. Définir la plage d'ID attribuée aux utilisateurs et aux groupes dans le domaine AD. Par exemple :

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

IMPORTANT

La plage ne doit pas se chevaucher avec une autre configuration de domaine sur ce serveur. De plus, la plage doit être suffisamment grande pour inclure tous les identifiants attribués à l'avenir. Pour plus de détails, voir Planification des plages d'ID Samba.

   d. Définir que Samba utilise le schéma RFC 2307 lors de la lecture des attributs d'AD :

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

   e. Pour permettre à Samba de lire le shell de connexion et le chemin d'accès au répertoire personnel de l'utilisateur à partir de l'attribut AD correspondant, définissez :

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

Vous pouvez également définir un chemin d'accès au répertoire d'accueil et un shell de connexion uniformes pour l'ensemble du domaine, qui seront appliqués à tous les utilisateurs. Par exemple :

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

f. Par défaut, Samba utilise l'attribut **primaryGroupID** d'un objet utilisateur comme groupe primaire de l'utilisateur sous Linux. Vous pouvez également configurer Samba pour qu'il utilise la valeur définie dans l'attribut **gidNumber**:

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

2. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

3. Recharger la configuration de Samba :

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

Ressources supplémentaires

- The * default domain
- **smb.conf(5)** et **idmap_ad(8)** pages de manuel
- **VARIABLE SUBSTITUTIONS** section dans la page de manuel **smb.conf(5)**

1.4.5. Utilisation du back-end de mappage de l'identifiant rid

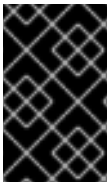
Cette section décrit comment configurer un membre du domaine Samba pour qu'il utilise le back-end **rid** ID mapping.

Samba peut utiliser l'identifiant relatif (RID) d'un SID Windows pour générer un ID sur Red Hat Enterprise Linux.

NOTE

Le RID est la dernière partie du SID. Par exemple, si le SID d'un utilisateur est **S-1-5-21-5421822485-1151247151-421485315-30014**, alors **30014** est le RID correspondant.

Le back-end de mappage d'ID **rid** implémente une API en lecture seule pour calculer les informations sur les comptes et les groupes sur la base d'un schéma de mappage algorithmique pour les domaines AD et NT4. Lorsque vous configurez le back-end, vous devez définir le RID le plus bas et le plus élevé dans le paramètre **idmap config *DOMAIN* : *range*** dans le paramètre Samba ne mappera pas les utilisateurs ou les groupes avec un RID inférieur ou supérieur à celui défini dans ce paramètre.



IMPORTANT

En tant que back-end en lecture seule, **rid** ne peut pas attribuer de nouveaux ID, comme pour les groupes **BUILTIN**. Par conséquent, n'utilisez pas ce back-end pour le domaine par défaut *.

Avantages de l'utilisation du back-end rid

- Tous les utilisateurs et groupes du domaine dont le RID se situe dans la plage configurée sont automatiquement disponibles sur le membre du domaine.

- Il n'est pas nécessaire d'attribuer manuellement des identifiants, des répertoires personnels et des shells de connexion.

Inconvénients de l'utilisation du back-end rid

- Tous les utilisateurs du domaine se voient attribuer le même shell de connexion et le même répertoire personnel. Vous pouvez toutefois utiliser des variables.
- Les ID d'utilisateurs et de groupes ne sont identiques entre les membres du domaine Samba que si tous utilisent le back-end **rid** avec les mêmes paramètres de plage d'ID.
- Vous ne pouvez pas exclure des utilisateurs ou des groupes individuels de la disponibilité sur le membre du domaine. Seuls les utilisateurs et les groupes en dehors de la plage configurée sont exclus.
- D'après les formules utilisées par le service **winbindd** pour calculer les ID, des doublons peuvent se produire dans les environnements multi-domaines si des objets de différents domaines ont le même RID.

Conditions préalables

- Vous avez installé Samba.
- La configuration de Samba, à l'exception du mappage des identifiants, existe dans le fichier **/etc/samba/smb.conf**.

Procédure

1. Modifiez la section **[global]** dans le fichier **/etc/samba/smb.conf**:
   a. Ajoutez une configuration de mappage d'ID pour le domaine par défaut (*) s'il n'existe pas. Par exemple :

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

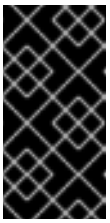
   b. Activer le back-end de mappage de **rid** ID pour le domaine :

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

   c. Définissez un intervalle suffisamment grand pour inclure tous les RID qui seront attribués à l'avenir. Par exemple :

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

   Samba ignore les utilisateurs et les groupes dont les RID dans ce domaine ne sont pas compris dans l'intervalle.



IMPORTANT

La plage ne doit pas se chevaucher avec une autre configuration de domaine sur ce serveur. De plus, la plage doit être suffisamment grande pour inclure tous les identifiants attribués à l'avenir. Pour plus de détails, voir Planification des plages d'ID Samba.

d. Définir un shell et un chemin d'accès au répertoire personnel qui seront attribués à tous les utilisateurs mappés. Par exemple :

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

2. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

3. Recharger la configuration de Samba :

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

Ressources supplémentaires

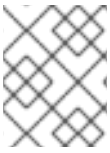
- The * default domain
- **VARIABLE SUBSTITUTIONS** section dans la page de manuel **smb.conf(5)**
- Calcul de l'ID local à partir d'un RID, voir la page de manuel **idmap_rid(8)**

1.4.6. Utilisation du back-end de mappage de l'identifiant autorid

Cette section décrit comment configurer un membre du domaine Samba pour qu'il utilise le back-end **autorid** ID mapping.

Le back-end **autorid** fonctionne de la même manière que le back-end **rid** ID mapping, mais il peut attribuer automatiquement des ID pour différents domaines. Cela vous permet d'utiliser le back-end **autorid** dans les situations suivantes :

- Uniquement pour le domaine par défaut *
- Pour le domaine par défaut * et les domaines supplémentaires, sans qu'il soit nécessaire de créer des configurations de mappage d'ID pour chacun des domaines supplémentaires
- Uniquement pour des domaines spécifiques



NOTE

Si vous utilisez **autorid** pour le domaine par défaut, l'ajout d'une configuration supplémentaire de mappage d'ID pour les domaines est facultatif.

Certaines parties de cette section ont été adoptées à partir de la documentation idmap config autorid publiée dans le Samba Wiki. Licence : CC BY 4.0. Auteurs et contributeurs : Voir l'onglet historique de la page Wiki.

Avantages de l'utilisation du back-end autorid

- Tous les utilisateurs et groupes du domaine dont l'UID et le GID calculés se trouvent dans la plage configurée sont automatiquement disponibles sur le membre du domaine.
- Il n'est pas nécessaire d'attribuer manuellement des identifiants, des répertoires personnels et des shells de connexion.

- Pas d'ID en double, même si plusieurs objets dans un environnement multi-domaines ont le même RID.

Inconvénients

- Les ID d'utilisateur et de groupe ne sont pas les mêmes pour tous les membres du domaine Samba.
- Tous les utilisateurs du domaine se voient attribuer le même shell de connexion et le même répertoire personnel. Vous pouvez toutefois utiliser des variables.
- Vous ne pouvez pas exclure des utilisateurs ou des groupes individuels de la disponibilité sur le membre du domaine. Seuls les utilisateurs et les groupes dont l'UID ou le GID calculé est en dehors de la plage configurée sont exclus.

Conditions préalables

- Vous avez installé Samba.
- La configuration de Samba, à l'exception du mappage des identifiants, existe dans le fichier **/etc/samba/smb.conf**.

Procédure

1. Modifiez la section **[global]** dans le fichier **/etc/samba/smb.conf**:
   a. Activer le back-end de mappage d'ID **autorid** pour le domaine par défaut *****:

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

   b. Définissez une plage suffisamment grande pour attribuer des identifiants à tous les objets existants et futurs. Par exemple :

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

   Samba ignore les utilisateurs et les groupes dont les ID calculés dans ce domaine ne sont pas compris dans cette plage.

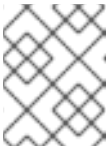
   AVERTISSEMENT

   Une fois que vous avez défini la plage et que Samba commence à l'utiliser, vous ne pouvez augmenter que la limite supérieure de la plage. Toute autre modification de la plage peut entraîner de nouvelles attributions d'ID, et donc la perte de propriétaires de fichiers.

   c. Il est possible de définir une taille de plage. Par exemple :

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

Samba assigns this number of continuous IDs for each domain's object until all IDs from the range set in the **idmap config * : *range*** parameter are taken.



NOTE

Si vous définissez une taille de plage, vous devez adapter la plage en conséquence. La plage doit être un multiple de la taille de la plage.

d. Définir un shell et un chemin d'accès au répertoire personnel qui seront attribués à tous les utilisateurs mappés. Par exemple :

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

e. En option, ajoutez une configuration supplémentaire de mappage d'ID pour les domaines. Si aucune configuration pour un domaine individuel n'est disponible, Samba calcule l'ID en utilisant les paramètres du back-end **autorid** dans le domaine par défaut ***** précédemment configuré.

IMPORTANT

La plage ne doit pas se chevaucher avec une autre configuration de domaine sur ce serveur. De plus, la plage doit être suffisamment grande pour inclure tous les identifiants attribués à l'avenir. Pour plus de détails, voir Planification des plages d'ID Samba.

2. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

3. Recharger la configuration de Samba :

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

Ressources supplémentaires

- **THE MAPPING FORMULAS** section dans la page de manuel **idmap_autorid(8)**
- **rangesize** description du paramètre dans la page de manuel **idmap_autorid(8)**
- **VARIABLE SUBSTITUTIONS** section dans la page de manuel **smb.conf(5)**

1.5. CONFIGURATION DE SAMBA EN TANT QUE SERVEUR MEMBRE D'UN DOMAINE AD

Si vous utilisez un domaine AD ou NT4, utilisez Samba pour ajouter votre serveur Red Hat Enterprise Linux en tant que membre du domaine afin d'obtenir ce qui suit :

- Accéder aux ressources du domaine sur d'autres membres du domaine
- Authentifier les utilisateurs du domaine pour les services locaux, tels que **sshd**

- Partager des répertoires et des imprimantes hébergés sur le serveur pour faire office de serveur de fichiers et d'impression

1.5.1. Joindre un système RHEL à un domaine AD

Samba Winbind est une alternative au System Security Services Daemon (SSSD) pour connecter un système Red Hat Enterprise Linux (RHEL) à Active Directory (AD). Cette section décrit comment joindre un système RHEL à un domaine AD en utilisant **realmd** pour configurer Samba Winbind.

Procédure

1. Si votre AD nécessite le type de chiffrement RC4, obsolète, pour l'authentification Kerberos, activez la prise en charge de ces algorithmes de chiffrement dans RHEL :

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

2. Install the following packages:

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

3. Pour partager des répertoires ou des imprimantes sur le membre du domaine, installez le paquet **samba**:

```
# dnf install samba
```

4. Sauvegarder le fichier de configuration de **/etc/samba/smb.conf** Samba existant :

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

5. Rejoindre le domaine. Par exemple, pour rejoindre un domaine nommé **ad.example.com**:

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

   En utilisant la commande précédente, l'utilitaire **realm** s'affiche automatiquement :

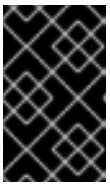
   - Crée un fichier **/etc/samba/smb.conf** pour un membre du domaine **ad.example.com**
   - Ajoute le module **winbind** pour les recherches d'utilisateurs et de groupes au fichier **/etc/nsswitch.conf**
   - Met à jour les fichiers de configuration du module d'authentification enfichable (PAM) dans le répertoire **/etc/pam.d/**
   - Démarre le service **winbind** et permet au service de démarrer lorsque le système démarre

6. Il est possible de définir un autre back-end de mappage d'identifiants ou des paramètres de mappage d'identifiants personnalisés dans le fichier **/etc/samba/smb.conf**.

Pour plus de détails, voir Comprendre et configurer le mappage des ID Samba .

1. Vérifiez que le service **winbind** est en cours d'exécution :

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



IMPORTANT

Pour permettre à Samba d'interroger les informations sur les utilisateurs et les groupes du domaine, le service **winbind** doit être en cours d'exécution avant que vous ne lanciez **smb**.

2. Si vous avez installé le paquetage **samba** pour partager des répertoires et des imprimantes, activez et démarrez le service **smb**:

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

3. En option, si vous authentifiez des connexions locales à Active Directory, activez le plug-in **winbind_krb5_localauth**. Voir Utilisation du plug-in d'autorisation locale pour MIT Kerberos .

Verification steps

1. Afficher les détails d'un utilisateur AD, tel que le compte administrateur AD dans le domaine AD :

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

2. Interroger les membres du groupe des utilisateurs du domaine dans le domaine AD :

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

3. Si vous le souhaitez, vérifiez que vous pouvez utiliser les utilisateurs et les groupes du domaine lorsque vous définissez les autorisations sur les fichiers et les répertoires. Par exemple, pour définir le propriétaire du fichier **/srv/samba/example.txt** comme étant **AD\administrator** et le groupe comme étant **AD\Domain Users**:

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

4. Vérifiez que l'authentification Kerberos fonctionne comme prévu :

   a. Sur le membre du domaine AD, obtenez un ticket pour le principal **administrator@AD.EXAMPLE.COM**:

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

   b. Affiche le ticket Kerberos mis en cache :

```
# 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. Affichez les domaines disponibles :

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

Ressources supplémentaires

- Si vous ne souhaitez pas utiliser les algorithmes de chiffrement RC4, qui sont obsolètes, vous pouvez activer le type de chiffrement AES dans AD. Voir
- Activation du type de cryptage AES dans Active Directory à l'aide d'un GPO . Notez que cela peut avoir un impact sur d'autres services dans votre AD.
- **realm(8)** page de manuel

1.5.2. Utilisation du plug-in d'autorisation locale pour MIT Kerberos

Le service **winbind** fournit des utilisateurs Active Directory au membre du domaine. Dans certaines situations, les administrateurs souhaitent permettre aux utilisateurs du domaine de s'authentifier auprès de services locaux, tels qu'un serveur SSH, qui s'exécutent sur le membre du domaine. Lorsque vous utilisez Kerberos pour authentifier les utilisateurs du domaine, activez le plug-in **winbind_krb5_localauth** pour mapper correctement les principaux Kerberos aux comptes Active Directory via le service **winbind**.

Par exemple, si l'attribut **sAMAccountName** d'un utilisateur Active Directory est défini sur **EXAMPLE** et que l'utilisateur tente de se connecter avec un nom d'utilisateur en minuscules, Kerberos renvoie le nom d'utilisateur en majuscules. Par conséquent, les entrées ne correspondent pas et l'authentification échoue.

En utilisant le plug-in **winbind_krb5_localauth**, les noms de comptes sont correctement mappés. Notez que cela ne s'applique qu'à l'authentification GSSAPI et non à l'obtention du ticket initial (TGT).

Conditions préalables

- Samba est configuré en tant que membre d'un Active Directory.
- Red Hat Enterprise Linux authentifie les tentatives de connexion par rapport à Active Directory.
- Le service **winbind** est en cours d'exécution.

Procédure

Modifiez le fichier **/etc/krb5.conf** et ajoutez la section suivante :

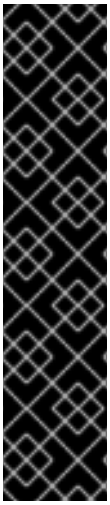
```
[plugins]
localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
}
```

Ressources supplémentaires

- **winbind_krb5_localauth(8)** page de manuel.

1.6. CONFIGURATION DE SAMBA SUR UN MEMBRE DU DOMAINE IDM

Cette section décrit comment configurer Samba sur un hôte qui est relié à un domaine Red Hat Identity Management (IdM). Les utilisateurs d'IdM et, le cas échéant, des domaines Active Directory (AD) approuvés, peuvent accéder aux partages et aux services d'impression fournis par Samba.



IMPORTANT

L'utilisation de Samba sur un membre de domaine IdM est une fonctionnalité de l'aperçu technologique qui n'est pas prise en charge et qui comporte certaines limitations. Par exemple, les contrôleurs de confiance IdM ne prennent pas en charge le service Active Directory Global Catalog, ni la résolution des groupes IdM à l'aide des protocoles Distributed Computing Environment / Remote Procedure Calls (DCE/RPC). Par conséquent, les utilisateurs AD ne peuvent accéder aux partages Samba et aux imprimantes hébergées sur des clients IdM que lorsqu'ils sont connectés à d'autres clients IdM ; les utilisateurs AD connectés à une machine Windows ne peuvent pas accéder aux partages Samba hébergés sur un membre du domaine IdM.

Les clients qui déploient Samba sur des membres de domaine IdM sont encouragés à fournir un retour d'information à Red Hat.

Conditions préalables

- L'hôte est joint en tant que client au domaine IdM.
- Les serveurs IdM et le client doivent fonctionner sous RHEL 9.0 ou une version ultérieure.

1.6.1. Préparation du domaine IdM pour l'installation de Samba sur les membres du domaine

Avant de pouvoir configurer Samba sur un client IdM, vous devez préparer le domaine IdM à l'aide de l'utilitaire **ipa-adtrust-install** sur un serveur IdM.

NOTE

Tout système sur lequel vous exécutez la commande **ipa-adtrust-install** devient automatiquement un contrôleur de confiance AD. Toutefois, vous ne devez exécuter **ipa-adtrust-install** qu'une seule fois sur un serveur IdM.

Conditions préalables

- Le serveur IdM est installé.
- Vous devez disposer des privilèges de root pour installer les paquets et redémarrer les services IdM.

Procédure

1. Installez les paquets nécessaires :

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

2. S'authentifier en tant qu'utilisateur administratif de l'IdM :

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

3. Exécutez l'utilitaire **ipa-adtrust-install**:

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

Les enregistrements de service DNS sont créés automatiquement si IdM a été installé avec un serveur DNS intégré.

Si vous avez installé IdM sans serveur DNS intégré, **ipa-adtrust-install** imprime une liste d'enregistrements de service que vous devez ajouter manuellement au DNS avant de pouvoir continuer.

4. Le script vous indique que le site /**etc**/**samba**/**smb.conf** existe déjà et qu'il va être réécrit :

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

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

5. Le script vous invite à configurer le plug-in **slapi-nis**, un plug-in de compatibilité qui permet aux anciens clients Linux de travailler avec des utilisateurs de confiance :

```
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. Lorsque vous y êtes invité, entrez le nom NetBIOS du domaine IdM ou appuyez sur **Enter** pour accepter le nom proposé :

```
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. Vous êtes invité à exécuter la tâche de génération de SID afin de créer un SID pour tous les utilisateurs existants :

```
Voulez-vous exécuter la tâche ipa-sidgen ? [non] : yes
```

Il s'agit d'une tâche gourmande en ressources, donc si vous avez un grand nombre d'utilisateurs, vous pouvez l'exécuter à un autre moment.

8. **(Optional)** Par défaut, la plage de ports Dynamic RPC est définie comme **49152-65535** pour Windows Server 2008 et les versions ultérieures. Si vous devez définir une plage de ports Dynamic RPC différente pour votre environnement, configurez Samba pour qu'il utilise d'autres

ports et ouvrez ces ports dans les paramètres de votre pare-feu. L'exemple suivant définit la plage de ports à **55000-65000**.

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

9. Redémarrez le service **ipa**:

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

10. Utilisez l'utilitaire **smbclient** pour vérifier que Samba répond à l'authentification Kerberos du côté IdM :

```
[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. Activation du type de cryptage AES dans Active Directory à l'aide d'un GPO

Cette section explique comment activer le type de chiffrement AES dans Active Directory (AD) à l'aide d'un objet de stratégie de groupe (GPO). Certaines fonctionnalités de RHEL, telles que l'exécution d'un serveur Samba sur un client IdM, nécessitent ce type de chiffrement.

Notez que RHEL ne prend plus en charge les types de chiffrement DES et RC4 faibles.

Conditions préalables

- Vous êtes connecté à AD en tant qu'utilisateur pouvant modifier les stratégies de groupe.
- Le site **Group Policy Management Console** est installé sur l'ordinateur.

Procédure

1. Ouvrez le site **Group Policy Management Console**.
2. Cliquez avec le bouton droit de la souris sur **Default Domain Policy**, puis sélectionnez **Edit**. Le site **Group Policy Management Editor** s'ouvre.
3. Naviguez vers **Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options**.
4. Double-cliquez sur la politique **Network security: Configure encryption types allowed for Kerberos**.
5. Sélectionnez **AES256_HMAC_SHA1** et, éventuellement, **Future encryption types**.
6. Cliquez sur **OK**.
7. Fermer le site **Group Policy Management Editor**.

8. Répétez les étapes pour le site **Default Domain Controller Policy**.

9. Attendez que les contrôleurs de domaine Windows (DC) appliquent automatiquement la stratégie de groupe. Pour appliquer manuellement le GPO sur un DC, entrez la commande suivante à l'aide d'un compte disposant d'autorisations d'administrateur :

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

1.6.3. Installation et configuration d'un serveur Samba sur un client IdM

Cette section décrit comment installer et configurer Samba sur un client inscrit dans un domaine IdM.

Conditions préalables

- Les serveurs IdM et le client doivent fonctionner sous RHEL 9.0 ou une version ultérieure.
- Le domaine IdM est préparé comme décrit dans Préparation du domaine IdM pour l'installation de Samba sur les membres du domaine.
- Si IdM a une confiance configurée avec AD, activez le type de cryptage AES pour Kerberos. Par exemple, utilisez un objet de stratégie de groupe (GPO) pour activer le type de cryptage AES. Pour plus de détails, voir Activation du chiffrement AES dans Active Directory à l'aide d'un GPO .

Procédure

1. Installez le paquetage **ipa-client-samba**:

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

2. Utilisez l'utilitaire **ipa-client-samba** pour préparer le client et créer une configuration Samba initiale :

```
[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. Par défaut, **ipa-client-samba** ajoute automatiquement la section **[homes]** au fichier **/etc/samba/smb.conf** qui partage dynamiquement le répertoire personnel d'un utilisateur lorsque celui-ci se connecte. Si les utilisateurs n'ont pas de répertoire personnel sur ce serveur, ou si vous ne voulez pas les partager, supprimez les lignes suivantes de **/etc/samba/smb.conf**:

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

4. Partager des répertoires et des imprimantes. Pour plus de détails, voir :
   - Configuration d'un partage de fichiers Samba utilisant des listes de contrôle POSIX
   - Configuration d'un partage utilisant les ACL de Windows
   - Configurer Samba en tant que serveur d'impression
5. Ouvrez les ports requis pour un client Samba dans le pare-feu local :

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

6. Activez et démarrez les services **smb** et **winbind**:

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

Verification steps

Exécutez l'étape de vérification suivante sur un autre membre du domaine IdM sur lequel le paquetage **samba-client** est installé :

- Dressez la liste des partages sur le serveur Samba utilisant l'authentification Kerberos :

```
$ 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)
...
```

Ressources supplémentaires

- **ipa-client-samba(1)** page de manuel

1.6.4. Ajout manuel d'une configuration de mappage d'ID si IdM fait confiance à un nouveau domaine

Samba nécessite une configuration de mappage d'ID pour chaque domaine à partir duquel les utilisateurs accèdent aux ressources. Sur un serveur Samba existant fonctionnant sur un client IdM, vous devez ajouter manuellement une configuration de mappage d'identifiants après que l'administrateur a ajouté une nouvelle confiance à un domaine Active Directory (AD).

Conditions préalables

- Vous avez configuré Samba sur un client IdM. Par la suite, une nouvelle confiance a été ajoutée à IdM.
- Les types de chiffrement DES et RC4 pour Kerberos doivent être désactivés dans le domaine AD de confiance. Pour des raisons de sécurité, RHEL 9 ne prend pas en charge ces types de chiffrement faibles.

Procédure

1. S'authentifier à l'aide de la base de données de l'hôte :

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

2. Utilisez la commande **ipa idrange-find** pour afficher l'ID de base et la taille de la plage d'ID du nouveau domaine. Par exemple, la commande suivante affiche les valeurs du domaine **ad.example.com**:

```
[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
----------------------------
```

   Vous aurez besoin des valeurs des attributs **ipabaseid** et **ipaidrangesize** dans les étapes suivantes.

3. Pour calculer l'ID utilisable le plus élevé, utilisez la formule suivante :

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

   Avec les valeurs de l'étape précédente, l'ID utilisable le plus élevé pour le domaine **ad.example.com** est **1918599999** (1918400000 200000 - 1).

4. Modifiez le fichier **/etc/samba/smb.conf** et ajoutez la configuration du mappage d'ID pour le domaine à la section **[global]**:

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

   Spécifiez la valeur de l'attribut **ipabaseid** comme étant la plus basse et la valeur calculée à l'étape précédente comme étant la plus haute de la plage.

5. Redémarrez les services **smb** et **winbind**:

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

Verification steps

- Dressez la liste des partages sur le serveur Samba utilisant l'authentification Kerberos :

```
$ 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. Ressources supplémentaires

- Installation d'un client de gestion de l'identité

1.7. CONFIGURATION D'UN PARTAGE DE FICHIERS SAMBA UTILISANT DES LISTES DE CONTRÔLE POSIX

En tant que service Linux, Samba prend en charge les partages avec des ACL POSIX. Elles vous permettent de gérer les autorisations localement sur le serveur Samba à l'aide d'utilitaires tels que **chmod**. Si le partage est stocké sur un système de fichiers qui prend en charge les attributs étendus, vous pouvez définir des ACL avec plusieurs utilisateurs et groupes.

NOTE

Si vous devez utiliser des ACL Windows à granularité fine à la place, voir Configuration d'un partage utilisant des ACL Windows.

Certaines parties de cette section ont été reprises de la documentation Setting up a Share Using POSIX ACLs publiée dans le Samba Wiki. Licence : CC BY 4.0. Auteurs et contributeurs : Voir l'onglet historique de la page Wiki.

1.7.1. Ajout d'un partage utilisant des ACL POSIX

Cette section décrit comment créer un partage nommé **example** qui fournit le contenu du répertoire **/srv/samba/example/** et utilise des ACL POSIX.

Conditions préalables

Samba a été configuré dans l'un des modes suivants :

- Serveur autonome
- Membre du domaine

Procédure

1. Créez le dossier s'il n'existe pas. Par exemple :

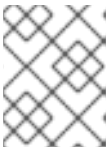
```
# mkdir -p /srv/samba/example/
```

2. Si vous utilisez SELinux en mode **enforcing**, définissez le contexte **samba_share_t** pour le répertoire :

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

3. Définir les ACL du système de fichiers sur le répertoire. Pour plus de détails, voir :
   - Définition d'ACLs standard sur un partage Samba qui utilise des ACLs POSIX
   - Définition d'ACL étendues sur un partage qui utilise des ACL POSIX .
4. Ajoutez l'exemple de partage au fichier **/etc/samba/smb.conf**. Par exemple, pour ajouter le partage en écriture :

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



NOTE

Indépendamment des ACL du système de fichiers, si vous ne définissez pas **read only = no**, Samba partage le répertoire en mode lecture seule.

5. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

6. Ouvrez les ports requis et rechargez la configuration du pare-feu à l'aide de l'utilitaire **firewall-cmd**:

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

7. Redémarrez le service **smb**:

```
# systemctl restart smb
```

1.7.2. Définition d'ACL Linux standard sur un partage Samba qui utilise des ACL POSIX

Les listes de contrôle d'accès standard de Linux permettent de définir des autorisations pour un propriétaire, un groupe et tous les autres utilisateurs non définis. Vous pouvez utiliser les utilitaires **chown**, **chgrp**, et **chmod** pour mettre à jour les ACL. Si vous avez besoin d'un contrôle précis, vous pouvez utiliser les ACL POSIX plus complexes, voir

Définition d'ACL étendues sur un partage Samba qui utilise des ACL POSIX .

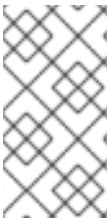
La procédure suivante définit le propriétaire du répertoire **/srv/samba/example/** comme étant l'utilisateur **root**, accorde les droits de lecture et d'écriture au groupe **Domain Users** et refuse l'accès à tous les autres utilisateurs.

Conditions préalables

- Le partage Samba sur lequel vous souhaitez définir les ACL existe.

Procédure

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



NOTE

L'activation du bit set-group-ID (SGID) sur un répertoire définit automatiquement le groupe par défaut pour tous les nouveaux fichiers et sous-répertoires sur celui du groupe du répertoire, au lieu du comportement habituel qui consiste à le définir sur le groupe primaire de l'utilisateur qui a créé la nouvelle entrée du répertoire.

Ressources supplémentaires

- **chown(1)** et **chmod(1)** pages de manuel

1.7.3. Définition d'ACL étendues sur un partage Samba qui utilise des ACL POSIX

Si le système de fichiers sur lequel le répertoire partagé est stocké prend en charge les ACL étendues, vous pouvez les utiliser pour définir des autorisations complexes. Les ACL étendues peuvent contenir des autorisations pour plusieurs utilisateurs et groupes.

Les ACL POSIX étendues vous permettent de configurer des ACL complexes avec plusieurs utilisateurs et groupes. Toutefois, vous ne pouvez définir que les autorisations suivantes :

- Pas d'accès
- Lire l'accès
- Accès en écriture
- Contrôle total

Si vous avez besoin d'autorisations Windows fines, telles que **Create folder** / **append data**, configurez le partage pour qu'il utilise les listes de contrôle d'accès Windows.

Voir Configuration d'un partage utilisant les ACL de Windows .

La procédure suivante montre comment activer les ACL étendues sur un partage. Elle contient également un exemple de configuration des ACL étendues.

Conditions préalables

- Le partage Samba sur lequel vous souhaitez définir les ACL existe.

Procédure

1. Activez le paramètre suivant dans la section du partage du fichier **/etc/samba/smb.conf** pour activer l'héritage des ACL étendues :

```
hériter des acls = oui
```

Pour plus de détails, voir la description des paramètres dans la page de manuel **smb.conf(5**).

2. Redémarrez le service **smb**:

```
# systemctl restart smb
```

3. Définissez les ACL sur le répertoire. Par exemple :

Exemple 1.2. Définition des ACL étendues

La procédure suivante définit les autorisations de lecture, d'écriture et d'exécution pour le groupe **Domain Admins**, les autorisations de lecture et d'exécution pour le groupe **Domain Users**, et refuse l'accès à tous les autres utilisateurs du répertoire **/srv/samba/example/**:

1. Désactiver l'attribution automatique des autorisations au groupe principal de comptes d'utilisateurs :

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

Le groupe primaire du répertoire est également mappé au principal dynamique **CREATOR GROUP**. Lorsque vous utilisez des ACL POSIX étendues sur un partage Samba, ce principal est automatiquement ajouté et vous ne pouvez pas le supprimer.

2. Définir les droits d'accès au répertoire :

   a. Accorder les droits de lecture, d'écriture et d'exécution au groupe **Domain Admins**:

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

   b. Accorder les droits de lecture et d'exécution au groupe **Domain Users**:

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

   c. Définissez les autorisations pour l'entrée ACL **other** afin de refuser l'accès aux utilisateurs qui ne correspondent pas aux autres entrées ACL :

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

Ces paramètres ne s'appliquent qu'à ce répertoire. Sous Windows, ces ACL sont associées au mode **This folder only**.

3. Pour permettre aux nouveaux objets du système de fichiers créés dans ce répertoire d'hériter des autorisations définies à l'étape précédente :

```
# 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/
```

Avec ces paramètres, le mode **This folder only** pour les mandants est maintenant réglé sur **This folder, subfolders, and files**.

Samba associe les autorisations définies dans la procédure aux listes de contrôle d'accès de Windows suivantes :

Principal	Accès	S'applique à
Domain\Administrateurs de domaine	Contrôle total	Ce dossier, ces sous-dossiers et ces fichiers
Domain\Utilisateurs du domaine	Lire & exécuter	Ce dossier, ces sous-dossiers et ces fichiers
Everyone [a]	Aucun	Ce dossier, ces sous-dossiers et ces fichiers
owner (*Unix User**owner*) [b]	Contrôle total	Ce dossier ne contient que
primary_group (*Unix User**primary_group*) [c]	Aucun	Ce dossier ne contient que
CREATOR OWNER [d] [e]	Contrôle total	Sous-dossiers et fichiers uniquement
CREATOR GROUP [e] [f]	Aucun	Sous-dossiers et fichiers uniquement

[a] Samba mappe les permissions pour ce principal à partir de l'entrée ACL **other**.

[b] Samba associe le propriétaire du répertoire à cette entrée.

[c] Samba associe le groupe primaire du répertoire à cette entrée.

[d] Sur les nouveaux objets du système de fichiers, le créateur hérite automatiquement des autorisations de ce principal.

[e] La configuration ou la suppression de ces principaux des listes de contrôle d'accès n'est pas prise en charge sur les partages qui utilisent des listes de contrôle d'accès POSIX.

[f] Pour les nouveaux objets du système de fichiers, le groupe principal du créateur hérite automatiquement des autorisations de ce principal.

1.8. DÉFINITION DES AUTORISATIONS SUR UN PARTAGE UTILISANT DES ACL POSIX

Pour limiter ou autoriser l'accès à un partage Samba, vous pouvez définir certains paramètres dans la section du partage dans le fichier **/etc/samba/smb.conf**.

NOTE

Les autorisations basées sur les partages déterminent si un utilisateur, un groupe ou un hôte peut accéder à un partage. Ces paramètres n'affectent pas les ACL du système de fichiers.

Utilisez les paramètres basés sur les partages pour restreindre l'accès aux partages, par exemple pour interdire l'accès à partir d'hôtes spécifiques.

Conditions préalables

- Un partage avec des ACL POSIX a été mis en place.

1.8.1. Configuration de l'accès au partage basé sur les utilisateurs et les groupes

Le contrôle d'accès basé sur l'utilisateur et le groupe vous permet d'accorder ou de refuser l'accès à un partage à certains utilisateurs et groupes.

Conditions préalables

- Le partage Samba sur lequel vous souhaitez définir un accès basé sur l'utilisateur ou le groupe existe.

Procédure

1. Par exemple, pour permettre à tous les membres du groupe **Domain Users** d'accéder à un partage alors que l'accès est refusé au compte **user**, ajoutez les paramètres suivants à la configuration du partage :

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

   Le paramètre **invalid users** a une priorité plus élevée que le paramètre **valid users**. Par exemple, si le compte **user** est membre du groupe **Domain Users**, l'accès est refusé à ce compte lorsque vous utilisez l'exemple précédent.

2. Recharger la configuration de Samba :

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

Ressources supplémentaires

- **smb.conf(5)** page de manuel

1.8.2. Configuration de l'accès au partage basé sur l'hôte

Le contrôle d'accès basé sur l'hôte vous permet d'accorder ou de refuser l'accès à un partage en fonction des noms d'hôte, des adresses IP ou des plages IP des clients.

La procédure suivante explique comment autoriser l'adresse IP **127.0.0.1**, la plage IP **192.0.2.0/24** et l'hôte **client1.example.com** à accéder à un partage, et comment refuser l'accès à l'hôte **client2.example.com**:

Conditions préalables

- Le partage Samba sur lequel vous souhaitez définir l'accès basé sur l'hôte existe.

Procédure

1. Ajoutez les paramètres suivants à la configuration du partage dans le fichier **/etc/samba/smb.conf**:

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

Le paramètre **hosts deny** a une priorité plus élevée que **hosts allow**. Par exemple, si **client1.example.com** se résout en une adresse IP qui figure dans le paramètre **hosts allow**, l'accès à cet hôte est refusé.

2. Recharger la configuration de Samba :

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

Ressources supplémentaires

- **smb.conf(5)** page de manuel

1.9. CONFIGURATION D'UN PARTAGE UTILISANT LES ACL DE WINDOWS

Samba prend en charge la définition des ACL Windows sur les partages et les objets du système de fichiers. Cela vous permet de :

- Utiliser les ACL Windows à granularité fine
- Gérer les autorisations de partage et les listes de contrôle d'accès au système de fichiers à l'aide de Windows

Vous pouvez également configurer un partage pour qu'il utilise des ACL POSIX.

Pour plus d'informations, voir Configuration d'un partage de fichiers Samba utilisant des ACL POSIX .

Certaines parties de cette section ont été reprises de la documentation Setting up a Share Using Windows ACLs publiée dans le Samba Wiki. Licence : CC BY 4.0. Auteurs et contributeurs : Voir l'onglet historique de la page Wiki.

1.9.1. Octroi du privilège SeDiskOperatorPrivilege

Seuls les utilisateurs et les groupes disposant du privilège **SeDiskOperatorPrivilege** peuvent configurer les autorisations sur les partages qui utilisent les ACL de Windows.

Procédure

1. Par exemple, pour accorder le privilège **SeDiskOperatorPrivilege** au groupe ***DOMAIN*\Domain Admins** groupe :

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

NOTE

Dans un environnement de domaine, accordez **SeDiskOperatorPrivilege** à un groupe de domaine. Cela vous permet de gérer le privilège de manière centralisée en mettant à jour l'appartenance d'un utilisateur à un groupe.

2. Pour dresser la liste de tous les utilisateurs et groupes auxquels **SeDiskOperatorPrivilege** a été accordé :

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

1.9.2. Activation de la prise en charge des ACL de Windows

Pour configurer des partages prenant en charge les ACL Windows, vous devez activer cette fonctionnalité dans Samba.

Conditions préalables

- Un partage d'utilisateurs est configuré sur le serveur Samba.

Procédure

1. Pour l'activer globalement pour tous les partages, ajoutez les paramètres suivants à la section **[global]** du fichier **/etc/samba/smb.conf**:

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

Vous pouvez également activer la prise en charge de Windows ACL pour des partages individuels, en ajoutant les mêmes paramètres à la section d'un partage.

2. Redémarrez le service **smb**:

```
# systemctl restart smb
```

1.9.3. Ajout d'un partage utilisant les ACL de Windows

Cette section explique comment créer un partage nommé **example**, qui partage le contenu du répertoire **/srv/samba/example/** et utilise les ACL de Windows.

Procédure

1. Créez le dossier s'il n'existe pas. Par exemple :

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

2. Si vous utilisez SELinux en mode **enforcing**, définissez le contexte **samba_share_t** pour le répertoire :

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

3. Ajoutez l'exemple de partage au fichier **/etc/samba/smb.conf**. Par exemple, pour ajouter le partage en écriture :

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

NOTE

Indépendamment des ACL du système de fichiers, si vous ne définissez pas **read only = no**, Samba partage le répertoire en mode lecture seule.

4. Si vous n'avez pas activé la prise en charge des ACL Windows dans la section **[global]** pour tous les partages, ajoutez les paramètres suivants à la section **[example]** pour activer cette fonctionnalité pour ce partage :

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

5. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

6. Ouvrez les ports requis et rechargez la configuration du pare-feu à l'aide de l'utilitaire **firewall-cmd**:

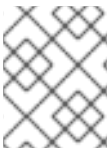
```
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

7. Redémarrez le service **smb**:

```
# systemctl restart smb
```

1.9.4. Gestion des autorisations de partage et des listes de contrôle d'accès au système de fichiers d'un partage utilisant les listes de contrôle d'accès de Windows

Pour gérer les autorisations de partage et les ACL du système de fichiers sur un partage Samba qui utilise des ACL Windows, utilisez une application Windows, telle que **Computer Management**. Pour plus de détails, voir la documentation Windows. Vous pouvez également utiliser l'utilitaire **smbcacls** pour gérer les ACL.



NOTE

Pour modifier les autorisations du système de fichiers à partir de Windows, vous devez utiliser un compte auquel le privilège **SeDiskOperatorPrivilege** a été accordé.

Ressources supplémentaires

- Gestion des ACL sur un partage SMB à l'aide de smbcacls
- Rendre le privilège SeDiskOperatorPrivilege inégalé

1.10. GESTION DES ACL SUR UN PARTAGE SMB À L'AIDE DE SMBCACLS

L'utilitaire **smbcacls** permet de lister, de définir et de supprimer les ACL des fichiers et des répertoires stockés sur un partage SMB. Vous pouvez utiliser **smbcacls** pour gérer les ACL du système de fichiers :

- Sur un serveur Samba local ou distant qui utilise des ACL Windows avancées ou des ACL POSIX
- Sur Red Hat Enterprise Linux pour gérer à distance les ACL sur un partage hébergé sur Windows

1.10.1. Entrées de contrôle d'accès

Chaque entrée ACL d'un objet du système de fichiers contient des entrées de contrôle d'accès (ACE) dans le format suivant :

> *security_principal*:*access_right*/*inheritance_information*/*permissions*

> **Exemple 1.3. Entrées de contrôle d'accès**
>
> Si le groupe **AD\Domain Users** dispose des autorisations **Modify** qui s'appliquent à **This folder, subfolders, and files** sous Windows, l'ACL contient l'ACE suivant :
>
> > AD\NUtilisateurs du domaine:ALLOWED/OI|CI/CHANGE

Un CAE contient les éléments suivants :

Principal responsable de la sécurité

Le principal de sécurité est l'utilisateur, le groupe ou le SID auquel s'appliquent les autorisations de la liste de contrôle d'accès.

Droit d'accès

Définit si l'accès à un objet est accordé ou refusé. La valeur peut être **ALLOWED** ou **DENIED**.

Informations sur l'héritage

Les valeurs suivantes existent :

Tableau 1.1. Paramètres d'héritage

Valeur	Description	Cartes à
OI	Héritage d'objet	Ce dossier et ces fichiers
CI	Héritage du conteneur	Ce dossier et ses sous-dossiers
IO	Hériter seulement	Le CAE ne s'applique pas au fichier ou au répertoire actuel
ID	Héritée	L'ACE a été hérité du répertoire parent

En outre, les valeurs peuvent être combinées comme suit :

Tableau 1.2. Combinaisons de paramètres d'héritage

Combinaisons de valeurs	Correspond à la configuration de Windows **Applies to**
OI|CI	Ce dossier, ces sous-dossiers et ces fichiers
OI|CI|IO	Sous-dossiers et fichiers uniquement
CI|IO	Sous-dossiers uniquement
OI|IO	Fichiers uniquement

Permissions

Cette valeur peut être soit une valeur hexagonale représentant une ou plusieurs autorisations Windows, soit un alias **smbcacls**:

- Valeur hexagonale représentant une ou plusieurs autorisations Windows.
  Le tableau suivant présente les autorisations avancées de Windows et leur valeur correspondante au format hexadécimal :

  Tableau 1.3. Permissions Windows et leur valeur smbcacls correspondante au format hexagonal

Autorisations Windows	Valeurs hexagonales
Contrôle total	**0x001F01FF**
Traverser un dossier / exécuter un fichier	**0x00100020**
Liste des dossiers / lecture des données	**0x00100001**
Lire les attributs	**0x00100080**
Lire les attributs étendus	**0x00100008**
Créer des fichiers / écrire des données	**0x00100002**
Créer des dossiers / ajouter des données	**0x00100004**
Écrire les attributs	**0x00100100**
Écrire des attributs étendus	**0x00100010**
Supprimer des sous-dossiers et des fichiers	**0x00100040**
Supprimer	**0x00110000**

Autorisations Windows	Valeurs hexagonales
Permissions de lecture	**0x00120000**
Modifier les autorisations	**0x00140000**
S'approprier le projet	**0x00180000**

Plusieurs autorisations peuvent être combinées en une seule valeur hexagonale à l'aide de l'opération bit à bit **OR**.

Pour plus de détails, voir le calcul du masque ACE.

- Un alias **smbcacls**. Le tableau suivant présente les alias disponibles :

Tableau 1.4. Les alias smbcacls existants et les autorisations Windows correspondantes

smbcacls alias	Cartes de l'autorisation Windows
R	Lire
READ	Lire & exécuter
W	Spécial : o Créer des fichiers / écrire des données o Créer des dossiers / ajouter des données o Écrire les attributs o Écrire des attributs étendus o Permissions de lecture
D	Supprimer
P	Modifier les autorisations
O	S'approprier le projet
X	Traverser / exécuter
CHANGE	Modifier
FULL	Contrôle total

NOTE

Vous pouvez combiner des alias à une lettre lorsque vous définissez des autorisations. Par exemple, vous pouvez définir **RD** pour appliquer l'autorisation Windows **Read** et **Delete**. Cependant, vous ne pouvez pas combiner plusieurs alias autres qu'à une lettre, ni combiner des alias et des valeurs hexadécimales.

1.10.2. Affichage des ACL à l'aide de smbcacls

Pour afficher les ACL sur un partage SMB, utilisez l'utilitaire **smbcacls**. Si vous exécutez **smbcacls** sans aucun paramètre d'opération, comme **--add**, l'utilitaire affiche les listes de contrôle d'accès d'un objet du système de fichiers.

Procédure

Par exemple, pour répertorier les listes de contrôle d'accès du répertoire racine du partage //**server**/**example**:

```
# 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
```

La sortie de la commande s'affiche :

- **REVISION**: La révision ACL interne de Windows NT du descripteur de sécurité
- **CONTROL**: Contrôle du descripteur de sécurité
- **OWNER**: Nom ou SID du propriétaire du descripteur de sécurité
- **GROUP**: Nom ou SID du groupe du descripteur de sécurité
- **ACL** entrées de contrôle d'accès. Pour plus de détails, voir Entrées de contrôle d'accès .

1.10.3. Calcul du masque ACE

Dans la plupart des cas, lorsque vous ajoutez ou mettez à jour un ACE, vous utilisez les alias **smbcacls** répertoriés dans Existing smbcacls aliases et les autorisations Windows correspondantes .

Toutefois, si vous souhaitez définir des autorisations Windows avancées telles qu'elles sont répertoriées dans les autorisations Windows et leur valeur smbcacls correspondante au format hexadécimal , vous devez utiliser l'opération bit-wise **OR** pour calculer la valeur correcte. Vous pouvez utiliser la commande shell suivante pour calculer la valeur :

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

Exemple 1.4. Calcul d'un masque ACE

Vous souhaitez définir les autorisations suivantes :

- Traverser le dossier / exécuter le fichier (0x00100020)
- Liste des dossiers / lecture des données (0x00100001)
- Lire les attributs (0x00100080)

Pour calculer la valeur hexadécimale des autorisations précédentes, entrez :

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

Utilisez la valeur renvoyée lorsque vous définissez ou mettez à jour un CAE.

1.10.4. Ajout, mise à jour et suppression d'une ACL à l'aide de smbcacls

En fonction du paramètre que vous transmettez à l'utilitaire **smbcacls**, vous pouvez ajouter, mettre à jour et supprimer les ACL d'un fichier ou d'un répertoire.

Ajout d'une ACL
Pour ajouter une ACL à la racine du partage **//server/example** qui accorde des permissions à **CHANGE** pour **This folder, subfolders, and files** au groupe **AD\Domain Users**:

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

Mise à jour d'une ACL
La mise à jour d'une ACL est similaire à l'ajout d'une nouvelle ACL. Vous mettez à jour une liste de contrôle d'accès en remplaçant la liste de contrôle d'accès à l'aide du paramètre **--modify** par un principal de sécurité existant. Si **smbcacls** trouve le principal de sécurité dans la liste ACL, l'utilitaire met à jour les autorisations. Dans le cas contraire, la commande échoue avec une erreur :

```
ACL pour SID principal_name introuvable
```

Par exemple, pour mettre à jour les autorisations du groupe **AD\Domain Users** et les définir à **READ** pour **This folder, subfolders, and files**:

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

Suppression d'une ACL
Pour supprimer une ACL, passez le paramètre **--delete** avec l'ACL exacte à l'utilitaire **smbcacls**. Par exemple :

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

1.11. PERMETTRE AUX UTILISATEURS DE PARTAGER DES RÉPERTOIRES SUR UN SERVEUR SAMBA

Sur un serveur Samba, vous pouvez configurer les utilisateurs pour qu'ils puissent partager des répertoires sans avoir les droits d'accès à la racine.

1.11.1. Activation de la fonction de partage des utilisateurs

Avant que les utilisateurs puissent partager des répertoires, l'administrateur doit activer les partages d'utilisateurs dans Samba.

Par exemple, pour permettre aux seuls membres du groupe local **example** de créer des partages d'utilisateurs.

Procédure

1. Créer le groupe local **example**, s'il n'existe pas :

```
# groupadd example
```

2. Préparez le répertoire dans lequel Samba stockera les définitions de partage des utilisateurs et définissez correctement ses permissions. Par exemple :

   a. Create the directory:

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

   b. Définir les droits d'écriture pour le groupe **example**:

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

   c. Activez le bit collant pour empêcher les utilisateurs de renommer ou de supprimer des fichiers stockés par d'autres utilisateurs dans ce répertoire.

3. Modifiez le fichier **/etc/samba/smb.conf** et ajoutez ce qui suit à la section **[global]**:

   a. Définissez le chemin d'accès au répertoire que vous avez configuré pour stocker les définitions des partages d'utilisateurs. Par exemple :

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

   b. Définir le nombre de partages d'utilisateurs que Samba autorise à créer sur ce serveur. Par exemple :

```
usershare max shares = 100
```

   Si vous utilisez la valeur par défaut de **0** pour le paramètre **usershare max shares**, les partages d'utilisateurs sont désactivés.

   c. En option, définissez une liste de chemins d'accès absolus aux répertoires. Par exemple, pour configurer que Samba n'autorise que le partage des sous-répertoires des répertoires **/data** et **/srv** à partager, définissez :

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

   Pour une liste d'autres paramètres liés au partage d'utilisateurs que vous pouvez définir, voir la section **USERSHARES** dans la page de manuel **smb.conf(5)**.

4. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

5. Recharger la configuration de Samba :

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

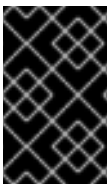
Les utilisateurs peuvent désormais créer des partages d'utilisateurs.

1.11.2. Ajout d'un partage d'utilisateur

Après avoir activé la fonction de partage par l'utilisateur dans Samba, les utilisateurs peuvent partager des répertoires sur le serveur Samba sans les autorisations **root** en exécutant la commande **net usershare add**.

Synopsis de la commande **net usershare add**:

net usershare add nom_partage chemin [[commentaire] | [ACLs]] [guest_ok=y|n]



IMPORTANT

Si vous définissez des ACL lors de la création d'un partage d'utilisateurs, vous devez spécifier le paramètre commentaire avant les ACL. Pour définir un commentaire vide, utilisez une chaîne vide entre guillemets.

Notez que les utilisateurs ne peuvent activer l'accès invité sur un partage d'utilisateur que si l'administrateur a défini **usershare allow guests = yes** dans la section **[global]** du fichier **/etc/samba/smb.conf**.

Exemple 1.5. Ajout d'un partage d'utilisateur

Un utilisateur souhaite partager le répertoire **/srv/samba/** sur un serveur Samba. Le partage doit être nommé **example**, n'avoir aucun commentaire et être accessible aux utilisateurs invités. En outre, les autorisations de partage doivent être définies comme un accès complet pour le groupe **AD\Domain Users** et des autorisations de lecture pour les autres utilisateurs. Pour ajouter ce partage, exécutez le programme en tant qu'utilisateur :

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

1.11.3. Mise à jour des paramètres d'un partage d'utilisateurs

Pour mettre à jour les paramètres d'un partage utilisateur, remplacez le partage en utilisant la commande **net usershare add** avec le même nom de partage et les nouveaux paramètres.

Voir Ajout d'un partage d'utilisateur.

1.11.4. Affichage d'informations sur les partages d'utilisateurs existants

Les utilisateurs peuvent entrer la commande **net usershare info** sur un serveur Samba pour afficher les partages des utilisateurs et leurs paramètres.

Conditions préalables

- Un partage d'utilisateurs est configuré sur le serveur Samba.

Procédure

1. Pour afficher tous les partages créés par un utilisateur :

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

   Pour ne répertorier que les partages créés par l'utilisateur qui exécute la commande, omettez le paramètre **-l**.

2. Pour n'afficher que les informations relatives à des partages spécifiques, indiquez le nom du partage ou des caractères génériques à la commande. Par exemple, pour afficher les informations sur les partages dont le nom commence par **share_**:

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

1.11.5. Liste des actions des utilisateurs

Si vous souhaitez répertorier uniquement les partages d'utilisateurs disponibles sans leurs paramètres sur un serveur Samba, utilisez la commande **net usershare list**.

Conditions préalables

- Un partage d'utilisateurs est configuré sur le serveur Samba.

Procédure

1. Pour dresser la liste des partages créés par un utilisateur :

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

   Pour ne répertorier que les partages créés par l'utilisateur qui exécute la commande, omettez le paramètre **-l**.

2. Pour ne répertorier que des partages spécifiques, indiquez le nom du partage ou des caractères génériques à la commande. Par exemple, pour répertorier uniquement les partages dont le nom commence par **share_**:

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

1.11.6. Suppression d'un partage d'utilisateur

Pour supprimer un partage utilisateur, utilisez la commande **net usershare delete** en tant qu'utilisateur ayant créé le partage ou en tant qu'utilisateur **root**.

Conditions préalables

- Un partage d'utilisateurs est configuré sur le serveur Samba.

Procédure

```
$ net usershare delete share_name
```

1.12. CONFIGURATION D'UN PARTAGE POUR AUTORISER L'ACCÈS SANS AUTHENTIFICATION

Dans certaines situations, vous souhaitez partager un répertoire auquel les utilisateurs peuvent se connecter sans authentification. Pour configurer cela, activez l'accès invité sur un partage.

AVERTISSEMENT

Les partages qui ne nécessitent pas d'authentification peuvent présenter un risque pour la sécurité.

1.12.1. Autoriser l'accès des invités à un partage

Si l'accès invité est activé sur un partage, Samba fait correspondre les connexions invitées au compte du système d'exploitation défini dans le paramètre **guest account**. Les utilisateurs invités peuvent accéder aux fichiers de ce partage si au moins l'une des conditions suivantes est remplie :

- Le compte est répertorié dans les listes de contrôle d'accès au système de fichiers
- Les permissions POSIX pour les utilisateurs de **other** l'autorisent

Exemple 1.6. Autorisations de partage pour les invités

Si vous avez configuré Samba pour que le compte invité soit mappé sur **nobody**, ce qui est le cas par défaut, les ACL de l'exemple suivant :

- Autoriser les utilisateurs invités à lire **file1.txt**
- Autoriser les utilisateurs invités à lire et à modifier **file2.txt**
- Empêcher les utilisateurs invités de lire ou de modifier **file3.txt**

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

Procédure

1. Modifiez le fichier **/etc/samba/smb.conf**:
   a. S'il s'agit du premier partage d'invités que vous configurez sur ce serveur :
      i. Définir **map to guest = Bad User** dans la section **[global]**:

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

      Avec ce paramètre, Samba rejette les tentatives de connexion qui utilisent un mot de passe incorrect, sauf si le nom d'utilisateur n'existe pas. Si le nom d'utilisateur spécifié n'existe pas et que l'accès invité est activé sur un partage, Samba traite la connexion comme une connexion invité.

      ii. Par défaut, Samba associe le compte invité au compte **nobody** sur Red Hat Enterprise Linux. Vous pouvez également définir un compte différent. Par exemple :

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

      Le compte défini dans ce paramètre doit exister localement sur le serveur Samba. Pour des raisons de sécurité, Red Hat recommande d'utiliser un compte auquel aucun shell valide n'a été attribué.

   b. Ajoutez le paramètre **guest ok = yes** à la section de partage **[example]**:

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

2. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

3. Recharger la configuration de Samba :

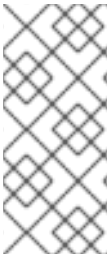
```
# smbcontrol all reload-config
```

1.13. CONFIGURATION DE SAMBA POUR LES CLIENTS MACOS

Le module Samba du système de fichiers virtuels (VFS) **fruit** offre une meilleure compatibilité avec les clients SMB (Server Message Block) d'Apple.

1.13.1. Optimiser la configuration de Samba pour fournir des partages de fichiers aux clients macOS

Cette section décrit comment configurer le module **fruit** pour tous les partages Samba hébergés sur le serveur afin d'optimiser les partages de fichiers Samba pour les clients macOS.



NOTE

Red Hat recommande d'activer le module **fruit** globalement. Les clients utilisant macOS négocient les extensions du protocole Apple (AAPL) server server message block version 2 (SMB2) lorsque le client établit la première connexion au serveur. Si le client se connecte d'abord à un partage sans que les extensions AAPL soient activées, le client n'utilise pas les extensions pour aucun partage du serveur.

Conditions préalables

- Samba est configuré comme serveur de fichiers.

Procédure

1. Modifiez le fichier **/etc/samba/smb.conf** et activez les modules VFS **fruit** et **streams_xattr** dans la section **[global]**:

```
objets vfs = fruits streams_xattr
```

IMPORTANT

Vous devez activer le module **fruit** avant d'activer **streams_xattr**. Le module **fruit** utilise des flux de données alternatifs (ADS). Pour cette raison, vous devez également activer le module **streams_xattr**.

2. En option, pour assurer la prise en charge de macOS Time Machine sur un partage, ajoutez le paramètre suivant à la configuration du partage dans le fichier **/etc/samba/smb.conf**:

```
fruit:machine à remonter le temps = oui
```

3. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

4. Recharger la configuration de Samba :

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

Ressources supplémentaires

- **vfs_fruit(8)** page de manuel.
- Configuration des partages de fichiers :
  - Configuration d'un partage de fichiers Samba utilisant des listes de contrôle POSIX
  - Configuration d'un partage utilisant les ACL de Windows .

1.14. UTILISATION DE L'UTILITAIRE SMBCLIENT POUR ACCÉDER À UN PARTAGE SMB

L'utilitaire smbclient vous permet d'accéder aux partages de fichiers sur un serveur SMB, de la même manière qu'un client FTP en ligne de commande. Vous pouvez l'utiliser, par exemple, pour télécharger des fichiers vers et depuis un partage.

Conditions préalables

- Le paquet **samba-client** est installé.

1.14.1. Fonctionnement du mode interactif de smbclient

Par exemple, pour s'authentifier sur le partage **example** hébergé sur **server** en utilisant le compte ***DOMAIN\user*** compte :

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

Une fois que **smbclient** s'est connecté avec succès au partage, l'utilitaire entre en mode interactif et affiche l'invite suivante :

```
smb : \N>
```

Pour afficher toutes les commandes disponibles dans l'interpréteur de commandes interactif, entrez :

```
smb : \N> help
```

Pour afficher l'aide d'une commande spécifique, entrez :

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

Ressources supplémentaires

- **smbclient(1)** page de manuel

1.14.2. Utilisation de smbclient en mode interactif

Si vous utilisez **smbclient** sans le paramètre **-c**, l'utilitaire passe en mode interactif. La procédure suivante montre comment se connecter à un partage SMB et télécharger un fichier à partir d'un sous-répertoire.

Procédure

1. Se connecter au partage :

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

2. Allez dans le répertoire **/example/**:

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

3. Liste les fichiers du répertoire :

```
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. Téléchargez le fichier **example.txt**:

```
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. Se déconnecter du partage :

```
smb : \NExemple : \N> exit
```

1.14.3. Utilisation de smbclient en mode script

Si vous passez le paramètre **-c** à **smbclient**, vous pouvez exécuter automatiquement les commandes sur le partage SMB distant. Cela vous permet d'utiliser **smbclient** dans des scripts.

La procédure suivante montre comment se connecter à un partage SMB et télécharger un fichier à partir d'un sous-répertoire.

Procédure

- Utilisez la commande suivante pour vous connecter au partage, accéder au répertoire **example** et télécharger le fichier **example.txt**:

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

1.15. CONFIGURER SAMBA EN TANT QUE SERVEUR D'IMPRESSION

Si vous configurez Samba en tant que serveur d'impression, les clients de votre réseau peuvent utiliser Samba pour imprimer. En outre, les clients Windows peuvent, s'ils sont configurés, télécharger le pilote à partir du serveur Samba.

Certaines parties de cette section ont été adoptées à partir de la documentation Setting up Samba as a Print Server publiée dans le Samba Wiki. Licence : CC BY 4.0. Auteurs et contributeurs : Voir l'onglet historique de la page Wiki.

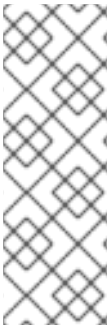
Conditions préalables

Samba a été configuré dans l'un des modes suivants :

- Serveur autonome
- Membre du domaine

1.15.1. Activation de la prise en charge du serveur d'impression dans Samba

Par défaut, la prise en charge des serveurs d'impression n'est pas activée dans Samba. Pour utiliser Samba comme serveur d'impression, vous devez configurer Samba en conséquence.



NOTE

Les travaux d'impression et les opérations d'impression nécessitent des appels de procédure à distance (RPC). Par défaut, Samba démarre le service **rpcd_spoolss** à la demande pour gérer les RPC. Lors du premier appel RPC, ou lorsque vous mettez à jour la liste des imprimantes dans CUPS, Samba récupère les informations relatives à l'imprimante auprès de CUPS. Cette opération peut prendre environ 1 seconde par imprimante. Par conséquent, si vous avez plus de 50 imprimantes, réglez les paramètres de **rpcd_spoolss**.

Conditions préalables

- Les imprimantes sont configurées dans un serveur CUPS.
  Pour plus de détails sur la configuration des imprimantes dans CUPS, voir la documentation fournie dans la console web CUPS (https://*printserver*:631/help) sur le serveur d'impression.

Procédure

1. Modifiez le fichier **/etc/samba/smb.conf**:

   a. Ajoutez la section **[printers]** pour activer le backend d'impression dans Samba :

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

   IMPORTANT

   Le nom du partage **[printers]** est codé en dur et ne peut pas être modifié.

   b. Si le serveur CUPS fonctionne sur un hôte ou un port différent, spécifiez le paramètre dans la section **[printers]**:

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

   c. Si vous avez beaucoup d'imprimantes, fixez le nombre de secondes d'inactivité à une valeur supérieure au nombre d'imprimantes connectées à CUPS. Par exemple, si vous avez 100 imprimantes, définissez dans la section **[global]**:

   ```
   rpcd_spoolss:idle_seconds = 200
   ```

   Si ce paramètre n'est pas adapté à votre environnement, augmentez également le nombre de travailleurs **rpcd_spoolss** dans la section **[global]**:

   ```
   rpcd_spoolss:num_workers = 10
   ```

   Par défaut, **rpcd_spoolss** démarre 5 travailleurs.

2. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

3. Ouvrez les ports requis et rechargez la configuration du pare-feu à l'aide de l'utilitaire **firewall-cmd**:

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

4. Redémarrez le service **smb**:

```
# systemctl restart smb
```

Après le redémarrage du service, Samba partage automatiquement toutes les imprimantes configurées dans le back-end CUPS. Si vous souhaitez partager manuellement des imprimantes spécifiques, reportez-vous à la section Partage manuel d'imprimantes spécifiques .

Vérification

- Soumettre un travail d'impression. Par exemple, pour imprimer un fichier PDF, entrez :

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

1.15.2. Partage manuel d'imprimantes spécifiques

Si vous avez configuré Samba en tant que serveur d'impression, Samba partage par défaut toutes les imprimantes configurées dans le back-end CUPS. La procédure suivante explique comment partager uniquement des imprimantes spécifiques.

Conditions préalables

- Samba est configuré comme serveur d'impression

Procédure

1. Modifiez le fichier **/etc/samba/smb.conf**:
   a. Dans la section **[global]**, désactivez le partage automatique de l'imprimante en définissant :

```
charger les imprimantes = non
```

   b. Ajoutez une section pour chaque imprimante que vous souhaitez partager. Par exemple, pour partager l'imprimante nommée **example** dans le back-end CUPS en tant que **Example-Printer** dans Samba, ajoutez la section suivante :

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

Vous n'avez pas besoin de répertoires spool individuels pour chaque imprimante. Dans le paramètre **path**, vous pouvez définir pour l'imprimante le même répertoire spool que celui que vous avez défini dans la section **[printers]**.

2. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

3. Recharger la configuration de Samba :

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

1.16. CONFIGURATION DU TÉLÉCHARGEMENT AUTOMATIQUE DES PILOTES D'IMPRIMANTE POUR LES CLIENTS WINDOWS SUR LES SERVEURS D'IMPRESSION SAMBA

Si vous utilisez un serveur d'impression Samba pour des clients Windows, vous pouvez télécharger des pilotes et préconfigurer des imprimantes. Lorsqu'un utilisateur se connecte à une imprimante, Windows télécharge et installe automatiquement le pilote localement sur le client. L'utilisateur n'a pas besoin d'autorisations d'administrateur local pour l'installation. En outre, Windows applique les paramètres préconfigurés du pilote, tels que le nombre de bacs.

Certaines parties de cette section ont été adoptées à partir de la documentation " Setting up Automatic Printer Driver Downloads for Windows Clients " publiée dans le Samba Wiki. Licence d'utilisation : CC BY 4.0. Auteurs et contributeurs : Voir l'onglet historique de la page Wiki.

Conditions préalables

- Samba est configuré comme serveur d'impression

1.16.1. Informations de base sur les pilotes d'imprimante

Cette section fournit des informations générales sur les pilotes d'imprimante.

Version du modèle de pilote pris en charge
Samba ne prend en charge que le modèle de pilote d'imprimante version 3, qui est pris en charge par Windows 2000 et les versions ultérieures, ainsi que par Windows Server 2000 et les versions ultérieures. Samba ne prend pas en charge le modèle de pilote version 4, introduit dans Windows 8 et Windows Server 2012. Toutefois, ces versions de Windows et les versions ultérieures prennent également en charge les pilotes de la version 3.

Pilotes attentifs aux paquets
Samba ne prend pas en charge les pilotes compatibles avec les paquets.

Préparation d'un pilote d'imprimante pour le téléchargement
Avant de pouvoir télécharger un pilote vers un serveur d'impression Samba :

- Décompressez le pilote s'il est fourni dans un format compressé.
- Certains pilotes nécessitent le lancement d'une application d'installation qui installe le pilote localement sur un hôte Windows. Dans certains cas, le programme d'installation extrait les fichiers individuels dans le dossier temporaire du système d'exploitation pendant l'exécution de l'installation. Pour utiliser les fichiers du pilote pour le téléchargement :

a. Lancez le programme d'installation.

b. Copiez les fichiers du dossier temporaire vers un nouvel emplacement.

c. Annuler l'installation.

Demandez au fabricant de votre imprimante s'il existe des pilotes qui prennent en charge le téléchargement vers un serveur d'impression.

Fournir à un client des pilotes 32 bits et 64 bits pour une imprimante
Pour fournir le pilote d'une imprimante aux clients Windows 32 bits et 64 bits, vous devez télécharger un pilote portant exactement le même nom pour les deux architectures. Par exemple, si vous téléchargez le pilote 32 bits nommé **Example PostScript** et le pilote 64 bits nommé **Example PostScript (v1.0)**, les noms ne correspondent pas. Par conséquent, vous ne pouvez affecter qu'un seul des pilotes à une imprimante et le pilote ne sera pas disponible pour les deux architectures.

1.16.2. Permettre aux utilisateurs de télécharger et de préconfigurer les pilotes

Pour pouvoir télécharger et préconfigurer les pilotes d'imprimante, un utilisateur ou un groupe doit disposer du privilège **SePrintOperatorPrivilege**. Un utilisateur doit être ajouté au groupe **printadmin**. Red Hat Enterprise Linux crée automatiquement ce groupe lorsque vous installez le paquetage **samba**. Le groupe **printadmin** se voit attribuer le GID dynamique du système le plus bas disponible et inférieur à 1000.

Procédure

1. Par exemple, pour accorder le privilège **SePrintOperatorPrivilege** au groupe **printadmin**:

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

NOTE

Dans un environnement de domaine, accordez **SePrintOperatorPrivilege** à un groupe de domaine. Cela vous permet de gérer le privilège de manière centralisée en mettant à jour l'appartenance d'un utilisateur à un groupe.

2. Pour dresser la liste de tous les utilisateurs et groupes auxquels **SePrintOperatorPrivilege** a été accordé :

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

1.16.3. Mise en place du partage de print$

Les systèmes d'exploitation Windows téléchargent les pilotes d'imprimante à partir d'un partage nommé **print$** sur un serveur d'impression. Ce nom de partage est codé en dur dans Windows et ne peut pas être modifié.

La procédure suivante explique comment partager le répertoire **/var/lib/samba/drivers/** en tant que **print$**, et permettre aux membres du groupe local **printadmin** de télécharger des pilotes d'imprimante.

Procédure

1. Ajouter la section **[print$]** au fichier **/etc/samba/smb.conf**:

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

   En utilisant ces paramètres :

   - Seuls les membres du groupe **printadmin** peuvent télécharger des pilotes d'imprimante sur le partage.
   - Le groupe de fichiers et de répertoires nouvellement créés sera défini sur **printadmin**.
   - Les permissions des nouveaux fichiers seront fixées à **664**.
   - Les permissions des nouveaux répertoires seront fixées à **2775**.

2. Pour télécharger uniquement des pilotes 64 bits pour toutes les imprimantes, incluez ce paramètre dans la section **[global]** du fichier **/etc/samba/smb.conf**:

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

   Sans ce paramètre, Windows n'affiche que les pilotes pour lesquels vous avez téléchargé au moins la version 32 bits.

3. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

4. Recharger la configuration de Samba

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

5. Créer le groupe **printadmin** s'il n'existe pas :

```
# groupadd printadmin
```

6. Accorder le privilège **SePrintOperatorPrivilege** au groupe **printadmin**.

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

7. Si vous utilisez SELinux en mode **enforcing**, définissez le contexte **samba_share_t** pour le répertoire :

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

8. Définissez les droits d'accès au répertoire **/var/lib/samba/drivers/**:

- Si vous utilisez des ACL POSIX, définissez :

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

- Si vous utilisez les ACL de Windows, définissez :

Principal	Accès	Postuler
CREATOR OWNER	Contrôle total	Sous-dossiers et fichiers uniquement
Authenticated Users	Lire & exécuter, Lister le contenu du dossier, Lire	Ce dossier, ces sous-dossiers et ces fichiers
printadmin	Contrôle total	Ce dossier, ces sous-dossiers et ces fichiers

Pour plus de détails sur la définition des ACL sous Windows, voir la documentation Windows.

Ressources supplémentaires

- Permettre aux utilisateurs de télécharger et de préconfigurer des pilotes .

1.16.4. Création d'une GPO pour permettre aux clients de faire confiance au serveur d'impression Samba

Pour des raisons de sécurité, les systèmes d'exploitation Windows récents empêchent les clients de télécharger des pilotes d'imprimante non compatibles avec les paquets à partir d'un serveur non fiable. Si votre serveur d'impression est membre d'un AD, vous pouvez créer un objet de stratégie de groupe (GPO) dans votre domaine pour faire confiance au serveur Samba.

Conditions préalables

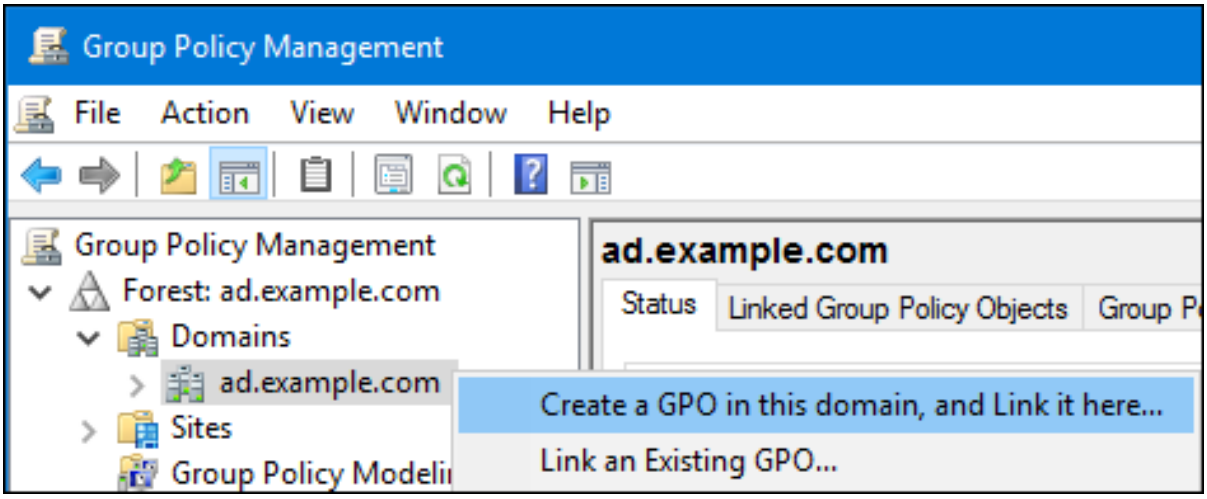
- Le serveur d'impression Samba est membre d'un domaine AD.
- L'ordinateur Windows que vous utilisez pour créer le GPO doit être équipé des outils d'administration à distance du serveur (RSAT). Pour plus de détails, voir la documentation Windows.

Procédure

1. Connectez-vous à un ordinateur Windows à l'aide d'un compte autorisé à modifier les stratégies de groupe, tel que l'utilisateur du domaine AD **Administrator**.

2. Ouvrez le site **Group Policy Management Console**.

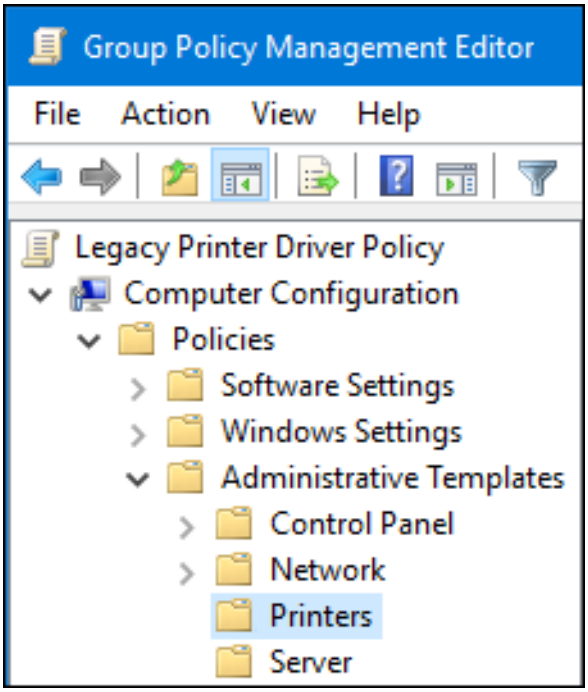
3. Cliquez avec le bouton droit de la souris sur votre domaine AD et sélectionnez **Create a GPO in this domain, and Link it here**.



4. Entrez un nom pour le GPO, par exemple **Legacy Printer Driver Policy** et cliquez sur **OK**. La nouvelle GPO sera affichée sous l'entrée du domaine.

5. Cliquez avec le bouton droit de la souris sur la GPO nouvellement créée et sélectionnez **Edit** pour ouvrir la fenêtre **Group Policy Management Editor**.

6. Naviguer vers **Configuration de l'ordinateur → Politiques → Modèles administratifs → Imprimantes**.

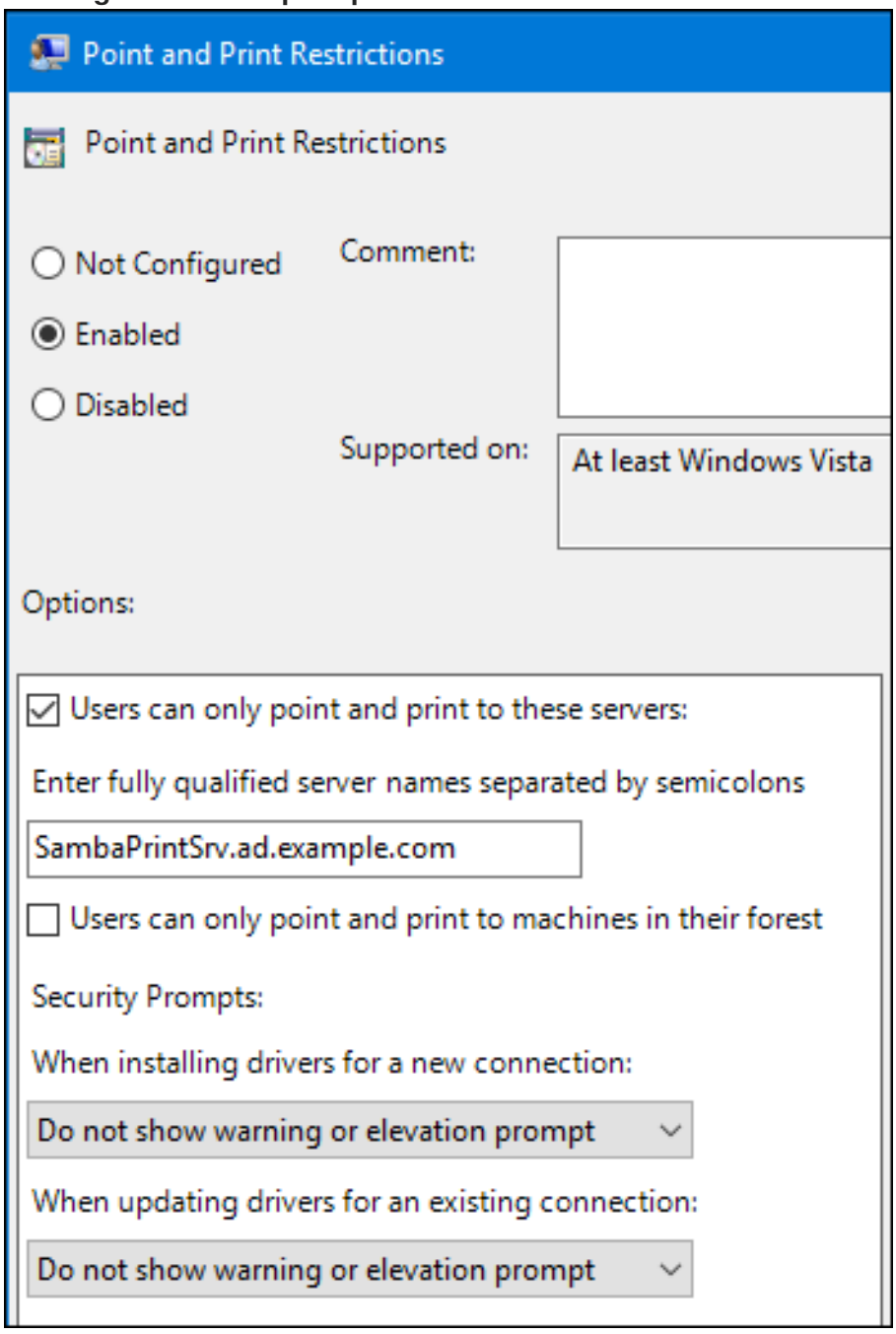


7. Dans la partie droite de la fenêtre, double-cliquez sur **Point and Print Restriction** pour modifier la politique :

   a. Activez la politique et définissez les options suivantes :

      i. Sélectionnez **Users can only point and print to these servers** et entrez le nom de domaine complet (FQDN) du serveur d'impression Samba dans le champ situé à côté de cette option.

ii. Dans les deux cases à cocher sous **Security Prompts**, sélectionnez **Do not show warning or elevation prompt**.

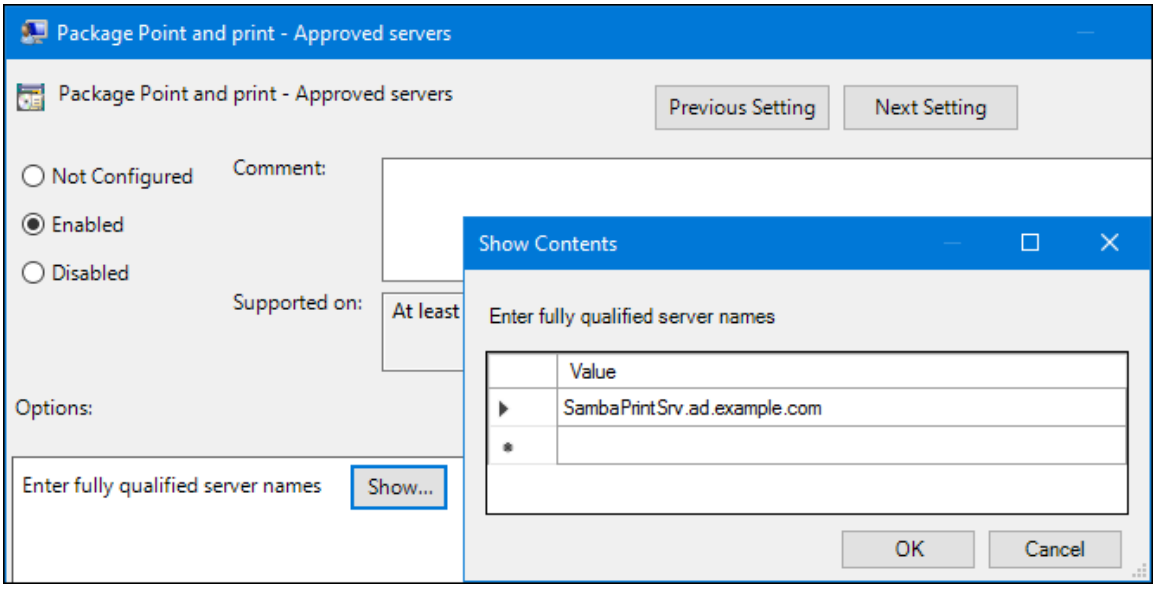


b. Click OK.

8. Double-cliquez sur **Package Point and Print - Approved servers** pour modifier la politique :

   a. Activez la politique et cliquez sur le bouton **Show**.

   b. Entrez le FQDN du serveur d'impression Samba.



c. Fermez la fenêtre **Show Contents** et la fenêtre des propriétés de la politique en cliquant sur **OK**.

9. Fermer le site **Group Policy Management Editor**.
10. Fermer le site **Group Policy Management Console**.

Après l'application de la stratégie de groupe par les membres du domaine Windows, les pilotes d'imprimante sont automatiquement téléchargés à partir du serveur Samba lorsqu'un utilisateur se connecte à une imprimante.

Ressources supplémentaires

- Pour l'utilisation des stratégies de groupe, voir la documentation Windows.

1.16.5. Téléchargement des pilotes et préconfiguration des imprimantes

Utilisez l'application **Print Management** sur un client Windows pour télécharger les pilotes et préconfigurer les imprimantes hébergées sur le serveur d'impression Samba. Pour plus de détails, voir la documentation Windows.

1.17. EXÉCUTER SAMBA SUR UN SERVEUR AVEC LE MODE FIPS ACTIVÉ

Cette section fournit une vue d'ensemble des limitations de l'exécution de Samba avec le mode FIPS activé. Elle fournit également la procédure d'activation du mode FIPS sur un hôte Red Hat Enterprise Linux exécutant Samba.

1.17.1. Limites de l'utilisation de Samba en mode FIPS

Les modes et fonctionnalités suivants de Samba fonctionnent en mode FIPS dans les conditions indiquées :

- Samba en tant que membre de domaine uniquement dans les environnements Active Directory (AD) ou Red Hat Identity Management (IdM) avec l'authentification Kerberos qui utilise des algorithmes de chiffrement AES.

- Samba en tant que serveur de fichiers sur un membre du domaine Active Directory. Cependant, cela nécessite que les clients utilisent Kerberos pour s'authentifier auprès du serveur.

En raison de la sécurité accrue de FIPS, les fonctions et modes suivants de Samba ne fonctionnent pas si le mode FIPS est activé :

- Authentification NT LAN Manager (NTLM) car les algorithmes de chiffrement RC4 sont bloqués
- Le protocole SMB1 (server message block version 1)
- Le mode serveur de fichiers autonome parce qu'il utilise l'authentification NTLM
- Contrôleurs de domaine de type NT4
- Les membres du domaine de type NT4. Notez que Red Hat continue à prendre en charge la fonctionnalité du contrôleur de domaine primaire (PDC) que l'IdM utilise en arrière-plan.
- Changement de mot de passe sur le serveur Samba. Les modifications de mot de passe ne peuvent être effectuées qu'à l'aide de Kerberos sur un contrôleur de domaine Active Directory.

La fonctionnalité suivante n'est pas testée en mode FIPS et n'est donc pas prise en charge par Red Hat :

- Exécuter Samba en tant que serveur d'impression

1.17.2. Utilisation de Samba en mode FIPS

Cette section explique comment activer le mode FIPS sur un hôte RHEL qui exécute Samba.

Conditions préalables

- Samba est configuré sur l'hôte Red Hat Enterprise Linux.
- Samba fonctionne dans un mode qui est pris en charge par le mode FIPS.

Procédure

1. Activer le mode FIPS sur RHEL :

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

2. Redémarrer le serveur :

```
# reboot
```

3. Utilisez l'utilitaire **testparm** pour vérifier la configuration :

```
# testparm -s
```

   Si la commande affiche des erreurs ou des incompatibilités, corrigez-les pour que Samba fonctionne correctement.

Ressources supplémentaires

- Section 1.17.1, « Limites de l'utilisation de Samba en mode FIPS »

1.18. OPTIMISER LES PERFORMANCES D'UN SERVEUR SAMBA

Découvrez quels paramètres peuvent améliorer les performances de Samba dans certaines situations, et quels paramètres peuvent avoir un impact négatif sur les performances.

Certaines parties de cette section ont été adoptées à partir de la documentation Performance Tuning publiée dans le Samba Wiki. Licence : CC BY 4.0. Auteurs et contributeurs : Voir l'onglet historique de la page Wiki.

Conditions préalables

- Samba est configuré comme un serveur de fichiers ou d'impression

1.18.1. Réglage de la version du protocole SMB

Chaque nouvelle version de SMB ajoute des fonctionnalités et améliore les performances du protocole. Les systèmes d'exploitation récents Windows et Windows Server prennent toujours en charge la dernière version du protocole. Si Samba utilise également la dernière version du protocole, les clients Windows qui se connectent à Samba bénéficient des améliorations de performance. Dans Samba, la valeur par défaut du protocole max du serveur est définie sur la dernière version stable du protocole SMB prise en charge.

NOTE

Pour que la dernière version stable du protocole SMB soit toujours activée, ne définissez pas le paramètre **server max protocol**. Si vous définissez ce paramètre manuellement, vous devrez le modifier à chaque nouvelle version du protocole SMB pour que la dernière version du protocole soit activée.

La procédure suivante explique comment utiliser la valeur par défaut du paramètre **server max protocol**.

Procédure

1. Supprimer le paramètre **server max protocol** de la section **[global]** du fichier **/etc/samba/smb.conf**.
2. Recharger la configuration de Samba

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

1.18.2. Optimisation des partages avec des répertoires contenant un grand nombre de fichiers

Linux prend en charge les noms de fichiers sensibles à la casse. C'est pourquoi Samba doit rechercher les noms de fichiers en majuscules et en minuscules dans les répertoires lors de la recherche ou de l'accès à un fichier. Vous pouvez configurer un partage pour qu'il crée de nouveaux fichiers uniquement en minuscules ou en majuscules, ce qui améliore les performances.

Conditions préalables

- Samba est configuré comme serveur de fichiers

Procédure

Procédure

1. Renommer tous les fichiers du partage en minuscules.

NOTE

En utilisant les réglages de cette procédure, les fichiers dont les noms ne sont pas en minuscules ne seront plus affichés.

2. Définissez les paramètres suivants dans la section du partage :

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

Pour plus de détails sur les paramètres, voir leur description dans la page de manuel **smb.conf(5)**.

3. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

4. Recharger la configuration de Samba :

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

Après avoir appliqué ces paramètres, les noms de tous les fichiers nouvellement créés sur ce partage utilisent des minuscules. Grâce à ces paramètres, Samba n'a plus besoin de rechercher les majuscules et les minuscules dans le répertoire, ce qui améliore les performances.

1.18.3. Paramètres pouvant avoir un impact négatif sur les performances

Par défaut, le noyau de Red Hat Enterprise Linux est réglé pour des performances réseau élevées. Par exemple, le noyau utilise un mécanisme de réglage automatique pour la taille des tampons. La définition du paramètre **socket options** dans le fichier **/etc/samba/smb.conf** remplace ces paramètres du noyau. Par conséquent, la définition de ce paramètre diminue les performances du réseau Samba dans la plupart des cas.

Pour utiliser les paramètres optimisés du noyau, supprimez le paramètre **socket options** de la section **[global]** du site **/etc/samba/smb.conf**.

1.19. CONFIGURER SAMBA POUR QU'IL SOIT COMPATIBLE AVEC LES CLIENTS QUI REQUIÈRENT UNE VERSION DE SMB INFÉRIEURE À LA VERSION PAR DÉFAUT

Samba utilise une valeur par défaut raisonnable et sûre pour la version minimale de Server Message Block (SMB) qu'il prend en charge. Cependant, si vous avez des clients qui ont besoin d'une version SMB plus ancienne, vous pouvez configurer Samba pour qu'il la prenne en charge.

1.19.1. Définition de la version minimale du protocole SMB prise en charge par un serveur Samba

Dans Samba, le paramètre **server min protocol** du fichier **/etc/samba/smb.conf** définit la version minimale du protocole SMB (Server Message Block) prise en charge par le serveur Samba. Cette section explique comment modifier la version minimale du protocole SMB.

NOTE

Par défaut, Samba sur RHEL 8.2 et les versions ultérieures ne prend en charge que le protocole SMB2 et les versions plus récentes. Red Hat recommande de ne pas utiliser le protocole SMB1, qui est obsolète. Cependant, si votre environnement nécessite SMB1, vous pouvez définir manuellement le paramètre **server min protocol** sur **NT1** pour réactiver SMB1.

Conditions préalables

- Samba est installé et configuré.

Procédure

1. Modifiez le fichier **/etc/samba/smb.conf**, ajoutez le paramètre **server min protocol** et définissez le paramètre sur la version minimale du protocole SMB que le serveur doit prendre en charge. Par exemple, pour définir la version minimale du protocole SMB sur **SMB3**, ajoutez :

```
protocole min du serveur = SMB3
```

2. Redémarrez le service **smb**:

```
# systemctl restart smb
```

Ressources supplémentaires

- **smb.conf(5)** page de manuel

1.20. UTILITAIRES DE LIGNE DE COMMANDE SAMBA FRÉQUEMMENT UTILISÉS

Ce chapitre décrit les commandes fréquemment utilisées pour travailler avec un serveur Samba.

1.20.1. Utilisation des commandes net ads join et net rpc join

En utilisant la sous-commande **join** de l'utilitaire **net**, vous pouvez joindre Samba à un domaine AD ou NT4. Pour rejoindre le domaine, vous devez créer manuellement le fichier **/etc/samba/smb.conf** et éventuellement mettre à jour d'autres configurations, telles que PAM.

IMPORTANT

Red Hat recommande d'utiliser l'utilitaire **realm** pour rejoindre un domaine. L'utilitaire **realm** met automatiquement à jour tous les fichiers de configuration concernés.

Procédure

1. Créez manuellement le fichier **/etc/samba/smb.conf** avec les paramètres suivants :
   - Pour un membre du domaine AD :

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

- Pour un membre de domaine NT4 :

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

2. Ajoutez une configuration de mappage d'ID pour le domaine par défaut ***** et pour le domaine que vous voulez joindre à la section **[global**] dans le fichier **/etc/samba/smb.conf**.

3. Vérifiez le fichier **/etc/samba/smb.conf**:

```
# testparm
```

4. Rejoignez le domaine en tant qu'administrateur du domaine :

   - Pour rejoindre un domaine AD :

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

   - Pour rejoindre un domaine NT4 :

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

5. Ajoutez la source **winbind** à l'entrée de la base de données **passwd** et **group** dans le fichier **/etc/nsswitch.conf**:

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

6. Activez et démarrez le service **winbind**:

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

7. Vous pouvez également configurer PAM à l'aide de l'utilitaire **authselect**.
   Pour plus de détails, voir la page de manuel **authselect(8)**.

8. Optionnellement, pour les environnements AD, configurer le client Kerberos.
   Pour plus de détails, voir la documentation de votre client Kerberos.

Ressources supplémentaires

- Joindre Samba à un domaine .
- Comprendre et configurer le mappage des identifiants Samba .

1.20.2. Utilisation de la commande net rpc rights

Dans Windows, vous pouvez attribuer des privilèges à des comptes et à des groupes pour effectuer des opérations spéciales, telles que la définition d'ACL sur un partage ou le téléchargement de pilotes d'imprimante. Sur un serveur Samba, vous pouvez utiliser la commande **net rpc rights** pour gérer les privilèges.

Liste des privilèges que vous pouvez définir
Pour dresser la liste de tous les privilèges disponibles et de leurs détenteurs, utilisez la commande **net rpc rights list**. Par exemple, vous pouvez consulter la liste des privilèges disponibles et de leurs propriétaires à l'aide de la commande :

```
# 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
```

Octroi de privilèges
Pour accorder un privilège à un compte ou à un groupe, utilisez la commande **net rpc rights grant**.

Par exemple, accorder le privilège **SePrintOperatorPrivilege** au groupe ***DOMAIN*\printadmin** groupe :

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

Révocation des privilèges
Pour révoquer un privilège d'un compte ou d'un groupe, utilisez la commande **net rpc rights revoke**.

Par exemple, pour révoquer le privilège **SePrintOperatorPrivilege** du groupe ***DOMAIN*\printadmin** groupe :

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

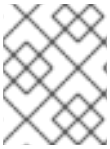
1.20.3. Utilisation de la commande net rpc share

La commande **net rpc share** permet de lister, d'ajouter et de supprimer des partages sur un serveur Samba ou Windows local ou distant.

Actions de cotation
Pour répertorier les parts d'un serveur SMB, utilisez la commande **net rpc share list**. Si vous le souhaitez, vous pouvez passer le paramètre **-S *server_name*** à la commande pour répertorier les parts d'un serveur distant. Par exemple, la commande

-

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



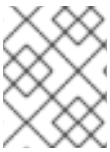
NOTE

Les partages hébergés sur un serveur Samba dont la section **browseable = no** est définie dans le fichier **/etc/samba/smb.conf** ne sont pas affichés dans la sortie.

Ajout d'une action
La commande **net rpc share add** permet d'ajouter un partage à un serveur SMB.

Par exemple, pour ajouter un partage nommé **example** sur un serveur Windows distant qui partage le répertoire **C:\example**:

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



NOTE

Vous devez omettre la barre oblique inverse dans le chemin d'accès lorsque vous spécifiez un nom de répertoire Windows.

Pour utiliser la commande afin d'ajouter un partage à un serveur Samba :

- L'utilisateur spécifié dans le paramètre **-U** doit disposer du privilège **SeDiskOperatorPrivilege** sur le serveur de destination.
- Vous devez écrire un script qui ajoute une section share au fichier **/etc/samba/smb.conf** et recharge Samba. Le script doit être défini dans le paramètre **add share command** de la section **[global]** de **/etc/samba/smb.conf**. Pour plus de détails, voir la description de **add share command** dans la page de manuel **smb.conf(5)**.

Suppression d'un partage
La commande **net rpc share delete** permet de supprimer un partage d'un serveur SMB.

Par exemple, pour supprimer le partage nommé exemple d'un serveur Windows distant :

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

Pour utiliser la commande afin de supprimer un partage d'un serveur Samba :

- L'utilisateur spécifié dans le paramètre **-U** doit bénéficier du privilège **SeDiskOperatorPrivilege**.
- Vous devez écrire un script qui supprime la section du partage du fichier **/etc/samba/smb.conf** et recharge Samba. Le script doit être défini dans le paramètre **delete share command** de la section **[global]** de **/etc/samba/smb.conf**. Pour plus de détails, voir la description de **delete share command** dans la page de manuel **smb.conf(5)**.

1.20.4. Utilisation de la commande net user

La commande **net user** vous permet d'effectuer les actions suivantes sur un AD DC ou un PDC NT4 :

- Liste de tous les comptes d'utilisateurs
- Ajouter des utilisateurs
- Supprimer des utilisateurs

NOTE

La spécification d'une méthode de connexion, telle que **ads** pour les domaines AD ou **rpc** pour les domaines NT4, n'est requise que lorsque vous répertoriez les comptes d'utilisateurs de domaine. D'autres sous-commandes liées à l'utilisateur peuvent détecter automatiquement la méthode de connexion.

Passez le paramètre **-U *user_name*** à la commande pour spécifier un utilisateur autorisé à effectuer l'action demandée.

Liste des comptes d'utilisateurs du domaine
Pour dresser la liste de tous les utilisateurs d'un domaine AD :

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

Pour dresser la liste de tous les utilisateurs d'un domaine NT4 :

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

Ajouter un compte d'utilisateur au domaine
Sur un membre du domaine Samba, vous pouvez utiliser la commande **net user add** pour ajouter un compte d'utilisateur au domaine.

Par exemple, ajoutez le compte **user** au domaine :

1. Ajouter le compte :

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

2. En option, utilisez l'appel de procédure à distance (RPC) pour activer le compte sur le DC AD ou le PDC NT4. Par exemple, vous pouvez utiliser le shell RPC pour activer le compte sur le DC AD ou le PDC NT4 :

```
# 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
```

Supprimer un compte d'utilisateur du domaine
Sur un membre du domaine Samba, vous pouvez utiliser la commande **net user delete** pour supprimer un compte d'utilisateur du domaine.

Par exemple, pour supprimer le compte **user** du domaine :

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

1.20.5. Utilisation de l'utilitaire rpcclient

L'utilitaire **rpcclient** vous permet d'exécuter manuellement des fonctions Microsoft Remote Procedure Call (MS-RPC) côté client sur un serveur SMB local ou distant. Cependant, la plupart des fonctions sont intégrées dans des utilitaires distincts fournis par Samba. N'utilisez **rpcclient** que pour tester les fonctions MS-RPC.

Conditions préalables

- Le paquet **samba-client** est installé.

Examples
Par exemple, vous pouvez utiliser l'utilitaire **rpcclient** pour :

- Gérer le sous-système de spool de l'imprimante (SPOOLSS).

  Exemple 1.7. Affectation d'un pilote à une imprimante

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

- Récupérer des informations sur un serveur SMB.

  Exemple 1.8. Liste de tous les partages de fichiers et imprimantes partagées

  ```
  # 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:
  ```

- Effectuer des actions à l'aide du protocole Security Account Manager Remote (SAMR).

  Exemple 1.9. Liste des utilisateurs d'un serveur SMB

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

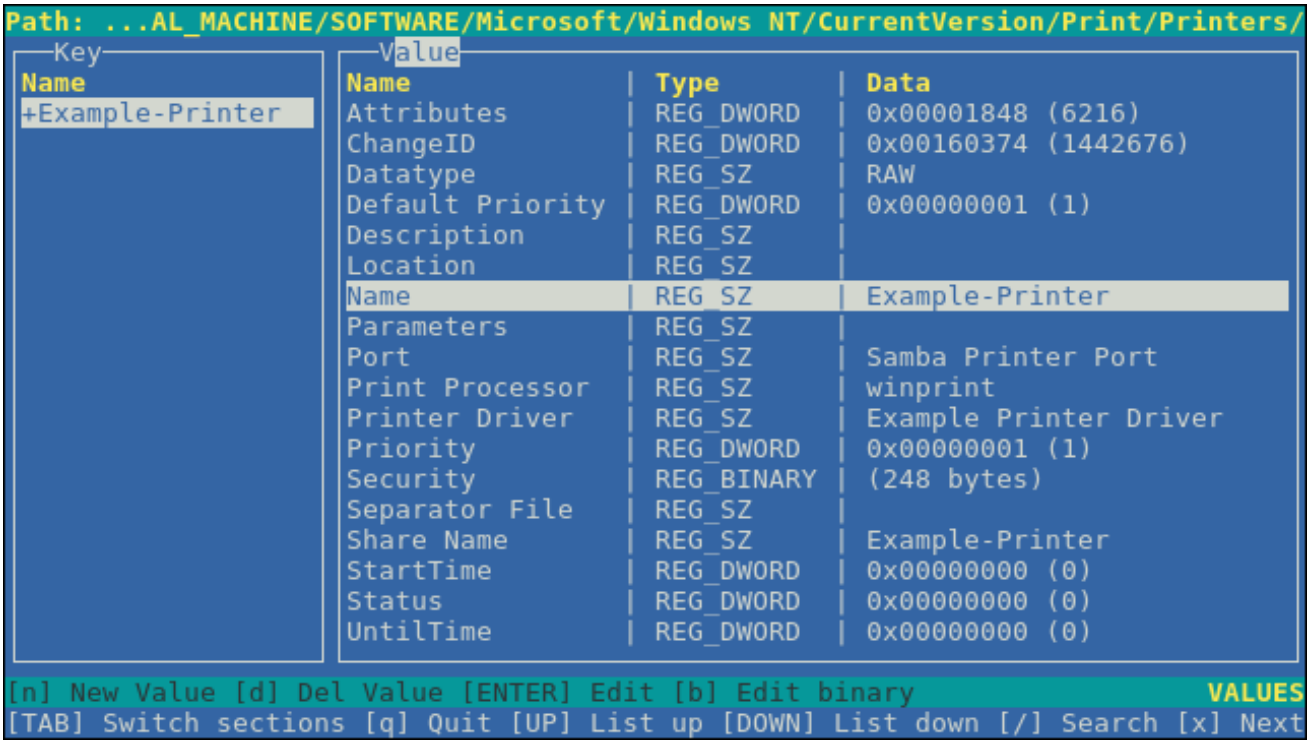
Si vous exécutez la commande sur un serveur autonome ou un membre de domaine, elle répertorie les utilisateurs de la base de données locale. L'exécution de la commande sur un AD DC ou un NT4 PDC permet d'obtenir la liste des utilisateurs du domaine.

Ressources supplémentaires

- **rpcclient(1)** page de manuel

1.20.6. Utilisation de l'application samba-regedit

Certains paramètres, tels que la configuration des imprimantes, sont stockés dans le registre du serveur Samba. Vous pouvez utiliser l'application **samba-regedit** basée sur ncurses pour modifier le registre d'un serveur Samba.



Conditions préalables

- Le paquet **samba-client** est installé.

Procédure

Pour lancer l'application, entrez :

```
# samba-regedit
```

Utilisez les touches suivantes :

- Curseur vers le haut et curseur vers le bas : Naviguer dans l'arborescence du registre et dans les valeurs.
- **Entrée**: Ouvre une touche ou modifie une valeur.
- **Tab**: Permet de passer du volet **Key** au volet **Value**.
- **Ctrl**+**C**: Ferme l'application.

1.20.7. Utilisation de l'utilitaire smbcontrol

L'utilitaire **smbcontrol** vous permet d'envoyer des messages de commande aux services **smbd**, **nmbd**, **winbindd** ou à l'ensemble de ces services. Ces messages de commande demandent au service, par exemple, de recharger sa configuration.

La procédure décrite dans cette section montre comment recharger la configuration des services **smbd**, **nmbd**, **winbindd** en envoyant le type de message **reload-config** à la destination **all**.

Conditions préalables

- Le paquet **samba-common-tools** est installé.

Procédure

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

Ressources supplémentaires

- **smbcontrol(1)** page de manuel

1.20.8. Utilisation de l'utilitaire smbpasswd

L'utilitaire **smbpasswd** gère les comptes d'utilisateurs et les mots de passe dans la base de données locale de Samba.

Conditions préalables

- Le paquet **samba-common-tools** est installé.

Procédure

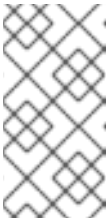
1. Si vous exécutez la commande en tant qu'utilisateur, **smbpasswd** modifie le mot de passe Samba de l'utilisateur qui a exécuté la commande. Par exemple, le mot de passe de l'utilisateur qui a exécuté la commande est modifié :

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

2. Si vous exécutez **smbpasswd** en tant qu'utilisateur de **root**, vous pouvez utiliser l'utilitaire, par exemple, pour :

   - Créer un nouvel utilisateur :

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



NOTE

Avant d'ajouter un utilisateur à la base de données Samba, vous devez créer le compte dans le système d'exploitation local. Voir la section Ajouter un nouvel utilisateur à partir de la ligne de commande dans le guide Configurer les paramètres de base du système.

- Activer un utilisateur Samba :

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

- Désactiver un utilisateur Samba :

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

- Supprimer un utilisateur :

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

Ressources supplémentaires

- **smbpasswd(8)** page de manuel

1.20.9. Utilisation de l'utilitaire smbstatus

L'utilitaire **smbstatus** fournit des informations sur

- Connexions par PID de chaque démon **smbd** au serveur Samba. Ce rapport comprend le nom de l'utilisateur, le groupe principal, la version du protocole SMB, le cryptage et les informations relatives à la signature.
- Connexions par partage Samba. Ce rapport comprend le PID du démon **smbd**, l'IP de la machine qui se connecte, l'heure à laquelle la connexion a été établie, les informations relatives au cryptage et à la signature.
- Liste des fichiers verrouillés. Les entrées du rapport comprennent des détails supplémentaires, tels que les types de verrou opportuniste (oplock)

Conditions préalables

- Le paquet **samba** est installé.
- Le service **smbd** est en cours d'exécution.

Procédure

```
# 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
```

Ressources supplémentaires

- **smbstatus(1)** page de manuel

1.20.10. Utilisation de l'utilitaire smbtar

L'utilitaire **smbtar** sauvegarde le contenu d'un partage SMB ou d'un sous-répertoire de celui-ci et le stocke dans une archive **tar**. Vous pouvez également écrire le contenu sur une bande magnétique.

Conditions préalables

- Le paquet **samba-client** est installé.

Procédure

- Utilisez la commande suivante pour sauvegarder le contenu du répertoire **demo** sur le partage //**server**/**example**/ et stocker le contenu dans l'archive /**root**/**example.tar**:

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

Ressources supplémentaires

- **smbtar(1)** page de manuel

1.20.11. Utilisation de l'utilitaire wbinfo

L'utilitaire **wbinfo** interroge et renvoie les informations créées et utilisées par le service **winbindd**.

Conditions préalables

- Le paquet **samba-winbind-clients** est installé.

Procédure

Vous pouvez utiliser **wbinfo**, par exemple, pour :

- Liste des utilisateurs du domaine :

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

- Liste des groupes de domaines :

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

- Afficher le SID d'un utilisateur :

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

- Afficher des informations sur les domaines et les trusts :

```
# 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
```

Ressources supplémentaires

- **wbinfo(1)** page de manuel

1.21. RESSOURCES SUPPLÉMENTAIRES

- **smb.conf(5)** page de manuel
- **/usr/share/docs/samba-version/** contient de la documentation générale, des scripts d'exemple et des fichiers de schéma LDAP, fournis par le projet Samba
- Configurer Samba et la Clustered Trivial Database (CDTB) pour partager des répertoires stockés sur un volume GlusterFS
- Montage d'un partage SMB sous Red Hat Enterprise Linux

CHAPITRE 2. EXPORTATION DE PARTAGES NFS

En tant qu'administrateur système, vous pouvez utiliser le serveur NFS pour partager un répertoire sur votre système via le réseau.

2.1. INTRODUCTION À NFS

Cette section explique les concepts de base du service NFS.

Un système de fichiers réseau (NFS) permet aux hôtes distants de monter des systèmes de fichiers sur un réseau et d'interagir avec ces systèmes de fichiers comme s'ils étaient montés localement. Cela vous permet de consolider les ressources sur des serveurs centralisés sur le réseau.

Le serveur NFS se réfère au fichier de configuration **/etc/exports** pour déterminer si le client est autorisé à accéder aux systèmes de fichiers exportés. Une fois cette vérification effectuée, toutes les opérations sur les fichiers et les répertoires sont accessibles à l'utilisateur.

2.2. VERSIONS NFS PRISES EN CHARGE

Cette section répertorie les versions de NFS prises en charge par Red Hat Enterprise Linux et leurs fonctionnalités.

Actuellement, Red Hat Enterprise Linux 9 prend en charge les versions majeures suivantes de NFS :

- La version 3 de NFS (NFSv3) prend en charge les écritures asynchrones sûres et est plus robuste que la version précédente NFSv2 en ce qui concerne la gestion des erreurs. Elle prend également en charge les tailles de fichiers et les décalages de 64 bits, ce qui permet aux clients d'accéder à plus de 2 Go de données de fichiers.

- NFS version 4 (NFSv4) fonctionne à travers les pare-feu et sur Internet, ne nécessite plus de service **rpcbind**, prend en charge les listes de contrôle d'accès (ACL) et utilise des opérations avec état.

NFS version 2 (NFSv2) n'est plus pris en charge par Red Hat.

Version NFS par défaut

La version par défaut de NFS dans Red Hat Enterprise Linux 9 est 4.2. Les clients NFS tentent de monter en utilisant NFSv4.2 par défaut, et reviennent à NFSv4.1 lorsque le serveur ne prend pas en charge NFSv4.2. Le montage revient ensuite à NFSv4.0, puis à NFSv3.

Caractéristiques des versions mineures de NFS

Voici les caractéristiques de NFSv4.2 dans Red Hat Enterprise Linux 9 :

Copie côté serveur

Permet au client NFS de copier efficacement des données sans gaspiller les ressources du réseau à l'aide de l'appel système **copy_file_range()**.

Fichiers épars

Permet aux fichiers d'avoir un ou plusieurs *holes*, qui sont des blocs de données non alloués ou non initialisés composés uniquement de zéros. L'opération **lseek()** dans NFSv4.2 prend en charge **seek_hole()** et **seek_data()**, ce qui permet aux applications de déterminer l'emplacement des trous dans le fichier clairsemé.

Réservation d'espace

Permet aux serveurs de stockage de réserver de l'espace libre, ce qui empêche les serveurs de

manquer d'espace. NFSv4.2 prend en charge l'opération **allocate()** pour réserver de l'espace, l'opération **deallocate()** pour libérer de l'espace et l'opération **fallocate()** pour pré-allouer ou désallouer de l'espace dans un fichier.

NFS étiqueté

Renforce les droits d'accès aux données et active les étiquettes SELinux entre un client et un serveur pour des fichiers individuels sur un système de fichiers NFS.

Amélioration de la mise en page

Fournit l'opération **layoutstats()**, qui permet à certains serveurs NFS parallèles (pNFS) de collecter de meilleures statistiques de performance.

Voici les caractéristiques de NFSv4.1 :

- Améliore les performances et la sécurité du réseau, et inclut également la prise en charge côté client de pNFS.
- Ne nécessite plus de connexion TCP distincte pour les rappels, ce qui permet à un serveur NFS d'accorder des délégations même lorsqu'il ne peut pas contacter le client : par exemple, en cas d'interférence due à la NAT ou à un pare-feu.
- La sémantique "exactement une fois" (sauf pour les opérations de redémarrage) permet d'éviter un problème antérieur dans lequel certaines opérations renvoyaient parfois un résultat inexact si une réponse était perdue et que l'opération était envoyée deux fois.

2.3. LES PROTOCOLES TCP ET UDP DANS NFSV3 ET NFSV4

NFSv4 nécessite l'utilisation du protocole de contrôle de transmission (TCP) sur un réseau IP.

NFSv3 pouvait également utiliser le protocole User Datagram Protocol (UDP) dans les versions antérieures de Red Hat Enterprise Linux. Dans Red Hat Enterprise Linux 9, NFS via UDP n'est plus pris en charge. Par défaut, UDP est désactivé dans le serveur NFS.

2.4. SERVICES REQUIS PAR LES SNF

Cette section répertorie les services système qui sont nécessaires à l'exécution d'un serveur NFS ou au montage de partages NFS. Red Hat Enterprise Linux démarre ces services automatiquement.

Red Hat Enterprise Linux utilise une combinaison de support au niveau du noyau et de processus de service pour fournir le partage de fichiers NFS. Toutes les versions de NFS reposent sur des appels de procédure à distance (RPC) entre les clients et les serveurs. Pour partager ou monter des systèmes de fichiers NFS, les services suivants fonctionnent ensemble en fonction de la version de NFS mise en œuvre :

nfsd

Module du noyau du serveur NFS qui traite les demandes de systèmes de fichiers NFS partagés.

rpcbind

Accepte les réservations de ports des services RPC locaux. Ces ports sont ensuite mis à disposition (ou annoncés) pour que les services RPC distants correspondants puissent y accéder. Le service **rpcbind** répond aux demandes de services RPC et établit des connexions avec le service RPC demandé. Ce service n'est pas utilisé avec NFSv4.

rpc.mountd

Ce processus est utilisé par un serveur NFS pour traiter les demandes **MOUNT** des clients NFSv3. Il vérifie que le partage NFS demandé est actuellement exporté par le serveur NFS et que le client est

autorisé à y accéder. Si la demande de montage est autorisée, le service **nfs-mountd** répond avec un statut "Success" et fournit au client NFS le File-Handle pour ce partage NFS.

rpc.nfsd

Ce processus permet de définir les versions et les protocoles NFS explicitement annoncés par le serveur. Il travaille avec le noyau Linux pour répondre aux demandes dynamiques des clients NFS, par exemple en fournissant des threads de serveur à chaque fois qu'un client NFS se connecte. Ce processus correspond au service **nfs-server**.

lockd

Il s'agit d'un thread du noyau qui s'exécute à la fois sur les clients et les serveurs. Il implémente le protocole Network Lock Manager (NLM), qui permet aux clients NFSv3 de verrouiller des fichiers sur le serveur. Il est démarré automatiquement à chaque fois que le serveur NFS est exécuté et qu'un système de fichiers NFS est monté.

rpc.statd

Ce processus met en œuvre le protocole RPC Network Status Monitor (NSM), qui notifie les clients NFS lorsqu'un serveur NFS est redémarré sans avoir été arrêté de manière gracieuse. Le service **rpc-statd** est démarré automatiquement par le service **nfs-server** et ne nécessite pas de configuration de la part de l'utilisateur. Il n'est pas utilisé avec NFSv4.

rpc.rquotad

Ce processus fournit des informations sur les quotas d'utilisateurs pour les utilisateurs distants. Le service **rpc-rquotad**, qui est fourni par le paquetage **quota-rpc**, doit être démarré par l'utilisateur lorsque le paquetage **nfs-server** est démarré.

rpc.idmapd

Ce processus fournit des appels ascendants aux clients et aux serveurs NFSv4, qui établissent une correspondance entre les noms NFSv4 sur le fil (chaînes de caractères sous la forme de ***user@domain***) et les UID et GID locaux. Pour que **idmapd** fonctionne avec NFSv4, le fichier **/etc/idmapd.conf** doit être configuré. Il faut au moins spécifier le paramètre **Domain**, qui définit le domaine de mappage NFSv4. Si le domaine de mappage NFSv4 est identique au nom de domaine DNS, ce paramètre peut être ignoré. Le client et le serveur doivent être d'accord sur le domaine de mappage NFSv4 pour que le mappage d'ID fonctionne correctement.

Seul le serveur NFSv4 utilise **rpc.idmapd**, qui est lancé par le service **nfs-idmapd**. Le client NFSv4 utilise l'utilitaire **nfsidmap**, basé sur un trousseau de clés, qui est appelé par le noyau à la demande pour effectuer le mappage des identifiants. En cas de problème avec **nfsidmap**, le client revient à l'utilisation de **rpc.idmapd**.

Les services RPC avec NFSv4

Les protocoles de montage et de verrouillage ont été incorporés dans le protocole NFSv4. Le serveur écoute également sur le port TCP 2049 bien connu. Ainsi, NFSv4 n'a pas besoin d'interagir avec les services **rpcbind**, **lockd** et **rpc-statd**. Le service **nfs-mountd** est toujours nécessaire sur le serveur NFS pour configurer les exportations, mais il n'est impliqué dans aucune opération sur le fil.

Ressources supplémentaires

- Configuration d'un serveur NFSv4 uniquement sans **rpcbind**.

2.5. FORMATS DES NOMS D'HÔTES NFS

Cette section décrit les différents formats que vous pouvez utiliser pour spécifier un hôte lors du montage ou de l'exportation d'un partage NFS.

Vous pouvez spécifier l'hôte dans les formats suivants :

Machine unique

L'un ou l'autre des éléments suivants :

- Un nom de domaine complet (qui peut être résolu par le serveur)
- Nom d'hôte (qui peut être résolu par le serveur)
- Une adresse IP.

Réseaux IP

L'un ou l'autre des formats suivants est valable :

- ***a.b.c.d/z***où ***a.b.c.d*** est le réseau et ***z*** est le nombre de bits du masque de réseau ; par exemple **192.168.0.0/24**.
- ***a.b.c.d/netmask***où ***a.b.c.d*** est le réseau et ***netmask*** est le masque de réseau ; par exemple, **192.168.100.8/255.255.255.0**.

Netgroups

Le format **@*group-name*** où ***group-name*** est le nom du groupe net NIS.

2.6. CONFIGURATION DU SERVEUR NFS

Cette section décrit la syntaxe et les options de deux façons de configurer les exportations sur un serveur NFS :

- Modification manuelle du fichier de configuration **/etc/exports**
- Utilisation de l'utilitaire **exportfs** sur la ligne de commande

2.6.1. Le fichier de configuration /etc/exports

Le fichier **/etc/exports** contrôle les systèmes de fichiers qui sont exportés vers des hôtes distants et spécifie des options. Il suit les règles syntaxiques suivantes :

- Les lignes vides sont ignorées.
- Pour ajouter un commentaire, commencez une ligne par le signe dièse (**#**).
- Vous pouvez entourer les lignes longues d'une barre oblique inverse (\).
- Chaque système de fichiers exporté doit se trouver sur sa propre ligne.
- Toute liste d'hôtes autorisés placée après un système de fichiers exporté doit être séparée par des caractères d'espacement.
- Les options pour chacun des hôtes doivent être placées entre parenthèses directement après l'identifiant de l'hôte, sans espace entre l'hôte et la première parenthèse.

Entrée de l'exportation
Chaque entrée d'un système de fichiers exporté a la structure suivante :

```
export host(options)
```

Il est également possible de spécifier plusieurs hôtes, ainsi que des options spécifiques pour chacun d'entre eux. Pour ce faire, il faut les énumérer sur la même ligne sous la forme d'une liste délimitée par des espaces, chaque nom d'hôte étant suivi de ses options respectives (entre parenthèses), comme dans l'exemple suivant :

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

Dans cette structure :

export

Le répertoire exporté

host

L'hôte ou le réseau vers lequel l'exportation est partagée

options

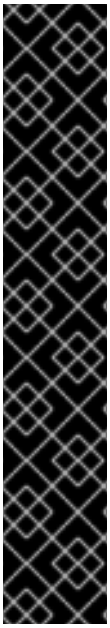
Les options à utiliser pour l'hôte

Exemple 2.1. Un simple fichier /etc/exports

Dans sa forme la plus simple, le fichier **/etc/exports** spécifie uniquement le répertoire exporté et les hôtes autorisés à y accéder :

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

Ici, **bob.example.com** peut monter **/exported/directory/** à partir du serveur NFS. Comme aucune option n'est spécifiée dans cet exemple, NFS utilise les options par défaut.



IMPORTANT

Le format du fichier **/etc/exports** est très précis, notamment en ce qui concerne l'utilisation du caractère espace. N'oubliez pas de toujours séparer les systèmes de fichiers exportés des hôtes et les hôtes les uns des autres par un caractère espace. Cependant, il ne doit pas y avoir d'autres caractères d'espacement dans le fichier, sauf sur les lignes de commentaires.

Par exemple, les deux lignes suivantes n'ont pas la même signification :

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

La première ligne autorise uniquement les utilisateurs de **bob.example.com** à accéder en lecture et en écriture au répertoire **/home**. La deuxième ligne permet aux utilisateurs de **bob.example.com** de monter le répertoire en lecture seule (par défaut), tandis que le reste du monde peut le monter en lecture/écriture.

Options par défaut

Les options par défaut pour une entrée d'exportation sont les suivantes :

ro

Le système de fichiers exporté est en lecture seule. Les hôtes distants ne peuvent pas modifier les données partagées sur le système de fichiers. Pour permettre aux hôtes d'apporter des modifications au système de fichiers (c'est-à-dire de lire et d'écrire), spécifiez l'option rw.

sync

Le serveur NFS ne répondra pas aux demandes avant que les modifications apportées par les demandes précédentes ne soient écrites sur le disque. Pour activer les écritures asynchrones, spécifiez l'option **async**.

wdelay

Le serveur NFS retardera l'écriture sur le disque s'il soupçonne qu'une autre demande d'écriture est imminente. Cela peut améliorer les performances car cela réduit le nombre de fois où le disque doit être accédé par des commandes d'écriture distinctes, réduisant ainsi la surcharge d'écriture. Pour désactiver cette fonction, spécifiez l'option **no_wdelay**, qui n'est disponible que si l'option sync par défaut est également spécifiée.

root_squash

Cela empêche les utilisateurs root connectés à distance (et non localement) d'avoir les privilèges root ; au lieu de cela, le serveur NFS leur attribue l'ID utilisateur **nobody**. Cela a pour effet de réduire les pouvoirs de l'utilisateur racine distant à ceux de l'utilisateur local le plus bas, empêchant ainsi toute écriture non autorisée sur le serveur distant. Pour désactiver l'écrasement de la racine, spécifiez l'option **no_root_squash**.

Pour écraser tous les utilisateurs distants (y compris root), utilisez l'option **all_squash**. Pour spécifier les ID d'utilisateur et de groupe que le serveur NFS doit attribuer aux utilisateurs distants d'un hôte particulier, utilisez les options **anonuid** et **anongid**, respectivement, comme dans l'exemple ci-dessous :

```
export host(anonuid=uidanongid=gid)
```

Ici, *uid* et *gid* sont respectivement le numéro d'identification de l'utilisateur et le numéro d'identification du groupe. Les options **anonuid** et **anongid** vous permettent de créer un compte d'utilisateur et de groupe spécial pour les utilisateurs NFS distants à partager.

Par défaut, les listes de contrôle d'accès (ACL) sont prises en charge par NFS sous Red Hat Enterprise Linux. Pour désactiver cette fonctionnalité, spécifiez l'option **no_acl** lors de l'exportation du système de fichiers.

Options par défaut et options prioritaires

Chaque valeur par défaut de chaque système de fichiers exporté doit être explicitement remplacée. Par exemple, si l'option **rw** n'est pas spécifiée, le système de fichiers exporté est partagé en lecture seule. Voici un exemple de ligne provenant de **/etc/exports** qui remplace deux options par défaut :

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

Dans cet exemple, **192.168.0.3** peut monter **/another/exported/directory/** en lecture et en écriture, et toutes les écritures sur disque sont asynchrones.

2.6.2. L'utilitaire exportfs

L'utilitaire **exportfs** permet à l'utilisateur root d'exporter ou de non-exporter sélectivement des répertoires sans redémarrer le service NFS. Lorsqu'il dispose des options appropriées, l'utilitaire **exportfs** écrit les systèmes de fichiers exportés sur **/var/lib/nfs/xtab**. Étant donné que le service **nfs-mountd** se réfère au fichier **xtab** lorsqu'il décide des privilèges d'accès à un système de fichiers, les modifications apportées à la liste des systèmes de fichiers exportés prennent effet immédiatement.

Options courantes d'exportfs

Voici une liste des options couramment utilisées pour **exportfs**:

-r

Provoque l'exportation de tous les répertoires répertoriés dans **/etc/exports** en construisant une nouvelle liste d'exportation dans **/var/lib/nfs/etab**. Cette option permet d'actualiser la liste d'exportation en fonction des modifications apportées à **/etc/exports**.

-a

Provoque l'exportation ou la non-exportation de tous les répertoires, en fonction des autres options transmises à **exportfs**. Si aucune autre option n'est spécifiée, **exportfs** exporte tous les systèmes de fichiers spécifiés dans **/etc/exports**.

-o *file-systems*

Spécifie les répertoires à exporter qui ne sont pas répertoriés dans **/etc/exports**. Remplacer *file-systems* par des systèmes de fichiers supplémentaires à exporter. Ces systèmes de fichiers doivent être formatés de la même manière qu'ils sont spécifiés dans **/etc/exports**. Cette option est souvent utilisée pour tester un système de fichiers exporté avant de l'ajouter définitivement à la liste des systèmes de fichiers exportés.

-i

Ignore **/etc/exports**; seules les options données sur la ligne de commande sont utilisées pour définir les systèmes de fichiers exportés.

-u

Désexporte tous les répertoires partagés. La commande **exportfs -ua** suspend le partage de fichiers NFS tout en maintenant tous les services NFS. Pour réactiver le partage NFS, utilisez la commande **exportfs -r**.

-v

Fonctionnement verbeux, où les systèmes de fichiers exportés ou non exportés sont affichés plus en détail lorsque la commande **exportfs** est exécutée.

Si aucune option n'est transmise à l'utilitaire **exportfs**, celui-ci affiche une liste des systèmes de fichiers actuellement exportés.

Ressources supplémentaires

- Formats des noms d'hôtes NFS.

2.7. NFS ET RPCBIND

Le service **rpcbind** associe les services RPC (Remote Procedure Call) aux ports sur lesquels ils écoutent. Les processus RPC informent **rpcbind** lorsqu'ils démarrent, en enregistrant les ports sur lesquels ils écoutent et les numéros de programme RPC qu'ils s'attendent à servir. Le système client contacte alors **rpcbind** sur le serveur avec un numéro de programme RPC particulier. Le service **rpcbind** redirige le client vers le numéro de port approprié afin qu'il puisse communiquer avec le service demandé.

Le système de fichiers réseau version 3 (NFSv3) nécessite le service **rpcbind**.

Étant donné que les services basés sur RPC s'appuient sur **rpcbind** pour établir toutes les connexions avec les requêtes entrantes des clients, **rpcbind** doit être disponible avant que ces services ne démarrent.

Les règles de contrôle d'accès pour **rpcbind** affectent tous les services basés sur RPC. Il est également possible de spécifier des règles de contrôle d'accès pour chacun des démons RPC NFS.

Ressources supplémentaires

- **rpc.mountd(8)** page de manuel
- **rpc.statd(8)** page de manuel

2.8. INSTALLATION DE NFS

Cette procédure installe tous les paquets nécessaires pour monter ou exporter des partages NFS.

Procédure

- Installez le paquetage **nfs-utils**:

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

2.9. DÉMARRAGE DU SERVEUR NFS

Cette procédure décrit comment démarrer le serveur NFS, qui est nécessaire pour exporter des partages NFS.

Conditions préalables

- Pour les serveurs qui prennent en charge les connexions NFSv3, le service **rpcbind** doit être en cours d'exécution. Pour vérifier que **rpcbind** est actif, utilisez la commande suivante :

```
$ systemctl status rpcbind
```

Si le service est arrêté, démarrez-le et activez-le :

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

Procédure

- Pour démarrer le serveur NFS et lui permettre de démarrer automatiquement au démarrage, utilisez la commande suivante :

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

Ressources supplémentaires

- Configuration d'un serveur NFSv4 uniquement .

2.10. DÉPANNAGE DE NFS ET RPCBIND

Comme le service **rpcbind** assure la coordination entre les services RPC et les numéros de port utilisés pour communiquer avec eux, il est utile d'afficher l'état des services RPC actuels à l'aide de **rpcbind** lors du dépannage. L'utilitaire **rpcinfo** affiche chaque service RPC avec les numéros de port, un numéro de programme RPC, un numéro de version et un type de protocole IP (TCP ou UDP).

Procédure

1. Pour s'assurer que les services NFS RPC appropriés sont activés pour **rpcbind**, utilisez la commande suivante :

```
# rpcinfo -p
```

Exemple 2.2. sortie de la commande rpcinfo -p

Voici un exemple de sortie de cette commande :

```
   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
```

Si l'un des services NFS ne démarre pas correctement, **rpcbind** sera incapable de faire correspondre les requêtes RPC des clients de ce service au port correct.

2. Dans de nombreux cas, si NFS n'est pas présent dans la sortie **rpcinfo**, le redémarrage de NFS permet au service de s'enregistrer correctement sur **rpcbind** et de commencer à fonctionner :

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

Ressources supplémentaires

- Configuration d'un serveur NFSv4 uniquement .

2.11. CONFIGURER LE SERVEUR NFS POUR QU'IL FONCTIONNE DERRIÈRE UN PARE-FEU

NFS nécessite le service **rpcbind**, qui attribue dynamiquement des ports pour les services RPC et peut poser des problèmes pour la configuration des règles de pare-feu. Les sections suivantes décrivent comment configurer les versions de NFS pour qu'elles fonctionnent derrière un pare-feu si vous

souhaitez les prendre en charge :

- NFSv3
  Il s'agit de tous les serveurs qui prennent en charge NFSv3 :
  - Serveurs NFSv3 uniquement
  - Serveurs supportant à la fois NFSv3 et NFSv4
- NFSv4 uniquement

2.11.1. Configurer le serveur NFSv3 pour qu'il fonctionne derrière un pare-feu

La procédure suivante décrit comment configurer les serveurs qui prennent en charge NFSv3 pour qu'ils fonctionnent derrière un pare-feu. Il s'agit des serveurs NFSv3 uniquement et des serveurs qui prennent en charge à la fois NFSv3 et NFSv4.

Procédure

1. Pour permettre aux clients d'accéder aux partages NFS derrière un pare-feu, configurez ce dernier en exécutant les commandes suivantes sur le serveur NFS :

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

2. Spécifiez les ports à utiliser par le service RPC **nlockmgr** dans le fichier **/etc/nfs.conf** comme suit :

```
[lockd]

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

   Vous pouvez également spécifier **nlm_tcpport** et **nlm_udpport** dans le fichier **/etc/modprobe.d/lockd.conf**.

3. Ouvrez les ports spécifiés dans le pare-feu en exécutant les commandes suivantes sur le serveur NFS :

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

4. Ajoutez des ports statiques pour **rpc.statd** en modifiant la section **[statd]** du fichier **/etc/nfs.conf** comme suit :

```
[statd]

port=port-number
```

5. Ouvrez les ports ajoutés dans le pare-feu en exécutant les commandes suivantes sur le serveur NFS :

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

6. Recharger la configuration du pare-feu :

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

7. Redémarrez d'abord le service **rpc-statd**, puis le service **nfs-server**:

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

Alternativement, si vous avez spécifié les ports **lockd** dans le fichier **/etc/modprobe.d/lockd.conf**:

a. Mettre à jour les valeurs actuelles de **/proc/sys/fs/nfs/nlm_tcpport** et **/proc/sys/fs/nfs/nlm_udpport**:

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

b. Redémarrez les services **rpc-statd** et **nfs-server**:

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

2.11.2. Configurer le serveur NFSv4-only pour qu'il fonctionne derrière un pare-feu

La procédure suivante décrit comment configurer le serveur NFSv4-only pour qu'il fonctionne derrière un pare-feu.

Procédure

1. Pour permettre aux clients d'accéder aux partages NFS derrière un pare-feu, configurez ce dernier en exécutant la commande suivante sur le serveur NFS :

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

2. Recharger la configuration du pare-feu :

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

3. Redémarrez le serveur nfs :

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

2.11.3. Configurer un client NFSv3 pour qu'il fonctionne derrière un pare-feu

La procédure de configuration d'un client NFSv3 derrière un pare-feu est similaire à la procédure de configuration d'un serveur NFSv3 derrière un pare-feu.

Si la machine que vous configurez est à la fois un client et un serveur NFS, suivez la procédure décrite dans la section Configurer le serveur compatible NFSv3 pour qu'il fonctionne derrière un pare-feu .

La procédure suivante décrit comment configurer une machine qui n'est qu'un client NFS pour qu'elle fonctionne derrière un pare-feu.

Procédure

1. Pour permettre au serveur NFS d'effectuer des rappels vers le client NFS lorsque ce dernier se trouve derrière un pare-feu, ajoutez le service **rpc-bind** au pare-feu en exécutant la commande suivante sur le client NFS :

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

2. Spécifiez les ports à utiliser par le service RPC **nlockmgr** dans le fichier **/etc/nfs.conf** comme suit :

```
[lockd]

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

   Vous pouvez également spécifier **nlm_tcpport** et **nlm_udpport** dans le fichier **/etc/modprobe.d/lockd.conf**.

3. Ouvrez les ports spécifiés dans le pare-feu en exécutant les commandes suivantes sur le client NFS :

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

4. Ajoutez des ports statiques pour **rpc.statd** en modifiant la section **[statd]** du fichier **/etc/nfs.conf** comme suit :

```
[statd]

port=port-number
```

5. Ouvrez les ports ajoutés dans le pare-feu en exécutant les commandes suivantes sur le client NFS :

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

6. Recharger la configuration du pare-feu :

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

7. Redémarrez le service **rpc-statd**:

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

Alternativement, si vous avez spécifié les ports **lockd** dans le fichier **/etc/modprobe.d/lockd.conf**:

a. Mettre à jour les valeurs actuelles de **/proc/sys/fs/nfs/nlm_tcpport** et **/proc/sys/fs/nfs/nlm_udpport**:

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

b. Redémarrez le service **rpc-statd**:

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

2.11.4. Configurer un client NFSv4 pour qu'il fonctionne derrière un pare-feu

N'effectuez cette procédure que si le client utilise NFSv4.0. Dans ce cas, il est nécessaire d'ouvrir un port pour les rappels NFSv4.0.

Cette procédure n'est pas nécessaire pour NFSv4.1 ou supérieur, car dans les versions ultérieures du protocole, le serveur effectue des rappels sur la même connexion que celle initiée par le client.

Procédure

1. Pour permettre aux rappels NFSv4.0 de traverser les pare-feux, définissez **/proc/sys/fs/nfs/nfs_callback_tcpport** et autorisez le serveur à se connecter à ce port sur le client comme suit :

```
# 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. Ouvrez le port spécifié dans le pare-feu en exécutant la commande suivante sur le client NFS :

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

3. Recharger la configuration du pare-feu :

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

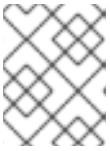
2.12. EXPORTER DES QUOTAS RPC À TRAVERS UN PARE-FEU

Si vous exportez un système de fichiers qui utilise des quotas de disque, vous pouvez utiliser le service RPC (Remote Procedure Call) quota pour fournir des données de quotas de disque aux clients NFS.

Procédure

1. Activez et démarrez le service **rpc-rquotad**:

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



NOTE

Le service **rpc-rquotad** est, s'il est activé, démarré automatiquement après le démarrage du service nfs-server.

2. Pour rendre le service quota RPC accessible derrière un pare-feu, le port TCP (ou UDP, si UDP est activé) 875 doit être ouvert. Le numéro de port par défaut est défini dans le fichier **/etc/services**.
   Vous pouvez remplacer le numéro de port par défaut en ajoutant **-p port-number** à la variable **RPCRQUOTADOPTS** dans le fichier **/etc/sysconfig/rpc-rquotad**.

3. Par défaut, les hôtes distants ne peuvent que lire les quotas. Si vous souhaitez autoriser les clients à définir des quotas, ajoutez l'option **-S** à la variable **RPCRQUOTADOPTS** dans le fichier **/etc/sysconfig/rpc-rquotad**.

4. Redémarrez **rpc-rquotad** pour que les modifications apportées au fichier **/etc/sysconfig/rpc-rquotad** prennent effet :

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

2.13. ACTIVATION DE NFS SUR RDMA (NFSORDMA)

Dans Red Hat Enterprise Linux 9, le service d'accès direct à la mémoire à distance (RDMA) sur du matériel compatible RDMA fournit une prise en charge du protocole Network File System (NFS) pour le transfert de fichiers à grande vitesse sur le réseau.

Procédure

1. Installez le paquetage **rdma-core**:

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

2. Vérifiez que les lignes contenant **xprtrdma** et **svcrdma** sont commentées dans le fichier **/etc/rdma/modules/rdma.conf**:

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

3. Sur le serveur NFS, créez le répertoire **/mnt/nfsordma** et exportez-le vers **/etc/exports**:

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

4. Sur le client NFS, montez le partage nfs avec l'adresse IP du serveur, par exemple, **172.31.0.186**:

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

5. Redémarrez le service **nfs-server**:

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

-

Ressources supplémentaires

- La norme RFC 5667

2.14. RESSOURCES SUPPLÉMENTAIRES

- Le wiki Linux NFS

CHAPITRE 3. SÉCURISATION DE NFS

Pour minimiser les risques de sécurité NFS et protéger les données sur le serveur, tenez compte des sections suivantes lorsque vous exportez des systèmes de fichiers NFS sur un serveur ou que vous les montez sur un client.

3.1. SÉCURITÉ NFS AVEC AUTH_SYS ET CONTRÔLE DES EXPORTATIONS

NFS propose les options traditionnelles suivantes pour contrôler l'accès aux fichiers exportés :

- Le serveur limite les hôtes autorisés à monter les systèmes de fichiers par adresse IP ou par nom d'hôte.
- Le serveur applique les autorisations du système de fichiers pour les utilisateurs des clients NFS de la même manière qu'il le fait pour les utilisateurs locaux. Traditionnellement, NFS utilise pour cela le message d'appel **AUTH_SYS** (également appelé **AUTH_UNIX**), qui s'appuie sur le client pour indiquer l'UID et le GID de l'utilisateur. Il faut savoir qu'un client malveillant ou mal configuré peut facilement se tromper et permettre à un utilisateur d'accéder à des fichiers qu'il ne devrait pas.

Pour limiter les risques potentiels, les administrateurs limitent souvent l'accès à la lecture seule ou écrasent les autorisations d'un utilisateur et d'un groupe d'ID communs. Malheureusement, ces solutions empêchent d'utiliser le partage NFS de la manière prévue à l'origine.

En outre, si un pirate prend le contrôle du serveur DNS utilisé par le système exportant le système de fichiers NFS, il peut faire pointer le système associé à un nom d'hôte particulier ou à un nom de domaine pleinement qualifié vers une machine non autorisée. À ce stade, la machine non autorisée *is* est le système autorisé à monter le partage NFS, car aucun nom d'utilisateur ou mot de passe n'est échangé pour fournir une sécurité supplémentaire pour le montage NFS.

Les caractères génériques doivent être utilisés avec parcimonie lors de l'exportation de répertoires via NFS, car il est possible que le champ d'application du caractère générique englobe plus de systèmes que prévu.

Ressources supplémentaires

- Pour sécuriser NFS et **rpcbind**, utilisez, par exemple, **nftables** et **firewalld**.
- **nft(8)** page de manuel
- **firewalld-cmd(1)** page de manuel

3.2. SÉCURITÉ NFS AVEC AUTH_GSS

Toutes les versions de NFS prennent en charge RPCSEC_GSS et le mécanisme Kerberos.

Contrairement à AUTH_SYS, avec le mécanisme Kerberos RPCSEC_GSS, le serveur ne dépend pas du client pour représenter correctement l'utilisateur qui accède au fichier. La cryptographie est utilisée pour authentifier les utilisateurs auprès du serveur, ce qui empêche un client malveillant d'usurper l'identité d'un utilisateur sans disposer des informations d'identification Kerberos de ce dernier. L'utilisation du mécanisme Kerberos RPCSEC_GSS est le moyen le plus simple de sécuriser les montages car, une fois Kerberos configuré, aucune autre installation n'est nécessaire.

3.3. CONFIGURATION D'UN SERVEUR ET D'UN CLIENT NFS POUR L'UTILISATION DE KERBEROS

Kerberos est un système d'authentification réseau qui permet aux clients et aux serveurs de s'authentifier les uns les autres en utilisant un cryptage symétrique et un tiers de confiance, le KDC. Red Hat recommande d'utiliser Identity Management (IdM) pour configurer Kerberos.

Conditions préalables

- Le centre de distribution de clés Kerberos (**KDC**) est installé et configuré.

Procédure

1. - Créer le **nfs/hostname.*domain@REALM*** du côté du serveur NFS.
   - Créer le **host/hostname.*domain@REALM*** tant du côté du serveur que du côté du client.
   - Ajouter les clés correspondantes aux keytabs du client et du serveur.
2. Côté serveur, utilisez l'option **sec=** pour activer les variantes de sécurité souhaitées. Pour activer toutes les saveurs de sécurité ainsi que les montages non cryptographiques :

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

   Les saveurs de sécurité valables à utiliser avec l'option **sec=** sont les suivantes :

   - **sys**: pas de protection cryptographique, la valeur par défaut de l'option
   - **krb5**authentification uniquement
   - **krb5i**protection de l'intégrité : protection de l'intégrité
     - utilise Kerberos V5 pour l'authentification des utilisateurs et effectue un contrôle d'intégrité des opérations NFS à l'aide de sommes de contrôle sécurisées afin d'empêcher la falsification des données.
   - **krb5p**protection de la vie privée : protection de la vie privée
     - utilise Kerberos V5 pour l'authentification des utilisateurs, le contrôle d'intégrité et le chiffrement du trafic NFS afin d'empêcher le reniflage du trafic. Il s'agit du paramètre le plus sûr, mais c'est aussi celui qui entraîne le plus de surcoût en termes de performances.
3. Côté client, ajoutez **sec=krb5** (ou **sec=krb5i**, ou **sec=krb5p**, selon la configuration) aux options de montage :

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

Ressources supplémentaires

- Création de fichiers en tant que root sur NFS sécurisé par krb5 . Déconseillé.
- **exports(5)** page de manuel
- **nfs(5)** page de manuel

3.4. OPTIONS DE SÉCURITÉ NFSV4

NFSv4 inclut un support ACL basé sur le modèle Microsoft Windows NT, et non sur le modèle POSIX, en raison des fonctionnalités du modèle Microsoft Windows NT et de son large déploiement.

Une autre caractéristique de sécurité importante de NFSv4 est la suppression de l'utilisation du protocole **MOUNT** pour le montage des systèmes de fichiers. Le protocole **MOUNT** présentait un risque de sécurité en raison de la manière dont il traitait les fichiers.

3.5. DROITS D'ACCÈS AUX FICHIERS SUR LES EXPORTATIONS NFS MONTÉES

Une fois que le système de fichiers NFS est monté en lecture ou en lecture et écriture par un hôte distant, la seule protection dont bénéficie chaque fichier partagé est celle de ses autorisations. Si deux utilisateurs partageant la même valeur d'ID utilisateur montent le même système de fichiers NFS sur des systèmes clients différents, ils peuvent modifier leurs fichiers respectifs. En outre, toute personne connectée en tant que root sur le système client peut utiliser la commande **su -** pour accéder à tous les fichiers du partage NFS.

Par défaut, les listes de contrôle d'accès (ACL) sont prises en charge par NFS sous Red Hat Enterprise Linux. Red Hat recommande de garder cette fonctionnalité activée.

Par défaut, NFS utilise *root squashing* lors de l'exportation d'un système de fichiers. L'ID utilisateur de toute personne accédant au partage NFS en tant qu'utilisateur root sur sa machine locale est ainsi défini sur **nobody**. L'écrasement de la racine est contrôlé par l'option par défaut **root_squash**; pour plus d'informations sur cette option, voir Configuration du serveur NFS.

Lorsque vous exportez un partage NFS en lecture seule, pensez à utiliser l'option **all_squash**. Cette option fait en sorte que chaque utilisateur accédant au système de fichiers exporté prenne l'identifiant de l'utilisateur **nobody**.

CHAPITRE 4. ACTIVATION DES CONFIGURATIONS SCSI PNFS DANS NFS

Vous pouvez configurer le serveur et le client NFS pour qu'ils utilisent la disposition pNFS SCSI pour accéder aux données. pNFS SCSI est utile dans les cas d'utilisation qui impliquent un accès à un fichier par un seul client pendant une longue période.

Conditions préalables

- Le client et le serveur doivent pouvoir envoyer des commandes SCSI au même périphérique de bloc. En d'autres termes, le périphérique de bloc doit se trouver sur un bus SCSI partagé.
- Le périphérique de bloc doit contenir un système de fichiers XFS.
- Le périphérique SCSI doit prendre en charge les réservations persistantes SCSI telles que décrites dans la spécification des commandes primaires SCSI-3.

4.1. LA TECHNOLOGIE PNFS

L'architecture pNFS améliore l'évolutivité de NFS. Lorsqu'un serveur met en œuvre pNFS, le client peut accéder aux données par l'intermédiaire de plusieurs serveurs simultanément. Cela permet d'améliorer les performances.

pNFS prend en charge les protocoles ou dispositions de stockage suivants sur RHEL :

- Dossiers
- Flexfiles
- SCSI

4.2. DISPOSITIONS SCSI PNFS

L'agencement SCSI s'appuie sur le travail des agencements de blocs pNFS. L'agencement est défini sur l'ensemble des périphériques SCSI. Elle contient une série séquentielle de blocs de taille fixe en tant qu'unités logiques (LU) qui doivent être capables de prendre en charge les réservations persistantes SCSI. Les périphériques LU sont identifiés par leur identification de périphérique SCSI.

pNFS SCSI donne de bons résultats dans les cas d'utilisation qui impliquent l'accès à un fichier par un seul client pendant une longue période. Il peut s'agir par exemple d'un serveur de messagerie ou d'une machine virtuelle hébergeant un cluster.

Opérations entre le client et le serveur

Lorsqu'un client NFS lit ou écrit dans un fichier, il effectue une opération **LAYOUTGET**. Le serveur répond en indiquant l'emplacement du fichier sur le périphérique SCSI. Il se peut que le client doive effectuer une opération supplémentaire (**GETDEVICEINFO**) pour déterminer le périphérique SCSI à utiliser. Si ces opérations fonctionnent correctement, le client peut envoyer des demandes d'E/S directement au périphérique SCSI au lieu d'envoyer les opérations **READ** et **WRITE** au serveur.

Des erreurs ou des conflits entre clients peuvent amener le serveur à rappeler des schémas ou à ne pas les transmettre aux clients. Dans ce cas, les clients se contentent d'envoyer les opérations **READ** et **WRITE** au serveur au lieu d'envoyer des demandes d'E/S directement au périphérique SCSI.

Pour surveiller les opérations, voir Surveillance de la fonctionnalité des layouts SCSI pNFS.

Réservations d'appareils

le pNFS SCSI gère les clôtures par l'attribution de réservations. Avant que le serveur n'envoie des layouts aux clients, il réserve le périphérique SCSI pour s'assurer que seuls les clients enregistrés peuvent y accéder. Si un client peut envoyer des commandes à ce périphérique SCSI mais qu'il n'est pas enregistré auprès de celui-ci, de nombreuses opérations effectuées par le client sur ce périphérique échouent. Par exemple, la commande **blkid** sur le client n'affiche pas l'UUID du système de fichiers XFS si le serveur n'a pas donné au client une disposition pour ce périphérique.

Le serveur ne supprime pas sa propre réservation persistante. Cela permet de protéger les données du système de fichiers sur le périphérique en cas de redémarrage des clients et des serveurs. Pour réutiliser le périphérique SCSI, il peut être nécessaire de supprimer manuellement la réservation persistante sur le serveur NFS.

4.3. RECHERCHE D'UN PÉRIPHÉRIQUE SCSI COMPATIBLE AVEC PNFS

Cette procédure permet de vérifier si un périphérique SCSI prend en charge l'agencement SCSI pNFS.

Conditions préalables

- Installez le paquetage **sg3_utils**:

```
# dnf install sg3_utils
```

Procédure

- Sur le serveur et le client, vérifiez que les périphériques SCSI sont correctement pris en charge :

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

Assurez-vous que le bit *Persist Through Power Loss Active* (**PTPL_A**) est activé.

Exemple 4.1. Un périphérique SCSI qui prend en charge pNFS SCSI

Voici un exemple de la sortie de **sg_persist** pour un périphérique SCSI qui prend en charge pNFS SCSI. Le bit **PTPL_A** indique **1**.

```
    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
```

Ressources supplémentaires

- **sg_persist(8)** page de manuel

4.4. CONFIGURATION DE PNFS SCSI SUR LE SERVEUR

Cette procédure permet de configurer un serveur NFS pour qu'il exporte une disposition SCSI pNFS.

Procédure

1. Sur le serveur, montez le système de fichiers XFS créé sur le périphérique SCSI.
2. Configurez le serveur NFS pour qu'il exporte la version 4.1 ou supérieure de NFS. Définissez l'option suivante dans la section **[nfsd]** du fichier **/etc/nfs.conf**:

```
[nfsd]

vers4.1=y
```

3. Configurez le serveur NFS pour exporter le système de fichiers XFS sur NFS avec l'option **pnfs**:

Exemple 4.2. Une entrée dans /etc/exports pour exporter pNFS SCSI

L'entrée suivante dans le fichier de configuration **/etc/exports** exporte le système de fichiers monté sur **/exported/directory/** vers le client **allowed.example.com** sous la forme d'une disposition SCSI pNFS :

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

NOTE

Le système de fichiers exporté doit être créé sur l'ensemble du périphérique de bloc, et pas seulement sur une partition.

Ressources supplémentaires

- Exportation des partages NFS.

4.5. CONFIGURATION DE PNFS SCSI SUR LE CLIENT

Cette procédure permet de configurer un client NFS pour monter une disposition SCSI pNFS.

Conditions préalables

- Le serveur NFS est configuré pour exporter un système de fichiers XFS via pNFS SCSI. Voir Configuration de pNFS SCSI sur le serveur .

Procédure

- Sur le client, montez le système de fichiers XFS exporté à l'aide de la version 4.1 ou supérieure de NFS :

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

Ne montez pas le système de fichiers XFS directement sans NFS.

Ressources supplémentaires

- Montage des partages NFS.

4.6. LIBÉRATION DE LA RÉSERVATION SCSI PNFS SUR LE SERVEUR

Cette procédure libère la réservation persistante qu'un serveur NFS détient sur un périphérique SCSI. Cela vous permet de réutiliser le périphérique SCSI lorsque vous n'avez plus besoin d'exporter pNFS SCSI.

Vous devez supprimer la réservation du serveur. Elle ne peut pas être supprimée d'un autre Nexus informatique.

Conditions préalables

- Installez le paquetage **sg3_utils**:

```
# dnf install sg3_utils
```

Procédure

1. Interroger une réservation existante sur le serveur :

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

Exemple 4.3. Interroger une réservation sur /dev/sda

```
# *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. Supprimer l'enregistrement existant sur le serveur :

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

Exemple 4.4. Suppression d'une réservation sur /dev/sda

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

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

Ressources supplémentaires

- **sg_persist(8)** page de manuel