Version : **2022.01**

Dernière mise-à-jour : 2022/12/07 06:12

Topic 209: File Sharing

Contenu du Module

- **Topic 209: File Sharing**
  - Contenu du Module
  - Gestion du Serveur NFS
    - Présentation
      - Options d'un Partage NFS
      - Commandes de Base
    - Installation
    - LAB #1 Mise en Place du Serveur NFS
      - 1.1 - Configuration du Serveur
      - 1.2 - Configuration du Client
      - 1.3 - Surveillance du Serveur
        - La Commande rpcinfo
        - La Commande nfsstat
  - Gestion du Serveur SMB/CIFS Samba
    - Les Réseaux Microsoft
      - Types de Réseaux Microsoft
      - Types de Clients Windows
    - Présentation de Samba
      - Daemons Samba
      - Commandes Samba
    - LAB #2 - Installation de Samba
      - 2.1 - Configuration de base
      - 2.2 - Démarrage manuel de Samba

- 2.3 - Configuration de Samba
  - Gestion des comptes et des groupes
  - Création du fichier smbpasswd
  - Comprendre la structure du fichier de configuration smb.conf
- Samba en tant que serveur membre d’un domaine
  - Windows Server 2008
  - LAB #3 - Samba en tant que serveur membre d’un domaine
    - 3.1 - Obtenir un ticket Kerberos pour le serveur Linux
    - 3.2 - Configuration de samba
    - 3.3 - Mettre le serveur Samba dans le domaine
    - 3.4 - Modifier le fichier /etc/nsswitch.conf
    - 3.5 - Vérifier les service winbind
    - 3.6 - Terminer la configuration de samba
    - 3.7 - Modifier PAM

Gestion du Serveur NFS

Présentation

Quand on parle de NFS, on parle d'**exportation** d'un répertoire sur le serveur afin que celui-ci puisse être vu par des clients sur le réseau. Ces clients peuvent ensuite monter le répertoire et l'utiliser comme si celui-ci faisait partie de son propre filesystem.

Le Network File System (NFS) est le protocole de partage de fichiers historique sur des systèmes Unix. Lors de l'introduction de Samba, NFS a vu sa popularité diminuée, essentiellement parce que la connexion est non-sécurisée :

- le partage ainsi que ses caractéristiques sont configurés par rapport à l'adresse IP du client, or l'IP Spoofing est de plus en plus répandu,
- aucun mot de passe n'est demandé lors de la connexion d'un utilisateur à une ressource car le serveur NFS présume que l'utilisateur *jean* distant est le même utilisateur du compte *jean* sur le serveur NFS.

Cependant l'arrivée sur le marché de serveurs NAS domestiques ainsi que l'utilisation de la virtualisation dans le milieu professionnel fait que NFS connait un regain d'intérêt en tant que stockage mutualisé raid, simple à mettre en œuvre.

Il existe actuellement 3 versions de NFS :

Version	Protocole Utilisé	Dépendance
NFSv2	TCP et UDP	portmap
NFSv3	TCP et UDP	portmap
NFSv4	TCP	Aucune - les fonctions de portmap sont incluses dans NFSv4

La version utilisée par défaut sous CentOS 8 est **NFSv4**.

Options d'un Partage NFS

Certaines options, appliquées à un partage, modifient le comportement du serveur NFS pour le partage concerné lors de son démarrage :

Option	Comportement
ro	Accès en lecture seule
rw	Accès en lecture / écriture
sync	Ecriture synchrone (écriture immédiate sur disque)
async	Ecriture asynchrone (écriture sur disque en utilisant une cache)
root_squash	Root perd ses prérogatives sur le partage concerné
no_root_squash	Root garde ses prérogatives sur le partage concerné
no_lock	Pas de verrous sur les fichiers accédés
all_squash	Force la mapping de tous les utilisateurs vers l'utilisateur **nobody**
anonuid	Fixe l'UID de l'utilisateur anonyme
anongid	Fixe le GID de l'utilisateur anonyme

Important : Si plusieurs options sont spécifiées, celles-ci doivent être séparées par des virgules.

Commandes de Base

Plusieurs commandes permettent de gérer et de s'informer sur l'activité du serveur NFS :

Commande	Comportement
exportfs	Affiche les partages actifs sur le serveur courant
nfsstat	Affiche les statistiques de l'activité NFS
rpcinfo	Affiche les démons gérés en effectuant une requête RPC sur le serveur courant
showmount	Affiche les partages actifs sur un serveur distant
mount	Permet de monter un partage distant sur un répertoire local

LAB #1 Mise en Place du Serveur NFS

Connectez-vous à la VM CentOS8 au 10.0.2.46.

Configuration du Serveur

Ajoutez une autre adresse IP pour le NFS :

```
[root@centos8 ~]# nmcli connection mod ip_fixe +ipv4.addresses 192.168.1.2/24

[root@centos8 ~]# nmcli con up ip_fixe
```

Continuez maintenant par la mise en place du service **nfs** :

```
[root@centos8 ~]# systemctl status nfs-server
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; disabled; vendor prese>
   Active: inactive (dead)

[root@centos8 ~]# systemctl enable nfs-server.service
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/nfs-server.service → /usr/lib/systemd/system/nfs-server.service.
```

La mise en place d'un partage ponctuel se fait en utilisant la commande **exportfs** en indiquant en argument le répertoire sous la forme de *adresse_ip_du_serveur:chemin_du_partage* :

```
[root@centos8 ~]# exportfs

[root@centos8 ~]# exportfs 192.168.1.2:/home/trainee

[root@centos8 ~]# exportfs
/home/trainee   192.168.1.2
```

Démarrez maintenant le service **nfs** :

```
[root@centos8 ~]# systemctl start nfs-server.service

[root@centos8 ~]# systemctl status nfs-server.service
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; vendor preset: disabled)
   Active: active (exited) since Mon 2022-11-21 11:02:13 CET; 9s ago
  Process: 3276 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then systemctl reload gssproxy ; fi
(code=exited, >
  Process: 3263 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
  Process: 3261 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
 Main PID: 3276 (code=exited, status=0/SUCCESS)

Nov 21 11:02:12 centos8.ittraining.loc systemd[1]: Starting NFS server and services...
Nov 21 11:02:13 centos8.ittraining.loc systemd[1]: Started NFS server and services.
```

Afin de mettre en place un ou des partages **permanents**, il est nécessaire d'éditer le fichier **/etc/exports** :

```
[root@centos8 ~]# vi /etc/exports
[root@centos8 ~]# cat /etc/exports
```

```
/home/trainee   192.168.1.1
/tmp            *(fsid=0)
```

> **Important** : Dans ce cas, nous avons partagé le répertoire **/home/trainee** pour la seule adresse IP 192.168.1.1.

Redémarrez maintenant le service nfs afin que le fichier **/etc/exports** soit re-lu :

```
[root@centos8 ~]# systemctl restart nfs-server.service

[root@centos8 ~]# systemctl status nfs-server.service
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; vendor preset: disabled)
   Active: active (exited) since Mon 2022-11-21 11:04:08 CET; 4s ago
  Process: 3309 ExecStopPost=/usr/sbin/exportfs -f (code=exited, status=0/SUCCESS)
  Process: 3307 ExecStopPost=/usr/sbin/exportfs -au (code=exited, status=0/SUCCESS)
  Process: 3305 ExecStop=/usr/sbin/rpc.nfsd 0 (code=exited, status=0/SUCCESS)
  Process: 3334 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then systemctl reload gssproxy ; fi
(code=exited, >
  Process: 3323 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
  Process: 3320 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
 Main PID: 3334 (code=exited, status=0/SUCCESS)

Nov 21 11:04:07 centos8.ittraining.loc systemd[1]: Starting NFS server and services...
Nov 21 11:04:07 centos8.ittraining.loc exportfs[3320]: exportfs: No options for /home/trainee 192.168.1.1:
suggest 192.168.>
Nov 21 11:04:08 centos8.ittraining.loc systemd[1]: Started NFS server and services.
```

Puisque aucune option ne soit spécifiée pour les montages, ceux-ci ont été exportés avec des option par défaut. En utilisant l'option **-v** de la commande **exportfs**, il est possible de consulter ces options :

```
[root@centos8 ~]# exportfs -v
/home/trainee   192.168.1.1(sync,wdelay,hide,no_subtree_check,sec=sys,ro,secure,root_squash,no_all_squash)
/tmp            <world>(sync,wdelay,hide,no_subtree_check,fsid=0,sec=sys,ro,secure,root_squash,no_all_squash)
```

Passez SELinux en mode permissive :

```
[root@centos8 ~]# getenforce
Enforcing

[root@centos8 ~]# setenforce permissive
```

Configurez ensuite le pare-feu :

```
[root@centos8 ~]# firewall-cmd --permanent --add-service=nfs

[root@centos8 ~]# firewall-cmd --permanent --add-service=rpc-bind

[root@centos8 ~]# firewall-cmd --permanent --add-service=mountd

[root@centos8 ~]# firewall-cmd --reload
```

Configuration du Client

Important : Connectez-vous à votre client au 10.0.2.45.

Ajoutez une autre adresse IP pour le NFS :

```
[root@centos8 ~]# nmcli connection mod ens18 +ipv4.addresses 192.168.1.1/24
```

```
[root@centos8 ~]# nmcli con up ens18
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/4)

[root@centos8 ~]# nmcli c show
NAME    UUID                                  TYPE      DEVICE
ens18   fc4a4d23-b15e-47a7-bcfa-b2e08f49553e  ethernet  ens18
virbr0  1a78c62f-785b-4c47-94de-c7bb1dbca968  bridge    virbr0

[root@centos8 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 5e:3f:e8:43:d5:f9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.45/24 brd 10.0.2.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet 192.168.1.1/24 brd 192.168.1.255 scope global noprefixroute ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::86b6:8d39:cab2:d84d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether ea:c8:86:9e:73:a6 brd ff:ff:ff:ff:ff:ff
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:79:02:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:79:02:66 brd ff:ff:ff:ff:ff:ff
```

A partir de votre client, consultez les répertoire exportés du serveur :

```
[root@centos8 ~]# showmount --exports 192.168.1.2
Export list for 192.168.1.2:
/tmp          *
/home/trainee 192.168.1.1
```

Créez maintenant le répertoire **/nfs** dans le client et montez le partage **192.168.1.2:/home/trainee** :

```
[root@centos8 ~]# mkdir /nfs

[root@centos8 ~]# mount -t nfs 192.168.1.2:/home/trainee /nfs
```

Vérifiez que vous acc-s au contenu de partage :

```
[root@centos8 ~]# cd /nfs
[root@centos8 nfs]# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

Surveillance du Serveur

La Commande rpcinfo

La commande **rpcinfo** permet de faire une requête RPC sur le serveur et de voir les démons gérés :

```
[root@centos8 nfs]# rpcinfo
   program version netid     address                service    owner
    100000    4    tcp6      ::.0.111               portmapper superuser
    100000    3    tcp6      ::.0.111               portmapper superuser
    100000    4    udp6      ::.0.111               portmapper superuser
    100000    3    udp6      ::.0.111               portmapper superuser
    100000    4    tcp       0.0.0.0.0.111          portmapper superuser
    100000    3    tcp       0.0.0.0.0.111          portmapper superuser
```

```
    100000    2    tcp       0.0.0.0.0.111          portmapper superuser
    100000    4    udp       0.0.0.0.0.111          portmapper superuser
    100000    3    udp       0.0.0.0.0.111          portmapper superuser
    100000    2    udp       0.0.0.0.0.111          portmapper superuser
    100000    4    local     /run/rpcbind.sock      portmapper superuser
    100000    3    local     /run/rpcbind.sock      portmapper superuser
    100024    1    udp       0.0.0.0.231.223        status     29
    100024    1    tcp       0.0.0.0.173.255        status     29
    100024    1    udp6      ::.144.182             status     29
    100024    1    tcp6      ::.155.95              status     29
    100021    1    udp       0.0.0.0.216.108        nlockmgr   superuser
    100021    3    udp       0.0.0.0.216.108        nlockmgr   superuser
    100021    4    udp       0.0.0.0.216.108        nlockmgr   superuser
    100021    1    tcp       0.0.0.0.178.151        nlockmgr   superuser
    100021    3    tcp       0.0.0.0.178.151        nlockmgr   superuser
    100021    4    tcp       0.0.0.0.178.151        nlockmgr   superuser
    100021    1    udp6      ::.226.111             nlockmgr   superuser
    100021    3    udp6      ::.226.111             nlockmgr   superuser
    100021    4    udp6      ::.226.111             nlockmgr   superuser
    100021    1    tcp6      ::.181.17              nlockmgr   superuser
    100021    3    tcp6      ::.181.17              nlockmgr   superuser
    100021    4    tcp6      ::.181.17              nlockmgr   superuser
```

Par exemple, pour vérifier la version du protocole NFS utilisé, tapez la commande suivante :

```
[root@centos8 ~]# rpcinfo -p | grep nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    3   tcp   2049  nfs_acl
```

La Commande nfsstat

La Commande **nfsstat** permet de vérifier l'activité sur le serveur NFS et vous montre les statistiques du noyau NFC :

```
[root@centos8 ~]# nfsstat
Server rpc stats:
calls      badcalls   badfmt     badauth    badclnt
33         0          0          0          0

Server nfs v3:
null             getattr          setattr          lookup           access
2         14%    7         50%    0         0%     0         0%     1          7%
readlink         read             write            create           mkdir
0         0%     0          0%    0         0%     0         0%     0          0%
symlink          mknod            remove           rmdir            rename
0         0%     0          0%    0         0%     0         0%     0          0%
link             readdir          readdirplus      fsstat           fsinfo
0         0%     0          0%    1         7%     0         0%     2         14%
pathconf         commit
1         7%     0          0%

Server nfs v4:
null             compound
1         5%     17        94%

Server nfs v4 operations:
op0-unused       op1-unused       op2-future       access           close
0         0%     0         0%     0         0%     1         2%     0          0%
commit           create           delegpurge       delegreturn      getattr
0         0%     0         0%     0         0%     0         0%     9         21%
getfh            link             lock             lockt            locku
1         2%     0         0%     0         0%     0         0%     0          0%
lookup           lookup_root      nverify          open             openattr
1         2%     0         0%     0         0%     0         0%     0          0%
open_conf        open_dgrd        putfh            putpubfh         putrootfh
0         0%     0         0%     9        21%     0         0%     2          4%
read             readdir          readlink         remove           rename
0         0%     0         0%     0         0%     0         0%     0          0%
```

```
renew             restorefh         savefh            secinfo           setattr
0          0%     0          0%     0          0%     0          0%     0          0%
setcltid          setcltidconf      verify            write             rellockowner
0          0%     0          0%     0          0%     0          0%     0          0%
bc_ctl            bind_conn         exchange_id       create_ses        destroy_ses
0          0%     0          0%     2          4%     1          2%     1          2%
free_stateid      getdirdeleg       getdevinfo        getdevlist        layoutcommit
0          0%     0          0%     0          0%     0          0%     0          0%
layoutget         layoutreturn      secinfononam      sequence          set_ssv
0          0%     0          0%     1          2%     12        28%     0          0%
test_stateid      want_deleg        destroy_clid      reclaim_comp      allocate
0          0%     0          0%     1          2%     1          2%     0          0%
copy              copy_notify       deallocate        ioadvise          layouterror
0          0%     0          0%     0          0%     0          0%     0          0%
layoutstats       offloadcancel     offloadstatus     readplus          seek
0          0%     0          0%     0          0%     0          0%     0          0%
write_same
0          0%
```

Gestion du Serveur SMB/CIFS Samba

Les Réseaux Microsoft

Le fonctionnement d'un réseau Windows™ se repose sur le protocole **CIFS** (*Common Internet FileSystem*) le successeur du protocole **SMB** (*Server Message Block*).

Types de Réseaux Microsoft

Les réseaux Microsoft™ se divisent en trois types distincts :

- **Un groupe de travail**,
  - Windows ™ 3.11, 9x, ME, NT Workstation, 2000 Workstation, XP, Vista, Seven,
  - Les systèmes se trouvent sur le même réseau physique,
  - La gestion des partages n'est pas centralisée,
  - La sécurité est fournie par des mots de passe qui protègent les ressources individuelles,
- **Un domaine**,
  - Windows™ NT Server 3.5, 3.51 ou 4,
  - Nécessite la mise en place d'un **PDC** (*Primary Domain Controller*),
  - La gestion des utilisateurs est accomplie via le service **SAM** (*Security Account Manager*),
  - La sécurité s'appuie sur des objets appelés **SIDs** (*Security IDentifiers*),
  - Peut contenir un ou plusieurs **BDC** (*Backup Domain Controller*),
- **Active Directory**,
  - Windows™ 2000 Server, Server 2003, Server 2008,
  - La gestion de l'authentification des utilisateurs est assurée par un annuaire **LDAP** (*Lightweight Directory Access Protocol*),
  - Le service des noms est assurée par le **DNS** (*Domain Name Service*),

Types de Clients Windows

Le fonctionnement du client Windows™ 2000 et les versions ultérieures implique que le protocole SMB s'appuie directement sur **TCP/IP** en utilisant le port **445**.

Le fonctionnement du client Windows™ antérieur à Windows™ 2000 nécessite le protocole **NBT** (*Network Basic Import/Export System over TCP/IP*) qui utilise les ports suivants :

- **137**,
  - *Name Service* - La résolution des noms et le parcours du réseau (*Browsing*),
- **138**,
  - *Datagram Service*,
- **139**,
  - *Session Service* - Le partage de fichiers et d'imprimante.

Un nom NetBIOS est codé sur 16 octets dont les 15 premiers sont définis par l'utilisateur. Le dernier contient une valeur hexadécimale qui indique le type de ressource fournie par le système :

Valeur Hexadécimale	Type de Ressource
00	Standard Workstation
03	Messenger Service
06	RAS Server Service
21	RAS Client Service
1B	Domain Master Browser Service
1D	Master Browser Name
20	Fileserver et/ou Printserver
BE	Network Monitor Agent
BF	Network Monitor Utility

Les noms NetBIOS peuvent aussi être utilisés pour des noms de groupes :

Valeur Hexadécimale	Type de Ressource
00	Standard Workstation Group
1C	Logon Server
1D	Master Browser Name
1E	Normal Group Name

Important : Le nom NetBIOS ne doit pas contenir les charactères suivants : **“ / \ [ ] : ; | = , ^ * ? > <**

La commande Windows™ **NBTSTAT** peut être utilisée pour visualiser la liste des types de ressources et les noms NetBIOS :

```
C:\Documents and Settings\Administrateur>NBTSTAT -n

Connexion au réseau local:
Adresse IP du noeud : [192.168.1.29] ID d'étendue : []

                Table nom local NetBIOS
```

```
      Nom               Type         Statut
   -------------------------------------------
   WINDOWS-FFC9AFA<00>  UNIQUE      Inscrit
   WORKGROUP      <00>  Groupe      Inscrit
   WINDOWS-FFC9AFA<20>  UNIQUE      Inscrit
   WORKGROUP      <1E>  Groupe      Inscrit
```

Présentation de Samba

Le serveur Samba est en réalité un ensemble de programmes qui permettent le **partage de fichiers et d'imprimantes** entre un serveur Unix ou Linux et des stations **Windows™** (3.11, 9x, NT4, 2000, XP, Vista, 2003, Seven et 10) ainsi que des stations **OS/2** , **Linux** et **Mac**.

Le serveur Samba3 était capable offrir :

- des services classiques d'un serveur de fichiers et d'impression,
- l'authentification des utilisateurs,
- la gestion des droits d'accès,
- la résolution des noms,
- le parcours du voisinage réseau (*Local Master Browser*, *Local Backup Browser*, *Domain Master Browser*),
- les services d'un serveur **WINS** primaire,
- les services d'un serveur **PDC** (*Primary Domain Controller*),
- les services d'un serveur Microsoft™ **DFS** (*Distributed FileSystem*),

Le serveur Samba n'est **pas** capable d'offrir :

- les services d'un serveur **WINS** secondaire,
- les services d'un contrôleur de domaine Active Directory,
- les services d'un **BDC** - contrôleur secondaire de domaine (*Backup Domain Controller*) quand le PDC est un serveur Windows™.

Samba4 apporte les nouveautés suivantes :

- Support de l'authentification et de l'administration d'Active Directory,
- Support complet de NTFS,
- Annuaire LDAP,

- Serveur Kerberos,
- Serveur DNS,
- Support du nouveau protocole RPC et de Python.

Daemons Samba

Samba se repose sur trois **Daemons** (*Disk And Extension MONitor*) :

- **smbd** qui :
  - fournit les services de gestion des ressources partagées et les fonctionnalités d'authentification,
  - génère un processus fils pour chaque connexion active,
- **nmbd** qui :
  - participe à la fonctionnalité du parcours du voisinage réseau et fournit un serveur compatible Microsoft™ WINS,
  - génère une deuxième instance de lui-même dans le cas où Samba joue le rôle d'un serveur WINS,
- **winbindd** qui :
  - permet d'obtenir des informations sur les utilisateurs définis sur des contrôleurs de domaine Windows™ NT ou 2000,
  - facilite l'intégration d'un serveur Samba dans un domaine ayant déjà un PDC.

Commandes Samba

Samba propose un nombre important de commandes et utilitaires :

Commande	Description
findsmb	Obtention d'informations sur les systèmes utilisant le protocole SMB
net	Commande similaire à la commande Windows™ du même nom
nmblookup	Interrogation d'un serveur de noms NetBIOS
pdbedit	Gestion de comptes stockés dans une base de données SAM
rpcclient	Exécution de programmes d'administration sur des clients Windows™
smbcacls	Gestion des ACL
smbclient	Programme interactif multifonction
smbcontrol	Interrogations simples auprès des deamons

Commande	Description
smbmount	Montage des ressources SMB sous Linux
smbpasswd	Gestion des mots de passe
smbspool	Gestion des impressions
smbstatus	Etat des connexions
smbtar	Utilitaire de sauvegarde
smbumount	Démontage d'une ressource SMB sous Linux
swat	Utilitaire de configuration
testparm	Vérification du fichier de configuration
testprns	Vérification des informations sur les imprimantes
wbinfo	Interrogation du deamon winbindd

Installation de Samba

Désactivez SELINUX afin de ne pas avoir des erreurs de ce dernier :

```
[root@centos7 /]# setenforce permissive
[root@centos7 /]# getenforce
Permissive
```

Editez ensuite le fichier **/etc/sysconfig/selinux** ainsi :

```
[root@centos7 /]# vi /etc/sysconfig/selinux
[root@centos7 /]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
```

```
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Afin d'éviter les problèmes liés au pare-feu arrêtez le service firewalld :

```
[root@centos7 /]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2017-07-28 11:10:59 CEST; 42min ago
     Docs: man:firewalld(1)
 Main PID: 616 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─616 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Jul 28 11:10:52 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Jul 28 11:10:59 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
[root@centos7 /]# systemctl stop firewalld.service
[root@centos7 /]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed symlink /etc/systemd/system/basic.target.wants/firewalld.service.
[root@centos7 /]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)

Jul 28 11:10:52 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Jul 28 11:10:59 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Jul 28 11:54:00 centos7.fenestros.loc systemd[1]: Stopping firewalld - dynamic firewall daemon...
Jul 28 11:54:00 centos7.fenestros.loc systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

Modifiez ensuite le fichier **/etc/hosts** pour définir votre **hostname** et votre adresse IP :

```
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.51   centos7.fenestros.loc
```

Important : Modifiez l'adresse IP dans votre fichier **/etc/hosts** en fonction de **votre** adresse IP réelle.

Maintenant installez le paquet samba-swat :

```
[root@centos7 ~]# yum install samba-swat
Loaded plugins: fastestmirror, langpacks
adobe-linux-x86_64                                                      |
2.9 kB  00:00:00
base                                                                    |
3.6 kB  00:00:00
extras                                                                  |
3.4 kB  00:00:00
updates                                                                 |
3.4 kB  00:00:00
(1/3): adobe-linux-x86_64/primary_db                                    |
2.7 kB  00:00:00
(2/3): extras/7/x86_64/primary_db                                       |
191 kB  00:00:00
(3/3): updates/7/x86_64/primary_db                                      |
7.8 MB  00:00:47
Determining fastest mirrors
 * base: centos.mirrors.ovh.net
 * extras: mirrors.standaloneinstaller.com
 * updates: mirrors.standaloneinstaller.com
Resolving Dependencies
--> Running transaction check
```

```
---> Package samba.x86_64 0:4.4.4-14.el7_3 will be installed
--> Processing Dependency: samba-libs = 4.4.4-14.el7_3 for package: samba-4.4.4-14.el7_3.x86_64
--> Processing Dependency: samba-common-tools = 4.4.4-14.el7_3 for package: samba-4.4.4-14.el7_3.x86_64
--> Processing Dependency: samba-common-libs = 4.4.4-14.el7_3 for package: samba-4.4.4-14.el7_3.x86_64
--> Processing Dependency: samba-common = 4.4.4-14.el7_3 for package: samba-4.4.4-14.el7_3.x86_64
--> Processing Dependency: samba-client-libs = 4.4.4-14.el7_3 for package: samba-4.4.4-14.el7_3.x86_64
--> Processing Dependency: libwbclient = 4.4.4-14.el7_3 for package: samba-4.4.4-14.el7_3.x86_64
--> Running transaction check
---> Package libwbclient.x86_64 0:4.4.4-12.el7_3 will be updated
---> Package libwbclient.x86_64 0:4.4.4-14.el7_3 will be an update
---> Package samba-client-libs.x86_64 0:4.4.4-12.el7_3 will be updated
--> Processing Dependency: samba-client-libs = 4.4.4-12.el7_3 for package: samba-client-4.4.4-12.el7_3.x86_64
--> Processing Dependency: samba-client-libs = 4.4.4-12.el7_3 for package: libsmbclient-4.4.4-12.el7_3.x86_64
---> Package samba-client-libs.x86_64 0:4.4.4-14.el7_3 will be an update
---> Package samba-common.noarch 0:4.4.4-12.el7_3 will be updated
---> Package samba-common.noarch 0:4.4.4-14.el7_3 will be an update
---> Package samba-common-libs.x86_64 0:4.4.4-12.el7_3 will be updated
---> Package samba-common-libs.x86_64 0:4.4.4-14.el7_3 will be an update
---> Package samba-common-tools.x86_64 0:4.4.4-12.el7_3 will be updated
---> Package samba-common-tools.x86_64 0:4.4.4-14.el7_3 will be an update
---> Package samba-libs.x86_64 0:4.4.4-12.el7_3 will be updated
---> Package samba-libs.x86_64 0:4.4.4-14.el7_3 will be an update
--> Running transaction check
---> Package libsmbclient.x86_64 0:4.4.4-12.el7_3 will be updated
---> Package libsmbclient.x86_64 0:4.4.4-14.el7_3 will be an update
---> Package samba-client.x86_64 0:4.4.4-12.el7_3 will be updated
---> Package samba-client.x86_64 0:4.4.4-14.el7_3 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================
======================
 Package                                Arch                        Version                                 Repository
```

```
Size
================================================================================================================
======================
Installing:
 samba                                  x86_64                 4.4.4-14.el7_3                      updates
610 k
Updating for dependencies:
 libsmbclient                           x86_64                 4.4.4-14.el7_3                      updates
126 k
 libwbclient                            x86_64                 4.4.4-14.el7_3                      updates
100 k
 samba-client                           x86_64                 4.4.4-14.el7_3                      updates
547 k
 samba-client-libs                      x86_64                 4.4.4-14.el7_3                      updates
4.6 M
 samba-common                           noarch                 4.4.4-14.el7_3                      updates
191 k
 samba-common-libs                      x86_64                 4.4.4-14.el7_3                      updates
161 k
 samba-common-tools                     x86_64                 4.4.4-14.el7_3                      updates
451 k
 samba-libs                             x86_64                 4.4.4-14.el7_3                      updates
260 k

Transaction Summary
================================================================================================================
======================
Install  1 Package
Upgrade             ( 8 Dependent packages)

Total download size: 7.0 M
Is this ok [y/d/N]: y
```

Les paquets ainsi installés sont :

```
[root@centos7 ~]# rpm -qa | grep samba
samba-libs-4.4.4-14.el7_3.x86_64
samba-client-4.4.4-14.el7_3.x86_64
samba-client-libs-4.4.4-14.el7_3.x86_64
samba-common-tools-4.4.4-14.el7_3.x86_64
samba-common-4.4.4-14.el7_3.noarch
samba-4.4.4-14.el7_3.x86_64
samba-common-libs-4.4.4-14.el7_3.x86_64
```

Les deamons **smb** et **nmb** ne sont pas démarrés :

```
[root@centos7 ~]# systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@centos7 ~]# systemctl status nmb
● nmb.service - Samba NMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/nmb.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

Notez que le démarrage automatique de Samba n'est pas configuré. Configurez donc le démarrage automatique de Samba :

```
[root@centos7 ~]# systemctl enable smb
Created symlink from /etc/systemd/system/multi-user.target.wants/smb.service to
/usr/lib/systemd/system/smb.service.
[root@centos7 ~]# systemctl enable nmb
Created symlink from /etc/systemd/system/multi-user.target.wants/nmb.service to
/usr/lib/systemd/system/nmb.service.
```

Configuration de base

La configuration de Samba est obtenue en éditant le fichier **/etc/samba/smb.conf**. Lors de l'installation des paquets Samba, un fichier smb.conf

minimaliste est créé. Vérifiez ce fichier à l'aide de la commande **testparm** :

```
[root@centos7 ~]# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
    workgroup = SAMBA
    printcap name = cups
    security = USER
    idmap config * : backend = tdb
    cups options = raw


[homes]
    comment = Home Directories
    browseable = No
    inherit acls = Yes
    read only = No
    valid users = %S %D%w%S


[printers]
    comment = All Printers
    path = /var/tmp
    browseable = No
```

```
    printable = Yes
    create mask = 0600


[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    create mask = 0664
    directory mask = 0775
    write list = root
```

Démarrage manuel de Samba

Démarrez maintenant les daemons smb et nmb et constatez les processus ainsi créés :

```
[root@centos7 ~]# systemctl start smb
[root@centos7 ~]# systemctl start nmb
[root@centos7 ~]# systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2017-07-29 11:53:31 CEST; 11s ago
 Main PID: 6793 (smbd)
   Status: "smbd: ready to serve connections..."
   CGroup: /system.slice/smb.service
           ├─6793 /usr/sbin/smbd
           ├─6794 /usr/sbin/smbd
           ├─6795 /usr/sbin/smbd
           └─6796 /usr/sbin/smbd

Jul 29 11:53:31 centos7.fenestros.loc systemd[1]: Starting Samba SMB Daemon...
Jul 29 11:53:31 centos7.fenestros.loc smbd[6793]: [2017/07/29 11:53:31.692284,  0]
../lib/util/become_daemon.c:124(daemon_ready)
Jul 29 11:53:31 centos7.fenestros.loc systemd[1]: Started Samba SMB Daemon.
```

```
Jul 29 11:53:31 centos7.fenestros.loc smbd[6793]:   STATUS=daemon 'smbd' finished starting up and ready to serve
connections
[root@centos7 ~]# systemctl status nmb
● nmb.service - Samba NMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/nmb.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2017-07-29 11:53:36 CEST; 15s ago
 Main PID: 6825 (nmbd)
   Status: "nmbd: ready to serve connections..."
   CGroup: /system.slice/nmb.service
           └─6825 /usr/sbin/nmbd

Jul 29 11:53:36 centos7.fenestros.loc systemd[1]: Starting Samba NMB Daemon...
Jul 29 11:53:36 centos7.fenestros.loc nmbd[6825]: [2017/07/29 11:53:36.108613,  0]
../lib/util/become_daemon.c:124(daemon_ready)
Jul 29 11:53:36 centos7.fenestros.loc systemd[1]: Started Samba NMB Daemon.
Jul 29 11:53:36 centos7.fenestros.loc nmbd[6825]:   STATUS=daemon 'nmbd' finished starting up and ready to serve
connections

[root@centos7 ~]# ps aux | grep mb
root      6793  0.0  0.3 410660  6164 ?        Ss   11:53   0:00 /usr/sbin/smbd
root      6794  0.0  0.1 404480  2880 ?        S    11:53   0:00 /usr/sbin/smbd
root      6795  0.0  0.1 404472  2600 ?        S    11:53   0:00 /usr/sbin/smbd
root      6796  0.0  0.1 410668  3512 ?        S    11:53   0:00 /usr/sbin/smbd
root      6825  0.0  0.1 337320  2716 ?        Ss   11:53   0:00 /usr/sbin/nmbd
root      7296  0.0  0.0 112648   960 pts/0    R+   11:54   0:00 grep --color=auto mb
```

Testez ensuite le bon fonctionnement de Samba grâce à la commande **smbclient** :

```
[root@centos7 ~]# smbclient -U% -L localhost
Domain=[SAMBA] OS=[Windows 6.1] Server=[Samba 4.4.4]

    Sharename       Type      Comment
    ---------       ----      -------
    print$          Disk      Printer Drivers
```

```
    IPC$            IPC       IPC Service (Samba 4.4.4)
Domain=[SAMBA] OS=[Windows 6.1] Server=[Samba 4.4.4]

    Server               Comment
    ---------            -------
    CENTOS7              Samba 4.4.4

    Workgroup            Master
    ---------            -------
    SAMBA                CENTOS7
```

Les options de la commande smbclient sont nombreuses :

```
[root@centos7 ~]# smbclient --help
Usage: smbclient service <password>
  -R, --name-resolve=NAME-RESOLVE-ORDER     Use these name resolution services only
  -M, --message=HOST                        Send message
  -I, --ip-address=IP                       Use this IP to connect to
  -E, --stderr                              Write messages to stderr instead of stdout
  -L, --list=HOST                           Get a list of shares available on a host
  -m, --max-protocol=LEVEL                  Set the max protocol level
  -T, --tar=<c|x>IXFqgbNan                  Command line tar
  -D, --directory=DIR                       Start from directory
  -c, --command=STRING                      Execute semicolon separated commands
  -b, --send-buffer=BYTES                   Changes the transmit/send buffer
  -t, --timeout=SECONDS                     Changes the per-operation timeout
  -p, --port=PORT                           Port to connect to
  -g, --grepable                            Produce grepable output
  -B, --browse                              Browse SMB servers using DNS

Help options:
  -?, --help                                Show this help message
  --usage                                   Display brief usage message
```

```
Common samba options:
  -d, --debuglevel=DEBUGLEVEL               Set debug level
  -s, --configfile=CONFIGFILE               Use alternate configuration file
  -l, --log-basename=LOGFILEBASE            Base name for log files
  -V, --version                             Print version
  --option=name=value                       Set smb.conf option from command line

Connection options:
  -O, --socket-options=SOCKETOPTIONS        socket options to use
  -n, --netbiosname=NETBIOSNAME             Primary netbios name
  -W, --workgroup=WORKGROUP                 Set the workgroup name
  -i, --scope=SCOPE                         Use this Netbios scope

Authentication options:
  -U, --user=USERNAME                       Set the network username
  -N, --no-pass                             Don't ask for a password
  -k, --kerberos                            Use kerberos (active directory) authentication
  -A, --authentication-file=FILE            Get the credentials from a file
  -S, --signing=on|off|required             Set the client signing state
  -P, --machine-pass                        Use stored machine account password
  -e, --encrypt                             Encrypt SMB transport
  -C, --use-ccache                          Use the winbind ccache for authentication
  --pw-nt-hash                              The supplied password is the NT hash
```

Celles qui nous intéressent ici sont :

- **-U%**
  - sert à éviter une authentification avec mot de passe,
- **-L**
  - liste les ressources disponibles sur **localhost**.

Configuration de Samba

Gestion des comptes et des groupes

Vous allez maintenant créer le groupe **staff**, utilisé pour le partage **Public**:

```
[root@centos7 ~]# groupadd staff
```

Pour insérer des utilisateurs dans le groupe **staff**, ouvrez le fichier **/etc/group** et ajoutez tous les utilisateurs à qui vous souhaitez donner accès au partage public de samba au groupe staff.

```
[root@centos7 ~]# vi /etc/group
[root@centos7 ~]# cat /etc/group
root:x:0:
...
trainee:x:1000:trainee
vboxsf:x:983:
staff:x:1001:trainee
```

Faites la même procédure pour le fichier **/etc/gshadow** :

```
[root@centos7 ~]# vi /etc/gshadow
[root@centos7 ~]# cat /etc/gshadow
root:::
...
trainee:!!::trainee
vboxsf:!::
staff:!::trainee
```

Création du fichier smbpasswd

Afin de pouvoir permettre des connexions au serveur Samba, il faut créer le fichier **/var/lib/samba/private/smbpasswd** qui contiendra les utilisateurs autorisés.

En effet, le serveur Samba n'utilise pas le fichier de mots de passe de la machine Linux, à savoir le fichier **/etc/passwd**. Cependant, une fois le serveur Samba fonctionnel, nous pouvons stipuler que les deux fichiers soient synchronisés lors des modifications futures.

Modifiez la directive **passdb backend** du fichier **/etc/samba/smb.conf** afin d'utiliser le fichier **/var/lib/samba/private/smbpasswd** pour stocker les mots de passe samba :

```
[root@centos7 ~]# vi /etc/samba/smb.conf
[root@centos7 ~]# cat /etc/samba/smb.conf
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.

[global]
    workgroup = SAMBA
    security = user

    #passdb backend = tdbsam
    passdb backend = smbpasswd

    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw

[homes]
    comment = Home Directories
    valid users = %S, %D%w%S
    browseable = No
    read only = No
    inherit acls = Yes

[printers]
    comment = All Printers
```

```
    path = /var/tmp
    printable = Yes
    create mask = 0600
    browseable = No

[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = root
    create mask = 0664
    directory mask = 0775
```

Le système de stockage des mots de passe peut être un des suivants :

- smbpasswd - utilise un fichier. Par défaut: **/etc/samba/smbpasswd**,
- tdbsam - utilise une base de données de type Trivial Database. Par défaut : **/var/lib/samba/private/passdb.tdb**,
- ldapsam - utilise un URL vers un LDAP, Par défaut : **ldap://localhost**.

La Commande smbpasswd

Créez maintenant les mots de passe samba pour chaque utilisateur dans le fichier /var/lib/samba/private/smbpasswd :

```
[root@centos7 ~]# smbpasswd -a root
New SMB password:
Retype new SMB password:
startsmbfilepwent_internal: file /var/lib/samba/private/smbpasswd did not exist. File successfully created.
Added user root.
[root@centos7 ~]# smbpasswd -a trainee
New SMB password:
Retype new SMB password:
Added user trainee.
```

Consultez le fichier **/var/lib/samba/private/smbpasswd**. Vous devez constater une ligne pour chaque utilisateur. Chaque ligne doit comporter une chaîne de caractères alphanumérique :

```
[root@centos7 ~]# cat /var/lib/samba/private/smbpasswd
root:0:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:E183384163AA4BFFAF24CC678CF19EAB:[U          ]:LCT-597C6334:
trainee:1000:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:2A217A32BDE94A23B26A8EEA26C70874:[U          ]:LCT-597C6343:
```

Créez ensuite un lien symbolique :

```
[root@centos7 ~]# ln -s /var/lib/samba/private/smbpasswd /etc/samba/smbpasswd
```

La Commande pdbedit

La commande pdbedit est utilisée pour la gestion de la base de données de SAMBA. Par exemple pour lister les utilisateurs de SAMBA :

```
[root@centos7 ~]# pdbedit -L
root:0:root
trainee:1000:trainee
```

Pour créer un compte SAMBA, l'utilisateur doit d'abord posséder un compte Unix :

```
[root@centos7 ~]# useradd sambauser
```

Il est ensuite possible d'utiliser la commande pdbedit pour créer l'utilisateur dans la base de données de SAMBA :

```
[root@centos7 ~]# useradd sambauser
[root@centos7 ~]# pdbedit -a sambauser
new password:
retype new password:
Unix username:        sambauser
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-3392617607-4065925175-2212523533-3002
Primary Group SID:    S-1-5-21-3392617607-4065925175-2212523533-513
Full Name:
Home Directory:       \\centos7\sambauser
```

```
HomeDir Drive:
Logon Script:
Profile Path:         \\centos7\sambauser\profile
Domain:               CENTOS7
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          never
Kickoff time:         never
Password last set:    Tue, 15 Aug 2017 16:21:39 CEST
Password can change:  Tue, 15 Aug 2017 16:21:39 CEST
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Cette commande a donc ajouté l'utilisateur au fichier **/var/lib/samba/private/smbpasswd** :

```
[root@centos7 ~]# cat /var/lib/samba/private/smbpasswd
root:0:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:E183384163AA4BFFAF24CC678CF19EAB:[U          ]:LCT-5993021B:
trainee:1000:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:2A217A32BDE94A23B26A8EEA26C70874:[U          ]:LCT-5993022B:
sambauser:1001:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:C27F8C725297C4466C963B7F88906297:[U          ]:LCT-59930373:
```

Pour visualiser les informations d'un utilisateur SAMBA existant, il convient d'utiliser les options **-Lv** :

```
[root@centos7 ~]# pdbedit -Lv sambauser
Unix username:        sambauser
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-3392617607-4065925175-2212523533-3002
Primary Group SID:    S-1-5-21-3392617607-4065925175-2212523533-513
Full Name:
Home Directory:       \\centos7\sambauser
```

```
HomeDir Drive:
Logon Script:
Profile Path:         \\centos7\sambauser\profile
Domain:               CENTOS7
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          never
Kickoff time:         never
Password last set:    Tue, 15 Aug 2017 16:21:39 CEST
Password can change:  Tue, 15 Aug 2017 16:21:39 CEST
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

La commande peut aussi être utiliser pour supprimer un utilisateur SAMBA :

```
[root@centos7 ~]# pdbedit -x sambauser
[root@centos7 ~]# cat /var/lib/samba/private/smbpasswd
root:0:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:E183384163AA4BFFAF24CC678CF19EAB:[U          ]:LCT-5993021B:
trainee:1000:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:2A217A32BDE94A23B26A8EEA26C70874:[U          ]:LCT-5993022B:
[root@centos7 ~]# cat /etc/passwd | grep sambauser
sambauser:x:1001:1002::/home/sambauser:/bin/bash
```

Comprendre la structure du fichier de configuration smb.conf

Ayant maintenant créé un fichier smbpasswd, il est le moment de terminer la configuration de votre serveur Samba.

Cette configuration est dictée par un seul et unique fichier – **/etc/samba/smb.conf**.

Avant de faire des manipulations, veillez à sauvegarder votre fichier smb.conf actuel :

```
[root@centos7 ~]# cp /etc/samba/smb.conf /etc/samba/smb.old
```

Examinez le fichier smb.conf suivant ainsi que le tableau récapitulatif des paramètres :

```
# Example d'un fichier smb.conf pour des partages par ressources
# Toute ligne commencant par un # ou un ; est un commentaire et
# n'est pas prise en compte lors de la lecture de ce fichier par
# samba. N'oubliez pas de lancer la commande 'service smb restart'
# lors de chaque changement et enregistrement de ce fichier.

#====================== Section Globale ======================

[global]

# 1. Options du nom du serveur:
# Modifiez la ligne qui suit pour votre workgroup
workgroup = WORKGROUP
# Modifiez la ligne qui suit pour votre nom de machine. Par défaut sa valeur est la valeur de hostname
netbios name = Machine01
server string = Samba Server %v

# 2. Options d'impression :
printcap name = cups
load printers = yes
printing = cups

# 3. Options de journalisation :
log file = /var/log/samba/log.%m
max log size = 50
log level = 5

# 4. Options de sécurité :
# Modifiez la ligne qui suit pour votre adresse reseau
hosts allow = 192.168.1.  127.
```

```
hosts deny = all
security = user
passdb backend = smbpasswd
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
unix password sync = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
*passwd:*all*authentication*tokens*updated*successfully*

# 5. Options du reseau:
# Modifiez la ligne qui suit pour l'adresse IP de votre carte reseau
interfaces = 192.168.1.22/255.255.255.0
# Modifiez la ligne qui suit à l'adresse de diffussion de votre reseau
remote announce = 192.168.1.255

# 6.Options de resolutions de nom Netbios:
name resolve order = wins lmhosts bcast host
dns proxy = yes

# 7. Options de nommage de fichiers:
dos charset = 850
unix charset = ISO8859-1

#======================= Definitions des Partages ==============================

[homes]
comment = Repertoires Personnels
browseable = no
writable = yes

[public]
comment = Repertoire Public
path = /home/samba/public
```

```
write list = @staff
read list = @staff
writable = yes
guest ok = no
create mode = 0755
#Fin
```

Ce fichier est un exemple d'un smb.conf avec **security = user**. De cette façon chaque utilisateur ne verra que les partages auxquels il a un droit d'accès. En équivalence Windows™, ceci correspond à mettre en place un réseau poste-à-poste avec Windows™ NT4.0 Workstation.

Toute ligne commençant par **#** ou **;** est un commentaire et n'est pas prise en compte lors de la lecture du fichier par Samba. Le fichier est divisé en deux parties – la section **globale** et la section **partages**.

L'exemple de smb.conf ci-dessus établira un **niveau de sécurité par ressource**. Dans ce cas, un utilisateur verra toutes les ressources partagées sur le serveur Linux dans le Voisinage Réseau Windows, mais il n'aura accès qu'aux ressources pour lesquelles il existe une autorisation explicite pour lui.

Afin de comprendre les paramètres dans le fichier précédent, consultez le tableau suivant :

Paramètre	**Valeur Par Défaut**	**Description**
Workgroup =	s/o	Le nom du groupe de travail
Netbios name =	La valeur de hostname	Le nom NetBIOS du serveur
Server string =	s/o	La description du serveur
path =	s/o	Désigne le chemin du répertoire à partager
comment =	s/o	Désigne le nom du partage visible dans le voisinage réseau Windows
guest ok = yes	no	Si yes, le partage est en accès libre sans restrictions de mot de passe.
guest account =	nobody	Le nom du compte d'accès libre.
valid users =	tout utilisateur	Désigne une liste d'utilisateurs qui peuvent avoir accès à la ressource. La liste d'utilisateurs est séparé par des espaces. Chaque groupe commence avec @. Ex: **valid users = user1 user2 @groupe3**
printable = true	false	Partager un service d'impression
writeable = yes	no	Désigne si oui ou non le droit d'écriture est accordé dans le répertoire concerné.
write list =	tout utilisateur	Désigne la liste des utilisateurs qui peuvent écrire dans un répertoire.

Paramètre	Valeur Par Défaut	Description
read list =	tout utilisateur	Désigne la liste des utilisateurs qui peuvent lire dans un répertoire.
browseable =	yes	Désigne si oui ou non le partage sera visible par tous, y compris les utilisateurs non authentifiés.
create mode =	0744	Désigne les droits maximum accordés à un fichier créés dans le répertoire concerné.
create mask =	0744	Idem create mode =.
directory mode =	0755	Désigne les droits maximum accordés à un répertoire créé dans la ressource.
directory mask =	0755	Idem directory mode =.
force create mode	s/o	Désigne les droits accordés à un fichier créés dans le répertoire concerné.
force directory mode	s/o	Désigne les droits accordés à un répertoire créé dans la ressource.
force group =	s/o	Impose un groupe propriétaire pour tout fichier créé dans le répertoire.
hide dot files =	yes	Cache les fichiers cachés de Linux.
hosts allow =	toute station	Liste d'adresses IP ayant accès à une ressource.
hosts deny =	aucune	Liste d'adresses IP n'ayant pas accès à une ressource.
max connections =	0	Désigne un nombre de connections illimités à la ressource concernée. Sinon spécifiez un nombre maximum de connexions.
Log file = /chemin/log.%m	s/o	Désigne le chemin des logs. L'opérateur **%m** implique que chaque log aura le nom de la machine associé. Ex: log.station1, log.station2 etc.
max log size =	s/o	La taille est à définir en Ko. C'est la taille maximale du fichier log.
interfaces =	s/o	Désigne l'adresse IP de la carte réseau connecté au réseau Windows. A exprimer sous la forme **N° IP/N° sous-masque.**
remote announce =	s/o	L'adresse de Broadcast du réseau, ici le 192.168.1.255.

Notez que lors de chaque changement et enregistrement de ce fichier, il faut que smb relise le fichier.

Le fichier smb.conf utilise également des variables :

Variable	Description
%a	L'architecture du client (Samba, Windows 2000, Windows NT, Unknown
%I	L'adresse IP du client
%M	Le nom DNS du client
%m	Le nom NetBIOS du client

Variable	Description
%u	L'identité de l'utilisateur
%U	L'identité souhaité par l'utilisateur
%H	Le répertoire de connexion de l'utilisateur
%g	Le groupe principal de l'utilisateur
%S	Le nom du partage
%P	Le répertoire racine du partage
%d	Le PID du process courant
%h	Le nom DNS du serveur SAMBA
%L	Le nom NetBIOS du serveur SAMBA
%N	Idem %L
%v	La version de SAMBA
%T	La date et l'heure du système
%var	La valeur de la variable var

Créez donc le fichier smb.conf ci-dessous et placez-le dans le répertoire **/etc/samba**. Modifiez les directives **hosts allow**, **interfaces** et **remote announce** en fonction de votre adresse IP :

smb.conf

```
[global]
workgroup = WORKGROUP
netbios name = Machine01
server string = Samba Server %v
printcap name = cups
load printers = yes
printing = cups
log file = /var/log/samba/log.%m
max log size = 50
log level = 5
hosts allow = 192.168.1.  127.
hosts deny = all
security = user
```

```
passdb backend = smbpasswd
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
unix password sync = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
*passwd:*all*authentication*tokens*updated*successfully*
interfaces = 192.168.1.103/255.255.255.0
remote announce = 192.168.1.255
name resolve order = wins lmhosts bcast host
dns proxy = yes
dos charset = 850
unix charset = ISO8859-1

[homes]
comment = Repertoires Personnels
browseable = no
writable = yes

[public]
comment = Repertoire Public
path = /home/samba/public
write list = @staff
read list = @staff
writable = yes
guest ok = no
create mode = 0755
```

Rechargez le fichier de configuration smb.conf :

```
[root@centos7 ~]# systemctl reload smb
```

Créez maintenant le répertoire **/home/samba/public** :

```
[root@centos7 ~]# mkdir -p /home/samba/public
```

Ensuite, afin que chaque utilisateur puisse écrire dans le répertoire public mais supprimer uniquement ses propres fichiers et répertoires, il faut modifier les permissions pour le répertoire **/home/samba/public** :

```
[root@centos7 ~]# chmod 1777 /home/samba/public
```

Vous pouvez tester votre fichier **smb.conf** avec la commande **testparm** :

```
[root@centos7 ~]# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[public]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
    dos charset = 850
    interfaces = 192.168.1.103/255.255.255.0
    netbios name = MACHINE01
    server string = Samba Server %v
    unix charset = ISO8859-1
    log file = /var/log/samba/log.%m
    max log size = 50
    remote announce = 192.168.1.255
    printcap name = cups
    name resolve order = wins lmhosts bcast host
    passdb backend = smbpasswd
    passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
*passwd:*all*authentication*tokens*updated*successfully*
```

```
    passwd program = /usr/bin/passwd %u
    security = USER
    smb passwd file = /etc/samba/smbpasswd
    unix password sync = Yes
    idmap config * : backend = tdb
    hosts allow = 192.168.1. 127.
    hosts deny = all


[homes]
    comment = Repertoires Personnels
    browseable = No
    read only = No


[public]
    comment = Repertoire Public
    path = /home/samba/public
    create mask = 0755
    read list = @staff
    read only = No
    write list = @staff
```

LAB #2 - Tester Samba en tant que Serveur de Fichiers

Pour tester votre configuration :

- Consultez la section **Réseau** de l'**Explorateur de Fichiers** de la VM Windows10 (10.0.2.58) ,
- Identifiez la machine **MACHINE01**,
- Connectez-vous à la **MACHINE01** avec le compte **trainee/trainee**,
- Vérifiez que vous pouvez créer un fichier dans le partage du serveur samba appelé **public** ainsi que dans le partage du répertoire personnel de trainee.

Samba en tant que serveur membre d'un domaine

Notre but ici est de faire d'un serveur samba un serveur membre d'un domaine AD sur un serveur Windows™ 2008 Standard. La procédure a été également testée avec un serveur Windows™ 2008 r2 Enterprise.

Important : Demandez au formateur de restaurer le snapshot d'origine de votre CentOS7.

Désactivez SELINUX afin de ne pas avoir des erreurs de ce dernier :

```
[root@centos7 /]# setenforce permissive
[root@centos7 /]# getenforce
Permissive
```

Editez ensuite le fichier **/etc/sysconfig/selinux** ainsi :

```
[root@centos7 /]# vi /etc/sysconfig/selinux
[root@centos7 /]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Afin d'éviter les problèmes liés au pare-feu arrêtez le service firewalld :

```
[root@centos7 ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2017-07-30 14:03:15 CEST; 1min 38s ago
     Docs: man:firewalld(1)
 Main PID: 576 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─576 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Jul 30 14:03:08 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Jul 30 14:03:15 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
[root@centos7 ~]# systemctl stop firewalld.service
[root@centos7 ~]# systemctl disable firewalld.service
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed symlink /etc/systemd/system/basic.target.wants/firewalld.service.
[root@centos7 ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)

Jul 30 14:03:08 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Jul 30 14:03:15 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Jul 30 14:05:09 centos7.fenestros.loc systemd[1]: Stopping firewalld - dynamic firewall daemon...
Jul 30 14:05:10 centos7.fenestros.loc systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

Modifiez ensuite le fichier **/etc/hosts** pour définir votre **hostname** et votre adresse IP :

```
[root@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
```

```
10.0.2.51   centos7.fenestros.loc
```

Maintenant installez le paquet samba-swat :

```
[root@centos7 ~]# yum install samba-swat
Loaded plugins: fastestmirror, langpacks
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
adobe-linux-x86_64                                                                                  |
2.9 kB  00:00:00
base                                                                                                |
3.6 kB  00:00:00
extras                                                                                              |
3.4 kB  00:00:00
updates                                                                                             |
3.4 kB  00:00:00
(1/3): adobe-linux-x86_64/primary_db                                                                |
2.7 kB  00:00:00
(2/3): updates/7/x86_64/primary_db                                                                  |
7.8 MB  00:00:03
(3/3): extras/7/x86_64/primary_db                                                                   |
191 kB  00:00:03
Determining fastest mirrors
 * base: centos.crazyfrogs.org
 * extras: mirrors.ircam.fr
 * updates: mirrors.ircam.fr
Resolving Dependencies
--> Running transaction check
---> Package samba.x86_64 0:4.4.4-14.el7_3 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
======================
```

```
 Package                       Arch                          Version                                Repository
Size
================================================================================================================
======================
Installing:
 samba                         x86_64                        4.4.4-14.el7_3                         updates
610 k

Transaction Summary
================================================================================================================
======================
Install  1 Package

Total download size: 610 k
Installed size: 1.8 M
Is this ok [y/d/N]: y
```

Les paquets ainsi installés sont :

```
[root@centos7 ~]# rpm -qa | grep samba
samba-client-libs-4.4.4-14.el7_3.x86_64
samba-libs-4.4.4-14.el7_3.x86_64
samba-common-tools-4.4.4-14.el7_3.x86_64
samba-common-libs-4.4.4-14.el7_3.x86_64
samba-client-4.4.4-14.el7_3.x86_64
samba-common-4.4.4-14.el7_3.noarch
samba-4.4.4-14.el7_3.x86_64
```

Les deamons **smb** et **nmb** ne sont pas démarrés :

```
[root@centos7 ~]# systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

```
[root@centos7 ~]# systemctl status nmb
● nmb.service - Samba NMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/nmb.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

Notez que le démarrage automatique de Samba n'est pas configuré. Configurez donc le démarrage automatique de Samba :

```
[root@centos7 ~]# systemctl enable smb
Created symlink from /etc/systemd/system/multi-user.target.wants/smb.service to
/usr/lib/systemd/system/smb.service.
[root@centos7 ~]# systemctl enable nmb
Created symlink from /etc/systemd/system/multi-user.target.wants/nmb.service to
/usr/lib/systemd/system/nmb.service.
```

Vérifiez que votre samba a été compilé avec le support pour **LDAP**, **Kerberos**, **AD** et **Winbind** :

```
[root@centos7 ~]# /usr/sbin/smbd -b | grep LDAP
   HAVE_LDAP_H
   HAVE_LDAP
   HAVE_LDAP_ADD_RESULT_ENTRY
   HAVE_LDAP_INIT
   HAVE_LDAP_INITIALIZE
   HAVE_LDAP_INIT_FD
   HAVE_LDAP_OPT_SOCKBUF
   HAVE_LDAP_SASL_WRAPPING
   HAVE_LDAP_SET_REBIND_PROC
   HAVE_LIBLDAP
   LDAP_DEPRECATED
   LDAP_SET_REBIND_PROC_ARGS
[root@centos7 ~]# /usr/sbin/smbd -b | grep KRB
   HAVE_GSSAPI_GSSAPI_KRB5_H
   HAVE_KRB5_H
   HAVE_KRB5_LOCATE_PLUGIN_H
   HAVE_ADDRTYPE_IN_KRB5_ADDRESS
```

```
HAVE_DECL_KRB5_AUTH_CON_SET_REQ_CKSUMTYPE
HAVE_DECL_KRB5_GET_CREDENTIALS_FOR_USER
HAVE_GSSKRB5_EXTRACT_AUTHZ_DATA_FROM_SEC_CONTEXT
HAVE_GSS_KRB5_CRED_NO_CI_FLAGS_X
HAVE_GSS_KRB5_EXPORT_LUCID_SEC_CONTEXT
HAVE_GSS_KRB5_IMPORT_CRED
HAVE_GSS_MECH_KRB5
HAVE_INITIALIZE_KRB5_ERROR_TABLE
HAVE_KRB5
HAVE_KRB5_AUTH_CON_SETUSERUSERKEY
HAVE_KRB5_AUTH_CON_SET_REQ_CKSUMTYPE
HAVE_KRB5_BUILD_PRINCIPAL_ALLOC_VA
HAVE_KRB5_CC_RETRIEVE_CRED
HAVE_KRB5_C_MAKE_CHECKSUM
HAVE_KRB5_C_STRING_TO_KEY
HAVE_KRB5_C_VERIFY_CHECKSUM
HAVE_KRB5_DEPRECATED_WITH_IDENTIFIER
HAVE_KRB5_ENCRYPT_BLOCK
HAVE_KRB5_ENCTYPE_TO_STRING
HAVE_KRB5_ENCTYPE_TO_STRING_WITH_SIZE_T_ARG
HAVE_KRB5_FREE_CHECKSUM_CONTENTS
HAVE_KRB5_FREE_DATA_CONTENTS
HAVE_KRB5_FREE_HOST_REALM
HAVE_KRB5_FREE_KEYTAB_ENTRY_CONTENTS
HAVE_KRB5_FREE_UNPARSED_NAME
HAVE_KRB5_FWD_TGT_CREDS
HAVE_KRB5_GET_CREDENTIALS_FOR_USER
HAVE_KRB5_GET_HOST_REALM
HAVE_KRB5_GET_INIT_CREDS_KEYTAB
HAVE_KRB5_GET_INIT_CREDS_OPT_ALLOC
HAVE_KRB5_GET_INIT_CREDS_OPT_FREE
HAVE_KRB5_GET_PERMITTED_ENCTYPES
HAVE_KRB5_GET_PROFILE
HAVE_KRB5_GET_PROMPT_TYPES
```

```
   HAVE_KRB5_GET_RENEWED_CREDS
   HAVE_KRB5_KEYTAB_ENTRY_KEY
   HAVE_KRB5_KEYUSAGE_APP_DATA_CKSUM
   HAVE_KRB5_KT_FREE_ENTRY
   HAVE_KRB5_MK_REQ_EXTENDED
   HAVE_KRB5_PRINCIPAL2SALT
   HAVE_KRB5_PRINCIPAL_COMPARE_ANY_REALM
   HAVE_KRB5_PRINC_COMPONENT
   HAVE_KRB5_PRINC_REALM
   HAVE_KRB5_SET_DEFAULT_TGS_ENCTYPES
   HAVE_KRB5_SET_DEFAULT_TGS_KTYPES
   HAVE_MAGIC_IN_KRB5_ADDRESS
   HAVE_TICKET_POINTER_IN_KRB5_AP_REQ
   KRB5_CREDS_OPT_FREE_REQUIRES_CONTEXT
   USING_SYSTEM_KRB5
[root@centos7 ~]# /usr/sbin/smbd -b | grep ADS
   WITH_ADS
[root@centos7 ~]# /usr/sbin/smbd -b | grep WINBIND
   WITH_WINBIND
```

Windows Server 2008

La machine virtuelle Windows™ Server 2008 a été configurée de la façon suivante :

- FQDN : server.fenestros.loc
- DOMAINE : fenestros.loc
- IP : 10.0.2.200/24
- MDP : Fenestr0$
- ROLES **DEJA** AJOUTES : **Gestion des identités pour Unix** (Gestionnaire de Serveur > Développez Rôles > Clic droit sur Services de domaine Active Directory > Ajouter des Services de Rôle > Gestion des Identités pour Unix > Installer)

LAB #2 - Samba en tant que serveur membre d'un domaine

Obtenir un ticket Kerberos pour le serveur Linux

Dans la machine virtuelle CentOS 7, éditez le fichier **/etc/krb5.conf** :

```
[root@centos7 ~]# vi /etc/krb5.conf
[root@centos7 ~]# cat /etc/krb5.conf

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

[libdefaults]
 default_realm = FENESTROS.LOC
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = yes

[realms]
 FENESTROS.LOC = {
  kdc = server.fenestros.loc:88
  admin_server = server.fenestros.loc:749
  default_domain = fenestros.loc
 }

[domain_realm]
 .fenestros.loc = FENESTROS.LOC
 fenestros.loc = FENESTROS.LOC
```

```
[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Important - Les directives **kdc** et **admin_server** dans la secion **[realms]** doivent être modifiées par rapport au FQDN de votre serveur Windows ™ 2008. Pour plus d'information sur le fichier **/etc/krb5.conf**, consultez le manuel **krb5.conf**.

Éditez ensuite le fichier **/etc/hosts** afin d'établir la correspondance entre l'**adresse IP** du serveur Windows™ et son **FQDN** :

```
[root@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.5    centos7.fenestros.loc
10.0.2.200  server.fenestros.loc
```

Important : La dernière ligne de ce fichier doit être modifiée en fonction du FQDN et de l'adresse IP de votre serveur Windows™ 2008.

Testez ensuite la connexion au domaine afin d'obtenir un ticket (ou jeton) kerberos :

```
[root@centos7 ~]# kinit Administrateur
```

```
Password for Administrateur@FENESTROS.LOC: Fenestr0$
```

> **Important** - La commande **kinit** sert à obtenir et mettre en cache un ticket (ou jeton) kerberos. Pour plus d'informations concernant la commande **kinit**, consultez la page du manuel : **man kinit**.

Visualisez ensuite le ticket :

```
[root@centos7 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrateur@FENESTROS.LOC

Valid starting     Expires            Service principal
30/07/17 14:58:54  31/07/17 00:58:54  krbtgt/FENESTROS.LOC@FENESTROS.LOC
    renew until 06/08/17 14:58:50
```

> **Important** - La commande **klist** sert à afficher les tickets (ou jetons) kerberos dans le cache. Pour plus d'informations concernant la commande **klist**, consultez la page du manuel : **man klist**.

Configuration de samba

Éditez ensuite le fichier **/etc/samba/smb.conf** :

```
[root@centos7 ~]# vi /etc/samba/smb.conf
[root@centos7 ~]# cat /etc/samba/smb.conf
[global]
```

```
workgroup = FENESTROS
realm = FENESTROS.LOC
preferred master = no
server string = Serveur Samba
security = ADS
encrypt passwords = yes
log level = 3
log file = /var/log/samba/%m
max log size = 50
interfaces = 127.0.0.1 enp0s3
bind interfaces only = true
winbind separator = @
idmap config *:backend = tdb
idmap config *:range = 40001-75000
idmap config FENESTROS:backend = idmap_rid:FENESTROS= 40001-75000
idmap config FENESTROS:schema_mode = rfc2307
idmap config FENESTROS:range = 500-40000
```

Les directives les plus importantes dans ce fichier sont :

- **realm = FENESTROS.LOC** - cette directive définit le nom du domaine Windows™,
- **winbind separator = @** - cette directive sert à définir le séparateur du nom du domaine et de l'utilisateur lors de la connexion (p.e. DOMAIN@utilisateur),
- **idmap config *:backend = tdb** - cette directive spécifie le plugin idmap utilisé pour gérer le stockage des correspondances SID/uid/gid. Dans ce cas, une base de données Trivial Data Base,
- **idmap config *:range = 40001-75000** - cette directive indique la plage de numéros UID & GID Linux que les utilisateurs du domaine Windows™ utiliseront,
- **idmap gid = 10000-25000** - cette directive indique la plage de numéros GID Linux que les utilisateurs du domaine Windows™ utiliseront.
- **idmap config FENESTROS:backend = idmap_rid:FENESTROS=10000-25000** - cette directive est nécessaire pour permettre samba de procéder à la création d'une cartographie des équivalences entre les SID de Windows™ et les UID et GID d'UNIX.

Ajoutez ensuite la ligne suivante à votre fichier **/etc/security/limits.conf** :

```
*               -       nofile          16384
```

Cette modification est nécessaire pour les clients Windows™ 7. L'étoile représente une entrée par défaut. Le mot clef **nofile** indique le nombre de fichiers maximum ouverts dont la valeur est fixée à **16384**. Cette valeur est en effet celle des serveurs Windows™. Sans cette modification la commande **testparm** retourne une ligne du type :

```
rlimit_max: rlimit_max (8192) below minimum Windows limit (16384)
```

ou

```
rlimit_max: rlimit_max (1024) below minimum Windows limit (16384)
```

En fait, le serveur samba modifie la valeur automatiquement pour éviter des erreurs **out of handles** lors de certaines opérations de copie de fichiers par les clients Windows™ 7. Cependant, il est conseillé de faire la modification comme même.

Vous obtiendrez alors :

```
[root@centos7 ~]# vi /etc/security/limits.conf
[root@centos7 ~]# cat /etc/security/limits.conf
# /etc/security/limits.conf
#
#This file sets the resource limits for the users logged in via PAM.
#It does not affect resource limits of the system services.
#
#Also note that configuration files in /etc/security/limits.d directory,
#which are read in alphabetical order, override the settings in this
#file in case the domain is the same or more specific.
#That means for example that setting a limit for wildcard domain here
#can be overriden with a wildcard setting in a config file in the
#subdirectory, but a user specific setting here can be overriden only
#with a user specific setting in the subdirectory.
#
#Each line describes a limit for a user in the form:
#
#<domain>        <type>  <item>  <value>
#
```

```
#Where:
#<domain> can be:
#        - a user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
#        - the wildcard %, can be also used with %group syntax,
#                for maxlogin limit
#
#<type> can have the two values:
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#        - core - limits the core file size (KB)
#        - data - max data size (KB)
#        - fsize - maximum filesize (KB)
#        - memlock - max locked-in-memory address space (KB)
#        - nofile - max number of open file descriptors
#        - rss - max resident set size (KB)
#        - stack - max stack size (KB)
#        - cpu - max CPU time (MIN)
#        - nproc - max number of processes
#        - as - address space limit (KB)
#        - maxlogins - max number of logins for this user
#        - maxsyslogins - max number of logins on the system
#        - priority - the priority to run user process with
#        - locks - max number of file locks the user can hold
#        - sigpending - max number of pending signals
#        - msgqueue - max memory used by POSIX message queues (bytes)
#        - nice - max nice priority allowed to raise to values: [-20, 19]
#        - rtprio - max realtime priority
#
#<domain>      <type>  <item>         <value>
#
```

```
#*               soft    core            0
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#@student        -       maxlogins       4
*                -       nofile          16384

# End of file
```

Vérifiez votre fichier smb.conf :

```
[root@centos7 ~]# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions

# Global parameters
[global]
    bind interfaces only = Yes
    interfaces = 127.0.0.1 enp0s3
    realm = FENESTROS.LOC
    server string = Serveur Samba
    workgroup = FENESTROS
    preferred master = No
    log file = /var/log/samba/%m
    max log size = 50
    security = ADS
    winbind separator = @
    idmap config fenestros:range = 500-40000
```

```
    idmap config fenestros:schema_mode = rfc2307
    idmap config fenestros:backend = idmap_rid:FENESTROS= 40001-75000
    idmap config *:range = 40001-75000
    idmap config * : backend = tdb
```

Démarrez le service samba :

```
[root@centos7 ~]# systemctl start smb
```

Mettre le serveur Samba dans le domaine

Mettez le serveur samba dans le domaine :

```
[root@centos7 ~]# net rpc join -S SERVEUR_FQDN -I SERVEUR_IP -U administrateur%SERVEUR_MDP [Entrée]
```

Par exemple :

```
[root@centos7 ~]# net rpc join -S server.fenestros.loc -I 10.0.2.200 -U administrateur
Enter administrateur's password:Fenestr0$
Using short domain name -- FENESTROS
Joined 'CENTOS7' to realm 'fenestros.loc'
```

Arrêtez ensuite le serveur samba :

```
[root@centos7 ~]# systemctl stop smb
```

Modifier le fichier /etc/nsswitch.conf

Faire une sauvegarde de votre fichier **/etc/nsswitch.conf** :

```
[root@centos7 ~]# cp /etc/nsswitch.conf /etc/nsswitch.conf.old
```

Editez ensuite le fichier **/etc/nsswitch.conf** et modifiez uniquement les lignes suivantes :

nsswitch.conf

```
passwd:      compat winbind
group:           compat winbind
shadow:      compat
hosts:           files dns wins
networks:    files dns
protocols:   db files
services:    db files
ethers:      db files
rpc:             db files
```

```
[root@centos7 ~]# vi /etc/nsswitch.conf
[root@centos7 ~]# cat /etc/nsswitch.conf
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Valid entries include:
#
#   nisplus            Use NIS+ (NIS version 3)
#   nis             Use NIS (NIS version 2), also called YP
#   dns             Use DNS (Domain Name Service)
```

```
#   files            Use the local files
#   db            Use the local database (.db) files
#   compat            Use NIS on compat mode
#   hesiod            Use Hesiod for user lookups
#   [NOTFOUND=return]    Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:      compat winbind
group:       compat winbind
shadow:      compat

#passwd:     files sss
#shadow:     files sss
#group:      files sss
#initgroups: files

#hosts:     db files nisplus nis dns
#hosts:      files dns myhostname

hosts:       files dns wins

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
```

```
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

networks:    files dns
protocols:   db files
services:    db files
ethers:      db files
rpc:             db files

#ethers:     files
netmasks:   files
#networks:   files
#protocols:  files
#rpc:        files
#services:   files sss

netgroup:   files sss

publickey:  nisplus

automount:  files sss
aliases:    files nisplus
```

Vérifier les service winbind

Installez le service winbind ainsi que les clients :

```
[root@centos7 ~]# yum install samba-winbind samba-winbind-clients
```

Démarrez ensuite le service winbind :

```
[root@centos7 ~]# systemctl status winbind
● winbind.service - Samba Winbind Daemon
   Loaded: loaded (/usr/lib/systemd/system/winbind.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@centos7 ~]# systemctl enable winbind
Created symlink from /etc/systemd/system/multi-user.target.wants/winbind.service to
/usr/lib/systemd/system/winbind.service.
[root@centos7 ~]# systemctl start winbind
[root@centos7 ~]# systemctl status winbind
● winbind.service - Samba Winbind Daemon
   Loaded: loaded (/usr/lib/systemd/system/winbind.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2017-07-30 15:20:58 CEST; 2s ago
 Main PID: 8619 (winbindd)
   Status: "winbindd: ready to serve connections..."
   CGroup: /system.slice/winbind.service
           ├─8619 /usr/sbin/winbindd
           └─8620 /usr/sbin/winbindd

Jul 30 15:20:57 centos7.fenestros.loc systemd[1]: Starting Samba Winbind Daemon...
Jul 30 15:20:58 centos7.fenestros.loc winbindd[8619]: [2017/07/30 15:20:58.167888,  0]
../source3/winbindd/winbindd_cache.c:32...cache)
Jul 30 15:20:58 centos7.fenestros.loc winbindd[8619]:   initialize_winbindd_cache: clearing cache and re-creating
with version number 2
Jul 30 15:20:58 centos7.fenestros.loc winbindd[8619]: [2017/07/30 15:20:58.174374,  0]
../lib/util/become_daemon.c:124(daemon_ready)
Jul 30 15:20:58 centos7.fenestros.loc systemd[1]: Started Samba Winbind Daemon.
Jul 30 15:20:58 centos7.fenestros.loc winbindd[8619]:   STATUS=daemon 'winbindd' finished starting up and ready
to serve connections
Jul 30 15:20:58 centos7.fenestros.loc winbindd[8620]: [2017/07/30 15:20:58.221519,  0]
../source3/libsmb/cliconnect.c:1895(cli..._send)
Jul 30 15:20:58 centos7.fenestros.loc winbindd[8620]:   Kinit for FENESTROS.LOC to access
cifs/server.fenestros.loc@FENESTROS....tabase
Hint: Some lines were ellipsized, use -l to show in full.
```

Ainsi que le service samba :

```
[root@centos7 ~]# systemctl start smb
```

Vérifiez ensuite que le service winbind fonctionne en interrogeant le serveur 2008 :

```
[root@centos7 ~]# wbinfo -u
FENESTROS@administrateur
FENESTROS@invité
FENESTROS@krbtgt
[root@centos7 ~]# wbinfo -g
FENESTROS@ordinateurs du domaine
FENESTROS@contrôleurs de domaine
FENESTROS@administrateurs du schéma
FENESTROS@administrateurs de l’entreprise
FENESTROS@éditeurs de certificats
FENESTROS@admins du domaine
FENESTROS@utilisateurs du domaine
FENESTROS@invités du domaine
FENESTROS@propriétaires créateurs de la stratégie de groupe
FENESTROS@serveurs ras et ias
FENESTROS@groupe de réplication dont le mot de passe rodc est autorisé
FENESTROS@groupe de réplication dont le mot de passe rodc est refusé
FENESTROS@contrôleurs de domaine en lecture seule
FENESTROS@contrôleurs de domaine d’entreprise en lecture seule
FENESTROS@dnsadmins
FENESTROS@dnsupdateproxy
```

Dernièrement, renseignez-vous sur le serveur 2008 :

```
[root@centos7 ~]# net ads info
LDAP server: 10.0.2.200
LDAP server name: server.fenestros.loc
Realm: FENESTROS.LOC
```

```
Bind Path: dc=FENESTROS,dc=LOC
LDAP port: 389
Server time: Sun, 30 Jul 2017 15:24:49 CEST
KDC server: 10.0.2.200
Server time offset: 0
Last machine account password change: Sun, 30 Jul 2017 15:12:07 CEST
```

Terminer la configuration de samba

Modifiez maintenant votre fichier **/etc/samba/smb.conf** :

smb.conf

```
[global]
workgroup = FENESTROS
password server = server.fenestros.loc
realm = FENESTROS.LOC
security = ADS
idmap config *:backend = tdb
idmap config *:range = 10000-50000
idmap config FENESTROS:backend = idmap_rid:FENESTROS=10000-50000
idmap config FENESTROS:schema_mode = rfc2307
idmap config FENESTROS:range = 500-40000
winbind separator = @
template homedir = /home/%D/%U
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = true
local master = no
preferred master = no
os level = 0
server string = Serveur Samba
encrypt passwords = yes
```

```
log level = 3
log file = /var/log/samba/%m
max log size = 50
interfaces = 127.0.0.1 enp0s3
bind interfaces only = true
winbind cache time = 15
winbind enum users = yes
winbind enum groups = yes
winbind nss info = rfc2307
obey pam restrictions = yes
allow trusted domains = no
```

Les directives les plus importantes dans ce fichier sont :

- **template homedir = /home/%D/%U** - cette directive stipule que les utilisateurs du domaine auront leurs répertoires personnels créé dans **/home/FENESTROS**,
- **winbind use default domain = true** - cette directive permet aux utilisateurs d'omettre le nom du domaine lors de leur connexion,
- **winbind offline logon = true** - cette directive permet aux utilisateurs de se connecter au serveur Linux même quand ils ne sont pas connectés au domaine. Les coordonnées de connexion de l'utilisateur sont stockés dans le fichier **winbindd_cache.tdb**. Il est important de noter que dans certaines distributions, si le service winbind est redémarré, le cache n'est pas persistant et l'utilisateur sera rejeté,
- **winbind cache time = 15** - cette directive stipule le nombre de secondes que les coordonnées de connexion des utilisateurs sont stockés localement avant que winbind les re-demande au serveur de domaine,
- **winbind enum users = yes** et **winbind enum groups = yes** - ces directives permettent l'utilisation des fonctions **NSS getpwent** et **getgrent** afin d'énumérer la liste des utilisateurs et groupes du domaine. Ces fonctions sont considérés d'être très inefficaces et ont été remplacées par les fonctions **getpwnam( )** et **getgrnam( )**. La raison de la présence de ces deux directives est d'assurer la compatibilité avec des vielles versions de logiciels tiers. Si vous n'en avez pas besoin, il est recommandé de les configurer en **no**. A noter que les commandes **wbinfo -u** et **wbinfo -g** ne dépendent pas de NSS et fonctionneront toujours.

Redémarrez les services winbind et samba :

```
[root@centos7 ~]# systemctl restart winbind
[root@centos7 ~]# systemctl restart smb
```

Vérifiez maintenant que les mots de passe sont authentifiés par le serveur Windows™ 2008 :

```
[root@centos7 ~]# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:998:996:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
colord:x:996:993:User for colord:/var/lib/colord:/sbin/nologin
libstoragemgmt:x:995:992:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
setroubleshoot:x:994:991::/var/lib/setroubleshoot:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
chrony:x:993:990::/var/lib/chrony:/sbin/nologin
unbound:x:992:989:Unbound DNS resolver:/etc/unbound:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
geoclue:x:991:988:User for geoclue:/var/lib/geoclue:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
sssd:x:990:987:User for sssd:/:/sbin/nologin
```

```
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:989:984::/run/gnome-initial-setup/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
trainee:x:1000:1000:trainee:/home/trainee:/bin/bash
vboxadd:x:988:1::/var/run/vboxadd:/bin/false
administrateur:*:40003:40006:Administrateur:/home/FENESTROS/administrateur:/bin/bash
invité:*:40001:40005:Invité:/home/FENESTROS/invité:/bin/bash
krbtgt:*:40002:40006:krbtgt:/home/FENESTROS/krbtgt:/bin/bash
```

Créez maintenant le répertoire **/home/FENESTROS** qui sera utilisé pour contenir les répertoires personnels des utilisateurs de l'AD :

```
[root@centos7 ~]# mkdir /home/FENESTROS
```

Accordez le permissions adéquates :

```
[root@centos7 ~]# chmod 777 /home/FENESTROS
```

Modifier PAM

Ajoutez la ligne suivante au fichier **/etc/pam.d/system-auth** :

```
session     required      pam_oddjob_mkhomedir.so skel=/etc/skel/ umask=0022
```

pam_oddjob_mkhomedir est utilisé par le système afin de créer le répertoire personnel d'un utilisateur autorisé si le répertoire n'existe pas. Si le répertoire personnel n'existe pas et **pam_oddjob_mkhomedir** ne fonctionne pas, la connexion de l'utilisateur sera rejeté.

Vous obtiendrez :

```
[root@centos7 ~]# vi /etc/pam.d/system-auth
[root@centos7 ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     required      pam_oddjob_mkhomedir.so skel=/etc/skel/ umask=0022
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

Redémarrez le service **winbind** et démarrez le service **oddjobd** :

```
[root@centos7 ~]# systemctl restart winbind
[root@centos7 ~]# systemctl status oddjobd
● oddjobd.service - privileged operations for unprivileged applications
```

```
   Loaded: loaded (/usr/lib/systemd/system/oddjobd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@centos7 ~]# systemctl enable oddjobd
Created symlink from /etc/systemd/system/multi-user.target.wants/oddjobd.service to
/usr/lib/systemd/system/oddjobd.service.
[root@centos7 ~]# systemctl start oddjobd
[root@centos7 ~]# systemctl status oddjobd
● oddjobd.service - privileged operations for unprivileged applications
   Loaded: loaded (/usr/lib/systemd/system/oddjobd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2017-07-31 13:45:56 CEST; 10s ago
 Main PID: 28054 (oddjobd)
   CGroup: /system.slice/oddjobd.service
           └─28054 /usr/sbin/oddjobd -n -p /var/run/oddjobd.pid -t 300

Jul 31 13:45:56 centos7.fenestros.loc systemd[1]: Started privileged operations for unprivileged applications.
Jul 31 13:45:56 centos7.fenestros.loc systemd[1]: Starting privileged operations for unprivileged applications...
```
