FORMATUX - Support de cours GNU/Linux

Les services et la sécurité sur CentOS 6

Version 1

17-04-2017

Table des matières

Préface

Table des matières

GNU/Linux est un **système d'exploitation** libre fonctionnant sur la base d'un **noyau Linux**, également appelé **kernel Linux**.

Linux est une implémentation libre du système **UNIX** et respecte les spécifications **POSIX**.

GNU/Linux est généralement distribué dans un ensemble cohérent de logiciels, assemblés autour du noyau Linux et prêt à être installé. Cet ensemble porte le nom de "**Distribution**".

- La plus ancienne des distributions est la distribution **Slackware**.
- Les plus connues et utilisées sont les distributions **Debian**, **Redhat** et **Arch**, et servent de base pour d'autres distributions comme **Ubuntu**, **CentOS**, **Fedora**, **Mageia** ou **Manjaro**.

Chaque distribution présente des particularités et peut être développée pour répondre à des besoins très précis :

- services d'infrastructure ;
- pare-feu ;
- serveur multimédia ;
- serveur de stockage ;
- etc.

La distribution présentée dans ces pages est la CentOS, qui est le pendant gratuit de la distribution RedHat. La distribution CentOS est particulièrement adaptée pour un usage sur des serveurs d'entreprises.

1. Crédits

Ce support de cours a été rédigé par les formateurs :

- Patrick Finet ;
- Antoine Le Morvan ;
- Xavier Sauvignon ;

2. Licence

3. Gestion des versions

Tableau 1. Historique des versions du document

Version	Date	Observations
1.0	Avril 2017	Version initiale.

1

Serveur de noms DNS - Bind

Le DNS (Domain Name System) est un système de résolution de nom.

Il s'agit d'une base de données distribuée hiérarchique, dont la racine est symbolisée par un « . ».

L'interrogation de cette base se fait selon le principe de client-serveur.

L'URL www.formatux.lan est appelée FQDN (Fully Qualified Domain Name).

Une table de correspondances permet la traduction d'un FQDN en informations de plusieurs types qui y sont associées, comme par exemple son adresse IP.

1.1. Généralités

Il existe 13 serveurs racines répartis dans le monde, dont une majorité se situe en Amérique du Nord.

La traduction d'un FQDN en adresse IP est le cas que l'on rencontre le plus fréquemment mais DNS permet également de renseigner le système sur les serveurs de messagerie, sur les services disponibles, de faire des alias de noms de service, etc.

Par exemple, il est possible de proposer un FQDN smtp.domain.tld sans qu'il y ait réellement de serveur nommé SMTP.

La résolution est possible en IPv4 comme en IPv6.

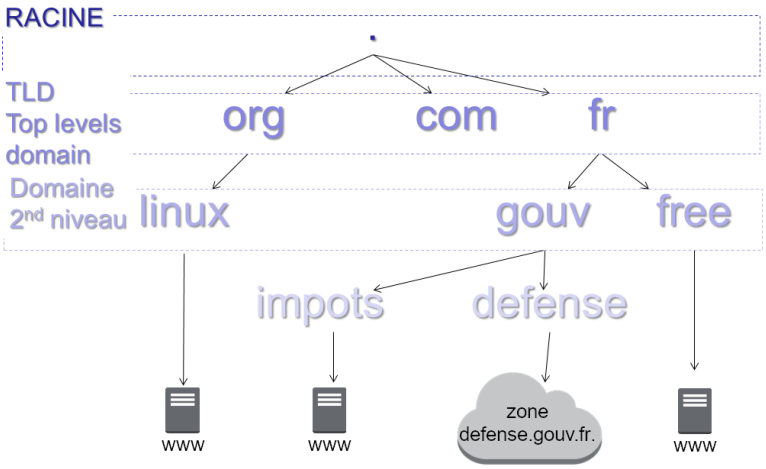


Figure 1.1. Principe de fonctionnement du DNS

Les Top Levels Domain TLD sont gérés par des organismes bien défini. Les Registars se chargent pour les clients d'enregistrer les noms de domaine auprès de ces organismes.

Le dialogue se fait en général via le protocole UDP (User Datagram Protocol) mais parfois aussi en TCP sur le port 53.

BIND (Berkeley Internet Name Daemon) est un serveur DNS populaire tournant sur système UNIX / Linux.

Bind est disponible sur les serveurs RedHat :

- RHEL 5 : Version 9.3
- RHEL 6 : Version 9.8
- RHEL 7 : Version 9.9

Le protocole peut aussi être utilisé en TCP (connecté) dans certains cas : transferts vers le ou les serveurs secondaires, requêtes dont la réponse est supérieure à la taille d'un paquet UDP, etc.

1.2. Installation du service

Le serveur DNS BIND s'articule autour du service named.

Installation à partir d'un dépôt YUM :

```
[root]# yum install bind
```

L'installation du service BIND ajoute un utilisateur named. Cet utilisateur sera le propriétaire des fichiers de configuration.

```
[root]# grep named /etc/passwd
named:x:25:25:Named:/var/named:/sbin/nologin
```

BIND étant un service réseau, il faut le paramétrer pour un démarrage dans les niveaux 3 et 5, puis le démarrer :

```
[root]# chkconfig --level 35 named on
[root]# service named start
```

Il peut être utile d'installer le paquet bind-utils pour disposer d'outils de test DNS.

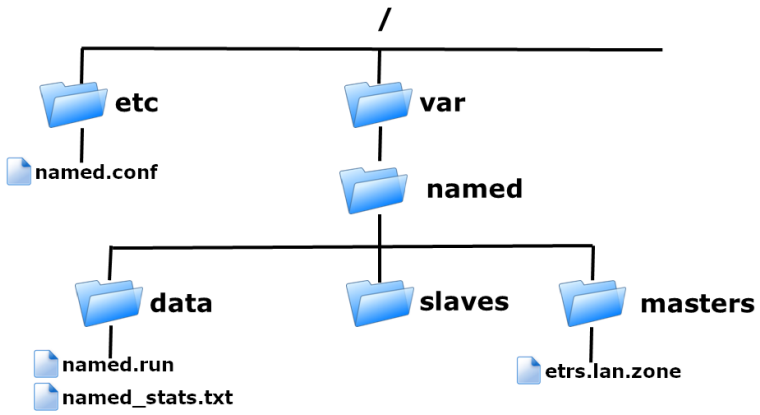


Figure 1.2. Arborescence du service Bind

Le dossier /var/named/masters n'est pas créé par défaut. Il faudra le créer et ne pas oublier d'y attribuer les droits à l'utilisateur named.

Le fichier de statistiques est généré par la commande rdnc (voir en fin de chapitre).

En environnement de production, les logs des requêtes clientes seront séparés des logs du service lui-même.

1.2.1. Cache DNS

Par défaut, Bind est configuré pour faire office de serveur de proxy-cache DNS (mandataire). Un serveur proxy, ou mandataire, effectue une requête réseau au nom d'un client.

Lorsqu'il résoud pour la première fois une requête DNS, la réponse est stockée dans son cache pour la durée de son TTL (Time To Live) restant. Si le même enregistrement est à nouveau demandé par un autre client DNS, le traitement de la requête sera plus rapide, puisque la réponse sera disponible depuis le cache du serveur.

Chaque enregistrement DNS dispose d'un TTL lorsqu'il est fourni par le serveur qui fait autorité pour la zone. Ce TTL est décrémenté jusqu'à la fin de sa validité. Il est ensuite supprimé des caches.

Lorsque l'enregistrement est mis en cache, le TTL qui lui est associé est le TTL restant.

1.2.2. Récursivité

Un serveur est configuré par défaut pour répondre de manière récursive aux requêtes de ses clients.

Il interroge tour à tour les serveurs DNS nécessaires à la résolution d'une requête jusqu'à obtenir la réponse.

Un serveur non-récursif déléguera la résolution du nom DNS à un autre serveur DNS.

Dans quel cadre utiliser un serveur non-récursif ?

Lorsque la latence entre le serveur DNS et le reste du réseau est trop forte, ou quand le débit est limité, il peut être intéressant de configurer un serveur DNS en non-récursif.

Ce sera par exemple le cas pour un théâtre d'opération ou un élément mobile d'une force.

Le serveur DNS local fera autorité sur la zone locale, mais déléguera la résolution des FQDN de l'intradef à un serveur en métropole, qui lui, prendra la requête en charge de manière récursive.

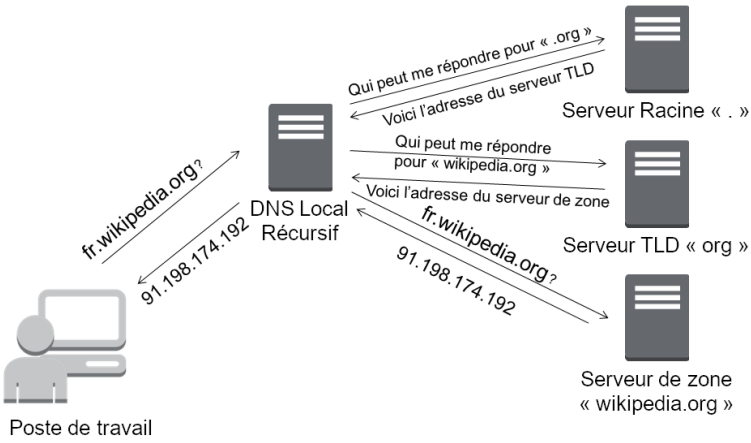


Figure 1.3. Le mode récursif

1.2.3. Architecture DNS

Un serveur DNS principal dispose d'une copie en écriture de la zone.

Il peut être intéressant de ne le rendre accessible que depuis le domaine local, et ne permettre l'interrogation des DNS depuis l'extérieur que vers les serveurs secondaires. D'un point de vue architectural cela lui évite ainsi les attaques ou les surcharges.

Le serveur est alors appelé serveur furtif.

Un serveur DNS n'est pas nécessairement le serveur maître de toutes les zones pour lesquels il fait autorité.

Un serveur DNS peut très bien être configurer pour être maître d'une zone et esclave d'une autre.

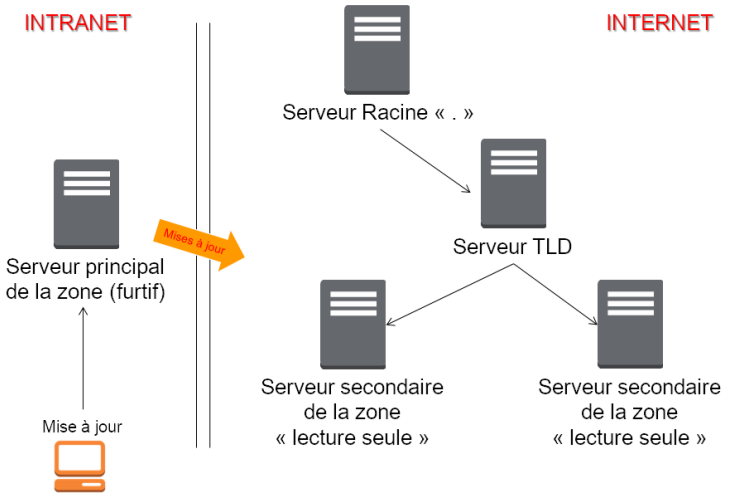


Figure 1.4. Architecture avec serveur furtif

La mise à jour du serveur se fait depuis le réseau local. Le serveur principal n'est pas accessible depuis l'extérieur.

La mise à jour se propage vers les serveurs secondaires.

L'interrogation par les clients internet ne se fait que sur les serveurs secondaires, ce qui protège le serveur principal des attaques par déni de service.

Pour un réseau complexe, il existe de nombreuses solutions architecturales de l'infrastructure DNS qu'il est important de bien étudier.

1.3. Configuration du serveur

1.3.1. Le fichier /etc/named.conf

Ce fichier contient les paramètres de configuration du service DNS.

```
[root]# less /etc/named.conf
options {
    listen-on port 53 { 192.168.1.200; };
 directory "/var/named";
 allow-query { 192.168.1.0/24; };
};
```

Chaque ligne du fichier /etc/named.conf (même à l'intérieur des accolades) se termine par un point-virgule.

L'oublie de ce ";" est l'erreur la plus fréquente dans la configuration d'un serveur Bind.

Les noms, sous la forme FQDN (Fully Qualified Domain Name) doivent se terminer par ".". En l'absence de ce ".", Bind suffixera automatiquement avec le nom de domaine l'enregistrement.

Eg : www.formatux.lan → www.formatux.lan.formatux.lan.

La rubrique options contient la configuration générale du serveur BIND via différentes directives :

- listen-on : Définit l'interface, l'adresse et le port du service sur le serveur.
- directory : Définit le répertoire de travail de BIND, contenant les fichiers de zone.
- allow-query : Définit les hôtes autorisés à faire des requêtes sur le serveur. Par adresse IP ou réseau.

Permettre qu'un serveur DNS résolve les requêtes de n'importe quel client est une très mauvaise idée. Il faut au moins restreindre les droits aux réseaux locaux.

Il est possible, pour cela, de créer des ACL pour simplifier l'administration du fichier de configuration.

Le fichier de configuration contient également les informations relatives aux fichiers de zone.

```
[root]# less /etc/named.conf
zone "formatux.lan" IN {
 type master;
 file "masters/formatux.lan.direct";
 allow-update { 192.168.1.0/24; };
};

zone "1.168.192.in-addr.arpa" IN {
 type master;
```

```
 file "masters/formatux.lan.inverse";
};
```

Les rubriques **zone** contiennent les configurations des zones de résolution de nom, inverses ou directes :

- type : Définit le type de serveur pour cette zone :
  - maître : possède la base de données en écriture
  - esclave : possède la base en lecture seule
  - forwarder : fait office de proxy-cache pour cette zone.
- file : Définit le chemin du fichier de zone.
- allow-update : Définit les hôtes ayant l'autorisation de mettre à jour les enregistrements DNS.

Les fichiers de zone inverse sont nommés en prenant l'adresse réseau de la zone (en inversant les octets) suivi du domaine in-addr.arpa.

1.3.2. Les rôles

Un serveur peut avoir le rôle de maître pour la zone, c'est-à-dire qu'il possède la zone en écriture.

```
[root]# less /etc/named.conf
zone "formatux.lan" IN {
 type master;
 file "masters/formatux.lan.direct";
 allow-update { 192.168.1.0/24; };
};
```

Seuls les clients figurant dans la variable allow-update pourront mettre à jour la base de données du DNS.

Un serveur peut également être un serveur secondaire (slave) pour la zone, c'est-à-dire qu'il possède la zone en lecture.

```
[root]# less /etc/named.conf
zone "formatux.lan" IN {
```

```
    type slave;
    file "slaves/formatux.lan.direct";
};
```

Un serveur peut enfin être expéditeur (forwarder) pour la zone, c'est-à-dire qu'il a connaissance de cette zone, et relaie les informations pour celle-ci.

```
[root]# less /etc/named.conf
zone "unautredomaine.fr" IN {
 type forwarder;
 forwarders {221.10.12.1};
};
```

Vous retrouverez cette notion sous Windows en tant que « redirecteur ».

1.4. Fichiers de zone

Les fichiers présents dans le répertoire /var/named doivent appartenir à l'utilisateur système named.

SELinux ne permettra pas l'enregistrement des fichiers de zone en dehors de ce répertoire.

Ces fichiers contiennent des enregistrements (RR : Resource Records) DNS de différents types. Ils permettent la résolution directe de noms (du nom vers l'adresse IP), ou la résolution inverse (de l'adresse IP vers le nom).

En plus de contenir les adresses IP et les noms des machines, les fichiers contiennent les paramètres de durée de vie des enregistrements (Time To Live, TTL).

Lorsqu'un enregistrement DNS est mis en cache, le temps restant sur son TTL est également conservé. À la fin du TTL, l'enregistrement est supprimé des caches.

- Un TTL plus long réduit les échanges DNS.
- Un TTL plus court permet une reconfiguration du réseau plus rapide.

1.4.1. Les types d'enregistrements

Tableau 1.1. Les types d'enregistrements

Type	Description
A	Nom attribué à une adresse de type IP V4
AAAA	Nom attribué à une adresse de type IP V6
CNAME	Alias d'un enregistrement A déjà défini **Éviter de faire un alias vers un alias**
MX	Serveur de messagerie destinataire pour la zone concernée
NS	Le ou les serveurs de noms de la zone (type A)
PTR	Enregistrement pointeur pour une zone inverse
SOA	Démarre la configuration (cf: diapos suivantes)
SVR	Service (protocole jabber,…)
TXT	Informations

- Champ MX : Le numéro précise la priorité, la plus faible étant la plus prioritaire. Ceci permet de définir un ou plusieurs serveurs de secours qui stockeront les mails en attendant le retour du serveur principal.
- Champ de type A : Enregistrement standard. Attribue un nom à une adresse IP.

Plusieurs enregistrements identiques de type A vers des adresses différentes permet de faire de l'équilibrage de charge par round-robin (RR).

Exemple :

```
mail A 192.168.1.10
     A 192.168.1.11
```

- Champ AAAA : On utilise quatre A pour symboliser IPv6 car une adresse IPv6 est codée sur 16 octets, soit 4 fois plus qu'une adresse IPv4.
- CNAME : Permet d'attribuer un ou plusieurs alias à un enregistrement A déjà défini. Plusieurs enregistrements du même alias permettent également de faire de l'équilibrage de charge type RR.

On trouvera des enregistrements typiques, comme autoconfig, qui permet le mécanisme de configuration automatique d'un client de messagerie.

1.4.2. Fichier de zone directe

Ce fichier est nécessaire au fonctionnement du système DNS. C'est par lui que se fait la résolution d'un nom en adresse IP.

```
[root]# less /var/named/formatux.lan.direct
$ORIGIN .
$TTL 3600
formatux.lan.  SOA  inf1-formatux.formatux.lan. contact.formatux.lan.
 (123; 14400; 3600; 604800; 3600; )

@      IN NS   inf1-formatux.formatux.lan.
poste1    IN A    192.168.1.10
inf1-formatux IN A    192.168.1.200
formatux.lan. MX 10   192.168.1.201
inf3-formatux IN A    192.168.1.202
www    IN CNAME inf1-formatux.formatux.lan.
```

- $ORIGIN : Définit la valeur par défaut du domaine courant pour les renseignements du fichier. Un . signifie la racine.
- $TTL : Durée de vie par défaut des enregistrements de la zone dans le cache, exprimée en secondes. Le TTL peut également être précisé enregistrement par enregistrement.
- SOA : Start Of Authority. La ligne démarre la configuration d'une zone. Définit :
  - le nom du serveur maître principal,
  - l'email de l'administrateur de la zone (un . remplace le @ de l'adresse mail).
  - Entre parenthèses, le numéro de série du fichier (incrémenté à chaque mise à jour) et les délais de mise à jour ou de rafraîchissement, exprimés en secondes.
    - Numéro de zone : Numéro incrémental (voir le paragraphe suivant)
    - Rafraîchissement : Durée en secondes avant une tentative de synchronisation avec le serveur maître

- Réitération : Intervalle de temps avant réitération si l'essai précédent n'a pas fonctionné
- Expiration : Durée en secondes avant l'expiration car le serveur maître est injoignable
- Cache négatif (TTL) : Durée de vie en secondes des enregistrements

Le @ a une signification particulière pour Bind. Il se représente lui même, raison pour laquelle le @ de l'adresse courriel d'administration est remplacée par un .

Le numéro de la zone sert à identifier la dernière modification du DNS maître. Tous les serveurs secondaires utilisent ce numéro pour savoir s'ils doivent se synchroniser.

Il existe deux méthodes d'incrémentation du numéro de zone :

- Incrémentale : 1, puis 2, puis 3 (pourquoi pas ?)
- Basée sur la date : AAAAMMJJXX, qui nous donne par exemple, pour la première modification du jour : 2017210101 (méthode à privilégier)

1.4.3. Le fichier de zone inverse

Bien que non obligatoire, ce fichier est fortement conseillé pour un fonctionnement optimal du système DNS. C'est par lui que se fait la résolution d'une adresse IP en nom.

Des services comme SSH s'appuie sur la résolution inverse.

```
[root]# more /var/named/formatux.lan.inverse
$ORIGIN 1.168.192.in-addr.arpa.
$TTL 259200
@    SOA inf1-formatux.formatux.lan. contact.formatux.lan.
 ( 123; 14400; 3600; 604800; 3600; )
@    NS  inf1-formatux.formatux.lan.
1 0   PTR  poste1.formatux.lan.
200  PTR  inf1-formatux.formatux.lan.
```

1.4.4. La commande nsupdate

L'usage de la commande nsupdate est exclusive. Il ne faut plus modifier les fichiers de zone manuellement, sous peine de pertes d'informations.

Syntaxe :

```
nsupdate
```

Exemple:

```
[root]# nsupdate
  > server 192.168.1.200
  > zone formatux.lan
  > update add poste2.formatux.lan 3600 A 192.168.1.11
  > update delete poste1
  > send
```

La commande nsupdate est interactive.

À la saisie, elle ouvre un prompt dans lequel il faut saisir les requêtes de mise à jour du fichier de zone.

Ces requêtes peuvent être :

- **server** : Précise le serveur BIND pour lequel les requêtes seront envoyées.
- **zone** : Précise la zone de résolution pour laquelle les requêtes seront envoyées.
- **prereq yxdomain nom** : L'existence de l'enregistrement nom est une condition de mise à jour.
- **update add nom TTL type @IP** : Ajoute l'enregistrement nom, en précisant son type, son adresse IP et son TTL.
- **update delete nom** : Supprime l'enregistrement nom.
- **send** : Valide et envoie les requêtes.

1.4.5. La commande rndc

La commande **rndc** permet de manipuler le serveur DNS à chaud.

Syntaxe de la commande rndc.

```
rndc reload
rndc querylog on|off
```

- **reload** : Prend en compte les modifications apportées sans devoir relancer le service
- **querylog** : Active ou non la journalisation

Après modification d'un fichier de zone, il est nécessaire de faire prendre en compte les modifications au service. Les fichiers étant lus au démarrage du service, cela permet de prendre en compte les modifications, mais résulte en la perte des statistiques. Il faut donc privilégier la méthode reload.

1.4.6. Le suivi des logs

La fonction d'enregistrement des fichiers journaux est activée ou désactivée par la commande rndc.

Le fichier de logs est par défaut /var/named/data/named.run

Exemple :

```
[root]# rndc querylog on
[root]# tail –f /var/named/data/named.run
```

Bind propose dans son fichier de configuration des options pour journaliser les informations :

- de transferts,
- de requêtes clients,
- d'erreurs,
- …

1.5. Configuration du client

NetworkManager est un outil de gestion du réseau. Sur un serveur dont le réseau est défini par cet outil, la configuration cliente de Bind est décrite dans le fichier de l'interface.

```
[root]#less /etc/sysconfig/network-scripts/ifcfg-ethX
DOMAIN="formatux.lan"
DNS1=192.168.1.200
DNS2=192.168.1.201
```

NetworkManager modifiera lui-même le fichier /etc/resolv.conf à chaque relance du service réseau.

Avant de lancer une recherche DNS, le logiciel client vérifiera si la requête porte sur un FQDN ou non. Si le nom n'est pas pleinement qualifié, le client suffixera la requête avec le premier suffixe DNS fourni.

Si la résolution est impossible, le client émettra une nouvelle requête avec le suffixe suivant, ainsi de suite jusqu'à l'obtention d'une réponse.

Par exemple, il est possible de fournir deux suffixes :

```
formatux.fr
formatux.lan
```

Lors d'une requête DNS portant sur, par exemple, portail, une première requête portail.formatux.fr sera faite. En l'absence de réponse positive, une seconde requête sera effectuée portant sur portail.formatux.lan. Pour éviter ce phénomène d'interrogation multiple, il est préférable de fournir une adresse pleinement qualifiée.

Veiller à spécifier au moins deux serveurs DNS pour assurer une redondance en cas de panne du serveur principal.

Sans outil de gestion du réseau, la configuration cliente de Bind est décrite dans le fichier /etc/resolv.conf.

```
[root]# less /etc/resolv.conf
search "formatux.lan"
nameserver 192.168.1.200
nameserver 192.168.1.201
```

NetworkManager, si actif, écrasera les valeurs entrées manuellement dans ce fichier.

L'utilitaire **system-config-network-tui** (**nmtui** sous CentOS 7) permet une configuration graphique correcte du réseau par une interface ncurse.

1.5.1. La commande dig

La commande dig (Domain Information Groper) permet d'interroger des serveurs DNS.

Dig doit être privilégié par rapport à NSLookup qui n'est plus maintenue.

Syntaxe de la commande dig.

```
dig [name] [type] [options]
```

Exemple :

```
[root]# dig centos65.formatux.lan A
…
;; QUESTION SECTION:
; centos65.formatux.lan. IN A

;; ANSWER SECTION:
centos65.formatux.lan. 86400 IN A 192.168.253.131

;; AUTHORITY SECTION:
formatux.lan.  86400 IN NS centos65.formatux.lan.
…
```

```
[root]# dig -t MX linux.fr
```

```
[root]# dig linux.fr MX +short
```

1.5.2. Mise en cache côté client

Le service NSCD est responsable de la mise en cache des requêtes réseaux type LDAP ou DNS.

Pour profiter de la mise en cache local, il faudra veiller à ce que le service NSCD soit démarré.

```
[root]# service nscd start
[root]# chkconfig nscd on
```

Nscd n'est pas installé par défaut sur les RHEL 6.

1.5.3. Mise à jour dynamique

Les clients peuvent s'enregistrer dynamiquement sur le serveur DNS, ce qui est intéressant dans le cadre d'une attribution de l'adressage IP dynamique avec DHCP.

1.6. Configuration du pare-feu serveur

Les règles iptables a configurer en tcp et udp sont les suivantes :

```
[root]# vi /etc/sysconfig/iptables
# Autoriser DNS
iptables –t filter –A INPUT –p tcp –dport 53 –j ACCEPT
iptables –t filter –A INPUT –p udp –dport 53 –j ACCEPT
```

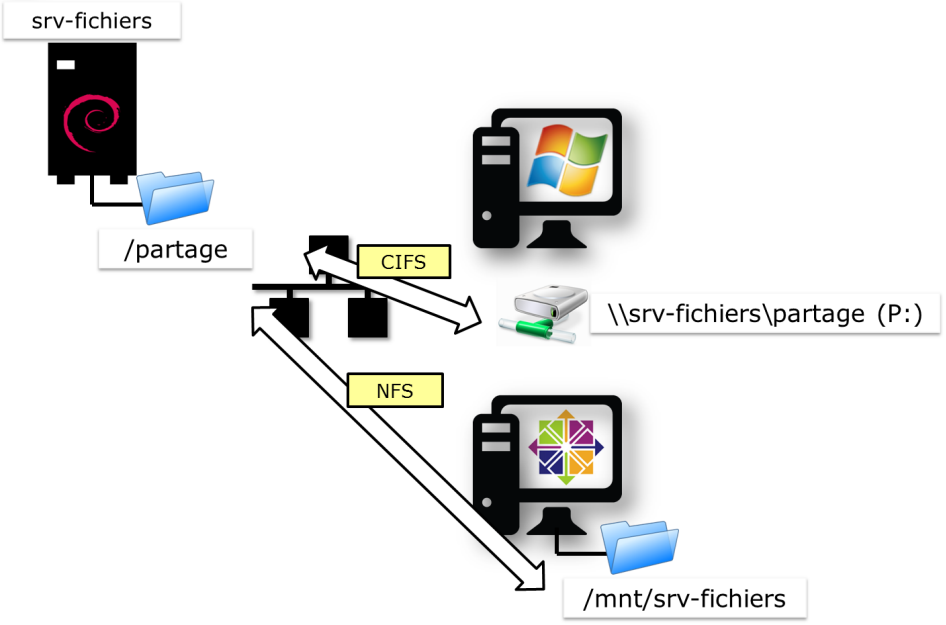
system-config-firewall-tui est l'outil graphique permettant de configurer le pare-feu.

2

Serveur de fichiers Samba

Samba est un serveur de fichiers permettant l'interopérabilité entre divers systèmes, notamment les systèmes Linux et Microsoft. Il permet à des systèmes Linux de créer des partages utilisables par des machines Windows et vice-versa.

Le projet Samba a été initié dès 1992 sous licence GPL (et donc gratuit).



Un même dossier partagé par NFS et par Samba est ainsi accessible depuis toutes les plateformes clientes.

2.1. Le protocole SMB

Le protocole SMB (Server Message Block) était une extension de Microsoft pour permettre la redirection des entrées/sorties vers NetBIOS (Network Basic Input/Output System).

SMB permettait :

- le transfert de données entre machines Windows : partages de fichiers, impressions et messagerie électronique ;
- le parcours du voisinage réseau (browsing) ;
- la résolution de noms NetBIOS en adresses IP (Windows Internet Name Server) ;
- l'authentification centralisée (notion de domaine).

Le protocole NetBIOS était une interface permettant la mise en place de noms de machines, de groupes de travail, de domaines, etc. Il faisait fonctionner le voisinage réseau jusqu'à Windows 2000, mais son mode de fonctionnement induisait une charge réseau importante.

NetBIOS était le système de noms des réseaux SMB comme l'est aujourd'hui le service DNS.

Les diffusions NetBIOS ne passant pas les routeurs, la notion de voisinage réseau désigne l'ensemble des stations de travail utilisant le protocole NetBIOS sur un même segment de réseau IP. Le **maître explorateur** (master browser) est le poste client ou serveur tenant à jour la liste des ordinateurs utilisés par le service de voisinage réseau.

2.2. Le protocole CIFS

Les améliorations apportées au protocole SMB ont permis de faire aboutir la suite de protocoles clients/serveurs CIFS (Common Internet File System) que le service Samba implémente.

2.3. Installation de Samba

```
[root]# yum install samba smbclient
```

La partie serveur de Samba est basée essentiellement sur 2 démons :

- Le démon **smb** est le serveur SMB : il répond aux requêtes des clients lorsque ceux-ci accèdent aux partages définis et il est le seul à accéder aux systèmes de fichiers Linux.
- Le démon **nmb** est le serveur de noms NetBIOS essentiel au fonctionnement de SMB. Il peut être configuré comme serveur WINS.
- Le fichier de configuration principal est **smb.conf**. C'est dans ce fichier que sont définis les paramètres de fonctionnement des 2 démons, ainsi que la définition des exports de ressources.

La partie cliente de samba (samba-client) contient les outils qui permettent le montage et le parcours des ressources Samba.

Le paquet **samba-client** fournit les binaires :

- **findsmb** : afficher de nombreuses informations sur les stations d'un sous-réseau qui répondent aux requêtes de noms SMB.
- **nmblookup** : interroger le protocole NetBIOS et associe les noms Netbios à des adresses IP.
- **sharesec** : manipuler les droits de partages de fichiers
- **smbcacls** : manipuler les ACL NT sur les partages de fichiers
- **smbclient** : offrir une interface FTP Like pour accèder à des partages de fichiers
- **smbget** : télécharger des fichiers depuis un partage windows
- **smbspool** : envoyer une impression à un serveur d'impression
- **smbtree** : fournir un explorateur de fichier en mode texte similaire au "Voisinage réseau" des ordinateurs Windows. Il affiche un arbre des domaines connus, desserveurs et des partages accessibles depuis les serveurs.
- …

Le paquet **samba-common** fournit les binaires :

- **net** : offrir les mêmes fonctionnalités que la commande net du monde Windows.

- **pdbedit** : gérer de la base SAM
- **smbcquotas** : manipuler les quotas NT d'un partage de fichiers
- **smbpasswd** : changer le mot de passe des utilisateurs
- **testparm** : tester la syntaxe d'un fichier de configuration smb.conf
- …

```
[root]# chkconfig smb on
[root]# chkconfig nmb on
[root]# service smb start
[root]# service nmb start
```

2.4. Sécurité SELinux

Par défaut, la sécurité SELinux est active. Pour vérifier le contexte de sécurité en place sur des fichiers, il faut utiliser la commande :

```
[root]# ls -Zd /export/
```

Le contexte de sécurité *samba_share_t* doit être positionné sur les dossiers partagés :

```
[root]# chcon -R -t samba_share_t /export/
```

Plus d'information sur la sécurité SELinux et Samba sur le site de RedHat[1]. Pensez à stopper le parefeu ou à le configurer dans le fichier **/etc/sysconfig/iptables** :

```
-A INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 139 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 445 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
```

[1] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Confined_Services/sect-Managing_Confined_Services-Samba-Booleans.html

Pour pouvoir utiliser Samba comme contrôleur de domaine et utiliser les commandes useradd et groupadd, il faudra mettre le booléen **samba_domain_controller** à on.

```
[root]# setsebool -P samba_domain_controller on
```

Pour rappel, il est possible d'obtenir tous les booléens SELinux concernant Samba avec la commande suivante :

```
[root]# getsebool -a | grep "samba"
samba_create_home_dirs --> off
samba_domain_controller --> off
samba_enable_home_dirs --> off
samba_export_all_ro --> off
samba_export_all_rw --> off
samba_portmapper --> off
samba_run_unconfined --> off
samba_share_fusefs --> off
samba_share_nfs --> off
sanlock_use_samba --> off
use_samba_home_dirs --> off
virt_use_samba --> off
```

Pour autoriser les partages via Samba des répertoires de connexions des utilisateurs, il faudra positionner le booléen **samba_enable_home_dirs** également à on.

```
[root]# setsebool -P samba_enable_home_dirs on
```

2.5. La configuration de SAMBA

La partie serveur de Samba est basée sur 1 seul fichier de configuration **/etc/samba/smb.conf** qui définit les paramètres de fonctionnement des 2 démons et des exports de ressources.

Chaque paramètre fait l'objet d'une ligne au format :

```
nom = valeur
```

Les commentaires commencent par un '**;**' ou un '**#**' et se termine à la fin de la ligne.

Le caractère '****' permet de scinder une ligne logique sur plusieurs lignes physiques.

Ce fichier est constitué de 3 sections spéciales :

- **[global]** : paramètres généraux ;
- **[homes]** : paramètres des répertoires utilisateurs ;
- **[printers]** : paramètres des imprimantes.

Les autres sections, déclarées entre '**[ ]**' sont des déclarations de partage.

2.5.1. Les niveaux de sécurité

Il existe cinq niveaux de sécurité (option security), mais un seul peut être appliqué par serveur :

- **share** : le niveau dit de partage, lié à une ressource. Un mot de passe est associé à chaque partage (Déprécié : ne plus utiliser) ;
- **user** : le niveau de sécurité de l'utilisateur, lié à son authentification. C'est le niveau recommandé et par défaut ;
- **server** : l'authentification est réalisée par un autre serveur (Déprécié : ne plus utiliser) ;
- **domain** : l'authentification est réalisée par un autre serveur, mais le serveur Samba doit être membre du domaine ;
- **ads** : l'authentification est réalisée par un serveur Active Directory.

2.5.2. Les variables internes à Samba

Tableau 2.1. Les variables internes à Samba

Variable	Observation
%a	Architecture du client
%I	Adresse IP du client
%M	Nom dns du client
%m	Nom NetBios du client

Variable	Observation
%u	Identité de l'utilisateur pour le partage concerné
%U	Identité souhaitée par l'utilisateur du partage
%H	Répertoire de connexion de l'utilisateur
%u%g ou %G	Groupe principal de l'utilisateur
%u ou %U %S	Nom du partage
%P	Répertoire racine du partage concerné
%d	PID du processus courant
%h	Nom DNS du serveur Samba
%L	Nom NetBIOS du serveur Samba
%v	Version de samba
%T	Date et heure système
%$var	valeur de la variable d'environnement var

2.5.3. La commande testparm

La commande **testparm** teste la validité du fichier /etc/samba/smb.conf.

L'option -v affiche tous les paramètres applicables.

```
[root]# testparm
Load smb config files from /etc/samba/smb.conf
...
Loaded services file OK.
Server role : ROLE_STANDALONE
...
```

Sans option, cette commande renvoie la configuration du serveur samba sans les commentaires et omet les paramètres positionnés à leur valeur par défaut, ce qui facilite sa lecture.

```
[root]# testparm
```

2.5.4. La section [global]

Tableau 2.2. Les directives de la section [global]

Directive	Exemple	Explication
workgroup	workgroup = FORMATUX	Définir le groupe de travail ou le nom de domaine NetBIOS. (À mettre en majuscule).
netbios name	netbios name = inf1-formatux	Nom NetBIOS de la station Maximum 15 caractères Pas de rapport direct avec le nom de la machine Linux
server string	server string = Samba version %v	Description du serveur apparaissant dans l'explorateur Windows
hosts allow	hosts allow = 127. 172.16.1.	Permet de restreindre les clients du serveur aux seuls réseaux mentionnés. Notez la présence d'un point à la fin de l'adresse et l'absence du 0.
log file	log file = /var/log/samba/log.%m	Enregistrer les évènements dans un fichier %m représente le nom NetBIOS du client
security	security = user	Modèle de sécurité du serveur
passdb backend	passdb backend = tdbsam	Stockage des utilisateurs et des mots de passe. Le format tdbsam (Trivial

Directive	Exemple	Explication
		Database) est le format par défaut, limité en performance à 250 utilisateurs. Au delà, il faudra passer au format ldapsam et stocker les utilisateurs et les groupes dans une base LDAP.

2.5.5. La section [homes]

La section [homes] contient la configuration des partages utilisateurs.

C'est une section réservée par Samba, qui lui applique un fonctionnement très particulier. Ce nom de partage ne doit pas être utilisé pour un autre partage ni modifié.

```
[homes]
    comment = Home Directories
    browseable = no
    writable = yes
```

Tous les utilisateurs verront le même partage "homes" mais le contenu sera personnalisé pour chacun.

Attention à bien configurer les booléens SELinux pour autoriser le partage des dossiers personnels.

2.5.6. La section [printers]

La section [printers] contient la configuration du serveur d'impression.

```
[printers]
    comment = All Printers
    browseable = no
    writable = yes
    guest ok = no
```

```
    printable = yes
```

Samba peut ainsi faire office de serveur d'impressions, ce qui est une fonctionnalité intéressante (ne nécessite pas l'acquisition de licences clientes).

2.5.7. Partages personnalisés

Avant de paramétrer une nouvelle section du fichier smb.conf qui correspondra à un nouveau partage, il convient de se poser quelques questions :

- Quel est le chemin du partage ?
- Qui peut modifier le contenu ?
- Le partage doit-il être visible sur le réseau ou au contraire sera-t-il masqué ?
- Y aura-t-il un accès anonyme ?

Un nouveau partage est représenté par une section [nomdupartage] dans le fichier smb.conf. En voici un exemple :

```
[partage]
    comment = Partage
    browseable = yes
    writable = yes
    path = /export/data
    valid users = @users
    read list = georges
    write list = bob, alice
    invalid users = maurice
    create mask = 0664
    directory mask = 0775
    force group = users
```

De nombreuses directives sont disponibles pour configurer les partages :

Directive	Exemple	Explication
comment	comment = Exemple de partage	Affiche un commentaire dans l'explorateur de fichiers.
browseable	browseable = yes	Affiche le partage dans le voisinage réseau.

Directive	Exemple	Explication
writeable	writeable = yes	Le partage est en lecture seule ou en écriture.
path	path = /export/data	Le chemin absolu à partager sur le réseau. Attention au contexte SELinux de ce dossier.
valid users	valid users = @users	Liste les utilisateurs ou les groupes autorisés à accéder au partage.
invalid users	invalid users = alice	Liste les utilisateurs ou les groupes qui ne sont pas autorisés à accéder au partage.
read list	read list = bob	Liste les utilisateurs ou les groupes autorisés à accéder au partage en lecture.
write list	write list = patrick, alain	Liste les utilisateurs ou les groupes autorisés à accéder au partage en écriture.
create mask	create mask = 0664	Les fichiers créés prendront les droits spécifiés.
directory mask	directory mask = 0775	Les dossiers créés prendront les droits spécifiés.
force group	force group = users	Les nouveaux fichiers et dossiers appartiendront au groupe spécifié. Dans ce cas, il n’y a pas d'@ devant le groupe !

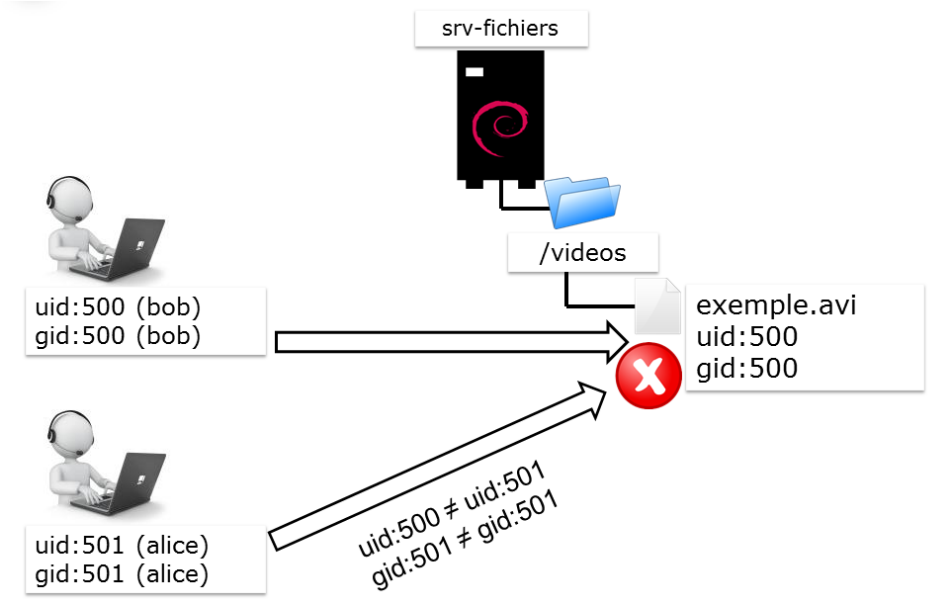
2.5.8. La directive force group

La directive **force group** permet de forcer l'appartenance d'un fichier créé à un groupe spécifique.

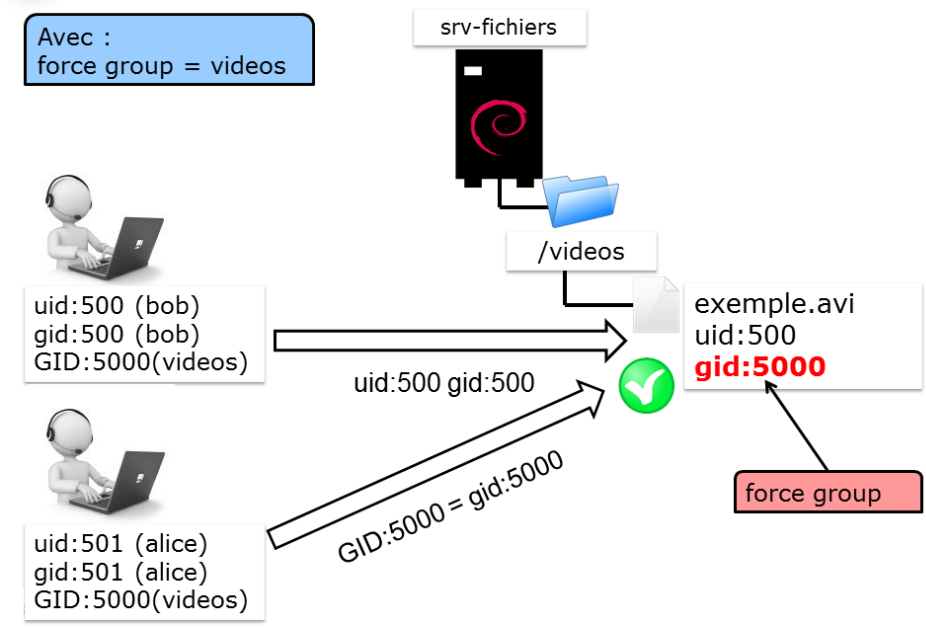
Cette directive est essentielle dans le fonctionnement de Samba, puisqu'elle assure que, quelque soit le groupe principal d'un utilisateur, celui-ci sera autorisé à accéder à un fichier sur le partage s'il fait parti, en tant qu'invité, du groupe spécifié dans la directive.

Les deux exemples ci-desous mettent en avant ce mécanisme :

Utilisation sans le mécanisme **force group** :



Utilisation avec le mécanisme **force group** :



2.6. Commandes d'administration

2.6.1. La commande pdbedit

La commande pdbedit permet de gérer la base SAM des utilisateurs Samba, que le backend soit au format tdbsam ou ldapsam, contrairement à la commande smbpasswd qui est limitée au format tdbsam.

Syntaxe de la commande pdbedit.

```
pdbedit [-a|-r|-x|-L] [-u username] ...
```

Exemple :

```
[root]# pdbedit -L
stagiaire:1000:Stagiaire SYS
```

Tableau 2.3. Options principales de la commande pdbedit

Option	Observation
-a	Ajouter un utilisateur

Option	Observation
-r	Modifier un utilisateur
-x	Supprimer un utilisateur
-L	Lister les utilisateurs
-u	Spécifier le nom de l'utilisateur pour les options -a, -r, et -x

Ajouter un utilisateur

Le format de cryptage du mot de passe entre le monde Microsoft et le monde Linux étant différent, Samba doit soit tenir à jour une base de données contenant les mots de passe au bon format ou déléguer cette gestion au serveur LDAP, ce qui explique l'usage de la commande smbpasswd.

```
pdbedit -a -u username [-f description]
```

Exemple :

```
[root]# pdbedit -a -u bob -f "Bob Leponge"
Unix username:     bob
User SID:          S-1-5-21-3024208064-2128810558-4043545969-1000
Full Name:         Bob Leponge
Home Directory:    \\srvfichiers\bob
Domain:            SRVFICHIERS
...
```

Option	Observation
-a	Ajouter un utilisateur. L'utilisateur doit exister dans le fichier /etc/passwd.
-u	Spécifier le nom de l'utilisateur à ajouter.

2.6.2. La commande smbpasswd

La commande smbpasswd permet de gérer les mots de passe des utilisateurs Samba.

Syntaxe de la commande smbpasswd.

```
smbpasswd [-d|-e] username
```

Exemple :

```
[root]# smbpasswd bob
New SMB password:
Retype new SMB password:
```

Option	Observation
-e	Réactive un compte.
-d	Désactive un compte.

Il est possible de synchroniser les mots de passe Unix et Samba :

```
[global]
    unix password sync = yes
    obey pam restrictions = yes
```

Directive	Exemple	Explication
unix password sync	unix password sync = yes	Synchronise le mot de passe entre le compte unix et le compte samba. Fonctionne uniquement avec la commande smbpasswd. La directive n'est pas prise en compte par la commande tdbedit.
obey pam restrictions	obey pam restrictions = yes	Applique les restrictions PAM.

2.6.3. La commande smbclient

La commande **smbclient** permet d'accéder à des ressources Windows (ou Samba) depuis le monde Unix.

Syntaxe de la commande smbclient.

```
smbclient '//serveur/partage' -U utilisateur
```

Exemple :

```
[root]# smbclient \\\\stat-wind\\partage-wind -U alain
smb: |> help
```

ou :

```
[root]# smbclient '//stat-wind/partage-wind' -U alain
smb: |> help
```

Le programme smbclient est couramment utilisé pour créer un interpréteur de type 'ftp' permettant ainsi d'accéder à des ressources SMB réseau.

Lister les partages :

```
[root]# smbclient -L inf1-formatux
```

Se connecter à un partage data du serveur inf1-formatux avec l'utilisateur bob :

```
[root]#  smbclient -L //inf1-formatux/data -U bob
Enter bob's password:
```

Glossaire

BASH
Bourne Again SHell

BIOS
Basic Input Output System

CIDR
Classless Inter-Domain Routing

Daemon
Disk And Execution MONitor

DHCP
Dynamic Host Control Protocol

DNS
Domain Name Service

FQDN
Fully Qualified Domain Name

LAN
Local Area Network

NTP
Network Time Protocol

nsswitch
Name Service Switch

POSIX
Portable Operating System Interface

POST
Power On Self Test

SHELL
En français "coquille". Á traduire par "interface système".

SMB

Server Message Block

SMTP

Simple Mail Tranfer Protocol

SSH

Secure SHell

TLS

Transport Layer Security, un protocole de cryptographie pour sécuriser les communications IP.

TTY

teletypewriter, qui se traduit téléscripteur. C'est la console physique.

UEFI

Unified Extensible Firmware Interface

Index