

عن أنس بن مالك رضي الله عنه خادم رسول الله صلى الله عليه وسلم أن النبي صلى الله عليه وسلم قال : ( لا يؤمن أحدكم حتى يحب لأخيه ما يحب لنفسه ) ، رواه البخاري ومسلم .

المرجو الدعوة لمن ساهم بنشر هذه الملخصات  
بالنجاح و الرحمة للوالدين

Résumer par : MeRT-NiBA

**FTP** : C'est un protocole qui permet de transférer des ressources (dossier et fichier). Il fonctionne avec TCP/21

#### Fichier de configuration FTP :

#Vim /etc/vsftpd/vsftpd.conf

**listen** : permet de définir si le démon est en standalone (YES) ou dirigé par (x)inetd (NO)

**anonymous\_enable=no** : Activer ou désactiver les connexions anonymes

**chroot\_local\_user=yes**: permet de "chrooter" la connexion de l'utilisateur

**allow\_writeable\_chroot=yes**: autorise l'écriture pour les utilisateurs "chrootés"

**listen\_port=21** // Spécifie le port d'écoute

**ftpd\_banner** : bannière d'affichage à la connexion FTP

**local\_enable=yes**: autorise les personnes à s'identifier avec un compte utilisateur local

**write\_enable=yes**: Autoriser le droit d'écriture

**userlist\_file=/etc/vsftpd/user\_list** // Fichier de user

**userlist\_deny=YES**// On refuse les utilisateurs de lecture la liste de user

**chroot\_list\_enable=NO**

**Dirmessage=YES/NO** # Accéder certain dossier

**Xferlog\_std\_format=YES/NO** # Activer ou non les fichiers log

**Connect\_from\_port\_20=YES/NO** # Activer ou non le port 20

**anon\_mkdir\_write\_enable=YES/NO** # Activer ou non la création des dossiers

**anon\_upload\_enable=no** : Refuser le upload pour les Anonymous

**xferlog\_file** : écriture d'un log des fichiers

**local\_umask=022** //Fixer le masque local a 022 (les fichiers créés auront des droits en 755)

**max\_clients=50** //Nombre maximum de connexion simultanée

**max\_per\_ip=4** // Nombre maximum de connexion venant de la même IP

**idle\_session\_timeout=600** // Temps avant déconnexion sur une session inactive

**pasv\_min\_port=30000** //

**pasv\_max\_port=31000** //

la commande pour redémarrer le service ftp :

#systemctl restart vsftpd

les commandes pare-feu :

#firewall-cmd --permanent --add-port=20-21/tcp

# firewall-cmd --permanent --add-port=30000-31000/tcp

#firewall-cmd --reload

La commande pour installer le package ftp :

#dnf install -y vsftpd

La commande pour vérifier le package ftp est installer :

#rpm -qa vsftpd

Créer un utilisateur :

adduser ftpuser

passwd ftpuser

mkdir -p /home/ftpuser/ftp\_dir

chmod -R 750 /home/ftpuser/ftp\_dir

chown -R ftpuser: /home/ftpuser/ftp\_dir

Ajouter un utilisateur un fichier user list

bash -c 'echo ftpuser >> /etc/vsftpd/user\_list'

**SSH** C'est un protocole de communication sécurisé, ainsi qu'il permet d'ouvrir une session à distance mais plus sécurisé que Telnet.

**OpenSSH** est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH.

#### Fichier de configuration ssh :

```
#vim /etc/ssh/sshd_config
```

**PermitRootLogin no** // Désactiver les connexions SSH en root

**AllowUsers user1 user2 user3** //Autoriser les utilisateurs en utilisent SSH

**AllowGroups groupe1 groupe2** //Autoriser les groupes en utilisent SSH

**DenyUsers user1 user2 user3** //Refuser les utilisateurs

**DenyGroups groupe1 groupe2** //Refuser les groupes

**Banner /var/banner.txt** //Afficher la bannière

**ListenAddress 192.168.10.1** //Adresse server SSH

**Port 22** //Modifier le port d'écoute

**Protocol 2** // VERSION SSH

**PermitEmptyPasswords no** //interdire mot de passe vide

**PasswordAuthentication yes** //Autoriser l'authentification par mot de passe

**MaxSessions 10** // spécifier le nombre maximal de sessions

**MaxAuthTries 4** // limiter le nombre de de tentative d'authentification

**ClientAliveInterval 600** // Envoie un message au client SSH après x secondes sans activité

**PubkeyAuthentication yes** // Autoriser authentification par clé publique

**LogLevel INFO** //Activer les logs

**ServerKeyBits 1024**

**AuthorizedKeysFile .ssh/authorized\_keys**

**Client SSH:**

```
$ ssh-keygen -t rsa -b 1024 -f id_rsa
```

**Copier les fichiers sur le serveur**

```
$scp id* ahmadi@192.168.1.1  
:/home/ahmadi/.ssh
```

**Server SSH:**

**Ajouter la clé publique dans un fichier qui contient les clés autorisées**

```
$ cat id_dsa.pub >> authorized_keys
```

Votre répertoire personnel sur le serveur doit au plus avoir comme permission 755

```
$ chmod 400 authorized_keys
```

```
# chmod 755 /home/ahmadi/
```

**Installation SSH:**

```
#yum install openssh-server
```

**Vérification d'installation ssh :**

```
# rpm -qa openssh-server
```

**Démarrage du service ssh :**

```
# systemctl start sshd
```

**Activation au démarrage du service ssh :**

```
# systemctl enable sshd
```

**Redémarrage du service ssh :**

```
# systemctl restart sshd
```

**Service BIND** : Le rôle principal de BIND est de traduire les noms de domaine en adresses IP pour que les ordinateurs puissent communiquer entre eux sur le réseau Internet.

#### **Le rôle DNS :**

\*recherche des serveurs de messagerie pendant la remise du courrier électronique

\*Recherche des CD est des serveurs de catalogue global

#### **Les types zones de recherche :**

\***Une zone de recherche directe** : permet de résoudre le nom DNS à son adresse IP.

\***Une zone de recherche inversée** : permet de résoudre l'adresse IP à son nom DNS.

**La différence entre server DNS principale et secondaire :**

**Serveurs DNS principaux** contiennent tous les enregistrements de ressources pertinents et traitent les requêtes DNS pour un domaine.

**Serveurs DNS secondaires** contiennent des copies de fichiers de zone qui sont en lecture seule, c'est-à-dire qu'ils ne peuvent pas être modifiés

#### **Le rôle fichier /etc/resolv.conf**

Est un fichier de configuration utilisé pour résoudre les DNS pour les systèmes d'exploitation Linux et UNIX

Il est utilisé pour configurer les serveurs de noms DNS

#### **syntaxe du fichier /etc/resolv.conf :**

**nameserver** <serveur DNS Primaire>

**nameserver** <serveur DNS Seconde>

**search** malekal.com

#### **Types de transferts de zone DNS :**

**Un transfert de zone** est le transfert total ou partiel des données d'une zone à partir du serveur DNS principale vers un serveur DNS secondaire.

**Transfert de zone complet** transfère l'intégralité de la zone (utilise une requête AXFR).

**Transfert de zone incrémentiel** transfère juste de la partie modifiée de la zone (IXFR).

#### **Processus de transfert de zone :**

- \* Requête SOA pour une zone
- \* Réponse à la requête SOA
- \* Requête IXFR ou AXFR pour une zone
- \* Réponse à la requête IXFR ou AXFR pour une zone
- \* Transfert de zone

#### **L'enregistrement de ressources :**

**A** : Mappage les noms d'hôtes en @ipv4

**MX** : Renseigne sur les serveurs de messageries.

**SOA** : Contient des informations de synchronisations entre des serveurs.

**CNAME** : Attribuer un alias à un enregistrement.

**PTR** : Mappage des @ip en noms d'hôtes.

**AAAA** : Mappage les noms d'hôtes en @ipv6.

**SRV** : Service de noms spécifique.

**NS** : Renseigne le nom des serveurs de nom pour le domaine.

#### **Les types de requêtes DNS :**

**Récursive**: envoyée par un client DNS à un serveur DNS local pour résoudre un nom DNS.

**Itératives** : envoyée entre un serveur DNS local à autre serveur DNS externe.

**<name>** : nom de la zone

**<class>** : classe du réseau

**<type>** : type d'enregistrement

**<mname>** : nom du serveur principal

**<rname>** : adresse email de l'administrateur responsable

**<serial>** : numéro de série incrémenté, permettant d'identifier la version du fichier de zone

**<refresh>** : intervalle précisant à quel moment un serveur secondaire doit interroger la version du serveur primaire

**<retry>** : intervalle précisant à quel moment un serveur secondaire doit renouveler sa requête en cas d'échec

**<expire>** : intervalle précisant à quel moment les informations DNS ne doivent plus être délivrées en cas d'absence de réponse de la part du serveur primaire

**<minimum>** : intervalle précisant combien de temps les informations peuvent être conservées dans le cache

#### Exemple enregistrement SOA :

```
$ORIGIN ista.org.  
$TTL 1750  
@ IN SOA srv.ista.org admin.ista.org (  
    2019040502; serial  
    86400; refresh  
    7200; retry  
    3600000; expire  
    1750; minimum)
```

#### Fichier de configuration DNS :

Vim /etc/named.conf

#### Exemple de configuration server DNS principales :

##### Zone directe :

```
zone "ISTA.COM" IN {  
    type master;  
    file "ISTA.COM.DIR";  
    allow-update {192.168.10.1}; //autorisé la mise à jour dynamique  
    allow-transfer {192.168.10.2 } ;  
    notify yes ;
```

```
};
```

##### Zone inverse :

```
zone "10.168.192.in-addr.arpa" IN {  
    type master;  
    file "ISTA.COM.INV";  
    allow-update {192.168.10.1};  
    allow-transfer {192.168.10.2 } ;  
    notify yes ;  
};
```

#### Exemple de configuration server DNS secondaire:

##### Zone directe :

```
zone "ISTA.COM" IN {  
    type slave;  
    file "slaves/ISTA.COM.DIR";  
    masters {192.168.10.1};  
};
```

##### Zone inverse :

```
zone "10.168.192.in-addr.arpa" IN {  
    type slave;  
    file "slaves/ISTA.COM.INV";  
    masters {192.168.10.1};  
};
```

#### Installation

```
#dnf install -y bind
```

#### Vérification d'installation

```
# rpm -qa bind
```

#### Démarrage du service

```
#systemctl start named
```

#### Activation au démarrage du service

```
#systemctl enable named
```

#### Redémarrage du service

```
#systemctl restart named
```

#### Vérification de la configuration

• **Fichier de configuration :**

**#named-checkconf**

• **Fichiers zone :**

**#named-checkzone -d ISTA.COM  
/var/named/ISTA.COM.DIR**

**#named-checkzone -d 10.168.192.in-  
addr.arpa /var/named/ISTA.COM.INV**

**La commande pour autoriser pare-feu:**

**Firewall-cmd --zone=public --add-  
service=dns --permanent**

**Firewall-cmd --reload**

**DHCP** : c'est un protocole qui permet la configuration des hôtes automatiquement. Il fonctionne avec UDP/67 pour le serveur et UDP/68 pour le client.

**Les étapes Création d'un bail :**

\*DHCP DISCOVER \*DHCP OFFER \*DHCP REQUEST \*DHCP ACK.

**Renouvellement d'un bail :**

\* DHCP REQUEST \*DHCP ACK

**Les avantages DHCP :**

- Fournit automatiquement des adresses IP
- Met à jour la configuration client automatiquement
- Garantit des informations de configuration correctes

**Etendue DHCP :**

Est une plage d'adresses IP qui peut être attribuée de manière dynamique aux ordinateurs.

**La réservation DHCP :**

L'attribution d'une adresse IP permanente à un client DHCP spécifique

**Installation**

```
#dnf install dhcp-server
```

**Vérification d'installation**

```
# rpm -qa dhcp-server
```

**Démarrage du service IPV4 :**

```
# systemctl start dhcpd
```

**Activation au démarrage du service**

```
# systemctl enable dhcpd
```

**chemin du fichier de configuration**

```
/etc/dhcp/dhcpd.conf
```

```
subnet 192.168.1.0 netmask
255.255.255.0 // spécifier le réseau
```

```
range 192.168.1.10 192.168.1.100;
//spécifier l'étendue
```

```
default-lease-time 600; //temps
d'utilisation d'adresse IP
```

```
max-lease-time 7200; //temps Max
d'utilisation d'adresse IP
```

```
option routers 192.168.1.1; //Définir la
passerelle
```

```
option domain-name-servers 192.168.1.3,
192.168.1.2; //Adresse IP des serveur DNS
```

```
option domain-name "est.com";
//spécifier le nom du domaine
```

```
option ntp-servers 192.168.1.1; //Adresse
du serveur NTP
```

```
option netbios-name-servers 192.168.1.27;
// Adresse IP du serveur Wins
```

```
option arp-cache-timeout 20 ; // Délai
d'attente en secondes pour les entrées de
cache ARP.
```

```
option default-ip-ttl 40 ; // durée de vie par
défaut que le client doit utiliser sur les
datagrammes sortants.
```

```
}
```

**Réservation Adresse IPV4**

```
host PC1 {
```

```
option host-name "PC1.example.com";
```

```
hardware ethernet 00:A0:78:8E:9E:AA;
```

```
fixed-address 192.168.1.4;
```

```
}
```

**Refus d'un hôte**

```
host PC1 {
```

```
hardware ethernet 00:A0:78:8E:9E:AA;
```

```
deny booting;
```

```
}
```

**Vérification de la configuration**

```
#dhcpd
```

**Redémarrage du service**

```
# systemctl restart dhcpd
```

**SAMBA** : permet de partager les ressources dans les systèmes Linux/Windows, utilise le protocole SMB. Le protocole SMB fonctionne avec UDP/445.

#### Exemple un partage Windows vers linux

Crée un dossier :

Mkdir /media/partage

Cd /media/partage

Cd ..

La commande Install SAMBA :

#Dnf install samba samba-clients samba-common cifs-utils

La commande pour montage un partage Windows avec le point de montage /media/partage

Mount -t cifs //192.168.1.50/data /media/partage/ -O user=ADMIN

#### Exemple un partage linux vers Windows :

Créer un utilisateur :

useradd -g 100 NIBA

passwd NIBA

Crée un groupe :

groupadd -g 100 IDOSR

Ajouter les utilisateurs la base de données SAMBA :

smbpasswd -a NIBA

La commande pour vérifier la base samba :

#pdbedit -L

La commande pour vérifier la configuration samba :

#testparm

Configuration du fichier :

vim /etc/samba/smb.conf

Configuration globale de samba :

[global]

workgroup = 2tri #Le nom du groupe

server string = samba server # Le serveur SAMBA

hosts allow = 192.168.1. # La partie réseau

security = user # Méthode d'authentification (user/domain/share)

Crée et partager le dossier :

[partage1]

Comment = Répertoire partagé 1 # Commentaire

path = /opt/partage1 # Le chemin du fichier partagé

valid users = NIBA # groupe et utilisateur avec accès au partage

write list =@IDOSR #les groupes et utilisateurs avec accès en écriture

read list =@IDOSR # les groupes et utilisateurs avec accès en lecture

directory mask=0700 #masque de création des dossiers

create mask=0664 #masque de création des fichiers

read only=yes/no# tous les utilisateurs et groupes ave accès en lecture

browseable = yes/no # partage visible ou non dans le réseau

locking=no #indique que les utilisateurs a la fois peuvent écrire dans le partage

public = yes/no #Activer ou non le partage en mode publique

writable = yes/no # Activer ou non l'option d'écriture

printable = yes/no # Activer ou non l'impression du partage

group = partage # Le groupe du partage

La commande pour redémarrer samba :

#Systemctl restart smb / nmp

La commande autoriser pare-feu samba :

#Firewall-cmd --zone=public --add-service=samba --permanent

#Firewall-cmd --reload

**HTTP:** le rôle de HTTP est de fournir un moyen fiable et standard de transmettre des données sur le Web et de permettre aux utilisateurs d'accéder à des ressources en ligne via leur navigateur Web.

**index.html** : ce fichier contiendra généralement le contenu de votre page d'accueil, c'est-à-dire le texte et les images que les gens verront lorsqu'ils arriveront sur votre site.

**La commande pour installer service http :**

**#Dnf install httpd**

**La commande pour vérifier la présence http :**

**#Rpm -qa httpd**

**Fichier de configuration http:**

**Vim /etc/httpd/conf/httpd.conf**

**ServerAdmin** <mailto:root@localhost>:

#désigne l'adresse e-mail de l'administrateur

**ServerName** [nom\\_serveur](#) #indique le nom du serveur

**DocumentRoot** ["/var/www/html"](#) #c'est le répertoire qui contient les sites Web hébergés sur le serveur.

**Listen** 80 #indique le port d'écoute

**Include** [conf.d/\\*.conf](#) #pour inclure tous les fichiers d'extensions .conf se trouvant dans le répertoire conf.d(/etc/httpd/conf.d)

**ServerRoot** ["/etc/httpd"](#) #indique le répertoire des fichiers de configuration d'Apache.

**La commande pour redémarrer http :**

**#Systemctl restart httpd**

**La commande autoriser pare-feu http :**

**#Firewall-cmd --zone=public --add-service=http --permanent**

**#Firewall-cmd --reload**

**Créer le fichier index.html :**

**#Cd /var/www/html/**

**#Vim index.html**

**<html>**

**<head>**

**<title>**

**Ma page de web**

**</title>**

**</head>**

**<body>**

**Bienvenue ista.local**

**</body>**

**</html>**

**Les virtuals host:**

**Vim /var/www/html/httpd/conf.d/vhost.conf**

**<VirtualHost \*:80>**

*# Virtualhost écoutant sur le port 80*

**ServerAdmin** [niba@ista.local](mailto:niba@ista.local)#

*Mail du webmaster*

**ServerName** [ista.local](#)

*#Nom du serveur auquel le vhost doit répondre*

**ServerAlias** [www.ista.local](#)

*# Eventuel alias supplémentaire*

**DocumentRoot** [/var/www/html/ista](#)

*# Racile des fichiers du site*

**ErrorLog** [/var/log/httpd/ista.local/error.log](#)

*# Délocaliser pour ce vhost les logs d'erreur*

**CustomLog** [/var/log/httpd/ista.local](#)

[/access.log](#) common

**</VirtualHost>**

*# Fin de la définition du vhost*

**#mkdir /var/www/html/ista**

**#mkdir /var/log/httpd/ista.local**

**#cd /var/www/html**

**Mv index.html/ ista/**

**Cp ista/index.html /est**



**#vim ista**

**#systemctl restart httpd**

**Le nom de trois distributions LINUX :**

- CENTOS
- REDHAT
- UBUNTU
- DEBIAN

**Donner deux commandes permettant l'installation du package sous CENTOS :**

- Rpm -ivh package
- Dnf install -y
- Yum install -y

**Donner les commandes permettant la planification des taches sous LINUX :**

- At
- Batch
- Les fichiers crontab