OFPPT مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Complexe de Formation dans les Métiers des Nouvelles Technologies de l'Information, de l'Offshoring et de l'Electronique -Oujda

Module 10 : Administration d'un réseau sous Linux

Groupe : TRI 202

Résumé d'installation et configuration des serveurs sous Centos7

Formatrice :ZITI Ilham

Table of Contents

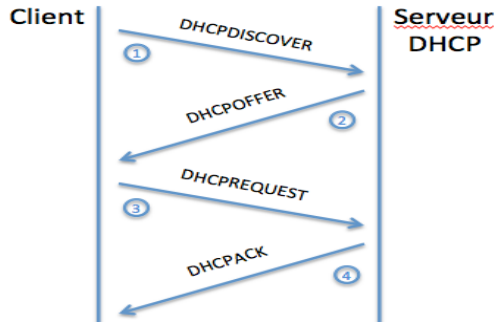
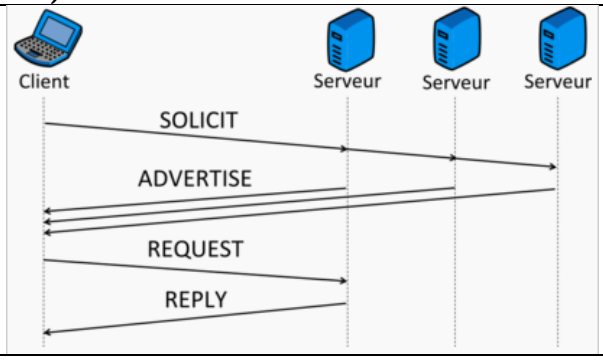
Remarque : Pour plus de détail référenciez-vous aux cours de chaque serveur

Configuration de base

Modifier le nom	1. Modifier le contennu du fichier : **#vi /etc/hostname** 2. Redemarrer la machine :**#reboot** 3. Tester :**#hostname**
Désactiver le Pare-Feu	1. **# systemctl stop firewalld.service** 2. **#systemctl disable firewalld.service** //desavtiver au demarrage automatiquement
Désactiver SELINUX	1. Editer le fichier /etc/selinux/config remplacer enforcing par disabled : **SELINUX=enforcing** 2. Redemarrer la machine :**#reboot**
Fixer adresse IPV4	1. Editer le fichier : **#vi /etc/sysconfig/network-scripts/ifcfg-X** 2. Modifier /Ajouter : **BOOTPROTO=static** ## Passer en mode static (non DHCP) **IPADDR=192.168.0.10** ## Adresse IP de la machine **NETMASK=255.255.255.0** ## Masque sous-reseau **NETWORK=192.168.0.0** ## Adresse reseau **ONBOOT=yes** ## Monter l'interface au boot 3. Editer le fichier : **#vi /etc/sysconfig/network** 4. Ajouter : **NETWORKING=yes** **## Activer le reseau** **GATEWAY=192.168.0.1** ## Adresse ip de votre passerelle 5. Editer le fichier : **#/etc/resolv.conf** 6. Ajouter l'adresse du serveur DNS : **nameserver 10.20.30.40** 7. Redemarrer le service réseau : **# systemctl restart network** 8. Tester : **#ifconfig**
Fixer adresse IPV6	1. Editer le fichier : **#vi /etc/sysconfig/network-scripts/ifcfg-X** 2. Modifier /Ajouter : **BOOTPROTO=static** ## Passer en mode static (non DHCP) **IPV6INIT=yes** ##Activer la configuration d'IPv6 sur l'interface **IPV6ADDR=2001 :DB8 ::3/64** ##Spécifie une adresse IPv6 statique **IPV6_DEFAULTGW=2001 :DB8 ::1** ##Ajoute une route par défaut via l'interface spécifiée **ONBOOT=yes** ## Monter l'interface au boot 3. Redemarrer le service réseau : # systemctl restart network 4. Tester : #ifconfig

Serveur DHCP

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine

Requête IPv4 (Port serveur : 67, Port client 68)	**Requête IPv6 (Port serveur : 547, Port client 546)**
	

Installation	#yum install dhcp
Vérification d'installation	# rpm -qa dhcp
Démarrage du service	**IPV4** : # systemctl start dhcpd **IPV6** : # systemctl start dhcpd6 **NB : avant la config le serveur ne démarre pas**
Activation au démarrage du service	**IPV4** : # systemctl enable dhcpd **IPV6** : # systemctl enable dhcpd6
Nom et chemin du fichier de configuration	**IPV4** : /etc/dhcp/dhcpd.conf **IPV6** : /etc/dhcp/dhcpd6.conf

Syntaxe du fichier de configuration **IPV4**	**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 "ofppt.ma"; //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** Ajouter l'option **-6** dans le cas de configuration IPV6
Démarrage du service **IPV4**	**# systemctl restart dhcpd**

Syntaxe du fichier de configuration **IPV6**	**subnet6** 2001:db8:0:1::/64 {
	range6 2001:db8:0:1::129 2001:db8:0:1::254;
	option dhcp6.name-servers fec0:0:0:1::1;
	option dhcp6.domain-search "domain.example";
	}

Réservation Adresse **IPV6**	**host** Nomclient {
	hardware ethernet 01:00:80:a2:55:67;
	fixed-address6 3ffe:501:ffff:100::4321;
	}
	host specialclient {
	host-identifier option dhcp6.client-id 00:01:00:01:4a:1f:ba:e3:60:b9:1f:01:23:45;
	fixed-address6 2001:db8:0:1::127;
	}

Test	Client Linux IPV4 **:#dhclient** Client Linux IPV6 **:#dhclient -6 -d NomInterface** Client Windows **: >ipconfig /release / >ipconfig /renew**
Agent relais dhcp **IPV4**	1. Copier et éditer le fichier dhcrelay.service **# cp /lib/systemd/system/dhcrelay.service /etc/systemd/system/** **# vi /etc/systemd/system/dhcrelay.service** 2. Modifier l'option ExecStart : **ExecStart=/usr/sbin/dhcrelay -d --no-pid AdessIPDHCP -i NomInterface** 3. Activer les changements : **# systemctl --system daemon-reload** **# systemctl restart dhcrelay**
Agent relais dhcp **IPV6**	4. Copier et éditer le fichier dhcrelay.service **# cp /lib/systemd/system/dhcrelay6.service /etc/systemd/system/** **# vi /etc/systemd/system/dhcrelay6.service** 5. Modifier l'option ExecStart ajouter l'argument -6 et ajouter les interfaces « lower interface » et « upper interface »: **ExecStart=/usr/sbin/dhcrelay -d --no-pid -6 -l eth1 -u eth2** 6. Activer les changements : **# systemctl --system daemon-reload** **# systemctl restart dhcrelay6**

Serveur DNS

DNS Domain Name System. C'est un système hiérarchique distribué permettant la résolution des noms de machines en adresses IP et inversement, utilise le **port 53.**
Il existe deux types de

- Requêtes : **requêtes récursives** et **requêtes itératives**.
- Serveur DNS **Principal** (**Master)** et DNS **secondaire (Slave)**.
- Zone : Zones de **recherche directe**, et zones de **recherche inversée**

Installation	#yum install -y bind
Vérification d'installation	# rpm -qa bind
Démarrage du service	#systemctl start named.service
Activation au démarrage du service	#systemctl enable named.service
Nom et chemin du fichier de configuration	**/etc/named.conf**
Configuration **globale**	**listen-on port 53 { localhost; };** // Autoriser les requêtes récursives que depuis lui-même ou any (tous le monde) ou Adresse IP **forwarders { 212.27.40.240; 212.27.40.241; };** //Envoyer les requête vers d'autre serveurs DNS

Configuration d'un serveur **DNS primaire (maître)**	**Zone directe :**
	zone "votredomaine.com" IN {
	type master;
	file "votredomaine.com.zone";
	allow-update { none; }; //ne pas autoriser la mise à jour
	};
	Zone inverse IPV4 :
	zone "**Adresse réseau inverse.in-addr.arpa**" IN {
	type master;
	file "votredomaine.com.inverse";
	allow-update { none; };
	};
	Zone inverse IPV6 : (mettre un point entre chaque élément d'adresse IP)
	zone "**Adresse réseau inverse. ip6.arpa**" IN {
	type master;
	file "votredomaine.com.inverse";
	allow-update { none; };
	};
	Autres options :
	allow-transfer { adresse ip ; }; //Autoriser le transfert
	notify yes/no; //Activer ou non la notification
	allow-notify { adresse ip ; }; //Autoriser les serveur à notifier en cas de modification

Configuration de la zone DNS **directe**	$TTL 86400 @ **IN SOA** ns.votredomaine.com. dnsmaster.votredomaine.com. (2019 //Numéro de série 2H // La période de rafraîchissement des données 1D // La période de nouvelle essaie 1W // La période d'expiration 38400) // la durée de validité des données communiquée par le serveur pour toute requête . @ **IN NS** ns.votredomaine.com.

	@ **IN NS** ns2.votredomaine.com. @ **IN MX 10** mail.votredomaine.com. @ **IN MX 20** mail2.votredomaine.com. _ldap_tcp.ntic.ma 86400 **IN SRV** 20 100 389 AD.ntic.ma. ns **IN A** votreip ns2 **IN A** votreip mail **IN A** votreip mail2 **IN A** votreip www **IN A** votreip www **IN AAAA** votreipV6 ftp **IN CNAME** www.votredomaine.com.
Configuration de la zone DNS **inversé**	$TTL 86400 @ **IN SOA** ns.votredomaine.com. dnsmaster.votredomaine.com. (2019 //Numéro de série 2H // La période de rafraîchissement des données 1D // La période de nouvelle essaie 1W // La période d'expiration 38400) // la durée de validité des données communiquée par le serveur pour toute requête . @ **IN NS** ns.votredomaine.com. Votreip (partie hote) **IN PTR** ns Votreip (partie hote) **IN PTR** mail Votreip (partie hote) **IN PTR** ns2
Modification des droits des fichiers de configuration de zone	#chown root.named votredomaine.com.zone #chown root.named votredomaine.com.inverse
Vérification de la configuration	▪ **Fichier de configuration** : #named-checkconf ▪ **Fichiers zone :** #named-checkzone -d nomdomaine.com /var/named/nomdomaine.zone #named-checkzone -d adresse inverse réseau.in-addr.arpa /var/named/nomdomaine.inverse
Redémarrage du service	#systemctl restart named.service
Test Client	1. Modifier resolv.conf en ajoutant l'adresse du serveur DNS **2. #nslookup Nom de domaine du hôte ou adresse IP** Il est possible de modifier le mode d'interrogation de la commande nslookup grâce à l'option type :**type=mx ,type=ns, type=aaaa, type=soa et type=cname** **3. #dig nom du domaine**

Configuration serveur secondaire	1. Configuration global : Modifier la ligne **allow-query { Adresse serveur secondaire; };**
	2. Configuration de la zone primaire :
	zone "ntic.ma" {
	type master;
	file "ntic.ma.direct";
	allow-transfer{AdresseIPserveurSlave;};
	notify yes;
	};
	3. Configuration de la zone secondaire :
	zone "ntic.ma" {
	type slave;
	file "ntic.ma.directe"
	masters {AdresseIPprimaire;};
	allow-notify { AdresseIPprimaire; };
	};

Configuration DDNS	1. Au niveau du serveur DNS :Dans named.conf indiquer l'adresse IP du serveur DHCP dans l'option **allow-update** 2. Au niveau du serveur DHCP : ajouter les lignes suivantes dans dhcpd.conf **ddns-updates on;** //Autoriser les mises à jour des zones DNS **ddns-update-style interim;** //Précise qu'il s'agit d'une mise à jour vers un serveur DNS local. **deny client-updates;** // Empêcher les clients de s'enregistrer eux-mêmes auprès du serveur DNS. **ddns-domainname "Nom de la zone directe";** **ddns-rev-domainname "nom de la zone inverse";** **authoritative;** //Serveur DHCP prioritaire sur le réseau local. **zone Nom de zone directe. {** **primary 192.168.2.1;** **}** **zone Nom de zone inverse. {** **primary 192.168.2.1;** **}**

Serveur NFS

NFS (Network File System) est un protocole permettant de monter des disques en réseau. Le port utilisé par NFS c'est 2049. NFS est compatible avec *l'IPv4* et *IPv6*

Configuration Serveur

Installation	#yum install nfs-utils
Vérification d'installation	# rpm -qa nfs-utils
Démarrage du service	# systemctl start nfs-server
Activation au démarrage du service	# systemctl enable nfs-server
Nom et chemin du fichier de configuration	/etc/exports
Syntaxe du fichier de configuration	<dossier partagé> <hôte>(<options>)
Explication	**<dossier partagé>** : chemin menant au dossier partagé <**hôte**> : indique quel est l'hôte qui peut accéder à ce partage (@IP, Nom Domaine, Adresse réseau) **<options>** : indique les options de partage tel que : ▪ **rw :** droit lecture et écriture, ▪ **ro :** droit de lecture seule (option par defaut) ▪ **root_squash** : spécifie que le root du serveur NFS n'a pas les droits de root sur le répertoire partagé ▪ **no_root_squash :** le contraire que root_squash. ▪ **all_squash :** force le *mapping* de tous les utilisateurs vers l'utilisateur anonyme. ▪ **anonuid :** indique l'UID de l'utilisateur ▪ **anongid :** indique le GID de l'utilisateur anonyme
Exemple de conf	/home/ofppt/testN 192.168.147.215(rw) /home/ofppt/testN1 *(ro) /home/ofppt/testN2 192.168.147.215(rw,all_squash,anonuid=1003,anongid=1003) /home/ofppt/testN3 *(rw,no_root_squash)
Redémarrage du service	# systemctl restart nfs-server
Exporter le partage	# exportfs -ra
Lister les info du montage	#showmount -e <IP_serveur_NFS>

Configuration Client

Créer un dossier pour contenir le partage	#mkdir /media/ntfPartgae
Montage temporaire	# mount –t nfs <Adressi_ip_serveur>:<repserveur> < point_montage_local>
Montage automatique via fstab	1- Editer le fichier /etc/fstab et ajouter : <ip_serveur>:<rep_serveur> <point_montage_local> nfs defaults,nfsvers=3,auto,user 0 0 2- Activer le montage : #mount -a

Serveur FTP

Le FTP (File Transfer Protocol) ou protocole de transfert de fichiers est un protocole de communication dédié à l'échange informatique de fichiers sur un réseau TCP/IP.Pour la connexion de contrôle, le numéro de port utilisé par le serveur ftp est 21.Pour la connexion de transfert de données, le numéro de port utilisé par le serveur ftp est 20.

VSFTPD est un deamon FTP très léger, rapide et sécurisé. Il peut gérer des services FTP de tous types. VsFTPd est un serveur FTP conçu avec la problématique d'une sécurité maximale.

Installation	#yum install vsftpd
Vérification d'installation	# rpm -qa vsftpd
Démarrage du service	# systemctl start vsftpd
Activation au démarrage du service	# systemctl enable vsftpd
Nom et chemin du fichier de configuration	/etc/vsftpd/vsftpd.conf
Options de configuration	**anonymous_enable=NO** //Pas de connexions en mode anonymous **listen_port=21** // Spécifie le port d'écoute **local_enable=YES** // Autoriser les utilisateurs locaux **write_enable=YES** //Autoriser le droit d'écriture **local_umask=022** //Fixer le masque local a 022 (les fichiers crées auront des droits en 755) **anon_upload_enable=NO** //Refuser le upload pour les anonymous **anon_mkdir_write_enable=NO** // Refuser l'ecriture pour les anonymous **idle_session_timeout=600** // Temps avant déconnexion sur une session inactive **max_clients=50** //Nombre maximum de connexion simultanée **max_per_ip=4** // Nombre maximum de connexion venant de la même IP **ftpd_banner=Bienvenue sur mon ftp perso** //Bannière de bienvenue **chroot_local_user=YES** **chroot_list_enable=NO** **allow_writeable_chroot=YES** //les trois lignes limite les utilisateurs à leur répertoire
Options : **ftpusers et user_list**	# Fichier de users **userlist_file=/etc/vsftpd/user_list** # Chargement de la liste userlist_file **userlist_enable=YES** # On refuse les utilisateurs de la liste **userlist_deny=YES**
Redémarrage du service	# systemctl restart vsftpd
Client Commande	# ftp Nom Serveur FTP (ou Adresse IP)
Client graphique	FileZilla, gFTP, AxyFTP par exemple

Serveur SSH

Secure Shell (SSH) est un programme mais aussi un protocole de communication sécurisé. Grâce à SSH, on peut se connecter à distance sur une machine et transférer des fichiers. Le numéro de port utilisé par le serveur est 22

OpenSSH (OpenBSD Secure Shell) est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH.

Installation	#yum install openssh-server
Vérification d'installation	# rpm -qa openssh-server
Démarrage du service	# systemctl start sshd
Activation au démarrage du service	# systemctl enable sshd
Nom et chemin du fichier de configuration	/etc/ssh/sshd_config
Syntaxe du fichier de configuration	**PermitRootLogin no** // Désactiver les connexions SSH en root **AllowUsers user1 user2 user3** //Autoriser les utilisateurs **AllowGroups goupe1 groupe2 //**Autoriser les groupes **DenyUsers user1 user2 user3** //Refuser les utilisateurs **DenyGroups goupe1 groupe2** //Refuser les groupes **Banner /etc/banner** //Afficher la bannière **Port numéro_du_port //**Modifier le port d'écoute **PermitEmptyPasswords no** //interdire mot de passe vide **PasswordAuthentication yes** //Autoriser l'authentification par mdp **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 **LogLevel INFO** //Activer les logs
Redémarrage du service	**# systemctl restart sshd**
Création de la paire de clé	**#ssh-keygen –t rsa –b 2048**
Autoriser votre clef publique	**#ssh-copy-id –i ~/.ssh/id_rsa.pub** user@ipmachine
Test client	**#ssh** utilisateur@AdresseIPduServeur (ou nom de domaine)
Test Graphique	Putty, WinSCP
Transfert fichier/ dossier	$**scp** Nom fichier Utilisateur@IPServeurCible:/Chemin Ajouter l'option **-r** en cas de transfert de dossier $**scp** -r -p user@serveur1:chemin/vers/dossier/source user@serveur2:chemin/vers/dossier/destination En IPV6 ajouter l'option -6 **:$scp -6**
Tunnel SSH	$**ssh -L** port-local:HOSTNAME:port-distant login@machine-distante **Proxy "SOCKS" :** **ssh -D** port-local login@machine-distante

Serveur SAMBA

Samba est une suite de logiciels permettant d'interconnecter Windows et toutes sortes d'Unix-like. La partie serveur de SaMBa est gérée par des programmes :

- smbd : il fournit les services de partage de fichiers et d'imprimantes
- nmbd : il répond aux requêtes NetBIOS de résolution de noms et de voisinage

NB : désactiver SELINUX setsebool -P samba_enable_home_dirs on

Installation	#yum install -y samba*
Vérification d'installation	# rpm -qa samba
Démarrage du service	#systemctl start smb.service #systemctl start nmb.service
Activation au démarrage du service	#systemctl enable smb.service #systemctl enable nmb.service
Nom et chemin du fichier de configuration	**/etc/samba/smb.conf**
Structure du fichier de configuration	▪ la section **[global]** contient les paramètres généraux du serveur. ▪ la section **[homes]** contient les paramètres pour l'accès aux répertoires des utilisateurs. ▪ la section **[printers]** contient les paramètres pour l'ensemble des imprimantes connectées au système ▪ Les autres sections sont considérées comme des **déclarations de partage.**
Option [global]	**workgroup =** Le nom du groupe de travail **server string =** La description du serveur **security =** Type de sécurité (USER, ADS, SHARE, DOMAINE, SERVER) **log file =** le nom du fichier qui contiendra le journal des activités du serveur **max log size=**taille maximale du fichier journal, en Kio.
Configuration du partage : Configuration du dossier partager	1. Créer un répertoire : **#mkdir partage** 2. Créer un groupe **: #grouadd ntic** 3. Modifier les droits du répertoire : **#chgrp -R ntic partage** **#chmod -R o+xw partage**
Configuration du partage : Configuration de l'utilisateur	1. Creér un utilisateur : **#useradd -G groupe user** 2. Définr un mot de passe Samba : **#smbpasswd -a user**
Configuration du partage :smb.conf	Ex de partage : **[ntic]** //Nom du partage **comment** = Exemple de partage //Description **path** = partage //Chemin du partage **public** = no //Refuser connexion sans mot de passe **valid users** = user, @ntic // liste d'utilisateurs ou groupe autorisés **writable** = yes // Droit d'écriture **browseable** = yes // Répertoire visible **create mask** = 0765 // droits appliqués en rajoutant un 0 devant. **read only** = Yes // Lecture seule pour tous **write list** = user1,user2 //droit d'écriture pour la liste
Vérification	testparm

Redémarrage du service	#systemctl restart smb.service #systemctl restart nmb.service
Afficher l'arborescence	#smbclient -L Localhost #smbtree
Test Client :smbclient	#smbclient //@IP serveurSamba/NomPartage -U user
Test Client :smbmount	#mkdir -p /mnt/samba # smbmount //@IP serveurSamba/NomPartage /mnt/smbmnt -o username=utilisateur
Client Windows	Dans la barre de recherche : \\nomServeurSamba\NomPartage Créer un lecteur réseau

Serveur Apache

Apache est le principal serveur web du monde de l'Open Source. Utilise par défaut le port 80 et 443(SSL) mais on peut modifier le port dans le fichier de configuration.

Installation	# yum -y install httpd
Vérification d'installation	#rpm -qa httpd
Démarrage du service	# systemctl start httpd
Activation au démarrage du service	#systemctl enable httpd
Nom et chemin du fichier de configuration	/etc/httpd/conf/httpd.conf
Syntaxe configuration général	**ServerRoot "/etc/httpd"** //Chemin du dossier de configuration **Listen 80** // Port d'ecoute **DocumentRoot "/var/www/html"** // le chemin de l'accès au repertoire du site exactement le fichier index.html définie par défaut **ServerAdmin root@localhost** //Adresse mail de l'administrateur **Include** ..... **//**permet l'inclusion d'autres fichiers de configuration dans httpd.conf **<Directory> ….. </Directory>** //regroupe un ensemble de directives qui ne s'appliquent qu'au répertoire précisé **ErrorLog "logs/error_log"** // Définit le chemin vers le journal des erreurs **CustomLog "logs/access_log" combined** //permet de contrôler la journalisation des requêtes destinées au serveur. **AddDefaultCharset //**paramètre le jeu de caractères par défaut pour les pages de texte **Timeout 300** //définit la durée, exprimée en secondes, pendant laquelle le serveur attend des réceptions **MaxClients 150** //fixe une limite au nombre total de processus serveur ou de clients connectés simultanément **LogLevel warn** // définit le niveau de détail avec lequel les messages d'erreur devraient être enregistrés dans les journaux d'erreurs
VirtualHost	1. #touch /etc/httpd/conf.d/nomdoamine.conf 2. <**VirtualHost** 192.168.2.3:80> // Adresse IP de la machine serveur, suivie du port 80 qui est le port http **ServerAdmin** admin@ntic.local //Adresse mail de l'administrateur **ServerName** ntic.local // le nom de domaine du serveur **ServerAlias** www.ntic.local // nom alternatif du serveur **DocumentRoot** /var/www/html/ntic.lcal/ // le chemin de l'accès au fichier index.html **ErrorLog /var/log/httpd/error_log** //permet de définir le nom du fichier dans lequel le serveur va journaliser toutes les erreurs qu'il rencontre **CustomLog /var/log/httpd/access_log combined** //permet de contrôler la journalisation des requêtes destinées au serveur. </VirtualHost>
Répertoire du site	1. Création du répertoire pour le site : #mkdir -p /var/www/html/ntic.local 2. Modification des droits : #chown -R apache:apache ntic.local #chmod -R 755 ntic.local 3. Création du fichier index.html : #vim /var/www/html/ntic.lcal/index.html 4. Exemple du fichier index : <html> <head>

	<title>Welcome to ntic.local</title> </head> <body> l'Exemple de virtual host fonctionne </body> </html>
Test de configuration	#apachectl configtest
Redémarrer le service	# systemctl restart httpd
Recharger le service	# systemctl reload httpd
Sécuriser Apache2 avec SSL	1. **Installation du mod ssl :** #yum install mod_ssl 2. **Création du certificat :** # openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out /etc/httpd/server.crt -keyout /etc/httpd/server.key 3. **Vérifier** dans le fichier « /etc/httpd/conf.d/ssl.conf » que la directive de configuration nommée **Listen** écouter sur le **port 443** 4. Ex de configuration : <VirtualHost *:80> ServerName ntic.local/ Redirect / https://ntic.local/ </VirtualHost> <VirtualHost ***:443**> ServerName ntic.local DocumentRoot /var/www/html/ntic **SSLEngine on** // Activer le moteur SSL **SSLCertificateFile /etc/httpd/server.crt** //définit le certificat authentifiant le Serveur auprès des clients **SSLCertificateKeyFile /etc/httpd/server.key** //définit la clé privée du Serveur </VirtualHost>

Serveur OpenLdap

Open LDAP est une implémentation open source du protocole LDAP. Il est constitué de 3 éléments principaux :

- **slapd (Stand-alone LDAP Daemon)** : démon LDAP autonome. Il écoute les connexions LDAP sur n'importe quel port (389 par défaut).
- Des **Bibliothèques** implémentant le protocole LDAP.
- Des **Utilitaires**, des outils et des exemples de clients.

Installation	#yum install openldap-clients openldap-servers openldap-devel migrationtools
Vérification d'installation	# rpm -qa openldap*
Démarrage du service	# systemctl start slapd
Activation au démarrage du service	# systemctl enable slapd
Configurer le mot de passe root LDAP	#slappasswd Le mot de passe est affiché crypter
Configuration	1- Editer le fichier /etc/openldap /ldap.conf modifier la ligne **BASE dc=NomDomaine,dc=local** 2- Editer le fichier slapd.d/cn\=config/olcDatabase\=\{1\}monitor.ldif et renseigner votre domaine "cn=Manager,**dc=NomDomaine,dc=local** 3- Editer le fichier slapd.d/cn\=config/olcDatabase\=\{2\}mdb.ldif, modfier le domaine puis ajouter le mot de passe crypté **olcSuffix: dc=NomDomaine,dc=local** **olcRootDN: cn=Manager,dc=NomDomaine,dc=local** **olcRootPW: {SSHA}ppNk4zYhzD9PUUohDERGxGJFRzaCzbuA**
Configurer la base de données LDAP	#cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG #chown ldap:ldap /var/lib/ldap/*
Mettre à jour le Schema	ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
Redémarrer le serveur	#systemctl restart slapd
Ex fichier ldif: Domaine, OU, groupe, user	dn: dc=ilham,dc=local ObjectClass: top ObjectClass: domain dc: ilham dn: ou=tri,dc=ilham,dc=local ObjectClass: top ObjectClass: organizationalUnit

	ou: tri dn: cn=202,ou=tri,dc=ilham,dc=local ObjectClass: posixGroup cn: 202 gidNumber: 202 memberuid: ahmed description: testgroupe dn: uid=ahmed,ou=tri,dc=ilham,dc=local ObjectClass: top ObjectClass: person ObjectClass: inetorgperson cn: ahmed serraji sn: serraji givenname: ahmed description: testuser uid: ahmed telephonenumber: 1233444 mail: eee@jhhhh
Ex : fichier ldif utilisateur généré par : **migrationtools**	1. Création utilisateur linux **:#useradd user** 2. Copier les informations de l'utilisateur dans un fichier nommé passwd.txt : #**grep user /etc/passwd > passwd.txt** 3. Créer le fichier ldif en utilisant le script migrate_passwd.pl : **/usr/share/migrationtools/migrate_passwd.pl passwd.txt > user.ldif**
Ajouter objets :Importation du fichier ldif	**ldapadd -x -W -D "cn=Manager,dc=NomDomaine,dc=local" -f NomFichier.ldif** **-x** : Authentification simple **-D** : identifiant connexion à la base **-W** : demande le mot de passe **-f** : le nom du chier ldif
Chercher	**#ldapsearch -x -b "dn "** Utiliser l'option -LLL :Afficher le resultat sans commentaires, sans version LDIF
Supprimer	**#ldapdelete -v –D "cn=Manager,dc=NomDomaine,dc=ma" -W "dn à supprimer"**
Modifier un attribut : Ajout	Ex : **Ajouter** l'attribut **description** 1. Créer le fichier ldif suivant : dn: uid=user,ou=stagiaire,dc=tmsir,dc=local changetype: **modify** **add:**description description: stagiaire ofppt 2. Lancer la commande : **ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f ajout.ldif**
Modifier un attribut :Modification	Ex : **Modifier** l'attribut **description** 1. Créer le fichier ldif suivant : dn: uid=user,ou=stagiaire,dc=tmsir,dc=local changetype: **modify** **replace**:description description: stagiaire NTIC de CMFMNTIOE

	2. Lancer la commande : **ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f modif.ldif**
Modifier un attribut :Suppression	Ex : Supprimer l'attribut **description** 1. Créer le fichier ldif suivant : dn: uid=user,ou=stagiaire,dc=tmsir,dc=local changetype: **modify** **delete:**description 2. Lancer la commande : **ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f sup.ldif**
Configuration client Linux	**1.** Installer le packet openldap client : **# yum -y install openldap-clients nss-pam-ldapd** 2. Configurer l'authentification LDAP **:# authconfig-tui** 3. Tester : **# getent passwd NomUtilisateur**

Serveur OpenVPN

Installation	#yum install epel-release openvpn
Vérification d'installation	# rpm -qa openvpn
Démarrage du service	# systemctl start openvpn@server.service
Activation au démarrage du service	# systemctl -f enable openvpn@server.service
Nom et chemin du fichier de configuration	Copier le fichier de configuration du serveur dans /etc/openvpn : **#cd /usr/share/doc/openvpn-2.X.X/sample/sample-config-files/** **server.conf /etc/openvpn**
Configuration	**push "route 10.1.0.0 255.255.0.0"** // **push "redirect-gateway def1 bypass-dhcp**" // rediriger tout son trafic via le serveur OpenVPN **push "dhcp-option DNS 8.8.8.8"** **push "dhcp-option DNS 8.8.4.4" //** Indiquer quels serveurs DNS il peut utiliser pour se connecter à OpenVPN **user nobody** **group nobody //** Exécute OpenVPN sans privilèges une fois démarré, donc fonctionner avec un utilisateur et un groupe de personne. **topology subnet** **server 10.8.0.0 255.255.255.0** //configure OpenVPN pour fonctionner comme un sous-réseau
Configuration certificat	1. #yum install easy-rsa 2. #mkdir –p /etc/openvpn/easy-rsa/keys 3. #cp –rf /usr/share/easy-rsa /2.0/* /etc/openvpn/easy-rsa 4. Dans **easy-rsa** éditer le fichier **vars** et modifier les lignes : **export KEY_COUNTRY="MA"** **export KEY_PROVINCE="JH"** **export KEY_CITY="OUJDA"** **export KEY_ORG="OFFSHORING"** **export KEY_EMAIL="ZTI@ofppt.ma"** **export KEY_OU="OFPPT"** 5. Au niveau du dossier easy-rsa on va créer les certificats : **#source. /vars** **#. /clean-all** **#. /build-ca** **#. /build-key-server $(hostname)** **#./build-dh** 6. Copier les fichiers ca.crt hostname.crt hostname.key dh2048.pem dans /etc/openvpn : **#cp ca.crt hostname.crt hostname.key dh2048.pem /etc/openvpn**
Redémarrer le service	# systemctl restart openvpn@server.service
Test client	**Coté serveur:** Copier les clefs dans la machine cliente /etc/openvpn/easy-rsa/keys/ca.crt

	/etc/openvpn/easy-rsa/keys/client.crt /etc/openvpn/easy-rsa/keys/client.key /etc/openvpn/myvpn.tlsauth **Coté client :** Crée un nouveau fichier avec l'extension. ovpn avec les informations **client** **tls-client** **ca /path/to/ca.crt** **cert /path/to/client.crt** **key /path/to/client.key** **tls-crypt /path/to/myvpn.tlsauth** **remote-cert-eku "TLS Web Client Authentication"** **proto udp** **remote your_server_ip 1194 udp** **dev tun** **topology subnet** **pull** **user nobody** **group nobody**

Quelques Commandes de base

Afficher la capacité DD	**#fdisk –l** ou **#df –h /**
Afficher les information RAM	**#free**
Afficher les information CPU	**#lscpu ou #cat /proc/cpuinfo**
Ps : Afficher les processus actifs ainsi que ces ressources utilisé à un instant t	**#ps aux** **#ps aux |grep bind**
mount : monter un système de fichier	**# mount -t *type_périphérique point_de_montage*** *Ex : #mount -t ext4 /dev/hdb1 /mn* #mount mount -t vfat /dev/hda1 /Dos/C/
mkfs :formater	Formater en ext4 : **#mkfs.ext4** /dev/votre_partition Formater en swap : **#mkswap** /dev/Votre_partition Formater en vfat : **#mkfs.vfat** /dev/Votre_partition
grep : rechercher un mot dans un fichier	**$grep mot nomfichier** **$grep -E [Aa]lias NomFichier** **$ grep -E [0-4] NomFichier** **#ps aux | grep service**
sort : trier les lignes	**-r :** trier en ordre inverse **-R :** trier aléatoirement **-n :** trier des nombres
wc :compteur lignes, mots et caractères	**-l** : compter le nombre de lignes **w** : compter le nombre de mots **-c** : compter le nombre d'octets $ls -l |wc -l #wc -l /etc/passwd #ps -aux |wc -l
uniq : supprimer les doublons	
Sed : Manipuler les fichiers automatiquement	**sed -e "s/[Ff]raise/FRAISE/g**" : substitue toutes les chaînes Fraise ou fraise par FRAISE **sed "20,30d" fichier** : supprimer les lignes 20 à 30 du fichier **sed "/ntic/d" fichier** : supprime les lignes contenant la chaîne ntic
Cut : afficher des zones spécifiques d'un fichier	**$cut -c1 /etc/passwd** : affichera la première colonne du fichier /etc/passwd. ▪ -c1-5 : Permet de sélectionner les colonnes 1 à 5 ▪ **-**c14- : Permet de sélectionner de la colonne 14 à la dernière ▪ **-**c1-3,14-18 : Permet de spécifier plusieurs plages de colonnes. **$cut -d: -f6 /etc/passwd :** affichera le 6eme champ du fichier /etc/passwd, dont le séparateur (``:")
awk : appliquer un certain nombre d'actions sur un fichier	
awk -F ":" '{ $2 = "" ; print $0 }' /etc/passwd	imprime chaque ligne du fichier /etc/passwd après avoir effacé le deuxième champs

awk 'END {print NR}' fichier	imprime le nombre total de lignes du fichiers
awk '{print $NF}' fichier	imprime le dernier champs de chaque ligne
who | awk '{print $1,$5}	imprime le login et le temps de connexion
awk 'length($0)>75 {print}' fichier	imprime les lignes de plus de 75 caractères. (print équivaur à print $
awk '$3>500' /etc/passwd	Imprime les lignes dont le GID est superieur à 500
awk -F : '$3 >= 500 {print "User : " $1 " - GID : " $3}' /etc/passwd **Crontab**	Imprime les lignes dont le GID est superieur à 500 sous forme User :nomutilisateur -GID :Numérogid
GRUB2	La configuration de GRUB2 est composé de trois principales dans des fichiers inclus : 1. **/etc/default/grub** - le fichier contenant les paramètres du menu de GRUB 2, 2. /**etc/grub.d/** - le répertoire contenant les scripts de création du menu GRUB 2, permettant notamment de personnaliser le menu de démarrage, 3. **/boot/grub2/grub.cfg** - le fichier de configuration final de GRUB 2, non modifiable. 4. grub-mkconfig -o <destination> génère une entrée de menu de niveau supérieur le contenu du fichier **/etc/default/grub** GRUB_TIMEOUT=5 GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)" GRUB_DEFAULT=saved GRUB_DISABLE_SUBMENU=true GRUB_TERMINAL_OUTPUT="console" GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet" GRUB_DISABLE_RECOVERY="true"