**COMPTE-RENDU TP Systèmes & réseaux 2**

TJNagence01\*

Login : nicolas mdp :Nico01

Agence 01, serveur serv-11

code porte: c1359x

mdp root mariaDB: DBs11NJT?

mdp apres installation du pack, open-LDAP pour l administrateur, mdp: root

nom d admin: bastiadmin, mdp LDAPs11NJT! ,new mdp: LDAPs11NJTs

MDP samba et unix pour le root: LDAPs11NJT

forme symbolique, octal pour les droits

[Philippe-cavret@u-bourgogne.fr](mailto:Philippe-cavret@u-bourgogne.fr)

Login ILO : login = etudiant mdp = etudiant

connaître 7 couches modèle OSI

3 séances de TP de 4h

Séance 1 : adressage et routage

Séance 2 : DNS / LAMP (15/03)

Séance 3 : Authentification / partage de ressources (29/03)

**12/04 : évaluation technique** -> note /6 pts

**19/04 : Rapport de 40 pages** –> équivalent à un cahier des charges, analyse des choix /7 pts

**10/04 : Texte à trou ou QCM (exam amphi solo) sur les TP** -> /7 pts

Depinfo.u-bourgogne.fr pour le VPN

Portables clients salle TP : login = etudiant

mdp = etudiant

Si le portable est mort => utiliser un boot PXE (Pre eXecution Environment), en faisant F12 sur l’ordi et connecter le portable sur une prise ethernet IEM (câble gris). => accès à un menu => faire entrée => régénération ordi portable

iPXE = évolution de PXE, permettant d’utiliser HTTP

iLO (accessible par navigateur, utile pour setup le serveur, après on utilise ssh pour communiquer avec) => allumer et éteindre serv, installer OS sur serveur (Debian 12)

protocole = ensemble de règles régissant la communication entre deux entités.

On utilise le protocole ssh pour communiquer avec le serveur.

NETINST = installation par le réseau

Package = ensemble de librairies, modules … pour faire fonctionner un programme sur Ubuntu, finit en .deb

Serveur de dépôt de l’IEM = sartre.iem

Partition = partie allouée du disque

Comment partitionner le disque dur ? (en cas de problème sur une partition, les autres ne sont pas endommagées) => choisir le formatage de chaque partition (càd cartographie du disque dur) (plus petite unité d’allocation = cluster)

Format de formatages Linux :

- Ext3 (ancien standard)

- Ext4

- Reiserfs (optimisé pour accès en lecture)

- SWAP (formatage entre mémoire vive et mémoire disque dur) = 1,5 x RAM (max 4096 Mb)

Disque de 500 Gb ?

Partition sur VAR/LOG (logs des utilisateurs), HOME (données utilisateurs). On fait une partition sur un système qui existe.

- / (racine) à 100 GB (là où on met l’OS)

- EFI 1GB

- HOME 20GB

- VAR/LOG 20GB (var ou log)

On taille la partition en fonction du nombre d’utilisateurs, des données.

Les BIOS sont UEFI (gère 128 partitions, de taille jusqu’à 2,2 To)

Bootloader : programme permettant de lancer divers systèmes d’exploitations.

Câble droit : utilisé pour connecter une machine à un élément actif (switch)

Pour connecter 2 ordis ensemble, on utilise un câble croisé.

1 1 3

2 2 6

3 3 1

4 4 4

5 5 5

6 6 2

7 7 7

8 8 8

Câble droit / câble croisé

Interco : serveur-switch, câble marron

Côté privé : câble par groupe.

Deux choix pour configurer adresse IP :

- iproute2 : ip a

- ifconfig

gateway : 1 ou 254

connection du réseau en static et en dynamique

**restart service du réseau :** systemctl restart networking

**supprimer un alias d’adresse ip :** ip addr del [adresse ip]/[val cidr] dev [nom interface réseau]

remplacer del par add pour ajouter une adresse IP.

**Pour rester en root :** su -

**TP1 : étapes de travail**

- config serv + installation debian

**commande pour avoir la version de l’OS** : cat /etc/os-release

Version :

NAME="Debian GNU/Linux"

VERSION\_ID="12"

VERSION="12 (bookworm)"

VERSION\_CODENAME=bookworm

- config interface réseau du serv avec adresse IP en fonction du réseau,

branchements serv avec switch interco et switch privé :

§ ports sur un switch : se voit par 3 ,branchement sur le port 19, on possèdesw alors le 20 et le 21

§ carte réseau principal serveur : ens1f0 172.31.20.130/24

§ réseau interco : ens1f1 192.168.0.11/27

* **installation du package net-tools sur le serveur pour l’utilisation de ifconfig :** apt install net-tools

- config adresse IP du client (100.3.11.10) + définition de la passerelle 100.3.11.1 sur le client

- connection de la gateway du serveur à celui de l’iem 172.31.20.10

-  **pour activer le routage pour une session**: **echo** 1 **>** **/**proc**/**sys**/**net**/**ipv4**/**ip\_forward

- problème sur ens1f2 (carte réseau réseau privée) lors des *restart networking* (ne pouvait pas bring up ens1f2 ->ip address flush dev ens1f2 ->ifup ens1f2) => *restart networking* marche.

- ping client 126.3.15.2 depuis client (100.3.11.10)

**IPTABLES pour aller sur Internet depuis privé :**  iptables -t nat -A POSTROUTING -s 10.3.11.0/24 -J MASQUERADE

remettre a 0 la chaine

exit

dhcp : soit du dynamique soit statique il doit y avoir un client static et un pool en dynamique

Changement de notre adresse de réseau privé en 10.3.11.1 pour une meilleure compréhension.

* mise en place du démon dhcp : /etc/dhcp/dhcpd.conf
* Spécifier les interfaces réseau d’écoute du démon dhcp : modification de interfacesv4 “ens1f2” dans le fichier /etc/default/isc-dhcp-server

mise en place du echo 1 dans le fichier de façon définitive photo 12/03/2024 16h67 => /etc/sysctl.conf : net.ipv4.ip\_forward=1 (ligne décommentée).

test de mise en place des routes avec un ping ?

soit utilisation journalctl en séparant les log même débat que ip route et ifconfig

soit dégradation ng soit r

open ssh -server

**tp1 bis :**

Installation du package dns

commande host

essai host

host [www.u-bourgogne.fr](http://www.u-bourgogne.fr) is an alias for tokyo.dmz.u-bourgogne.fr

commande dig

donne plus d’information le temps que cela a pris notamment

commande nslookup

adresse du dns dans le réseau local puis l’adresse de site rechercher

c’est le serveur tokyo.dmz.u-bourgogne.fr qui répond le [www.u-bourgogne.fr](http://www.u-bourgogne.fr) et un alias pour celle-ci

(unutile de ping un site weeb iem refuse)

**3** Le serveur dns utilisé correspond au serveur DNS de l’iem(172.31.21.35, On peut changer le serveur DNS avec un parametre a la commande dig @8.8.8.8 [www.u-bourgogne.fr](http://www.u-bourgogne.fr) ou avec le fichier /etc/resolv.conf

**4.1** name serveur on a 2 serveur possible

**5.**

on commence par la racine “.” puis celui qui a le domaine u-bourgogne, le serveur dns possède un cache pour optimiser .Le TLD top level domain du . et (fr)

dns1 193.50.50.2

dns2 193.50.50.6

voir 23eme minutes video

POUR LA CONNEXION root en SSH

nano /etc/ssh/sshd\_config

on cherhce la ligne:

#permiterootlogin prohibit .

on enlever le # et on met yes a la place du prohibit

soit: permiterootlogin yes

systemctl restart sshd

pour mettre en place notre DNS on installe le package

apt install bind9

on va d' abord créer la zone normal, pour commencer on va faire une copie de notre fichier named.conf.default-zones

pour ensuite apporter les modifications au fichier de base, (nom de notre agence Bastia)

ajoutez une photo avant après

modification du dns dans le dhcp

/etc/bind/named.conf.local => fichier qui définit le domaine et l’inverse (spécification de fichiers db…)

zone normale => agence.bastia => /etc/bind/db.agence.bastia

–ajouter photo

dans : /etc/bind

nslookup - 10.3.11.1

>agence.bastia revoie ::1

>serveur11.agence.bastia revoie 10.3.11.1

zone inverse => ”11.3.10.in-addr.arpa” => /etc/bind/db.agence.bastia.inv

–ajouter photo

nslookup - 10.3.11.1

>10.3.11.1 renvoie name = serveur11.agence.bastia.

**TP2 :**

Gparted

ssh -y root@ ipDeNotreServeur

modifier sauvegarde bd maria db et posgresql dans la partition réservée BD pour plus de protection

on installe apache

apt install apache2

systemctl start apache2

systemctl statut apache2

pour effectuer les test(accéder au site de notre serveur) on tape dans l url 172.31.20.130

apache utilise un compte systeme [www.data](http://www.data) pour plus de securité

compte system utilise un applicatif il a ses propres doit

https://friendhosting.net/fr/blog/install-apache-on-debian-11.php

commande pour créer un user

>useradd ou >adduser

pour supprimer un user >deluser manuel par exemple.

web1 pour le mot de passe de l' utilisateur web1

pour mettre les droits à web1 on utilise la commande

>chown -R web1 web1/

on creer un répertoire www dans web1

alias et virtual host que l’on créer dans le fichier 000-default.conf :

alias /web1 /srv/web1/www

<Directory “/srv/web1/www”>

On a ajouté “User web1” dans /etc/apache2/apache2.conf.

On a aussi ajouter dans ce fichier :

<Directory /srv/web1>

Options Indexes FollowSymLinks

AllowOverride None

Require all granted

</Directory>

<Directory /srv/web2>

Options Indexes FollowSymLinks

AllowOverride None

Require all granted

</Directory>

voir site <https://friendhosting.net/fr/blog/install-apache-on-debian-11.php> ou video

**20/03 travail plus**

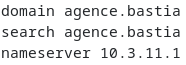
ajout du forwader avec le dns changement dans le dhcp du dns dans dhcp.conf

essai du dns pas de client dans les fichier dns donc ajout de celui-ci plus teste

ajout client fixe dans dhcp

verif avec checkzone ok pour normal et inverse , voir script pour commande

resolv.conf changer la backup et au meme niveau avec le nom resolv.conf\_backup

modif effectuer 

Vérifier depuis le client mais ok depuis le serveur.

ajout dns de bastien serveur 11

ajout alias dns de agence.bastia

attention penser a mettre les “ “ dans apache2/sites-enabled/000-default.conf

user web2, mot de passe: web2

modification du fichier apache2.conf

/etc/apache2/sites-enabled# ln -s /srv/web2 web2

ajouté dans dns l’adresse agence informatique.bastia

Pour web3 : il a fait: a2enmod userdir, cest un module qui permet de publier plusieurs pages html sous un même répertoire utilisateur de /home

question 5 tp2: ssh -X root@172.31.20.130

on a execute gparted

50go pour la partition de la base de données /BD, pourquoi 50go car il nous faut de la place pour stocker la base de données.

nous installons par la suite mariaDB avec la commande suivant: apt get install mariaDB

mdp root mariaDB: DBs11NJT?

on a utilisé mkdir /BD puis mount /dev/sda6 BD

on a fait df -h et lsblk pour verifier le montage de notre partition

on stop mariadb : systemctl stop mariadb

chmod 755 pour donner les droits a mariaDB

on a changer cette ligne dans le fichier /etc/mysql/mariadb.conf.d/50-server.cnf

datadir = /BD/mariaDB

on peut alors redémarrer maridb

on donne les droit pour l’utilisateur mysql les droit dans le dossier

**Nouveau test pour changer la location de mariaDB :**

<https://www.tecmint.com/change-default-mysql-mariadb-data-directory-in-linux/>

déterminer le répertoire utilisé pour stocker les données : mysql -u root -p -e “SELECT @@datadir;” => /var/lib/mysql/

arrêter le service MariaDB : systemctl stop mariadb + systemctl is-active mariadb

création du nouveau dossier pour stocker les tables : mkdir /BD/mariaDB-data

donner les droits : chown -R mysql:mysql /BD/mariaDB-data

copier les données de l’ancien dossier de stockage vers le nouveau : cp -R -p /var/lib/mysql/\* /BD/mariaDB-data/

changer dans mariadb le dossier par défaut : nano /etc/mysql/my.cnf => voir #ajout\_perso de [client] et [mysql]

relancer le service : systemctl start mariadb

Connexion à mariadb = ligne de commande : mysql

—--------------------------PARTIE DANS MariaDB—--------------------------------------------------

Création de la table animaux : CREATE DATABASE animaux;

Création de l’utilisateur ‘usersql’, avec mot de passe ‘usersqlpassword’ : CREATE USER ‘usersql’@localhost IDENTIFIED BY ‘usersqlpassword’;

Vérifier la création : SELECT User from mysql.user;

Donner les droits à ‘usersql’ : GRANT ALL PRIVILEGES ON animaux.\* TO ‘usersql’@localhost;

Supprimer les anciens droits des users et appliquer les nouveaux : FLUSH PRIVILEGES;

Vérifier les droits : SHOW GRANTS FOR ‘usersql’@localhost

Choisir la database utilisée pour les modifs (car il en existe plusieurs par défaut) : use animaux;

Créer une table sur cette bd : CREATE TABLE ANIMAUX(nom\_animal varchar(40) PRIMARY KEY, couleur varchar(40));

Vérifier les tables d’animaux : show tables; (lorsque animaux est sélectionné en BD)

Insérer des valeurs dans la BD (le nom de la table est sensible à la casse) : INSERT ANIMAUX values (‘lion’,’bleu’);

—------------------------------Fin partie mariaDB—----------------------------------------------------------

Installation de php.

activation de l’extension mysqli dans /etc/php/8.2/apache2

modification de la ligne “;extension=mysqli” en enlevant le ;

Installation de mysqli car classe manquante dans php pour charger la BD : apt install php8.2-mysql

montage automatique de la partition /BD grâce au fichier /ect/fstab avec l’utilisation de blkid pour voir le uuid

Rechargement des démons pour appliquer les changements : systemctl daemon-reload

Création de la page php pour tester la table MySql ANIMAUX : on a dû spécifier la socket pour la connexion directement dans le code php.

Installation de postgressql

<https://www.linuxtricks.fr/wiki/debian-10-installer-et-utiliser-postgresql>

Configuration de postgresql : modification de /etc/postgresql/15/main/postgresql.conf pour le répertoire par défaut de stockage des données (cp -arp /var/lib/postgresql/15/main /BD/postgresql-data/15/main/main).

Config mot de passe du super admin postgres : su - postgres

psql -c “ALTER USER postgres WITH password ‘DBs11NJT?’”

Se connecter à Postgres :

connection a l’user postgres

3

**Erreur sur les connexions postgres après modification des fichiers de stockage de donnée :**

postgres@S11:~$ psql -h localhost

psql: erreur : la connexion au serveur sur « localhost » (::1), port 5432 a échoué : Connexion refusée

Le serveur est-il actif sur cet hôte et accepte-t-il les connexions ?

la connexion au serveur sur « localhost » (127.0.0.1), port 5432 a échoué : Connexion refusée

Le serveur est-il actif sur cet hôte et accepte-t-il les connexions ?

utilisation des log de postgres pour debugger on s'est rendu compte que postgres protéger les donner , on avait donner trop de droit au dossier 770 a la place de 750 ou 700 ce qui a eu pour effet de nous bloquer l'accès.

Vérification du répertoire de stockage de PostgresSQL :

sudo - postgres

psql -h localhost => mettre mot de passe

SHOW data\_directory;

—--------------------------------Partie PostgresSQL—------------------------------------------------

Création de l’utilisateur : create user userpostgres with encrypted password 'userpgpassword';

Création de la BD : create database animaux;

Donner les droits à userpostgres : grant all privileges on database animaux to userpostgres;

Connexion avec userpostgres sur la BD animaux : psql animaux -h localhost -U userpostgres.

Manque des droits pour créer la table :

animaux=> CREATE TABLE ANIMAUX( nom\_animal varchar(40), couleur varchar(40));

ERREUR: droit refusé pour le schéma public

LIGNE 1 : CREATE TABLE ANIMAUX ( nom\_animal varchar(40), couleur varch…

Ajout des droits via postgres :

psql -h localhost -U postgres -d animaux

animaux=# GRANT ALL ON SCHEMA public TO userpostgres;

Insérer des données dans la table : INSERT INTO ANIMAUX VALUES ('jaguar', 'brun');

Vérifier l’ajout : SELECT \* FROM animaux;

—------------------------------Fin partie Postgresql—-------------------------------------------------

Installation de postgres car classe manquante dans php pour charger la BD : apt install php-pgsql

création de la page web et vérification du bon fonctionnement.

**PENSER A MODIFIER LES SOCKETS DE BD POUR EVITER DE DEVOIR LES SPECIFIER DANS LES SCRIPTS PHP.**

**TP3 :**

SSII : Société de service en ingénierie informatique.

SSII -> infotech -> 4 employés -> Directeur, Secrétaire, Développeur, Technicien -> Dijon - Local

Annuaire d’entreprise :

* protocole de type X500 dans les années 90, basé sur les 7 couches du modèle OSI, mais plus efficace maintenant.
* Avec le développement du Web, on a essayé de mettre en parallèle IP et les annuaires => LDAP (Lightweight Directory Access Protocol) => Comme pour les pages web et les navigateurs Web, il existe des navigateurs LDAP (LUMA, LDP, …).

LDAP est devenu une norme. LDAP gère la BD, stockée dans une partition dédiée (BD), il faut définir un admin de cette BD, les sauvegardes, les ACL. Pour mettre en place la BD, il faut faire un “dictionnaire des données” (savoir quelle donnée à stocker), ici ce sera un annuaire (Prénom, Nom, Courriel). En LDAP, chaque donnée a son nom et son type figé, on appelle cela un attribut :

* Nom = CN
* Prénom = givenName
* Courriel = Mail

**PORT LDAP : 389 (point d’entrée IP)**

**web : 80**

* LDAP met à disposition des éléments car c’est une norme : O pour Organization, C pour Country, DC pour Domain Components. Ici, pas besoin de O et C car petite société et seulement à Dijon.

**DC = infotechDijon** (dans ce cas-là, sachant que le modèle est figé, on ne pourra pas rajouter de ville par exemple)

OU

**DC = infotech, DC=Dijon** (ce modèle permet de laisser la possibilité d’avoir une autre ville, par exemple DC=Besançon)

* Pour la modélisation de l’admin (appelé Distinguished Name (DN) = chemin d’accès complet à l’admin // Si on met juste le CN, c’est le Relative DN (RDN)) :

CN = admin, DC = infotech, DC = dijon

* Pour ranger les attributs, la norme apportée par LDAP est le Directory Information Tree (DIT). Pour chaque attribut, on va devoir les arranger sur des branches, appelées Organizational Unit.

Pour l’OU : users des users, on peut l’appeler “collaborateur”.

* Pour l’authentification en LDAP, on a besoin d’un login (appelée uid en LDAP) et d’un mdp (userPassword). Ces attributs sont liés aux collaborateurs, il faut donc les ranger dans le même OU que les users.
* Pour authentifier une machine Linux : on utilise le fichier /etc/nsswitch.conf, dans cela il y a deux attributs => passwd : systemd files et groups : systemd files. Il faudra rajouter ldap, mais voir si on le met avant files, entre files et groups, ou après groups.
* Les groupes facilitent la gestion de tous les utilisateurs : primaires (par exemple étudiants) et secondaires (L3 informatique) sont les deux types de groupe chez Linux. Les groupes sont stockés dans une OU : groups, qu’on peut renommer fonction par exemple, avec comme subdivision employé en primaire (GP) / RH et technique en secondaire (GS).
* La jonction entre nsswitch.conf et l’annuaire défini se fait avec libnss-ldapd.
* Pour partager des ressources sur les disques, on utilisera SAMBA, qui a deux versions (client et serveur). SAMBA est une émulation libre de Microsoft. SAMBA a besoin de comptes machines pour démarrer. Ces comptes machines aura besoin d’un OU dans l’annuaire, qu’on peut appeler Computers.

Samba aura un nom de domaine (sambaDomainName) et d’un mdp spécifique (sambaLMPassword et sambaNTPassword) => faire un schéma de ça.

Format LDIF pour implémenter des trucs LDAP => on n’utilise pas.

=> On rajoute une abstraction entre ça et nous : smbldap-tools.

Pour ajouter un user : SMBLDAP-TOOLS.

On utilise Open-LDAP : apt install Open-LDAP

Sur un réseau, on peut partager des données, logiciels (espaces de stockage) et des périphériques (ordi, imprimantes).

ldap inclue aussi la BD,Definir l’admin sauvegarder les ACL

dictionnaire des donner mise en place de l’annuaire (nom-> CN prenom-> givenName courriel-> Mail) chaque donner a nom et type de donner figée on appele cela un attribut

chaque branche et un OU Organizational Unit

**TP3:**

1)

**Ajouter photo schéma Nicolas**

DC: agenceBastia

nom d admin: bastiadmin, mdp: LDAPs11NJT! ,new mdp: LDAPs11NJT

nom user: employe, mdp:

nom ou groups, fonctions(technicien, banquie)

2)

installation des paquets open-LDAP, SMBLDAP-TOOLS, samba.

3)

arret de slapd avant la degradation pour utiliser ldiff

suppression du fichier slapd.d dans le repertoire /etc/ldap/slapd.d

4)

on recupere l’archive wget <http://aragon.iem/~cavret/FichiersconfTP3.zip> qui nous servira d exemple pour constituer notre annuaire d’entreprise permettra l acces aux informations comme le nom, le prenom, le mail, authentifier les utilisateurs ainsi que partager des ressoruces.

On modifie ainsi le fichier slapd.conf recuperer dans la l archive pour avec nous informations, DC: agenceBastia.. etc que l on stockera dans /BD/ldap

pour definir le mdp de l admin on entre la commande ldappasswd -x -D cn=bastiadmin, dc=agenceBastia -W -S dans /etc/ldap

on installe le paquet libnss-ldap avec apt get install.

/etc/nslcd.conf nous permet de verifier la configuration du fichier qui est url ldap://127.0.0.1 et DC= agenceBastia

nano /etc/nsswitch.conf dans password et dans groupe on a ajouter ldap au debut car

l ordi commence par chercher dans ldap puis files puis systemd pour la connexcíon des users

passwd: ldap files systemd

group: ldap files systemd

on modifie le fichier smbldap\_bind.conf : ajout du mot de passe et de admin dans la partie master pour permettre aux outils de modifier ldap.

modification de smb.conf

ldap suffix = dc=agenceBastia

ldap machine suffix = ou=computer

ldap user suffix= ou=employe

ldap group suffix = ou=fonctions

ldap dmin dn=cn=bastiadmin, dc=agenceBastia

ldap ssl = off

ldap passwd sync = Yes

workgroup = agenceBastia

faire un partage public et privé, /home pour le privé, le user doit pouvoir se connecter dans son directory privé, exemple /home/toto -> /home/%u

Si pas d'utilisation attention erreur failed, on ne trouve pas l' utilisateur puisqu il n' existe pas.

attention uid user commence a 1000.

jexplorer pour tester le mdp de bastiadmin depuis le client

MDP samba et unix pour le root: LDAPs11NJT

[prive]

comment=

patch = /home/

browseable = yes

writable = yes

directory mode = 707

create mode = 706

17h9 voir dernière video 31eme minutes tp3

Checker les groupes : net groupmap list

Mapper utilisateurs en Windows et Linux : net groupmap add unixgroupe=banquiers ntgroup”Domain Users”

On crée notre groupe principal Banquiers

pour creer notre groupe: smbldap-groupadd -g 1020 banquiers dans le répertoire /etc/ldap

groupe secondaire secretaires,conseillers

pour creer notre groupe: smbldap-groupadd -g 1021 secretaires

pour creer notre groupe: smbldap-groupadd -g 1022 conseillers

fixer gid uid

Erreur dans le fichier nsswitch.conf (voir fichier nsswitch.conf.etudiant) : ldap mis avant files et systemd => problème de connexion sur root car il existe un user root sous LDAP, donc quand on essaye de se connecter en root, c’est cet user qui est pris et non le root “unix”, hors on ne connaît pas son mot de passe donc pas de connexion possible.

Ordre correct : files systemd ldap

commande pour vérifier les utilisateurs LDAP : ldapsearch -x -b "dc=agenceBastia" -H ldap://127.0.0.1

smbldap-useradd -a -g banquiers -G conseillers -M jimmy@gmail.com -N jimmy -u 1050

Créer user Tristan LDAP : smbldap-useradd -a -A 1 -B 1 -g banquiers -G conseiller

s -M tristan@gmail.com -N HOARAU -S Tristan -u 1051 -P tristan

-A = 1 : autoriser changement de mdp

-B = 1 : forcer changement de mot de passe

-g : groupe principal

-G : groupe secondaire

-M : mail

-N : givenName (nom de famille)

-S : Tristan (Surnom = prénom)

-u : numéro uid de l’user

-P : appel de smbldap-passwd à la fin de la commande pour mettre le mot de passe

MDP users :

tristanLDAP

jimmyLDAP

Changer le directory de l’user : smbldap-usermod -d /home/LDAP/tristan tristan

Configurer fichier partagé : fin fichier /etc/samba/smb.conf

Relancer le service : sytemctl restart smbd

Création fichier partage3.txt d’un user (jimmy) dans le répertoire Share : fonctionne, mais pas les bons droits de sur les fichiers (par exemple, sous tristan, je ne peux pas modif partage3.txt). Cependant, en tant que jimmy, on peut modifier les droits sur ce fichier.

=>Reconfiguration des droits avec smb.conf sur Directory mode & Create mode

**MATRICE DE FILTRAGE**

| De \ vers | routeur (serveur) | internet | réseau privé | réseau d’interconnexion |
| --- | --- | --- | --- | --- |
| routeur (serveur) |  | https, http, dns, dhcp, ~http, ~https | ~samba, ~dhcp, ~dns, ~LDAP, ~mariaDB, ~postgreSQL | dns, sftp, ssh, ~ssh, ~sftp, ~dns |
| internet | ~https, ~http, ~dns, ~dhcp, http, https |  | ~http, ~https | ~dns ? |
| réseau privé | dhcp, dns, samba, LDAP, mariaDB, postgresSQL | http, https |  | dns, ~dns |
| réseau d’interconnexion | ~dns, ~sftp, ~ssh, ssh, sftp, dns | dns ? | ~dns, dns |  |

HTTP : 80 / HTTPS : 443 / SSH + SFTP : 22 / mySQL : 3306 / postgreSQL : 5432 / samba : 137, 138, 139, 445 / DNS : 53 / DHCP : 67,68 / LDAP : 389,636

Explications :

Routeur -> internet : http/https pour les maj, dns pour trouver des sites, dhcp pour l’adresse IP du routeur sur le Web.

routeur -> réseau interco : communications dns pour trouver des adresses auprès d’autres agences, sftp et ssh pour organiser les backup du serveur.

réseau privé -> routeur : requêtes dhcp et dns des clients, accès dossiers partagés samba et authentification par LDAP, accès DB mariaDB et postgresSQL.

réseau privée -> internet : accès internet des clients (forward par le serveur).

Réseau d’interco -> internet : DHCP et DNS ? (mais géré par la fac en principe ?)

Internet -> routeur : connexion aux pages internet depuis l’extérieur

voir script /etc/network/iptables\_ajout …

Sauvegarde avec cron :

* Script d’essai : /home/script\_backup.sh
* Mettre en place les clés vers l’autre serveur avec ssh-keygen depuis notre serveur et copier vers autre serveur (<https://cloud.ibm.com/docs/ssh-keys?topic=ssh-keys-generating-and-using-ssh-keys-for-remote-host-authentication>)

Créer user webmaster avec certains droits :

adduser webmaster => créer webmaster

creation webmaster mdp: masterwebS11:

changement mdp pour jesuislemasterduweb

ajout au groupe sudo de webmaster: usermod -a -G sudo webmaster

visudo (/etc/sudo/sudoers.d …) : ajout de la ligne webmaster ALL=(ALL) NOPASSWD:commande restart apache et nano fichiers config …

Test des commandes depuis webmaster

=>problème : webmaster peut tout faire avec sudo, même les commandes qui n’ont pas été spécifiés dans visudo

suppression de webmaster du groupe sudo : gpasswd -d webmaster sudo

Test ok pour webmaster => il peut exécuter les tâches voulues sur Apache avec sudo sans mdp

modification de smb.cof pour ajouter le netbios name AGENCEBASTIA

Connection partage nom utilisateur jimmy

DOMAIN AGENCEBASTIA

creation de la secrétaire micheline mdp michelineLDAP

mise en place de la backup serv11backup mdp serv11backupmdp

sur le serveur de romain 172.31.20.149 interco 192.168.0.22

mise en place de la sauvegarde avec le script a optimiser pour supprimer l’ancienne sauvegarde seulement après.