Exercice 1 : Métiers Ops

1. Les composants d’un ordinateur sont :

Le processeur fait les calculs

Si une machine n’a pas une bonne ram, elle va être lente

On stocke les données dans le disque dur

Le type du système 64 ou 32 bites

1. Dans paramètres, à propos, il y’a 4 sous rubriques qui donnent des informations clés.
2. Pour modifier les dates systèmes, on se rends dans à date et heure, on a le fuseau horaire, le format de l’heure.
3. Les applications par défaut de Linux sont le navigateur, un client de messagerie, agenda, et des lecteurs de multimédia (un lecteur audio, un lecteur vidéo et un visionneur d’image).
4. On peut créer ou supprimer des utilisateurs en graphique sous linux.
5. Comment installer des applications ubuntu en graphique ?

Les micro logiciels d’un ordinateur (BIOS, UEFI).

Les différents systèmes de fichiers (VFAT, NTFS, ext2, ext3, ext4…). Les systèmes de fichiers qui ont des journaux sont :

Comment accéder à une partition NTFS à partir de Linux ?

Les technologies de disque dur (SSD, HDD, SSHD) le choix se fait par rapport à la performance.

Chaque version de ubuntu a un nom, ubuntu 18 c’est bionic. On peut taper la commande **lsb\_release –a** pour connaitre le nom de sa version.

Pour ajouter des sources de logiciels, il faut avoir la clé du consultant.

Format du disque (GPT, MBR)

Le format MBR date un peu. On ne peut pas dépasser 4 partitions si on utilise ce format.

Windows permet jusqu’à 128 partions avec le format GPT.

Telnet est un protocole orienté caractère alors que ftp est orienté message. Telnet n’est pas sécurisé.

Ssh est sécurisé dans la mesure où les entités utilisent l’algo Diffie Helman pour construire une clé commune de chiffrement.

Un client et un serveur communiquent à travers une paire de socket (IP et port).

L’adresse du serveur de temps de microsoft est **time.windows.com**. On peut afficher l’adresse avec la commande nslookup.

Gpasswd –a nomuser sudo ajoute l’utilisateur au groupe sudo.

Alt+Crtl+F2 pour aller en ligne de commande.

Dans le travail de ops, il est important de laisser l’utilisateur définir son propre mot de passe

Grub est un lanceur de système d’exploitation. Il donne seulement 10 secondes par défaut. Pour pouvoir le modifier on installe grub-customizer.

Windows load manager est aussi un lancer de SE.

// l’informatique est unique

Exercice 2 : sécurité

Notions de iptables :

1. Filtrage de paquet
2. NAT

Filtrage :

1. -p protocole à utiliser
2. -j la politique (REJECT, ACCEPT, DROP)
3. -s pour définir la source

La politique DROP permet d’être invisible dans un réseau

Passwd -l nomuser pour verrouiller le mot de passe, -u pour déverrouiller

Certaines régles de sécurités peuvent se contredire, comment donner la priorité ?

Il est important pour moi de savoir fixer la politique par défaut, la bonne politique chez les noirs serait de tout bloquer et autoriser les services qu’on veut.

Sous Linux il y’a des politiques par défaut

Exo : afficher la politique par défaut sous windows et sous Linux.

**Le protocole http**

* Développer des API (Interface de programmation)
* Utiliser des API pour administrer des plate-forme réseaux et télécoms
* Gérer des réseaux définis par logiciels (SDN)
* Gestion et hébergement de sites web
* Le protocole de signalisation SIP utilisé en ToIP s’inspire du protocole http

1. Prise en compte des caractères accentués
2. Hébergement de sites par dossier
3. Comment faire pour que apache puisse exécuter du code php (libapache2-mod-php)
4. Comprendre les verbes ou méthodes http (GET, POST, PUT, DELETE, PATCH)
5. Comprendre les formats des messages http

* 1XXX : réponses provisoires ;
* 2XXX : réponses définitives ;
* 3XXX : réponses de redirections :
* 4XXX : réponses erreurs côté client ;
* 5XXX : réponses erreurs côté serveur.

1. Clients HTTP avancés : curl et postman.
2. Maitrise de curl : curl –X méthode… “URL”
3. Gestion de base données sous Linux

* Etre capable de faire le CRUD ;
* Se connecter au server BD ;
* Création de la BD banque ;
* Utilisation d’une base de donnés en réseau et activation du journal d’événement de Mysql ;
* Paramètres :

1. Bind-address= 0.0.0.0
2. General\_log= 1
3. General\_log\_file= /var/log/mysql/mysql.log

**Les modules PHP**

Php-mysql : pour la gestion des BD ;

Php-json

Php-curl

**\*\*\*Algo de connexion à une bd dans un programme php\*\*\***

1. On se connecte à la base
2. On prépare la requête dans une variable
3. On exécute la requête
4. On traite éventuellement les résultats

NB : le verbe PUT met ses données dans la ligne de requête.

Php est un langage de programmation dynamique, on peut y générer du code html

**\*\*\*\* Messagerie classique (email) \*\*\*\***

Paquets à installer :

* Postfix
* Dovecot-imapd
* Dovecot-pop3d
* Roundcube
* Roundcube-mysql

**Entités de la messagerie**

3 programmes appelés agent de messagerie qui collaborent dans le service.

1. MUA (Mail User Agent) qui s’occupe de l’écriture ou lecture de mail

Exemple : Thunderbird, roundcube

MUA est appelé aussi client de messagerie.

1. MTA (Mail Transfert Agent) ou serveur SMTP qui s’occupe de la réception des mails venant des clients, soit les transfère à un autre agent qui s’occupe de la distribution locale soit les transfère à un autre MTA.

Exemple : Postfix, exim4

1. MDA (Mail Deliver Agent) qui s’occupe de la distribution des lettres dans les boites des utilisateurs.

Exemple : Dovecot

NB : un serveur de mail complet c’est MTA + MDA.

**Protocoles de la messagerie**

4 grands protocoles de messagerie

1. SMTP (Simple Mail Transfert Protocol)
2. POP (Post Office Protocol
3. IMAP (Internet Mail Access Protocol)
4. MIME (Mutlipurpose Internet Mail Extension)

Y’a 2 format de boites à lettre :

* Format mailbox: tous les mails d’un utilisateur sont concaténés dans un même fichier.
* Format maildir: chaque utilisateur a un dossier dans lequel il y a au minimum 3 sous-dossiers (file-d’attente >> nouveaux mails >> mails lus)

**\*\*\*\* DNS \*\*\*\***

Un enregistrement c’est juste une correspondance.

Le nom complet de la machine est le nomdelamachine.domaine.

SOA: Start Of Authority. Syntaxe: nomdomaine IN SOA nomdel’utilisateur.

CNAME c’est pour surnommer les machines.

Mise en place :

1. Installation des paquets bind9 et bind9utils
2. Déclaration de zones (domaines)
3. Création du fichier d’enregistrement

**\*\*\*\* Bureau à distance \*\*\*\***

**VNC**

Guacamole à installer

Exo : comment synchroniser les deux sessions entre la machine A et la machine B ?

Exo : le problème de type de sécurité entre vnc et vini-server

Exo : combiner ce qu’on vu avec le dyndns.

A faire pour le prochain cours py mysql.

**\*\*\*\* Bases de données \*\*\*\***

* Bases de données relationnelles
* Bases de données non relationnelles

Exemple de BD non relationnelles : MongoDB, Cassandra

Exo : installer MongoDB

Règle générale : Pour se connecter à une BD, il faut un pilote (driver).

En Java pour se connecter à une BD, il faut le pilote JDBC (Java DataBase Connectivity).

Exemple : python-mysql

On fait le commit sur la connexion alors qu’on exécute sur le cursor.

Pip3 est un utilitaire qui permet d’installer des modules pythons.

Il est impératif dans le programme :

1. Préciser dans l’entête des messages http le type de contenu
2. Séparer les parties entête et corps par une ligne vide
3. Pour pouvoir utiliser les formulaires avec cgi, il fait absolument importer les modules cgi,cgitb

Avec la méthode de récupération des données d’un formulaire, peu importe la méthode d’envoie des formulaires.

Comment crée-ton un module python ?

On crée un fichier dans lequel on importe la fonction.

On a vu deux manières d’importer les modules : crud.lecture() et le from

\*\*\*\* Le journal d’événement est très important.

Un développeur back-end doit maitriser les clients avancés tels que **curl** pour tester ses programmes.

Avec curl pour utiliser DELETE on met les données au niveau dans le corps.

Truncate table nomtable pour supprimer toutes les données d’une table.

* Import et export dans une BD

1. A partir d’un fichier SVG, remplie une table d’une BD
2. Sauvegarde et restauration de BD

* Sauvegarde et restauration de BD avec mysqldump
* Les applications utilisant une BD sont livrées avec des scripts SQL à exécuter pour générer les données de l’application.

C’est quoi la notion de sous requête ?

\*\*\*\*APPLICATION\*\*\*\*

Free Radius

Entités du service

* Supplicants (terminaux, users)
* Clients radius (NAS: Network Access Service)
* Serveur Radius

À faire

1. On installe freeradius et freeradius-mysql
2. On crée un compte pour le point d’accès

Les bases de données NoSQL sont généralement utilisées en BIG-DATA

* Pandas
* Cassandra
* Spark
* Mongodb

Les annuaires LDAP

* Active Directory de Microsoft
* openLDAP sous Windows et Linux

EC2 : Concepts généraux sur les annuaires LDAP et mise en œuvre

Les annuaires étant beaucoup utilisés en TIC, il est important de les maitriser.

Quelques cas d’utilisations d’annuaire LDAP

* Un annuaire LDAP peut être utilisé pour stocker les informations sur les comptes systèmes
* Cas d’Active Directory de Microsoft
* Cas de Linux avec l’utilisation du service de gestion de noms NSS et le service d’authentification à chaud (PAM)

Application pratique : Centralisation des comptes utilisateurs pour avoir un contrôleur de domaine.

* Un annuaire LDAP peut être utiliser comme base d’information d’authentification pour accès à un réseau sans fil ou filaire par l’intermédiaire d’un serveur AAA tel que RADIUS.
* Un annuaire peut être utilisé pour agréger des sources de données **méta-annuaire**

**Bilan :**

Coupler freeradius et mysql

**Méthodologie :**

* Mysql-server
* Freeradius-mysql pour avoir le schéma de base de données mais aussi les share object de connexion de freeradius à mysql
* Donner des paramètres de connexion de freeradius à la base : mods-available/sql et créer un lien vers mods-enable/sql
* Aller dans le sous dossier de mods-config/sql/main/mysql pour avoir les schémas schéma.sql et setup.sql.

En tant qu’ingénieur je prendrais le temps de personnaliser les scripts sql avant de les exécuter.

* On active la prise en compte de sql dans les sections **authorize, accounting et post-auth** du fichier site-available/default

Couplage de freeradius et LDAP

* Installer freeradius-ldap
* Paramétrer Radius pour lui donner les éléments de connexion à LDAP dans mods-available/ldap
* Création de liens entre mods-available/ldap et mods-enable/ldap
* Aller dans le fichier sites-available/default pour activer la prise en compte de LDAP

NB : j’ai appris les modes de sécurités des points d’accès

* None : la sécurité n’est pas activée
* Wpa-personnel : un secret partagé pour tout le monde
* Wpa-entreprise : on passe par un serveur Radius pour l’authentification

Je me suis rendu compte qu’un client Radius tel qu’un point d’accès doit partager un secret avec son serveur radius sinon le serveur radius refuse de répondre à ces requêtes.

J’ai remarqué aussi que freeradius accepte simultanément plusieurs bases d’informations : le fichier **users, BDR, LDAP**.

La pub dit que LDAP est très important, il faut maitriser ses concepts théoriques.

Les types de bases de données qu’utilise LDAP : mbd, bdb, hdb. Avec hdb et mdb on peut stocker plusieurs informations.

À connaitre par Coeur:

* Nis.schema: contient les classes posixAccount, shadowAccount et posixGroup
* Core.schema : contenant les informations d’un utilisateur. On y trouve les classes person, inetOrgPerson.
* Inetorgperson.schema : contenant la classe inietorgperson permettant de stocker les informations des employés d’une entreprise
* Cosine.schema : contenant des informations relatives à DNS (DNSdomaine qui permet de coupler bind avec ldap).

Pour modifier, ajouter, changer de dn, on le fait dans un fichier ldif alors que pour supprimer on exécute directement la commande.

**\*\*\*\*\*\*\*\*\*\*\*Contrôleur de domaine avec LDAP**

Etape 1 : le login et le mot de passe se trouvait dans un même fichier /etc/passwd.

Etape 2 : on enlève le mot de passe dans /etc/passwd en le remplaçant par **x** puis en le stockant sans /etc/shadow.

Notre architecture :

1. Un serveur LDAP avec des objets définis par les classes :

* posixAccount
* shadowAccount
* inetOrgPerson
* posixGroup

1. On dispose des machines linux qu’on va intégrer dans le domaine

A faire au niveau des clients :

On installe les paquets : apt install sssd libpam-sss libnss-sss

Sssd exige un canal sécurisé pour l’échange de mot de passe avec le serveur LDAP. Pour cela, il a fallu générer :

* Un certificat de l’autorité de certification
* Une clé privée pour le serveur LDAP
* Un certificat pour le serveur LDAP

Le système PAM est à maitriser notamment les règles d’authentifications, de gestion de mot de passe et de gestion de session.

TP personnel : étude du service PAM.

**Messagerie instantanée**

Le protocole du service est XMPP appelé Jabber. Un serveur XMPP écoute par défaut sur le port 5222 et utilise le protocole de transport TCP. Il échange des données avec un serveur XMPP au format XML.

Il y’a plusieurs serveur XMPP qui existe comme prosody, openfire. XMPP est le protocole qui a permis la mise en place de Facebook. Google aussi a beaucoup soutenu ce protocole.

Le webrtc est standard de communication en temps réel à travers le web.

Le websocket est un mécanisme permettant de créer un canal bidirectionnel entre des navigateurs en vue de faire passer des communications en temps réel.

**Exo :**

Quand on a plusieurs versions java sur sa machine, comment choisir une application donnée la version qu’il faut ?

Quand on plusieurs versions de php, comment choisir la bonne version selon l’application ?

Idem pour python ?

Exercice : DNS coupler avec LDAP

\*\*\* synchronisation de base de données

Il y’a trois entité en sécurité pour la certification : l’autorité de certification, le certificat du serveur et celui du client.

**A lire ce week-end:**

La programmation Shell

Administration L2TR

Document official LPI

LPIC2

Linux provident d’un grand système UNIX.

1. Les distributions Linux :

* RED HAT (rpm) sous distribution fedor a -- centos
* DEBIAN (yum)
* SUSE

1. Environnement graphique

* KDE, GNOME

1. Développement d’internet

* Beaucoup de service internet (proftpd, vsftpd, apache2…)

Ce qui a entrainé l’adoption massive en tant que serveur internet.

1. Suite bureautique

* Traitement de texte
* Tableau
* Présentation

1. Ubuntu

* Postes de travail

Exo : comment transformer un disque de format MBR en GPT ?

Rsyslog à rechercher

C’est quoi la notion d’API ?

C’est quoi la notion de Framework ?

Tp :

1. Les partionnements, montage des systèmes de fichier NFS, CIFS
2. Automatisation de montage de système de fichier /etc/fstab
3. Montage à la demande avec autofs.
4. Systemd.automont

La différence entre USB 3.0 et 2.0 ?

Systemd remplace etc/inittab et est le premier processus lancer par le noyau au démarrage.

Systemctl set default : pour fixer un niveau par défaut

Comment ordonner le démarrage des services ?

Exo : apprendre à générer le démarrage des services

Systemctl deamon reload : après avoir modifier un service gérer par systemd

Quelle est la différence entre heure système et heure matérielle ?

\*\*\*\*\*\*Gestion de systèmes de fichiers réseaux

Objectifs :

Connaitre les possibilités de partage de ressources en réseau

1. NFS (qui peut être utilisé aussi bien sous Windows que Linux), NFS, initialement ne gérait pas les utilisateurs mais affectait des ressources à des UidNumber.

Solution : faire en sorte qu’un UidNumber soit unique dans votre réseau en faisant appel à un serveur NIS (un contrôleur yellow page).

Aujourd’hui nous sommes à la version 4 de NFS.

Idée :

1. Une machine partage (exporte) des dossiers vers d’autres machines.
2. Les machines clientes montent ces dossiers sur des points de montage qui sont des répertoires en local (mount). Dès que la machine cliente redémarre, il faut remonter les ressources.

Pour régler cette question de montage automatique de ressources au démarrage, on a fait appel au fichier de gestion de tables de systèmes de fichiers qui est **/etc/fstab**

L’inconvénient du montage automatique dans /etc/fstab des grands parents : immobilisation des ressources réseaux alors personne n’utilise la ressource montée

Pour régler cette question de gaspillage inutile de ressources réseaux, on a mis en place le système **autofs** qui permet de faire un montage à la demande.

Principe :

1. On définit un point de montage global et le fichier devant contenir comment accéder à la ressource dans **/etc/auto.master : /dossierparentpartage /etc/autonomchoisi –ghost,--timeout=30**
2. On crée le fichier **/etc/auto.nomchoisi : nommontage –fstype=cifs,user=login,pass=mdp://IPserveur/nomdepartage**
3. On redémarre le service **autofs**
4. Accès à la ressource :

On va dans **/dossierparentpartage/nommontage**

**Avantage de autofs :** la ressource n’est montée que si on manipule le point de montage.

En exo : expliquer comment faire un montage à la demande :

1. Sur un ressource ssh (penser à sshfs)
2. Sur une ressource d’un serveur FTP (penser au système fuse)

En 2023, on peut changer autofs par systemd.automount avec 2 méthodes :

1. Faire la déclaration des ressources dans **/etc/fstab**
2. Faire la déclaration dans le répertoire **/etc/systemd/system**

**Tp1 : créer un probléme dans /ect/fstab et le régler**

**Tp2 : quelles sont les types de gestionnaires de réseaux sous Linux ?**

Dump permet de sauvegarder de manière automatique.

**Synthèse :**

1. Fichiers virtuels

* /proc/sys/net/ipv4/ip\_forward
* Sysctl
* Combinaison avec ip tables

1. sysVinit contre systemd

* niveaux de démarrage

1. systemd-automount

* les anciens systems de montages
* Structure d’une ligne du fichier /etc/fstab
* Autofs (montage à la demande) (nfs,cifs,sshfs,fuse)

1. iSCSI

Target : la machine qui a la ressource

Initiateur c’est le client

Au niveau du serveur :

1. On installe tgt
2. On va dans le dossier /etc/tgt/conf.d pour créer un fichier de publication de ressources se terminant par .conf :

* Nom de la ressource
* Le chemin de la ressource

**Bilan partiel phase 1**

1. **Maitrise des systèmes d’exploitation**

* Versions de windows utilisateurs : familiale, professionnelle et entreprise.
* Affichage des différentes informations
* Services de bases
* Sécurité minimale
* Installations des logiciels

1. **Services réseaux de base**

* Services de connexions à distance (telnet, ssh)
* Services de bureau à distance (VNC, RustDesk, environnement graphique : gnome, xcfe4)
* Service FTP
* Service Web
* Service de messagerie classique
* Service de tchat (XMPP avec openfire et spark)
* Service de BD
* Service DNS
* Service ToIP
* Journal d’évènement des services apache et mysql
* HTML et PHP
* Php-Mysql
* Clients avancés http : curl et postman
* CGI (Common Gateway Interface) avec apache

1. **Bases de données**

* Plusieurs types de bases de données: noSQL (Cassandra, MongoDB, Pandas), bases de données relationnelles, Annuaires LDAP
* Requêtes SQL avancées
* La maitrise des fonctions d’agrégation
* Chargement des données à partir de fichier CSV
* Sauvegarde et restauration de BD
* Paramétrer une application pour l’utilisation d’une BD (installateur : openfire, accompagnée d’un schéma SQL : freeradius)
* Comment faire pour qu’une application qui a besoin de BDR puisse avoir fonctionner ?
* Faire accompagner son application du schéma de la base : freeradius
* Faire un installateur qui demande les paramètres de connexion à l’administrateur et créer le nécessaire : cas de openfire
* Savoir sauvegarder ses bases de données avec mysqldump
* Les annuaires LDAP : DIT, dn, classe d’objet, schémas, classes abstraites (Top), classes auxiliaires, classes de type structural
* Requêtes LDAP (ldapsearch, ldapmodify,ldapdelete,ldapmordn)
* Comment paramétrer une application pour qu’elle utilise LDAP ?
* Couplage du serveur d’authentification RADIUS avec LDAP
* TP de sécurisation d’un réseau sans fil (mode de sécurité : NONE, Wpa-personnal, Wpa-entreprise avec l’utilisation de radius
* Freeradius supporte de manière simultané plusieurs systèmes d’infos : texte, BDR et LDAP
* SSSD : gère beaucoup de moyens d’authentification (SSSD+ LDAP, NFS, Kerberos à venir dans le cours de sécurité, Samba)

1. **Expert en système Linux : LPI**

* Noyaux Linux : partage de connexion internet
* Technologies : RAID, LVM, iSCSI
* Systemd
* Autofs
* Systemd.automount : n’importe quelle ressource
* Crontab et at

A revoir :

* POO
* Conception Orienté Objet

Td

1. Une zone de swap est une zone située au niveau du disque, que le système utilise quand la RAM est saturée.
2. On utilise la commande dd pour créer un fichier swap avec l’option **bs** et **count**.
3. On formate un fichier swap avec la commande mkswap.
4. On active une zone de swap avec swpaon et on désactive avec swapoff.
5. On affiche une zone de swap avec swapon –s ou avec cat /proc/swaps.
6. Free –h permet de voir les statistiques de la RAM
7. /etc/fstab

**Dd : device to device**

1. Copier physiquement disque 1 sur un disque 2 : dd if=/dev/disk1 of=/dev/disk2
2. Sauvegarder un disque sous forme de fichier bloc : dd if=/dev/sdb of=/dev/sauve.img
3. Inverse de la question 9
4. dd if=/dev/cdrom of=fichier.iso bs=2048
5. Dd : device to device

Avec LVM on peut élargir la taille des partitions et les diminuer à chaud

1. On prépare d’abord les disques physiques, les transforme en volumes physiques ensuite les ajouter dans un groupe de volume, on crée des volumes logiques qui sont l’équivalent de partitions et en fin on formate le système de fichier avant l’utilisation
2. Définition de PV, VG, LV
3. L’interer de LV par rapport à une partition c’est qu’on peut augmenter le volume à chaud
4. La commande fdisk –l | grep sd affiche le nombre de disques sd et de partitions
5. Apt install lvm2
6. Pvcreate
7. La commande wipefs –a permet d’effacer la table de partition concernant GPT.

Une archive permet d’arranger des documents en ajoutant une étiquette. Pour archiver on utilise **tar –cvf nom\_archive /nom\_dossier.** La bonne manière c’est **tar -cvPf**

Pour voir ce qui se trouve dans une archive on fait **tar –tvf nom\_archive**

Comment extraire un fichier d’une archive ? Pour ce faire on tape la commande **tar –x –extract** ou **–get**

Pour compresser on utilise **gzip nom\_fichier\_archivé**

**NB : en informatique, on ne peut pas compresser un dossier. Il faut d’abord archiver le dossier pour qu’il devienne un fichier.**

Exo : comment se connecter avec SSH par clé ?