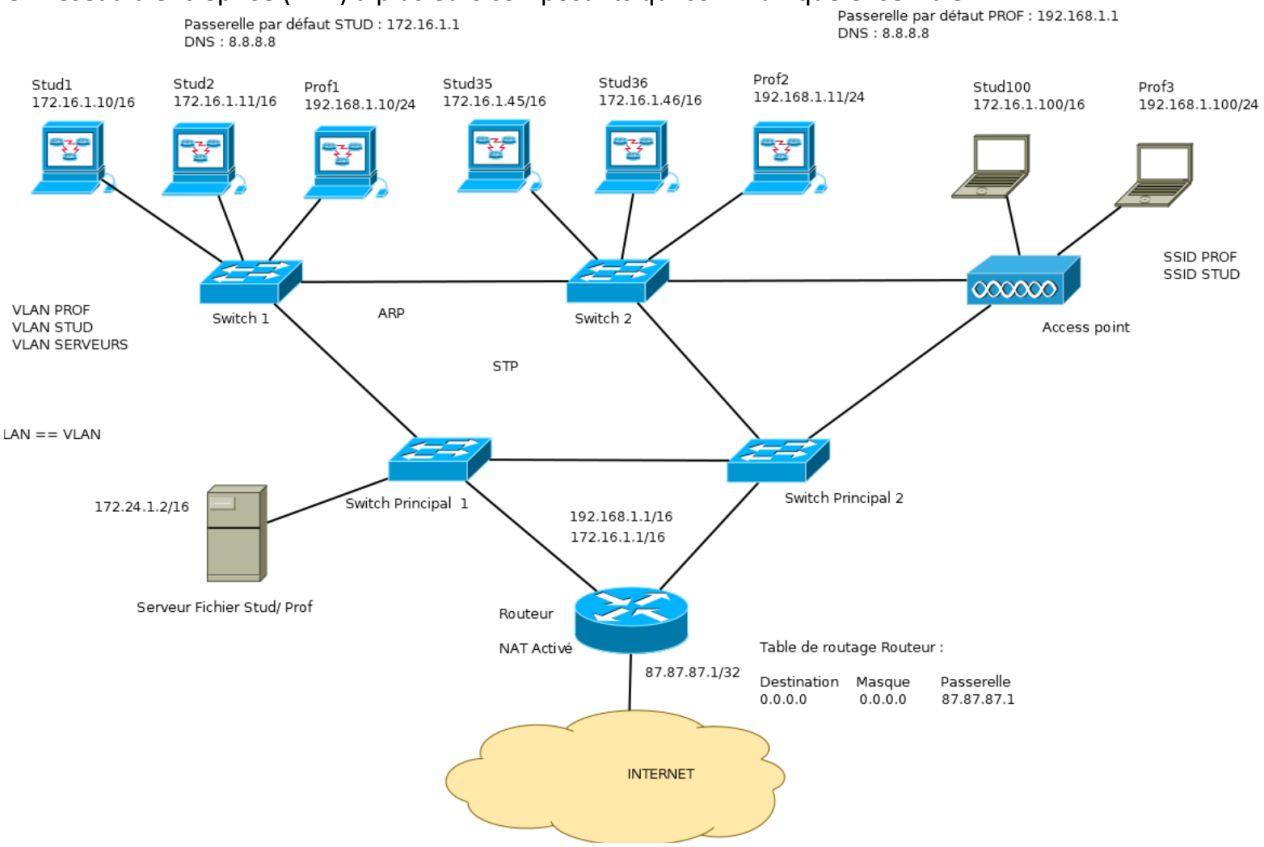
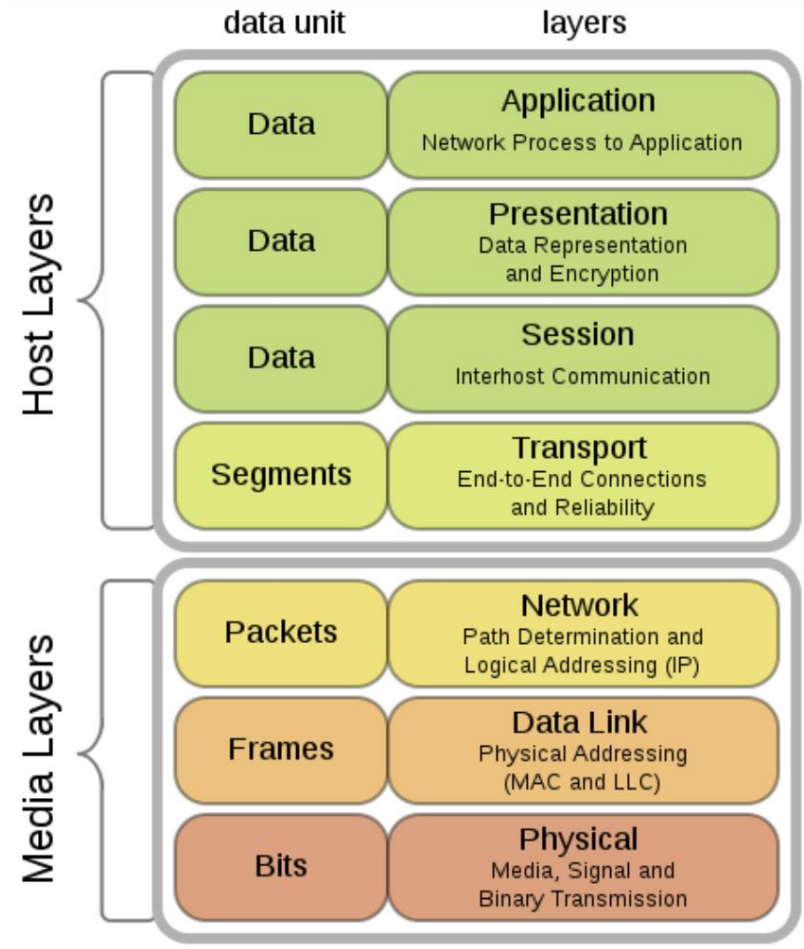
Réseaux et infrastructure

Un réseau d'entreprise (LAN) a plusieurs composants qui communique ensemble.



A connaitre le modelé OSI



Couche 1 : Matériel

Plusieurs solutions pour implémenter son réseau physique existent. Cependant l'utilisation d'un réseau avec une topologie en étoile et des câbles Ethernet s'impose.

Couche 2 : Liaison de données

Dans cette couche on parle de frames (trame). L'identifiant d'une machine est la MAC address. Le composant principal de cette couche est le switch qui conserve une table d'address permettant d'associer chaque port du switch à une adress MAC. Elle se mets à jour automatiquement en fonction de l'activité du réseau.

VLAN

La vlan (Virtual Local Area Network) permet de séparer certains ports d'un switch par rapport a un autres. Chaque switch aura alors une table par VLAN. Son intérêt ? pouvoir utiliser un switch pour connecter des machines de réseaux diffèrent tout en ayant une sécu.
Les ports seront attribués un numéro de VLAN et les ports ayant un même numéro pourront communiquer entre eux.

L'interet des VLAN est multiple :

- Sécurité : séparation en sous réseaux

- Économique : on peut utiliser au maximum les ports disponibles sur les switchs
- Bande passante : optimisation de la bande passante en réduisant la taille des domaines de diffusion
- Facilité de gestion : on peut facilement changer le numéro de VLAN d'un port et donc faire basculer une machine d'un sous réseau a un autres.

STP

L'architecture en Etoile a un point faible, c'est le cœur, si celui-ci tombe les machines ne peuvent alors plus communiqué.

Le spanning tree protocol va autoriser à créer des boucles en désactivant logiquement certains liens et réactivant en cas de pannes.

Couche 3 : réseau

Cette couche est implémentée dans une infrastructure par des routeurs. Ils feront transiter des paquets IP d'un réseau a un autre. L'identifiant d'une machine dans cette couche est l'IP. Cette IP est composé d'un masque et d'une adresse réseaux.

Adresses spéciale (à connaitre)

Plage	Usage
127.0.0.0/8	Boucle locale
10.0.0.0/8	Adresses privées
172.16.0.0/12	Adresses privées
192.168.0.0/16	Adresses privées
224.0.0.0/4	Multicast

La boucle locale permet de créer un mini-réseau sur la machine permettant à l'user de tester un service réseau sans y êtres connecter. Les adresses privées sont réservées pour être utilisées dans les réseaux LAN et ne sont pas routables sur internet.

Commande réseau (à connaitre)

Linux	Windows	Explication
ifconfig / ip addr	ipconfig	Configuration / Consultation des informations IP d'une machine
route	route	Configuration / Consultation des informations de routage d'une machine
ping	ping	Tester la connectivité IP d'une machine
traceroute	tracert	Voir le chemin parcouru par un paquet IP

ARP

Il permet de retrouver l'adresse MAC s'une machine sur base de son adresse IP. Envoie un broadcast et la machine avec l'adresse IP renvoie son adresse MAC. Il existe un cache ARP pour éviter de faire trop de requête ARP.

Découpage en sous-réseaux

2.5.5 Découpage en sous-réseaux

Vous devez être capable de découper un réseau en sous-réseau. Ceci peut être demandé dans la partie pratique de l'examen. La tâche d'un administrateur système sera de découper de manière intelligente son réseau. Ce découpage permet d'isoler les réseaux pour des raisons de sécurité et d'efficacité. Il devra calculer une adresse réseau et un masque de sous-réseau. Celui-ci permettra de donner le nombre de machines maximales que le sous-réseau pourra accueillir.

Exemple : un réseau employés composé de 25 machines

1. 25 machines → recherche de la puissance de 2 supérieure à 25 → 2^5
2. Choix d'une adresse réseau parmi les plages d'adresses privées : 192.168.5.0 par ex.
3. Calcul du masque : 32 bits – 5 bits (puissance de 2 calculée précédemment) → /27
4. Résultat : 192.168.5.0/27

Une plage d'adresses pour un réseau débutera par l'adresse du réseau et se terminera par l'adresse de diffusion(broadcast). Entre ces 2 adresses, les autres adresses peuvent être utilisées par des machines.

Exemple : un réseau employés composé de 25 machines

1. Adresse réseau : 192.168.5.0/27
2. Adresse machine 1 : 192.168.5.1/27
3. Adresse machine 2 : 192.168.5.2/27
4. Adresse machine … : …
5. Adresse broadcast : 192.168.5.31/27

L'adresse de diffusion(broadcast) est la dernière adresse de la plage calculée. Tous les bits machines de cette adresse sont donc à 1.

Adresse réseau : 192.168.5.0/27 → 192.168.5.00011111 → 192.168.5.31/27 Astuce : une adresse réseau est toujours paire et une adresse de diffusion toujours impaire !

Table de routage

Le composant principal de cette couche est le routeur qui maintient une table de routage.

Une table de routage est un tableau qui précise pour une destination d'un sous-réseau (adresse réseau + masque) une passerelle (adresse IP d'une machine/routeur)

Passerelle par défaut

Chaque machine possède une passerelle par défaut. Celle-ci sera utilisée lorsque aucune règle plus précise ne peut être utilisée dans la table de routage. Grâce à cette passerelle par défaut, il est plus simple d'automatiser la connexion de machines clientes à son réseau. Il suffira de fournir à chaque machine cliente une adresse IP, un masque et une passerelle par défaut et celle-ci pourra utiliser notre réseau. Cette automatisation se fait via un serveur DHCP.

Couche 4 : Transport

Permet la communication entre applications. Elles respecteront le modèle client-serveur. Cette couche utilise la notion de port. **Une application sera donc identifiée par son port.**

A CONNAITRE

Application	Port réservé
Web(HTTP)	80
SSH	22
HTTPS	443
DNS	53

Service réseaux (DHCP-DNS-NAT)

DNS

Le DNS permet de traduire un nom de domaine en une adresse IP et inversement. Pour traduire les noms de domaine Internet, on peut utiliser des serveurs DNS tiers comme celui de Google. Cependant, dans un réseau d'entreprise, l'administrateur système installe un serveur DNS pour gérer les noms des machines, assurer la redondance en cas de défaillance, et gérer les enregistrements DNS liés au nom de domaine de l'entreprise.

Configurations DNS

- SOA: start of authority (info générales sur la zone DNS)
- A : enregistrement d'un hôte (correspondance Nom -> IP)
- CNAME : alias
- PTR : Enregistrement d'une IP (correspondance (IP-> Nom)
- MX : Mail server (adresse IP du serveur mail de la zone)
- NS : name server (serveur DNS pour la zone)

Exemple d'une conf (pas connaitre)

```
$TTL    604800
@       IN      SOA     ns.monbeaurezo.be. emailadmin.monbeaurezo.be. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

      @       IN      NS      ns.monbeaurezo.be.
      @       IN      A       127.0.0.1
      @       IN      AAAA    ::1
      ns      IN      A       192.168.1.1
      h1      IN      A       192.168.1.5
      aliasH1 IN      CNAME   h1
```

Résolution d'un nom

Il est très important de ne pas oublier que toute résolution de noms sur une machine commence par l'inspection du fichier hosts. Ce fichier est présent sous Linux à cet endroit /etc/hosts et sous Windows à cet endroit c://windows/System32/Drivers/hosts.

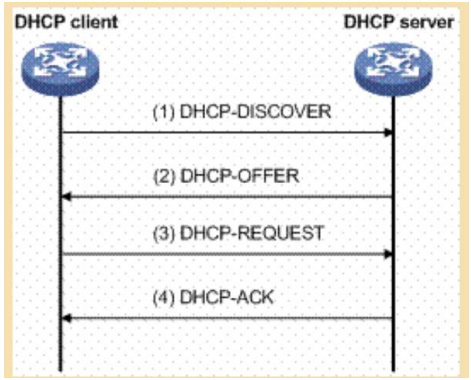
Les administrateurs système utilisent abondamment ce fichier pour tester des services car cela évite l'installation d'un serveur DNS. En prod, un serveur DNS sera employé.

DHCP

Pour qu'une machine cliente puisse connecter à un réseau et surfer sur internet, elle a besoin au minimum des informations suivante :

- Se voir attribuer une adresse IP et un masque au sein de ce réseau
- Obtenir une passerelle par défaut (pour aller sur internet notamment)
- Obtenir des serveurs DNS (traduire les noms en adresse IP)

Un serveur DHCP permettra de répondre à ces besoins de manière automatique.



Les informations reçues par le serveur DHCP ne seront valables qu'un certain temps. On parle de bail. Le client pourra évidemment renouveler son bail.
un admin sys installera plusieurs serveurs DHCP pour se prémunir de la panne d'un serveur. 2 serveurs DHCP ne pouvant pas distribuer les mêmes adresses IP, l'admin système devra répartir ces adresses de manière intelligente entre les 2 serveurs.

NAT

Le NAT est utilisé par les réseaux d'entreprise pour traduire les adresses IP privées de client en adresses publiques routables sur internet.

Source NAT (SNAT)

Chaque machine cliente dans le réseau de l'entreprise utilisera une adresse IP privée et se connectera à Internet via un routeur, agissant comme passerelle par défaut. Le routeur, ayant une adresse IP publique fournie par le fournisseur d'accès à Internet et une adresse IP privée interne, utilisera le NAT pour traduire les adresses IP sources des paquets sortants en utilisant son adresse IP publique.

Le routeur va en fait identifier les machines clientes via un port choisi aléatoirement.

Avant NAT	Après NAT
IP Source : 192.168.1.2	IP Source : 87.87.87.1 (adresse du routeur)
IP Destination : 89.89.89.1	IP Destination : 89.89.89.1
Port Source : /	Port Source : 10527 (port aléatoire, le routeur note l'association de ce port à la machine natée à savoir 192.168.1.2)
Port Destination : 80	Port Destination : 80

Port Forwarding

Par défaut il est impossible de se connecter à une machine d'une entreprise depuis l'extérieur. La seule machine atteignable est le routeur. Pour atteindre un serveur présent dans le réseau de l'entreprise il nous faut configurer le NAT pour qu'il fasse du port forwarding.

Le principe est : pour accéder au serveur de l'entreprise, on attribue un port sur le retour dédié à ce serveur. Dès que le retour reçoit une connexion de l'extérieur pour ce port, il transfère les paquets vers l'adresse privé du serveur.

Le port forwarding est largement utilisé dans les réseaux, en particulier avec la virtualisation. Dans des environnements comme VirtualBox, où un réseau NAT est configuré par défaut entre la machine hôte et la machine virtuelle, le port forwarding est nécessaire pour accéder à un serveur dans la machine virtuelle depuis l'extérieur. Cela implique simplement d'associer un port de la machine hôte à un port de la machine virtuelle.

Installation Serveurs linux et Windows

Licences

Logiciel Libre – GPL

Un logiciel libre est un logiciel qui peut être étudier, modifié et diffusé. La licence s'est le GPL (GNU public licence). Cette licence se caractérise par 4 libertés a respecté :

- La liberté d'exécuter le logiciel, pour n'importe quel usage
- La liberté d'étudier le fonctionnement d'un programme et de l'adapter à ses besoins, ce qui passe par l'accès aux code source
- La liberté de redistribuer des copies
- L'obligations de faire bénéficier la communauté des versions modifier.

Ce qui veut dire qu'un logiciel utilisant une licence GPL doit être distribué sous licence GPL.

LGPL

La licence LGPL (LESSER GNU Public Licence) reprends tout d'un GPL sauf l'hérédité de la licence GPL. Cette permet également la cohabitation de plusieurs licences au sein d'un logiciel. Il s'agit pour ces raisons de la licence préférée des développeurs de librairies.

Remarque

Gratuit ne veut pas dire libre, la gratuité veut seulement dire que l'on ne paie pas le produit.
Open source ne veut pas dire libre, l'Open source dit simplement que nous avons la possibilité d'avoir accès au code.

Pour qu'un logiciel soit libre il doit respecter les 4 libertés.

RAID

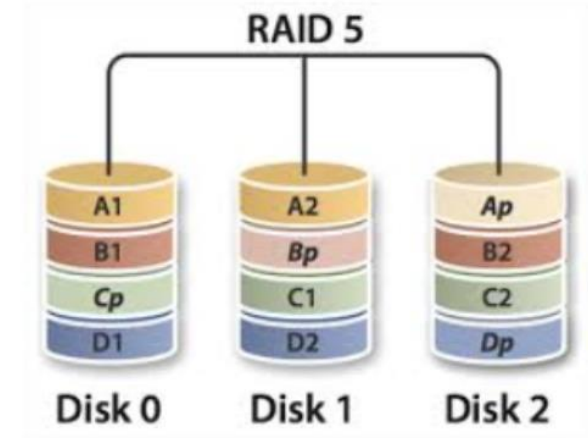
Le RAID permet éviter toute panne Disque dure qui pourrait rendre le serveur indisponible. C'est un mécanisme de redondance de disque. Il a plusieurs objectifs :

- Se prémunir contre la panne d'un disque
- Améliorer les performances en écriture sur les disques

Il existe diffèrent type de RAID :

Niveau	Explication	Avantages	Inconvénients
RAID 0	Les données sont écrites en parallèle sur plusieurs disques	Gain en performance	Perte d'un disque == perte des données
RAID 1	Les données sont écrites sur des disque en miroir	Tolérance aux pannes disques	Coût -> disque en double
RAID 5	Les données sont écrites en parallèle sur au minimum 3 disques (2 disques de données + 1 disque de parité)	Tolérance aux pannes disques + performance	Minimum de 3 disques requis

!! le RAID 5 s'appuie sur l'operateur logique XOR. La parité de chaque écriture est calculé grâce a cet opérateur. En cas de perte d'un disque, l'information peut être reconstitué a partir des 2 autre grâce au XOR



Disk 0	Disk 1	Disk 2
11	00	11
10	01	11

Installation linux

Partionnement

Le partionnement est le fait de diviser un disque en partie afin de mieux le géré, le maintenir. Par exemple une partition système et une partition utilisateur.

LVM

Logicial Volume Manager est une solution permettant une gestion dynamique du partionnement de la dispo sous linux.

Système de fichier

Lors du choix de partionnement il sera nécessaire de préciser le système de fichier de chaque partition, a connaitre :

- Ext2,ext3,ext4 : système de fichier linux
- NTFS : système de fichiers windows
- FAT32 : ancien système de fichier limité a des fichiers de max 4GB
- Swap : partition d'échange (extension de la mémoire RAM sous linux)

- Btrfs : nouveau système de fichier permettant la prise de snapshot d'une partition (instantané) et le redimensionnement de celle-ci a chaud, ce système utilise en interne des arbes B-TREE

Montage de partitions

le fichier /etc/fstab sous linux contient le montage de partition.

Chaque ligne de ce fichier indique une partition, son point de montage, le système de fichier, les options, si une sauvegarde doit être faite avec l'utilitaire dump (peu utilisé), l'ordre de vérification des disques lors d'une demande de vérification (fsck)

Chiffrement des partitions

Une partition non chiffrée peut être lu facilement avec un live-cd si on a accès physique a la machine.

Linux propose LUKS (Linux Unified Key Setup) et windows BitLocker pour crypter ses partitions.

Amorçage

Le chargeur d'amorçage permet lors du lancement de lancer le système d'exploitation ou de présenté les diffèrent système (multi boot). Windows propose winload et Linux propose GRUB (Grand Unified Bootloader)

Installation Windows (serveur)

Son installation est assez simple. C'est l'ajout de service, appelé rôle, qui est complexe. Les rôles permettent d'installer un Active directory, un serveur DNS, DHCP,…

La gestion des licences sous Windows, les licences serveurs doivent être comptabilisé suivant le nombre de cœur physique du processeur. Il faut également comptabiliser les licences d'accès client

Debian

APT

Toutes les distribution linux possède un système de gestion de packages. L'outil apt dispose d'un fichier de conf (/etc/apt/source.list) permettant de renseigner les dépôts a utilisé.

Mise à jour du dépôt local :

```
apt-get update
```

Mise à jour des logiciels installés :

```
apt-get upgrade
```

Installer un logiciel :

```
apt-get install <paquet1> <paquet2> ...
```

Supprimer un logiciel :

```
apt-get remove <paquet1> <paquet2> ...
```

Rechercher un logiciel/paquet :

```
apt-cache search <word>
```

SSH

Les systèmes linux sont souvent géré en ligne de commande et à distance.

Pour cela ssh est souvent utilisé, le protocole SSH effectue un échange de clé de chiffrement avant d'utilisé ces derniers pour crypter toutes les communications entre le client et le serveur. Le port 22 est le port utilisez par défaut.

Ssh est un service qui est initialisé par systemd.

Configurations

Après avoir effectué une modification dans une fichier de configuration, il faut redémarrer le service pour que les modifications soit effectué

```
systemctl restart ssh
```

Utilisation

Un cllient ssh a besoin des informations suivante : un nom de machine ou une adresse IP, un login, un mdp, il est possible de remplacé le login et mdp par une clées.

Copie de fichier

Des que l'on a un accès ssh on peut copier des fichiers entre la machine hote et la machine invité via les protocole SCP/SFTP. Ceci peut se faire sur linux en ligne de commande ou via winSCP sur Windows.

Tunnel SSH

La création d'un tunnel ssh permet de connecter 2 machines en encapsulant le trafic de la premier et en le redirigeant vers la seconde. Cette technique est aussi appelé VPN du pauvre car permet de données accès a une machine local de l'entreprise a des ordinateurs distant à moindre frais.

Gestion des utilisateurs

Adduser,deluser,addgroup,delgroup

Add user crée un profil utilisateur basé sur un repertoire squelette situé dans /etc/skel. Tout fichier placé la par l'admin sera copié dans les nouveau utilisateur.

Par défaut, la home directory créée par adduser est accesible en lecture par tout le monde. Ceci peut être changé dans /etc/adduser.conf.

SUDO

Pour qu'un utilisateur puissent utilisé SUDO il doit faire partie du groupe sudo.

Avantage de sudo :

- Permettre à des utilisateurs d'exécuté des commande privilégié sans pour autant devoir avoir le mdp du root,
- Travailler en mode non privilégié et utilisé le mode privilégié que quand nécessaire.
- Contrôler et enregistrer qui fait quoi (tout est enregistrer dans /var/log/auth.log)
- Renforcer la sécurité. En désactivant le compte root et en le remplaçant par des sudo un attaquant ne connaitrai pas le nom du compte et le mdp.

Passwd

Permet de changer le mdp de son compte et de tout les compte (root)

SystemD

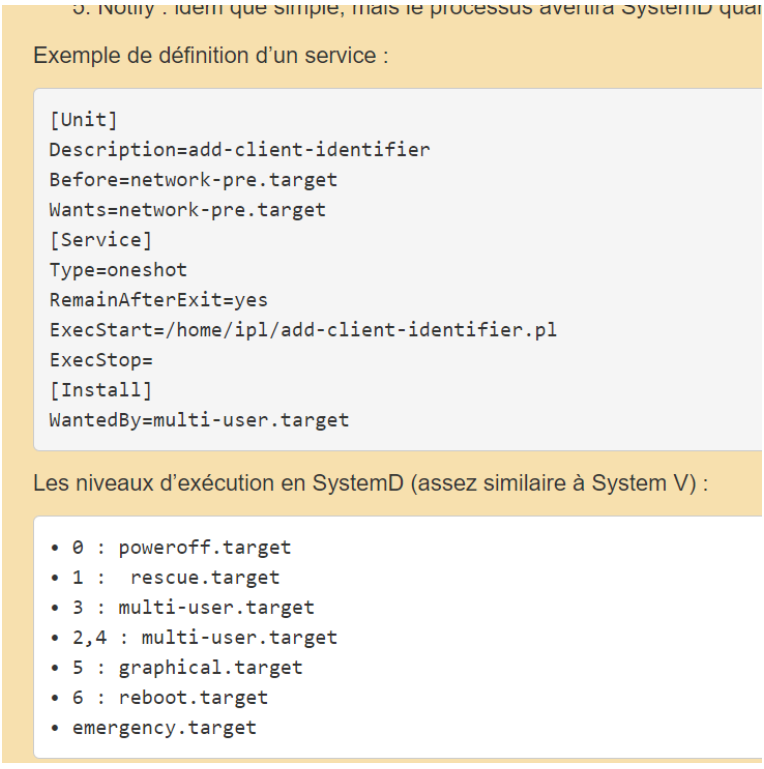
Le système d'exploitation Linux, dérivé d'Unix, a hérité de nombreuses caractéristiques de ce dernier, y compris son système d'initialisation basé sur l'architecture System V. Cette architecture, avec ses avantages tels que la mémoire partagée et les sémaphores toujours utilisés, comportait un processus initial (init) lancé au démarrage des systèmes Unix et Linux. L'architecture System V organisait l'environnement d'exécution en runlevels, avec un fichier inittab spécifiant les applications lancées en fonction du runlevel.

Les niveaux d'exécution :

- 0 : arrêt (la commande init 0 arrête le système)
- 1 : mono-utilisateur (utiliser par exemple pour la maintenance)
- 3 : multi-utilisateur sans environnement graphique
- 2 – 4 : idem que 3 mais peut être défini par l'user
- 5 : multi-utilisateur sans environnement graphique
- 6 : redémarrage (la commande init 6 redémarre le system)

L'objectif principale de systemD est de démarrer les services, appelle daemons dans le monde linux. Il est donc normal que celui-ci propose différente manière d'implémentâtes son service.

Ex de definition d'un service :



Apache

Etape de déploiement d'un site apache

1. Installer le paquet apache
2. Transférer et installer le code dans /var/www
3. Créer un virtual host
4. Activer le site
5. Faire la correspondance entre la directive ServerName et /etc/hosts
6. Tester le site en local

Caractéristique apache

Apache se caractérise par une configurations modelé :

- **/etc/apache2/sites-available : définitions de site Web (VirtualHost)**
- **/etc/apache2/sites-enabled : définitions de site Web (VirtualHost) activés**
- **/etc/apache2/mods-available : liste des modules (SSL, proxy, ..) installés**
- **/etc/apache2/mods-enabled : liste des modules (SSL, proxy, ..) activés**
- **/etc/apache2/conf-available : liste des configurations (charset, ..) disponibles**
- **/etc/apache2/conf-enabled : liste des configurations (charset, …) activés**
- **/etc/init.d/apache2 : un service qui sera démarré/arrêté par SystemD**
- **/etc/apache2/ports.conf : la configuration des ports pour apache (80 et 443 par défaut)**

VirtualHost

Les virtualHosts permettent de déployer plusieurs sites web sur un même serveur (même ip). La distinction se fait sur le nom du site. Apache doit savoir suivant l'url quel site presenté.

Exemple Vhost:

```
<VirtualHost *:80>
        ServerName monsite

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/htdocs/monsite
        ErrorLog ${APACHE_LOG_DIR}/monsite_error.log
        CustomLog ${APACHE_LOG_DIR}/monsite_access.log combined

        <Directory /var/www/htdocs/monsite>
        Require all granted
        AllowOverride All
        </Directory>
</VirtualHost>
```

Il est possible de déboguer et de vérifier la syntaxe du vhost avec la commande suivante :

```
apache2ctl configtest
```

Ensuite, il faut activer le site comme suit :

```
#activer un site
#commande à entrer dans /etc/apache2/sites-available
a2ensite monsite.conf
```

Reverse Proxy

C'est un serveur exposé par lequel toutes les requetes vont passer avant d'être redirigé vers d'autre serveurs interne. Le reverse proxy ne s'occupe pas de les traité.

Les intérêts de ces mécanismes sont multiple :

- Un seul point d'accès donc sécurité simplifiée
- Mise en œuvre de load balancing parmi les serveur interne
- Facilite le fait de rendre disponible un serveur interne sur le web.

Pour mettre en place un reverse proxy, il faut activer le module apache « proxy_http »

```
a2enmod proxy proxy_http && systemctl restart apache2
```

Ensuite dans le fichier VirtualHost:

```
<VirtualHost *:80>
        ServerName siteReverseProxy
        ServerAdmin webmaster@localhost

        # attention / final !!!
        ProxyPass /  http://www.example.com/
          ProxyPassReverse / http://www.example.com/

        ErrorLog ${APACHE_LOG_DIR}/siteReverse_error.log
        CustomLog ${APACHE_LOG_DIR}/siteReverse_access.log combined
</VirtualHost>
```

Le port par défaut pour les communications https est le 443.

Let's encrypt 7

Let's encrypt est une autorité de certification libre, gratuite et automatisée. Ceci permet d'obtenir un certificat valide pour son site Web sans trop d'effort.

Partage et accès réseau

NFS

Nfs est un protocole reseau utilisé pour partagé des fichiers sur un réseau. Il fonctionne en mode client serveur. C'est un protocole performant mais sans sécurité elevé. Il est utilisé sous linux et macos.

Son fonctionnement

NFS vérifie l'identité des user via les UID et GID. Il faut donc que les ID des machines (local et distante) corresponde. L'UID du root est toujours 0.

!! NFS ne demande pas aux user de s'authentifier. (on autorise via un fichier export une série d'hôte a se connecter)

Il est principalement utilisé pour des partages en lecture ou pour des back up.

SAMBA

SMB/CIFS est un protocole Windows pour les partages de réseau.

Certain partage reseau on le path UNC suivant:\\machineserveur\partage

SAMBA est un logiciel née sur linux qui implémente SMB/CIFS. Il permet une interopérabilité entre linux et windows comme :

- Créer des partages sous linux accessible de Windows
- Transformer un serveur linux en Domain contrôler
- Authentifier des clients linux sur un active Directory

SAMBA fonctionne comme NFS en mode client server. Il possède une gestion plus élaborée au niveau de l'authentification et des droits des user par rapport a NFS

CONFIGURATIONS SAMBA

!! pas obliger mais bon a savoir

La config s'effectue dans /etc/samba/smb.conf ce fichier contient des section :

- Global : paramètres globaux du serveur samba
- Homes : partager automatiquement les homedirs des user du server
- Printers : partager les imprimantes du serveur

7.3.3 Partage public

Le but est ici de donner accès à tout le monde en lecture seule à un répertoire situé sur le serveur.

```
[global]
        server string = monserveurLinux
        security = user
        # les utilisateurs qui se connecte au partage seront mappés sur le compte anonyme
        map to guest = Bad user
        # compte anonyme pour les «  Bad user »
        guest account = nobody
        # compatibilité protocole SMB et Windows 10
        min protocol = LANMAN2
        max protocol = NT1
    [public]
        # chemin local du partage
        path = /home/samba/allusers

        # accès possible en anonyme à ce partage
        public = yes
        readonly = yes
        # répertoire visible dans l'explorateur de fichiers
        browseable = yes
```

7.3.4 Partage en écriture

```
    [partageEcriture]
        # chemin local du partage
        path = /home/samba/partageEcriture
        browseable = yes
        write list = user1, user2
```

Ici plus question d'accès anonyme, il est nécessaire d'ajouter un compte SAMBA avec mot de passe.

```
smbpasswd -a user1
```

7.3.5 Partage des "homedirs"

Le but ici est permettre l'accès en écriture à leur home directory (depuis Windows par ex.) aux utilisateurs enregistrés sur le serveur Linux.

```
[global]
        server string = monserveurLinux
        security = user
    [homes]
        # inutile de rendre visibles à tout le monde ces partages
        browseable = no
        writable = yes
        # les utilisateurs pouvant accéder à ce partage sont ceux
        # correspondant à %S c'est-à-dire au nom du partage ...
        # c'est-à-dire le nom de l'utilisateur ici
        valid users = %S
```

7.3.6 Lancer/redémarrer SAMBA

```
systemctl restart samba
```

VPN

Un vpn (virtual private network) est un système permettant de relier 2 réseaux via un réseau non sûr tout en garantissant un trafic crypté et transparent. On parle d'un tunnel.

Il existe different type de vpn :

- LAN to LAN : permettant de relier 2 réseaux (ex relier plusieurs succursales de la même entreprise)
- RoadWarrieor permettant à un pc externe de se connecter a l'entreprise

Le vpn créer un réseau et le configure pour que le réseau distant ou pc distant soit considéré comme s'il était dans l'entreprise. L'user pourra donc utiliser tout ce qui est accessible dans le LAN

7.4.3 Protocoles VPN

Protocole	Couche Réseau	Remarques
PPTP (Point to Point Tunneling Protocol)	Couche Liaison des données	Road Warrior
L2TP (Layer 2 Tunneling Protocol)	Couche Liaison des données	Road Warrior / Remplaçant PPTP
IPSec	Couche Réseau	Site To Site / intégré à IPV6 / se configure essentiellement sur les routeurs-firewalls des entreprises
OpenVPN	**Couche Application**	**OpenVPN est un logiciel créant un VPN en se basant sur SSL/TLS – RoadWarrior ou Site to Site**

7.4.4 Exemple OpenVPN

```
# Serveur VPN (server.conf)
mode server
proto udp
dev tun
topology subnet
# clé et certificat SSL
ca keys/ca.crt
cert keys/cert.crt
dh keys/dh2048.pem
# réseau créé
server 10.50.0.0 255.255.255.0
keepalive 10 120
# compression des échanges
comp-lzo
```

```
#client VPN (client.conf)
client
proto udp
dev tun
remote 89.89.89.89 1194
nobind
ca /etc/keys/ca.crt
cert /etc/keys/roadwarrior.crt
key /etc/keyroadwarrior.key
comp-lzo
```

FTP

C'est un protocole de réseau standard. Ce protocole utilise un canal pour le transfert de données et un autre pour le contrôle. Il utilise donc 2 port les 20 pour les données et 21 pour le contrôle. Le canal de contrôle permet d'envoyer des commande FTP (get,put,open….à

Il peut etre sécurisé via SSL/TLS (FTPS) ou par ssh (SFTP).

Modes

FTP peut s'utiliser en mode passif ou actif.

En passif : le serveur impose le port de connexion pour le transfert. Le port est envoyé au client qui initalise alors la connexion.

En actif : le client peut choisir son port pour la réception de données. Le serveur initialisera une connexion sur la port 20 vers le port choisi par le client. Le client doit accepter les connexion sur le port choisi. Parfois probleme car client se trouvent dans un LAN qui a un NAT vers l'exterieur donc c'est pour cela que c'est peut utiliser.

Terminal Serveur

Ceci repose sur le protocole RDP (REMOTE DESKTOP PROTOCOL) développé par Microsoft. Il permet de prendre a distance un server avec son interface mais aussi de monter des lecteurs locaux sur le serveur distant

Annuaires et authentification

LDAP

C'est un protocole (Lightweight Directory Access Protocol) qui permet d'interroger et modifier un annuaire. Il est devenu référence et un standard d'authentification.

Ce protocole est enfaite une norme qui defini :

- Un protocole : Comment sont echangées le données ,
- Un modèle de nommage : comment sont nommées les entrées dans l'annuaire
- Un modèle fonctionnel : quelles sont les méthodes pour accéder aux données
- Un modèle d'information : nature et description des données
- Un modèle de secu : description de la sécur des données (quel chiffrement…)
- Réplication : comment répliquer les données entre serveur LDAP pour evité les pannes (pas encore standariser)

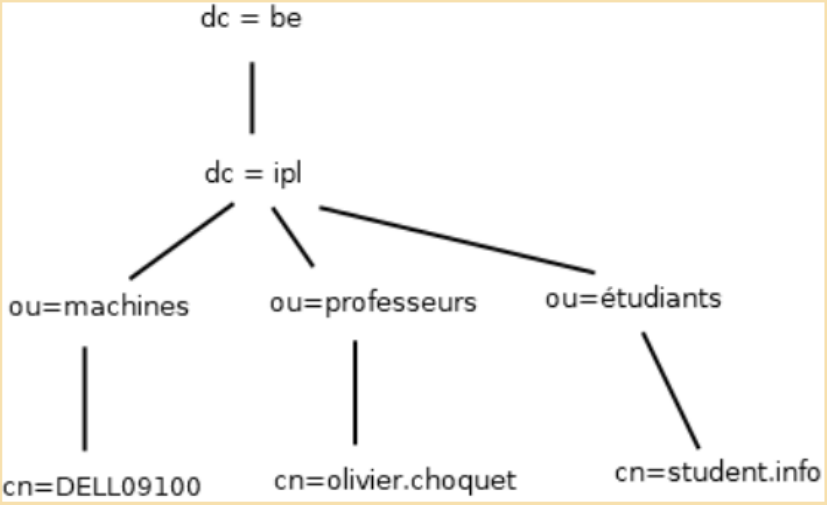
Ils existent diffèrent implémentation de LDAP. OpenLDAP est la solution reconnue du monde libre. La solution Active directory de Microsoft est la plus connue et répandue.

Modèle de nommage

Vocabulaire de base utilisé dans un annuaire LDAP :

- DC : domain component. Racine de l'arbre
- DN : Distinguished name. Chemin complet vers un element (DN sont uniques)
- OU : organizarional Unit. Divion de l'entreprise rassemblant des CN
- CN : common name. Nom d'un élément

Exemple :



Modèle fonctionnel

LDAP a défini des méthodes permettant de modifier et consulter l'annuaire. A connaitre :

- Bind : s'authentifier auprès du serveur LDAP. Nécessaire avant de demander au serveur une opération
- Add/Modify/Delete : mise à jour de l'annuaire
- Search : permet de rechercher un élément ou plusieurs éléments dans l'annuaire en précisant une base, portée et des filtres
- Compare : vérifie qu'un élément contient ou non un attribut
- Unbind : se déconnecter

Modèle d'informations

Il a aussi défini le modèle d'info :

- Entrée : composé d'attributs, possède un type (classe objets)
- Schéma : définition des attributs possibles et classes d'objets
- DN (distinguished Name)

Exemple:

```
dn: cn=olivier.choquet, ou=profs, dc=ipl,dc=be\
objectClass: user\
cn: olivier.choquet\
mail: olivier.choquet@vinci.be\
bureau: A050\
```

Modèle de sécurité

Le transport de message sera chiffré en SSL/TLS. L'user authentifier (bind) a accès aux données suivant les règles de ACL (Access control List)

Modèle de réplication

La réplication est importante pour assurer une redondance pour prévenir des pannes. Les différentes implémentations de LDAP on chacune leur systèmes de réplication.

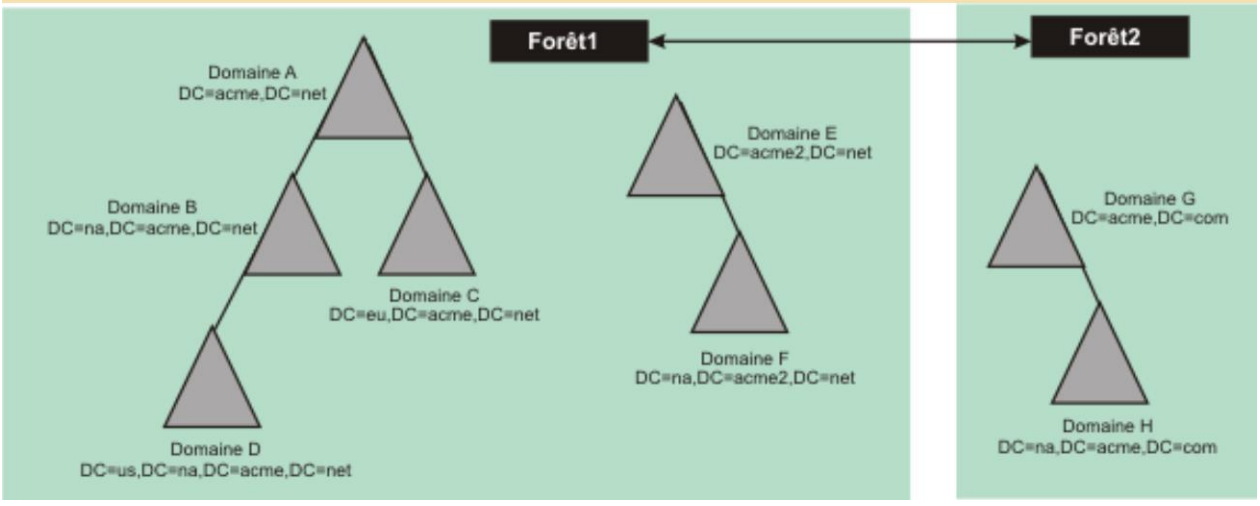
LDAP fournit un format d'échange standard nommé LDIF (LDAP Data Interchange Format) qui permet d'échanger/sauvegarder de l'info entre serveurs LDAP. Cependant ne permet pas une réplication facile.

LDAP VS SGBD (système de gestion de base de données)

LDAP	SGBD
Optimiser pour la lecture, faible en écriture	Optimiser pour les lectures et écritures
Isolation pas garantie	**Support Transaction (ACID)**
Réplication aisée	Réplication plus complexe
Attribut multi-valeurs	/
Query LDAP	**Query SQL**
Modèle de données défini, **mais extensible facilement**	**Définition du modèle par le développeur, extensible mais difficile**

Active directory

Cela permet de gérer l'authentification des users d'un ou de plusieurs domaine, de gérer les droits des users via des group de secu. Il définira une forêt qui est composée d'arbres (domaine parents avec des enfants) et/ou domaine. Les domaines sont constitués d'unités d'organisation et enfin d'ordinateurs, de groupes et utilisateurs.



Dans un Active Directory, on va retrouver des objets, les plus important les users, les ordiateurs du domane, les group de secu , les GPO et les unités d'organisation.

Un serveur Hébergeant un Active Directory est un contrôleur de domaine, conseillé d'en avoir minimum 2 pour les pannes.

Unité d'organisation

C'est un regroupement d'objets de l'active Directory. C'est un nœud dans l'arbre LDAP.
elles contiennent la définition des GPO.

!! à ne pas confondre avec le Groupes de sécurité qui eux n'ont pas de définitions de GPO.

Des permissions ne peuvent pas être définies sur des unités d'organisations.

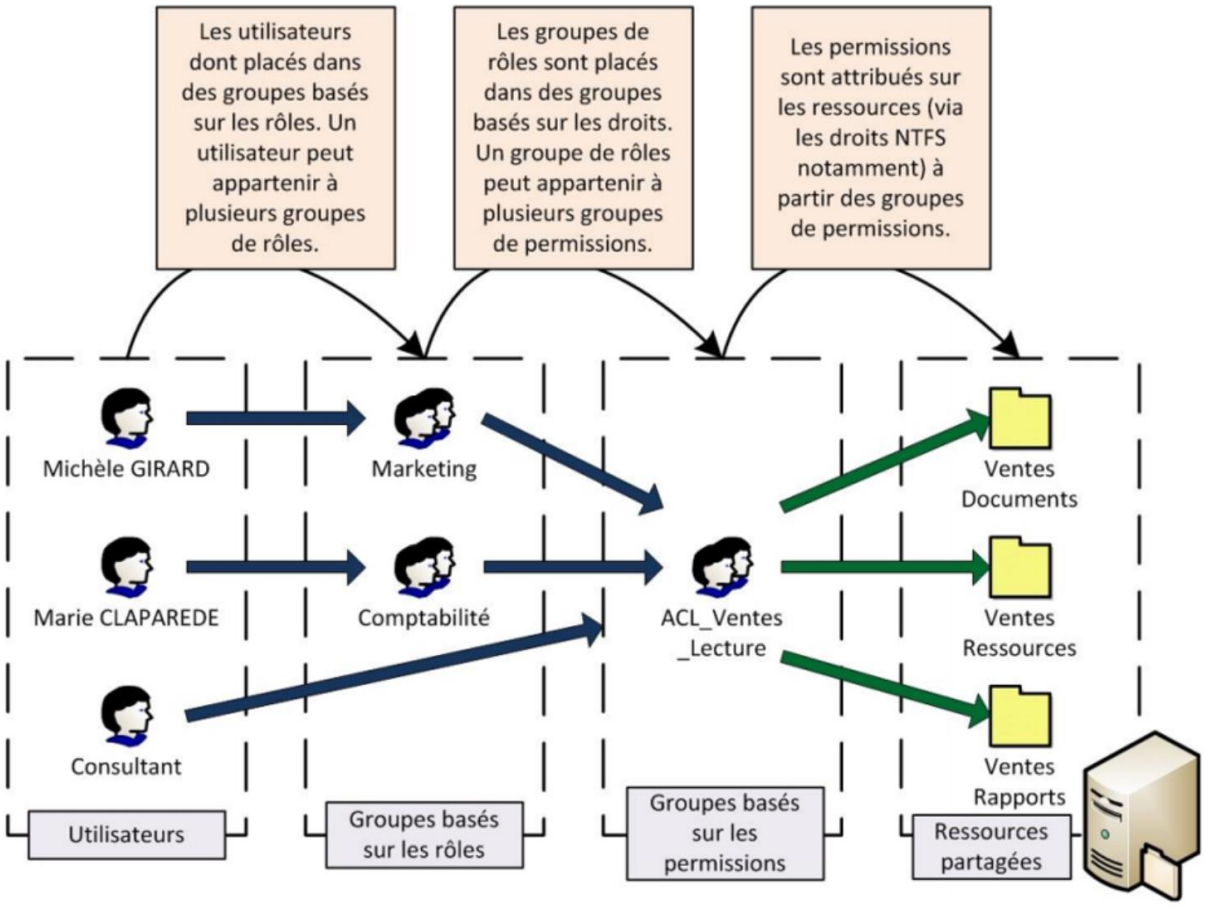
Un objet peut appartenir à plusieurs groupes mais ne pourra être placé que dans une seule organisation

Groupes de sécurité

Microsoft proporse une recommandation pour la gestion des droits et des groupe. AG(U)DLP.

Account → Global → (Universel) → Domain Local → Permission

Le principe est de placer les users dans des group globaux, de placer ceux-ci dans groupe locaux et d'appliquer les permissions sur les groupes.



mage labo-microsoft.supinfo.com / **schéma utile à connaître pour expliquer AG(U)DLP**

Permissions

Usage de fichier NTFS par miscrosoft pour les droits. Les permissions seront des permissions NTFS. Celle-ci sont très riches (beaucoup de possibilité)
il existent aussi des permissions de partage réseau. A ne pas confondre avec les permissions NTFS qui s'appliquent directement sur des fichiers et dossier locaux tandis que les permissions de partages s'appliquent sur les partages réseau.

Lors de l'accès à un partage réseau, le système évalue d'abord toute les permission du partage réseau et ensuite NTFS (tout partage se retrouve toujours physiquement sur un système de fichiers)

GPO

Les Group Policy Objects (GPO) sont des outils essentiels dans les environnements Windows, permettant une gestion centralisée des politiques de sécurité et des paramètres système.

En configurant des stratégies pour des utilisateurs et des ordinateurs au sein de l'Active Directory, les GPO facilitent le déploiement uniforme de directives telles que l'imposition d'un proxy, la personnalisation du fond d'écran, et la définition de politiques de mot de passe.

Les GPO machines prennent effet au démarrage, tandis que les GPO utilisateurs s'appliquent à l'ouverture de session, assurant un contrôle efficace et cohérent sur la configuration et le comportement des systèmes au sein d'un réseau Windows.

Gestion des données

Base de données

DBA (pas forcement connaitre)

Les DBA est le database administrator, il se charge de :

- Documenter la base de données,
- Gérer le stockage
- Vérifier la structuration de la base de données
- Sécuriser l'accès aux données,
- Optimiser la base de données
- Fournir aux devs des jeux de données
- Migration/mise à jour de la base de données
- Sauvegarder la base de données.

PostgreSQL

Un moteur de BD est constitué de plusieurs programmes. Postgres est composé d'une prog supervisuer (postmaster), du serveur exécutant les requêtes (postgres) et d'un client interactif (psql)

Sauvegarde PostgreSQL

Important de sauvegarder la BD. Erreur à ne pas commettre :

- Pas de sauvegarde,
- Sauvegarde jamais testée,
- Ne pas documenter sa sauvegarde (qui a fait, quand, comment)
- Sauvegarder sur le même disque
- Sauvegarder au même endroit (incendie)
- N'avoir qu'une sauvegarde très récente car peut contenir l'erreur aussi

Les sauvegarde fichier ou instantanés ne conviennent pas au BD, il est préférable d'utiliser l'outil fourni par le moteur de BD. Pour PostgreSQL nous avons **pg_dump**

Performance

Important de connaitre les limitations des BD se situent au niveau des composant (CPU,RAM,vitesse disque….)

Il est possible d'accélérer la performance grâce a l'ajout d'index (accélérer de 1000000 requêtes)

LIMIT : est à envisager pour améliorer les performances. A-t-on besoin de toutes la table ? peut-on prendre uniquement les premiers résultats ?

VACUUM (à utiliser régulièrement) : permet de supprimer définitivement les données expirées. (Particulièrement sur les bd dev ou l'on créer et supprime régulièrement)

ANALYSE : permet de collecter des stats pour optimiser la BD

Les ORM (outils permettant de facilité l'interaction entre logicielle et bd) sont très utile mais complexe a optimisé. A utilisé en fonction de la performance voulu.

Réplication PostgreSQL

Possible de permettre a 2 moteurs de BD de partager des bases de données, les données sont alors répliquées au minimum sur 2 serveurs de BD. Cela permet de se prémunir contre la panne d'une des BD.

La réplication la plus usé est maitre- esclave, toutes les opérations sont faites sur le maitre et celui-ci envoie régulièrement au serveurs esclave des journaux de transaction. Il se mets alors à jour grâce aux journaux.

Sauvegarde

Un admin sys est en charge de la pérennité des données. Des sauvegardes ou backups sont alors nécessaires. Il est impossible de tout sauvegarder voila pourquoi il faut une politique de sauvegarde qui réponds au question suivante :

- Que faut il sauvegarder ?
- sur quel support sauvegarder ?

    - Les entreprise auront souvent recours à des NAS (network area storage) ou SAN distant ou un stockage dans le cloud
- Quel type de sauvegarde, quelle fréquence ?
    - **Complète** : une copie complète des données est faite
    - **Incrémentielle** : une copie des modifications depuis la dernière sauvegarde (complète ou incrémentielle) est faite
    - **Différentielle** : une copie des modifications depuis la dernière sauvegarde complète est faite
    - **Miroir** : une seule sauvegarde complète
    - **Instantané/ snapshot** : pas vraiment une sauvegarde car difficile de restaurer un seul fichier.
- Conservations des données ?
    - La déduplication est un moyen mis en place par les entreprise. Ce mecanisme est souvent intégré au SAN (il s'agit de découper les données en bloc et toute nouvelle occurrence d'un bloc est remplacée par un poiteur)
    - Il est nécessaire de crypter ses backups pour éviter à une personne mal intentionné de récupérer trop facilement les données. L'usage du cloud renforce également cette sécurité.
- La règles du 3-2-1
    - C'est une régle fortement conseillée pour les sauvegardes de données :
        - 3 : conserver 3 copies des données (originale + 2 sauvegardes)
        - 2 : conserver sur 2 supports différents
        - 1 : conserver 1 copie de sauvegarde dans un lieu différent (des 2 autres copies)

Quotas

Les quotas permettent de régler le problème de ressources en limitant l'usage des utilisateurs. Le mécanisme propose une limite soft et hard. Quand un user dépasse le soft il reçois un avertissement lui indiquant qu'il lui reste une période de travail, cette période écoulé il est bloqué si il n'est pas redescendu en dessous du soft

Virtualisation

La virtualisation consiste en l'abstraction des éléments du monde réel en les rendant virtuel. Ca a comme objectif de rendre plus facilement :

- Configurable
- Transportable
- Optimisé (meilleure allocation de ressource)
- Disponible (facilité de déploiement)
- Sécurisé (isolation)

L'inconvénient majeur de la virtualisation est l'ajour d'une couche de virtualisation entre le système physique et le composant virtualisé. Ceci permet d'obtenir les avantages mais dégrades les performances.

HYPERVISEURS

Le virtualisation se fait via des hyperviseurs. C'est un logiciel de virtualisation permettant à plusieurs machines virtuelles de fonctionner simultanément sur un même système physique.

Il y a 2 types d'hyperviseur :

- Type 1 / natif / bare-metal
    - Sera utilisé dans le cadre de virtualisation de serveurs. S'agit de système d'exploitation spécialement dédié à virtualisation qui s'exécute sur la machine.
- Type 2 /hosted
    - Cela s'installe dans un os comme un logiciel classique (VirtualBox)

A note qu'avec le cloud il est possible d'avoir des serveurs privés virtuel (VPS), c'est un hyperviseur bare-metal hébergé dans le cloud

Virtualisation du stockage

Cela consiste en la création d'une baie de stockage (un ensemble de disque physique) qui sera présentée en un ou plusieurs ensembles logiques et dynamiques. On parle de LUN (Logical Unit Number). Une LUN est un espace de stockages dynamique et logique.

Un SAN est donc une baie de stockage avec des LUN accessibles via le réseau

Conteneurs Docker

C'est une solution d'architecture à base de conteneurs, elles sont une évolution avantageuse de la virtualisation. Cependant docker n'est pas un logiciel de virtualisation mais un isolateur.

Pour faire cela docker s'appuyé sur 2 éléments du noyau linux :

- CGroups (control groups) : permettent de fixer/limité les ressources (CPU,RAM…) allouées à un conteneur ou un ensemble de conteneurs.

- Namespaces : permettent d'isoler des ressources. Un conteneur ou ensemble ne voient que les ressources de son namespace.

Les conteneurs sont très utilisés car ils permettent de facilité le scaling. On peut facilement augmenter le nombre de conteneurs (horizontal) ou augmenter les ressources des conteneurs (vertical)

Docker VS Virtualisation

La grosse differences est l'interaction avec l'OS hôte.

- Docker partagera le même noyau pour tous les conteneurs
- Chaque VM géré par un hyperviseur aura son propre OS

Différences	Docker	Machine Virtuelle
Optimisation	léger (taille et empreinte mémoire)	+ lourd (taille et empreinte mémoire)
Transport	Transport facile (taille légère)	Taille élévée
Disponibilité	Dockerhub et registry privée	Images sur Azure, …
Configurable	moins d'options configurables	+ options configurables
Sécurité	moins de sécurité (partage du noyau par les conteneurs)	isolation peut être totale

Usage de docker

Pour déployer une app docker il y a 3 etapes :

- Creation d'un dockerFile
- Créer l'image docker
- Créer un conteneur à partir de l'image créée

Dockerfile et instructions principales.

On commence par la création d'un dossier contenant tout ce qui est nécessaire à l'application. Il est nécessaire d'avoir : le code et un dockerFile.

Dans le docker file on trouve :

- FROM : qui dit l'images de l'application sur laquel on va se baser
- RUN : qui permet d'ajouter à l'image des elements en exécutant des commande
- COPY : qui permet de copyer des elements dans l'image. COPY SRC DEST
- CMD : qui permet d'executer une commande une fois le conteneur démarré

DockerHub et registry

Dockerhub est l'endroit ou on dois rechercher notre image de base.

Docker Compose

Docker est prévu pour fonctionner en micro service. On aura un conteneur par service.

- Comment gère-t-on la communication entre les diffs conteneurs ?
- Comment rendre les données persistantes ?

Docker compose permet de crée du volumes facilement (créer bcp) et permet d'effectuer la persistence de données en dehors du conteneurs.

Directives a connaitres

- Build : permet de construire une image docker a partir d'un dockerFile
- Ports : permet d'effectuer la redirection de ports entre la machine et le conteneur
- La directives volumes : permets de lier un répertoire de la machine hôte aux conteneurs. Ils ne sont pas détruits par défaut lors de la destruction du conteneur.

Le noms des services(conteneurs) deviennent des noms réseaux.

The twelve Factor App

La conception de docker s'est inspirée de la methodologique 12 facteurs, c'est une méthodologie pour créer des applications SaaS.
voici comment Docker applique celle-ci : (retenir 5 avec leur exemple)

- Code de base : la notion d'image en docker permet de déployer plusieurs fois un même code
- Dépendance : dockerFile rend explicite les dépendances
- Configurations : il est possible de passer des variables d'env a un conteneur. Cependant un orchestrateur (K8S) le fait de manière plus élégante.
- Service externes : les ressources peuvent être découvertes via leur nom. Cependant un orchestrateur (K8S) le fait de manière plus élégante.
- Build, release, run : docker build, docker run
- Processus : Docker est principalement stateless. Les volumes existent mais il sera plus élégant de gérer cela avec un orchestrateur. Pas rassurant de savoir ces volumes stockés sur un hote sui peut faillir
- Association de ports : docker run -p 8080 :80
- Concurrence : le coté stateless des conteneurs permet d'en ajouter facilement pour faire face a la monté en charge
- Jetable : avec docker, on crée, on déploie et surpprime facilement
- Parité DEV/PROD : la même image peut etre lancé en prod ou dev
- Processus d'admin : il est facile de se connecter et interagir avec le conteneur
- Logs : par défauts tout les logs sont envoyé au stdout.

Kubernates (K8s)

C'est un orchestrateur de conteneurs.

Utilité ?

- L'équilibrage de charge entre plusieurs conteneurs (load balancing)
- Gestion des différents stockages pour les conteneurs. Ceux-ci peuvent être locaux,cloud,…
- Gestion et allocation des ressources au conteneurs de manière dynamique
- Gestion de l'état de santé des conteneurs
- Gestion des informations de conf et secrets.

Vue general et concepts k8s

Kubernetes est composé d'un nœud maitre qui permet de gérer les clusters K8s.

Un cluster est l'ensemble de machines physique ou virtuelles. Chaque machine du cluster est appelée un worker node et contient une solution de déploiement de conteneurs.

Chaque worker héberge un pod. Un pod est l'unité de déploiement d'une app k8s. c'est un ou plusieurs conteneurs. (souvent un pod==un conteur)

Un label clé::valeur peut être attaché à un pod. Les selectors permettent de sélectionner un objet k8s suivant son label.

On définit comment un pod sera déployé grâce à un fichier deployment.yml. Ce fichier contient une instruction « réplica » qui indiquera à K8s combien d'instance de ce pod il devra lancé/maintenir.

Un fichier services.yml permet de définir et gérer le réseau à l'intérieur du cluster. Le pods peuvent être créer, détruit et recréés il est nécessaire qu'un service puisse cibler des pods encore actifs à un moment.

Ingress est un load balancer qui permet de faire comm le monde extérieur avec le cluster k8s

Les persistant Volume Claim (PVC) permettent de faire persister les données. Il s'agit d'une demande d'espace adressé à k8s. il attribuera au pod un stockage suivant sa demande. L'intérêt de k8s par rapport au stockage est de pouvoir utiliser des stockages variés.

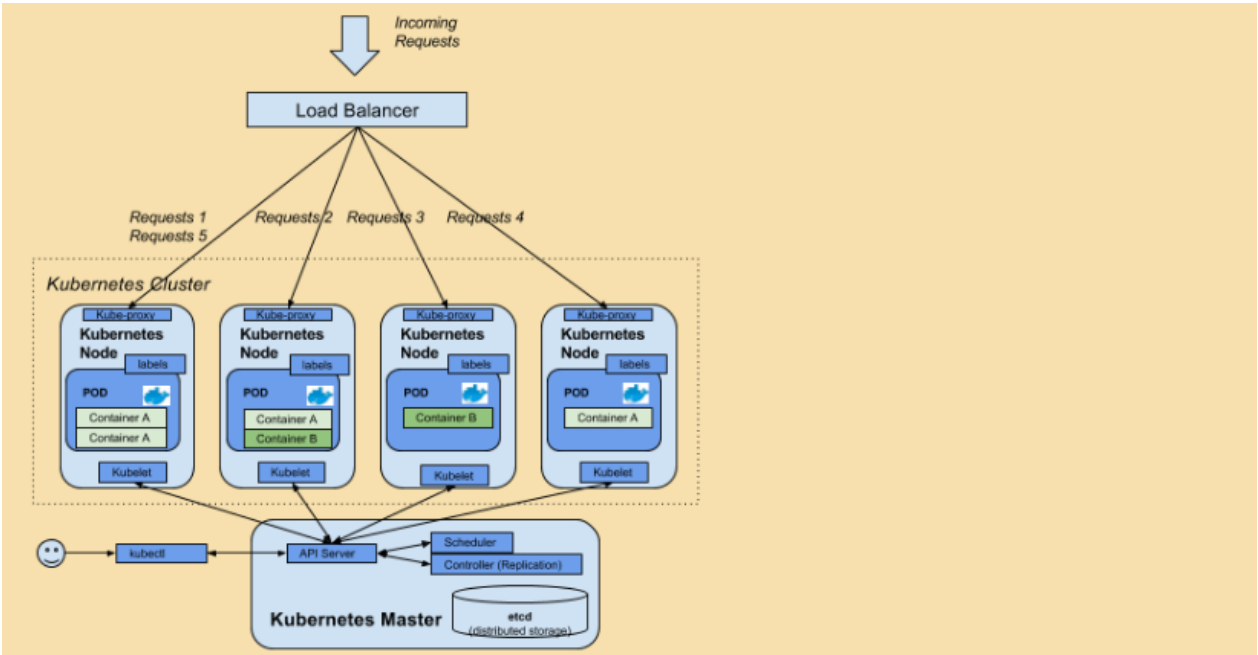
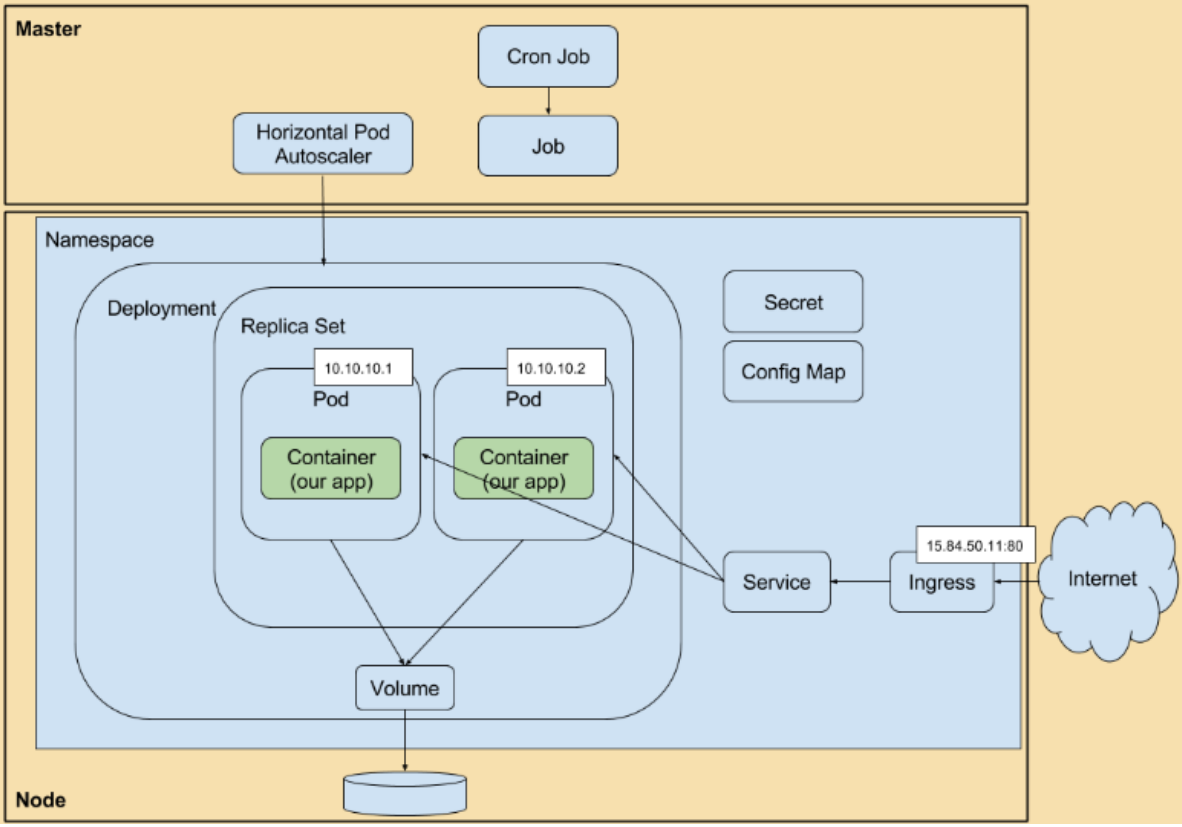


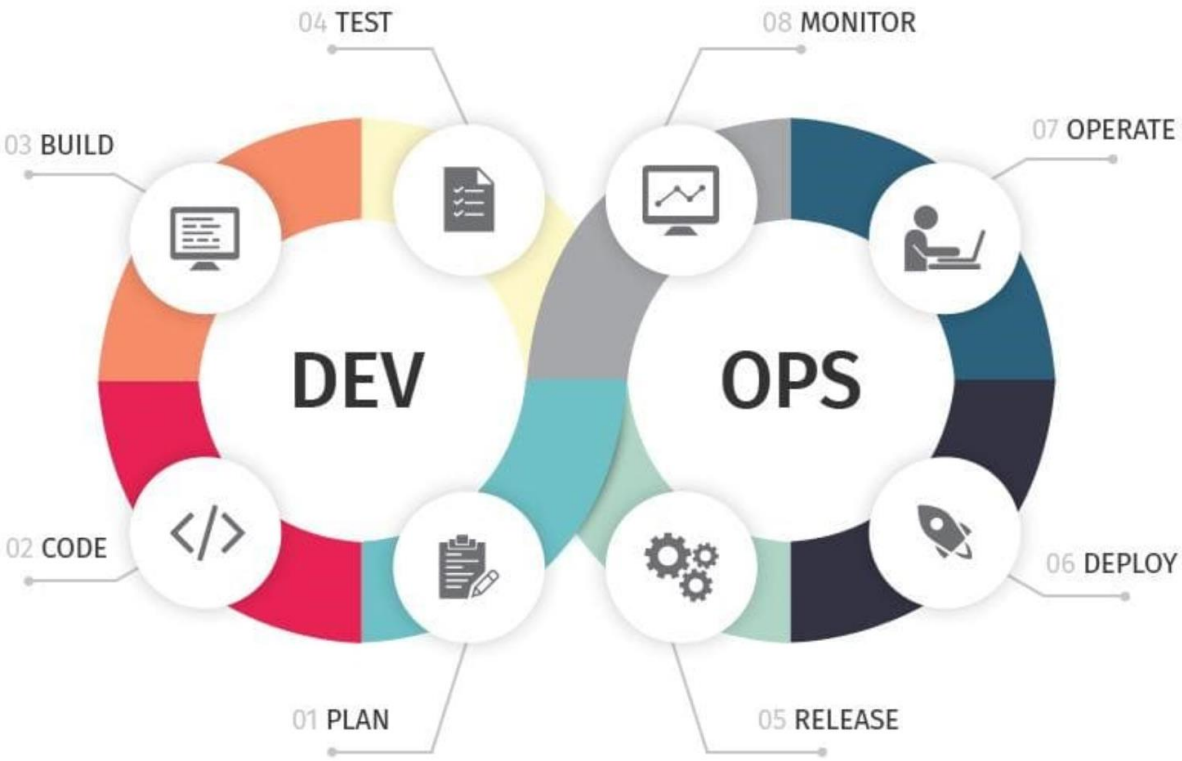
Image issue de : https://hub.alfresco.com/t5/alfresco-process-services/activiti-7-deep-dive-series-deploying-and-running-a-business/ba-p/288347



Devops (ansible)

Le déploiement d'une app fait partie du produit ainsi que les mises à jour en continue, donc nécessaires d'avoir une infra avec le concours des opérationnels pour mener à bien ce nouveau mode de développement logiciel.

A connaitre :



Pipeline de développement

L'approche devops mise aussi sur l'automatisation via des outils. On parle la de pipeline de dev. C'est une chaine de production logicielle la plus automatisée jusqu'au client.

Les pipelines utiliseront des conteneurs, les orchestrateurs, le cloud et les outils de conf

Cloud

Le cloud est une abstraction qui se déroule en plusieurs étapes du réseau, du web, de l'infrastructure. Il est très populaire car permet d'accélérer la transition numérique pour les entreprises.

Caractéristique :

- Accès au services à la demande,
- Accès réseau large bande
- Réservoir de ressources
- Elascticité – scalling
- Facturation a l'usages
- Automatisation
- Résilience
- Sécu

Modele de service

Infrastructure as a service IaaS

Déploiement d'une infrastructure via les outils du cloud. L'user peut paramétrer le réseau, les serveur. Ex (azure VM)

Terraform est l'outils le plus utilisé pour déployer de IaaS. Il permet de créer des VM et d'autres éléments d'infrastructure

Platform as a Service (Paas)

Deployment d'une plateforme via les outils cloud, l'user peut paramétrer la platforme mais il n'a aucun accès vu sur l'infra. C'est le modele le plus utilisé par le dev. Ex Heroku, AWS Elastic Beanstalk

Software as a Service (SaaS)

C'est une application accès via internet, aucun accès, vue sur l'infra et paramétrage limité.
ex gmail,office.

Architecture multi-tenant et cloud

Dans ce genre d'architecture une même instance d'une application logicielle est utilisée par plusieurs clients, ces derniers sont appelés des tenants.

Ce modelé est économique car les couts liés au dev et maintenance des logiciel sont partagé.

Les modeles SaaS présentes souvent des approches multi-tenant et single-tenant en fonciton des budgets.

Approches	Description	Avantages	Inconvénients
Multi-tenant	Les clients se partage la même application et la même DB	Coût de location et maintenance faible, mise à l'échelle aisée, déploiement facile des mises à jour	Effets de bords liés aux colocataires (sécurité, performance)
Multi-DB	Les clients se partage la même application mais ont chacun leur propre base de données	Isolation totale des données (sécurité)	Coût location et maintenance plus élevé. Mise à l'échelle compliquée
Multi-instances / Single tenant	Chaque client a sa propre instance d'application et sa propre DB	Isolation totale, mise à l'échelle aisée, personnalisations possibles	Coût très élevé

Terraform

C'est un outil permettant des déployer des ressources dans le cloud. Il permet d'automatiser la création de ressources. Il dispose de nombreux connecteurs (provider) permettant des créer des ressources un peu près partout. C'est ce qui le rend vraiment intéressant.