LINUX : ADMINISTRATION REDHAT

PLAN DÉTAILLE

- PARTIE I : IP, DNS ET SSH
- PARTIE II : TRANSFERT DE DATA, ANALYSE ET FILTRAGE DE FLUX
- PARTIE III : SURVEILLANCE DU SYSTÈME, GESTION DES SERVICES (SYSTEMD)
- PARTI IV : ZOOM SUR QUELQUES SERVICES (WEB, BDD, NFS, LB)
- PARTIE V : DISQUE ET PARTITIONNEMENT (LVM)

PARTIE I

Configurations IP

Service DNS

Protocole ssh

CONFIGURATION IP : ÉLÉMENTS DE CONFIGURATION

Une adresse ip : cette adresse identifie votre *hôte* sur le réseau où il est connecté

Un masque de sous-réseau : permets de connaitre le réseau où vous êtes connecté

Une passerelle par défaut (gateway) : pour communiquer avec des machines hors de mon réseau

Des serveurs dns : pour la résolution des noms de domaine

Des routes réseaux

On verra les configurations **volatiles** et celles **permanentes**

Volatiles : avec les commandes disponibles

Permanentes : en éditant les fichiers de configuration

CONFIGURATION IP : CONF VOLATILES

Actions	Commandes
attribuer une adresse IP à une interface spécifique	ip addr add *IP/mask* dev *interface*
vérifier une adresse IP	ip addr
supprimer une adresse IP	ip addr del *IP/mask* dev *interface*
Activer/déactiver une interface réseau	ip link set interface up/down
Changer le Hosname	hostnamectl set-hostname *nom_du_serveur*
Vérifier la table de routage	Ip route
Ajouter une route statique	ip route add *IP_Reseau/mask* via gateway dev *interface*
Supprimer une route statique	ip route del *IP_Reseau/mask*
Ajouter une passerelle par défaut	ip route add default via *Gateway*

CONFIGURATION IP : CONF PERMANENTES

- IP, masques réseau, gateway et routes réseaux
  - le fichier /etc/network/interfaces sous Debian et derivés
  - les fichiers /etc/sysconfig/network-scripts/* sous Redhat et derivés
- Dns : /etc/resolv.conf
- Résolution dns interne au serveur : /etc/hosts
- Hostname de la machine : /etc/hostname

COMMANDES RÉSEAU

ip	ifconfig	route	arp
ss	netstat	ping, ping6	tcpdump

DNS : SERVICE DE RÉSOLUTION DES NOMS

- **L'IDENTIFICATION DES MACHINES**
  - **POINT DE VUE SYSTÈME**
    - LES MACHINES POSSÈDENT DES NOMS INTELLIGIBLES
  - **POINT DE VUE RÉSEAU**
    - UN PAQUET IP CONTIENT UNE ADRESSE SOURCE ET DESTINATION : FORME
- X.Y.Z.A (IPV4)
    - L'IDENTIFICATION IP EST EFFICACE POUR LE ROUTAGE
  - **BESOIN D'ASSOCIER CES DEUX FORMES DE NOMMAGE**
    - POUR LES HÔTES CONNECTÉS EN RÉSEAU
  - **LA RÉSOLUTION DES NOMS : ASSOCIATION ENTRE UN NOM D'HÔTE ET UNE ADRESSE**
    - SERVICE D'ANNUAIRE

DNS : OBJECTIFS ET SPECTRE COUVERT

- PAS DE CONFLITS DE NOMMAGE
  - GARANTIE DE L'UNICITÉ
- SUPPORT DU FACTEUR D'ÉCHELLE
  - AUGMENTATION DU NOMBRE D'HÔTES ET DE NOMS RÉFÉRENCÉS
- PERFORMANCE DU SYSTÈME
  - PAS DE GOULOT D'ÉTRANGLEMENT
- MAINTIEN DE LA COHÉRENCE
  - VALIDITÉ DE L'INFORMATION FOURNIE

DNS : APPROCHE HIERARCHIQUE

- **SUPPRIME LES CONFLITS DANS LE SCHÉMA DE NOMMAGE**
- STRUCTURE MAÎTRISÉE
  - ANALOGIE AVEC LES SYSTÈMES DE FICHIERS ET LE MONTAGE DE PARTITIONS DISTANTES
- **PARCOURS DE L'ARBRE L'ARBRE DES FEUILLES À LA RACINE**
  - PARCOURS INVERSÉ PAR RAPPORT AUX SYSTÈMES DE FICHIERS
  - UTILISATION DU POINT COMME SÉPARATEUR

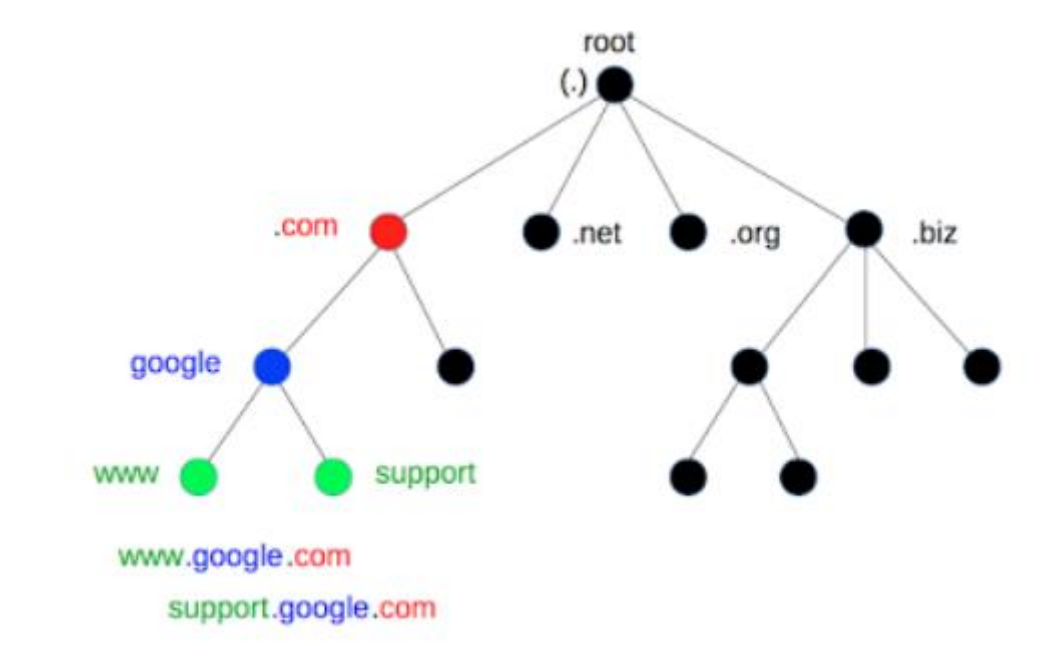
DNS : STRUCTURE DE L'ESPACE

- **RACINE**
  - NE POSSÈDE PAS DE NOM EXPLICITE : REPRÉSENTÉE PAR UNE CHAINE VIDE
  - LES OUTILS DNS UTILISENT UN POINT (« . ») POUR L'IDENTIFIER EXPLICITEMENT
- **NŒUD**
  - EST UN DOMAINE DE L'ESPACE DE NOM
  - DÉFINIT UN SOUS-ARBRE DE L'ESPACE DE NOMS
  - POSSÈDE UN NOM UNIQUE À UN NIVEAU DONNÉ D'UN SOUS-ARBRE
  - PEUT AVOIR COMME FILS DES NŒUDS (SOUS-DOMAINES) OU DES FEUILLES
  - UN SOUS-DOMAINE EST LUI-MÊME UN DOMAINE
  - CLASSEMENT EN NIVEAUX CORRESPONDANT À LA POSITION DU DOMAINE DANS L'ESPACE DE NOMS
    - UN NOEUD DE PREMIER NIVEAU EST APPELÉ *TOP LEVEL DOMAIN* (TLD)

DNS : STRUCTURE DE L'ESPACE

- **FEUILLE**
  - **EST UN HÔTE RÉFÉRENCÉ DANS L'ESPACE DE NOMS**
  - **ASSOCIE UN NOM À UNE ADRESSE**
    - PAS DE CONTRAINTE SUR L'ADRESSE ASSOCIÉE : DEUX MACHINES DU MÊME DOMAINE PEUVENT APPARTENIR À DES RÉSEAUX DIFFÉRENTS
    - PAS DE CONTRAINTE SUR LA NATURE DU MATÉRIEL : TYPE D'HÔTE, OS,
  - **ACCÈS À DES INFORMATIONS SUPPLÉMENTAIRES**
    - FONCTION D'ANNUAIRE UNIFIÉ
    - INFORMATION SUR LES HÔTES : PAS UTILISÉ DANS LA PRATIQUE
    - RÉSOLUTION DE SERVICES : UTILISÉ COMME EXTENSION DU SERVICE ORIGINEL

DNS : EXEMPLE


root
(.)
.com
.net
.org
.biz
google
www
support
www.google.com
support.google.com

DNS : DOMAINES DE PREMIER NIVEAU (TLD)

- **RENSEIGNENT SUR LA NATURE DU DOMAINE**
  - EMPLACEMENT GÉOGRAPHIQUE
  - TYPE D'ORGANISATION QUI EST RÉFÉRENCÉE PAR LE DOMAINE
- **SEULE PARTIE DE L'ESPACE DE NOMS QUI EST CONVENTIONNÉE**
- **LES TLD NATIONAUX**
- **LES TLD SPONSORISÉS**
- **LES TLD GÉNÉRIQUES**
  - NOTÉS GTLD (GENERIC TLD)
  - IDENTIFIENT DES TYPES D'ORGANISATION
  - ILS SONT LES 7 TLD INITIALEMENT STANDARDISÉS POUR L'ARPANET
  - CONCENTRATION SUR LES INSTITUTIONS AMÉRICAINES
  - LE 8ÈME TLD : « ARPA »
    - N'EST MAINTENANT UTILISÉ QUE POUR LA RÉSOLUTION INVERSE

DNS : LES TLD

Type	TLD	Sémantique	Exemple
Generic	com	Entreprises commerciales	ibm.com
	edu	Organismes universitaires des Etats-Unis	berkeley.edu
	gov	Organismes gouvernementaux des Etats-Unis	nsf.gov
	mil	Organismes militaires des Etats-Unis	navy.mil
	net	Organismes fournissant une infrastructure réseau. Ouvert depuis 1996 aux entreprises commerciales	uu.net
	org	Organismes non-commerciaux	eff.org
	int	Organismes internationaux	nato.int
Country Code	fr	Organismes résidant administrativement sur le territoire français	interieur.gouv.fr
Sponsored	aero	Sponsorisé pour l'industrie aéronautique	
	biz	Générique	
	coop	Sponsorisé pour les coopérations	
	info	Générique	
	museum	Sponsorisé pour les musés	
	name	Générique pour les particuliers	
	pro	Générique pour les professionnels	

DNS : FQDN

- **DÉFINITION**
  - **FQDN** : ***FULLY QUALIFIED DOMAIN NAME***
  - DÉSIGNE LE NOM DE DOMAINE COMPLET AVEC L'HÔTE ET PERMET DE RETROUVER LE CHEMIN DANS L'ESPACE DE NOMS
  - DE LA FORME :HÔTE.<DOMAINE>[1*].TLD
  - NE PEUT EXCÉDER 255 CARACTÈRES
- **NE PAS CONFONDRE FQDN ET URL**
  - URL : *UNIFIED RESOURCE LOCATOR*
    - IDENTIFICATEUR DE RESSOURCE QUI MENTIONNE SA LOCALISATION (FQDN)
    - UTILISÉ PRINCIPALEMENT SUR LE WEB
  - L'URL CONTIENT ÉGALEMENT LES PARAMÈTRES DE LA PAGE ET DU PROTOCOLE
  - LE FQDN N'EST QU'UN ÉLÉMENT D'UNE URL
    - FORME GÉNÉRIQUE D'UNE URL : **PROTOCOLE://FQDN:PORT/RESSOURCE?PARAM**

DNS : CONVENTIONS USUELLES POUR LE NOMMAGE

- **LE DOMAINE RACINE**
  - LE SEUL DOMAINE DONT LE NOM EST VIDE
- **LES DOMAINES DE PREMIER NIVEAUX**
  - SONT DÉFINIS DE MANIÈRE STANDARD
- **LES DOMAINES ET SOUS/DOMAINES DE NIVEAUX INFÉRIEURS**
  - 127 NIVEAUX AU MAXIMUM
  - CHAQUE NOM D'UN DOMAINE NE PEUT EXCÉDER 63 CARACTÈRES
  - LE FQDN NE PEUT EXCÉDER 255 CARACTÈRES
- **LES HÔTES**
  - PAS DE CONVENTION MAIS DES HABITUDES
  - SERVEUR WEB : WWW
  - LES SERVEURS D'AUTRES SERVICES : PORTENT SOUVENT LE NOM DU SERVICE
- EX : LDAP, SMTP, IMAP, POP

DNS : LES ENREGISTREMENTS

Type	Nom	Description
A	IPv4 Host Address	Associe un nom à une adresse IPv4
AAAA	IPv6 Host Address	Associe un nom à une adresse IPv6
CNAME	Canonical Name	Association d'un nom au nom canonique d'un hôte. Permet de créer des alias.
SOA	Start of Authority	Nom du domaine racine du sous-arbre où débute l'autorité du serveur. Des métadonnées lui sont associées.
PTR	Pointer	Un pointeur vers un hôte. Permet d'associer une adresse IP à un hôte pour la résolution inverse.
HINFO	Host Information	Description de l'hôte (système, configuration matérielle). Non renseigné par sécurité.
MX	Mail Exchange	Nom et priorité des serveurs de messagerie qui relaient le courrier électronique pour un domaine.
NS	Name Server	Délègue l'autorité d'une zone à un serveur donné
SRV	Locate Services	Généralisation de la localisation de services par extension de MX.

DNS : LE CLIENT DNS (RESOLVER)

- **DÉFINITION**
  - **LIBRAIRIE OFFERTE PAR LE SYSTÈME D'EXPLOITATION AUX APPLICATIONS**
    - LES APPLICATIONS OU ROUTINES SUR LA MACHINE DU CLIENT UTILISENT LE RESOLVER
  - **COMMUNIQUE AVEC LES MACHINES EXTERNES**
  - INTERROGE LA BASE DE DONNÉES DU SERVEUR DE NOMS
- **TÂCHES**
  - **INTERROGATION DES SERVEURS DE NOMS**
  - INTERPRÉTATION DES RÉPONSES
  - RENVOI DE L'INFORMATION AU PROGRAMME DEMANDEUR
-

DNS : LA RÉSOLUTION

- **PRINCIPE GÉNÉRAL**
  - PROCESSUS QUI PERMET À UNE APPLICATION CLIENTE D'ACCÉDER À UNE INFORMATION RÉFÉRENCÉE DANS L'ESPACE DE NOMS PAR LE BIAIS DES SERVEURS DNS
- **UN MODÈLE CLIENT/SERVEUR**
  - **PARCOURS DE L'ESPACE DE NOMS PAR LE BIAIS DE L'INTERROGATION SUCCESSIVE DES SERVEURS AYANT AUTORITÉ SUR UNE ZONE DE L'ESPACE**
  - RENVOI D'INFORMATIONS PAR LES RR NS
    - ON LES APPELLE LES « GLUE RECORDS »

LAB1 CONFIGURATION IP ET DNS

PROTOCOLE SSH

04/03/2022

- C'est un protocole de communication entre différentes machines
- Il vient améliorer le protocole telnet, en chiffrant le flux de données
- Le chiffrement protège ainsi contre le piratage d'informations sur le réseau
- Deux méthodes de chiffrement existe : **symétrique** et **asymétrique**
  - **Symétrique :** utilisation d'une seule clés pour le chiffrement/déchiffrement
  - **Asymétrique :** utilisation d'un couple de clés
- SSH utilise une combinaison de ces deux méthodes.

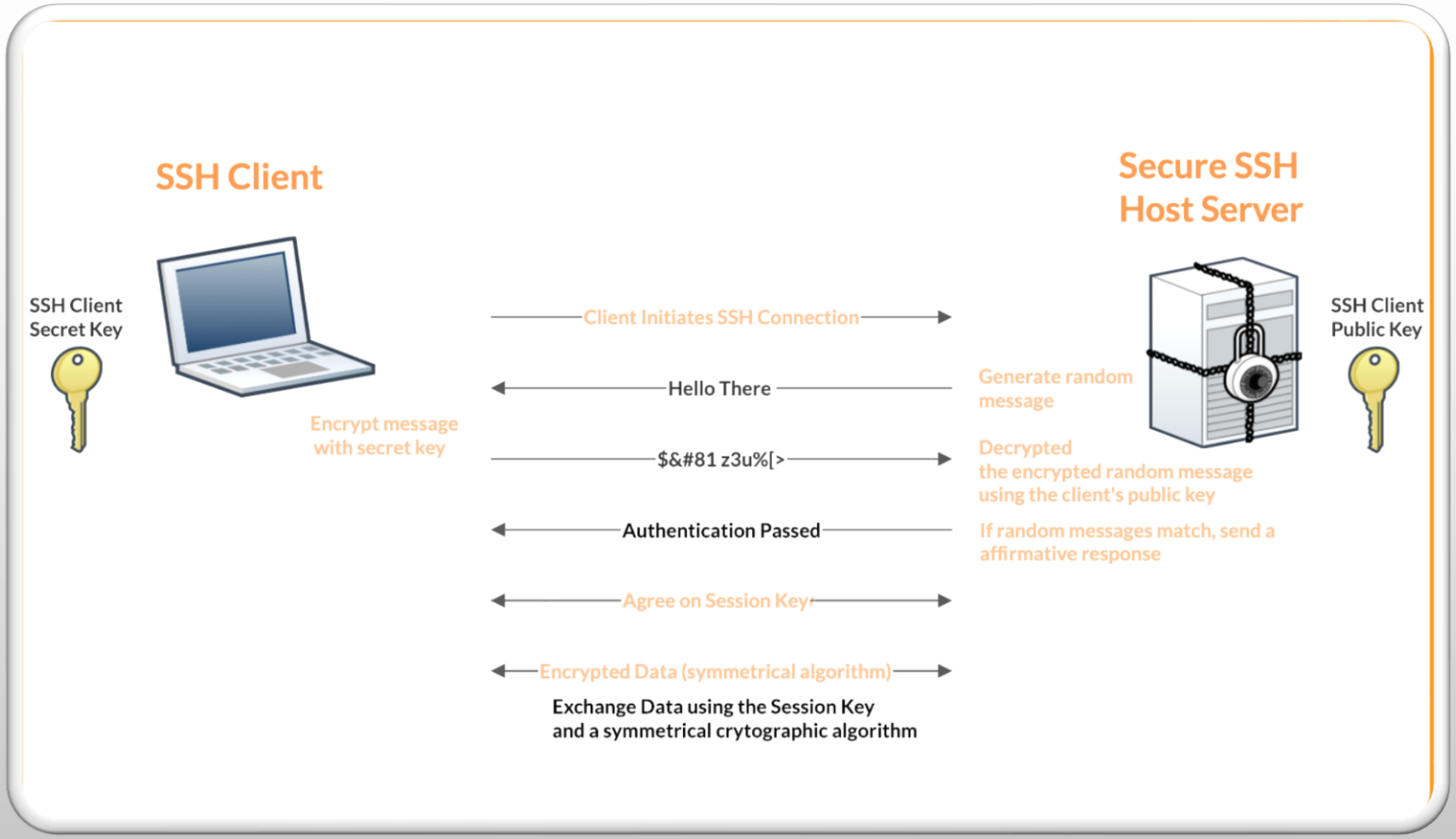
SSH, MOYEN DE MISE EN ŒUVRE

Via login/passwd linux

- on tape le mdp à chaque connexion
- c'est interactif

Via couple de clés publique/privée

- ***la clé publique est stockée sur le serveur et la clé privée sur le client ssh***
- on peut protéger la clé privée par une passphrase
- un démon permet de saisir sa passphrase une seule fois durant la session
- c'est plus pratique



SSH : SEQUENCE DES ÉCHANGES

SSH : CONFIGURATION (OPENSSH)

Paramètres	Signification
Protocol	Version du protocole
ListenAddress	Adresses sur lesquelles le serveur SSH attend les demandes de connexion
Port	Numéro de port du serveur
PermitRootLogin	Autorise ou non un client à se connecter avec le compte root
AllowUsers	Liste des utilisateurs autorisés. Les autres sont interdits
DenyUsers	Liste des utilisateurs interdits. Les autres sont autorisés.
PasswordAuthentication	Autorise ou non la connexion en fournissant le mot de passe de l'utilisateur
PubkeyAuthentication	Autorise ou non l'authentification par clé publique.

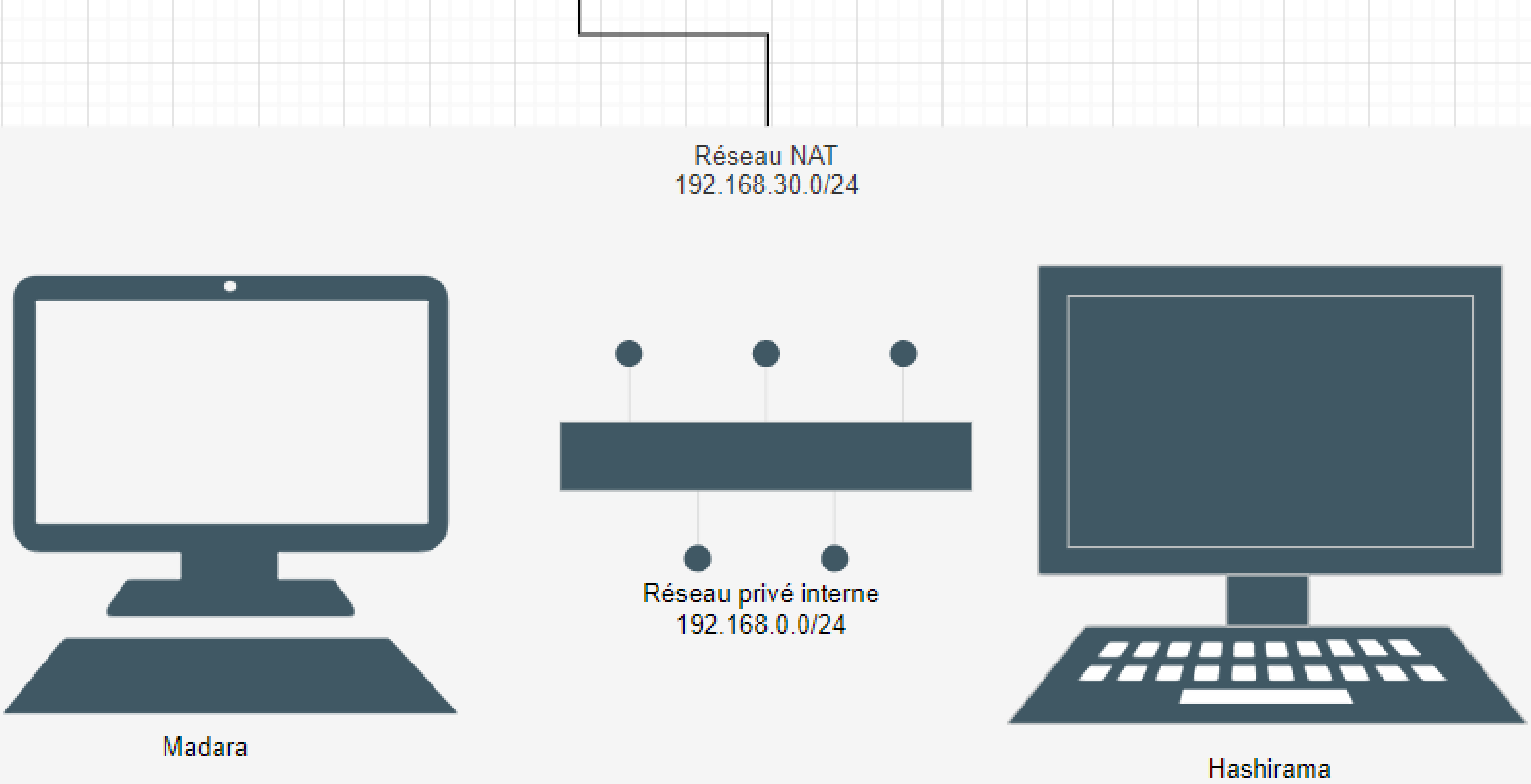
- Le fichier de conf par defaut est : **/etc/ssh/sshd_config**

Voici quelques paramètres du fichier .

- Le fingerprint du serveur est stocké dans **~/.ssh/known_hosts** du client. Il contient une ligne par serveur connu
- La keypair de l'utilisateur est stockée par defaut dans **~/.ssh/**

SSH : QUELQUES COMMANDES

Commandes	Utilisation
ssh	Connexion à un hôte
ssh-keygen	Génération de keypair
ssh-copy-id	Copie de clés publique sur un hôte distant
ssh-agent	Lancement de l'agent ssh
ssh-add	Evoie des clés privées à l'agent


Réseau NAT
192.168.30.0/24
Réseau privé interne
192.168.0.0/24
Madara
Hashirama

DEMO SSH

- Créer le nouvel utilisateur à configurer (sur Madara et Hashirama)
  - adduser naruto
- Escalader vers le nouveau user
  - su naruto
- Créer le couple de clés
  - ssh-keygen -t rsa
- Se déplacer ou se trouve le couple de clés
  - cd .ssh/
- Copier la clés publique sur le serveur distant
  - ssh-copy-id -i id_rsa.pub naruto@hashirama
- test la connexon
  - ssh naruto@hashirama

PLACE AUX TPS

LAB2 ECHANGE DE CLES SSH

PARTIE II

Transfert de data

Analyse du traffic

Filtrage de flux

TRANSFERT DE DATA : LES OUTILS

wget : supporte le http, https et le stp

curl : supporte la plupart des protocoles de transfert de data, tel http(s), ftp(s), imap(s), ldap(s), smtp(s) etc…

scp : transfert de data via ssh

winscp : client graphique pour faire du scp

ftp/sftp : transfert avec un serveur ftp

rsync : pour faire de la synchronisation de fichiers

TRANSFERT DE DATA : WGET ET CURL

Wget

- Sert principalement pour télécharger des fichiers
- wget http://hashirama/archives.tar
- wget http://hashirama/archives.tar -O archives_wget.tar

Curl

- Par défaut il fait un GET http
- Le contenu de la page est affiché a l'ecran
- curl http://hashirama/archives.tar --output archives_curl.tar

LAB3 : WGET ET CURL

TRANSFERT DE DATA : SCP ET WINSCP

- Se base sur ssh, d'où son utilisation identique a ssh
- Télécharger les fichiers distants :
  - scp user@ip_ou_hostname _distant :/chemin/vers/le/fichier/distant /chemin/vers/la/copie_locale
  - ***Exemple*** : scp naruto@hashirama:/home/ulrich/WEBROOT/scp.txt /tmp/toto.scp
- Uploader un fichier sur un serveur distants :
  - scp /chemin/vers/le/fichier_local user@ip_ou_hostname_distant:/chemin/vers/la/copie_distante
  - ***Exemple*** : scp /tmp/toto.scp naruto@hashirama:/home/ulrich/WEBROOT/scp.txt

TRANSFERT DE DATA : FTP ET SFTP

ftp :

- transferts sur les ports 20 (la data) et 21 (les commandes)
- on doit installer un tools supplépentaire (vsftpd par exemple)

sftp

- transfert les data sur le port 22
- passe par le serveur ssh, d'où chiffrement via ssh

TRANSFERT DE DATA : COMMANDES SFTP

Actions	Primitives/commandes
connexion	sftp *user@hostname*
Changer de répertoire	cd *répertoire_cible*
Lister les fichiers	ls
Télécharger un fichier	get *nom_du_fichier*
Afficher le répertoire courant	pwd
Uploader un fichier	put *nom_du_fichier*
Supprimer un fichier	rm
Se déconnecter	bye, exit, quit

- ***PS1*** : pour utilizer ces commandes sur la machine locale, les précéder de !.
  Exemple : lister les fichier sur la machine locale : !ls
- ***PS2*** : Certaines commandes ne sont pas les mêmes en ftp, se referrer au manuel ☺

TRANSFERT DE DATA : RSYNC

- permet de synchroniser deux dossiers
- les 2 dossiers peuvent être locaux ou entre deux serveurs différents
- il fait de la sauvegarde incrémentielle
- il se base sur le ssh pour la synchronisation distante
- la synchronisation est unidirectionnelle

TRANSFERT DE DATA : SYNTAXE RSYNC

synchro, locale

- rsync -arv dossier_source/ dossier_destination/
- a : conserve les métadata du fichiers (droits, user, groupe, etc …)
- r : synchro récursive sur les sous répertoires
- v : mode verbeux

Synchro distance (via ssh):

- rsync -arv dossier_source/ user@IP_du_serveur:dossier_destination/
- rsync -arv test_rsync/ naruto@hashirama:/home/naruto/test_rsync

PLACE AUX TPS

LAB4 ECHANGE DE DATA VIA SSH

ANALYSE DU TRAFFIC : NETSTAT

- les commandes host et nslookup permettent de requêter le dns pour avoir l'équivalent ip d'un nom de machine, et inversement
- **netstat** permet d'analyser les flux réseaux
- **netstat -i** : afficher les stats des interfaces réseau
- **netstat -uta** : lister toutes les connexions ouvertes
- **netstat -lt** : liste des connexions en état d'écoute
- **netstat -s** : statistiques résumées

QUELQUES OPTIONS DE NETSTAT

- -p : affiche le nom et le pid des processus
- -i : affiche la table de toutes les interfaces réseau
- -u : afficher les connexions udp
- -t : afficher les connexions tcp
- -a : afficher toutes les connexions quel que soit leur état
- -l : afficher les connexions en écoute
- -s : afficher un résumé
- -n : afficher les numéro de port

FILTRAGE DE FLUX : IPTABLES

- Pare-feu natif linux
- Permets de filtrer le traffic par, ip et par port
- C 'est pas un antivirus, le but est juste, de limiter les programmes pouvant communiquer avec votre machine
- Le principe est de tout bloquer par défaut et autoriser uniquement le traffic identifié (***système close to open)***
- Si aucune règle ne match, la règles par défaut sera appliquée

FILTRAGE DE FLUX : SYNTAXE GÉNÉRALE ET OPTIONS IPTABLES

- Syntaxe : iptables -A (chain) -p (protocole) --dport (port) -j (décision)
  - chaine = INPUT / OUTPUT / FORWARD
  - protocole = tcp / udp / icmp / smtp / ldap / etc …
  - port = le port à configurer (22, 80, 8080, etc …)
  - décision = ACCEPT / REJECT / DROP
- -L : afficher les règles configurées
- -F : Reinitialiser les règles
- -A chain : ajoute une règle en fin de liste
- -D chain num : supprime la règle num
- -R chain num : remplace la règle num
- -P chain décision : modifie la règle par défaut pour la chain

FILTRAGE DE FLUX : QUELQUES RÈGLES IPTABLES

- Par defaut, refuser toutes les connexions
  - iptables -P INPUT DROP
- Par defaut, accepter toutes les connexions
  - iptables -P INPUT ACCEPT
- Refuser tout le trafic sur l'interface enp0s8
  - iptables -A INPUT -i enp0s8 -j ACCEPT
- Autorise les connexions déjà établies
  - iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

IPTABLES : ANNEXES

- PETIT ARTICLE UTILE :
  - HTTPS://CONNECT.ED-DIAMOND.COM/GNU-LINUX-MAGAZINE/GLMFHS-041/INTRODUCTION-A-NETFILTER-ET-IPTABLES

PLACE AUX TPS

- LAB5 NETSTAT ET IPTABLES

PARTIE III

- SURVEILLANCE DES RESSOURCES PHYSIQUES DU SYSTÈME
- SURVEILLANCE DE L'ACTIVITÉ DU SYSTÈME
- GESTION DES SERVICES : SYSTEMD

SURVEILLANCE DU SYSTÈME : LES RESSOURCES PHYSIQUES

- Connaitre sa distribution Linux : cat/etc/os-release
- utilisation de la mémoire : free
  - free -m ; free -g ; free -ht
- utilisation du disque : df
  - df -h ; df -H ; df -m
- la swap : cat /proc/swaps ; free ; swapon -s
- Taille d'un répertoire et son contenu : du
  - du -m ; du ; du -ks
- Infos sur le CPU : lscpu ; cat /proc/cpuinfo
- Les interfaces réseau : ifconfig ; ethtool (package à installer)

SURVEILLANCE DU SYSTÈME : ACTIVITÉ

- w : c'est un condensé des commandes uptime, who et date
- top : permet d'afficher les métriques en temps réels
- atop : donne plus d'informations que top, possèdes des fichiers journaux exploitables. Programme à installer car pas disponible par défaut
- ss : analyse des sockets, similaire à netstat
- ps : permet d'afficher les processus en cours
  - ps -ejH ; ps –ef

SYSTEMD : SYSTEM DAEMON

- UN DÉMON EST UN PETIT PROGRAMME QUI A POUR BUT D'ASSURER UNE TÂCHE PARTICULIÈRE
- LE **DÉMON DU SYSTÈME** EST UN ENSEMBLE DE PROGRAMMES DESTINÉ À LA GESTION SYSTÈME
- IL EST SPÉCIFIQUEMENT CONÇU POUR LE NOYAU LINUX
- IL PERMET LE CHARGEMENT EN PARALLÈLE DES SERVICES AU DÉMARRAGE
- SON BUT EST DE REMPLACER LE DÉMON **INIT SYSTEM V**

SYSTEMD : **GESTION DES SERVICES**

- LA CONFIGURATION DES SERVICES SE TROUVE PAR DÉFAUT DANS LE RÉPERTOIRE **/lib/systemd/system** OU **/usr/lib/systemd/system.**
- LE **/etc/systemd/system** SERVIRA À STOCKER SES MODIFICATIONS ET CONFIGURATIONS PERSONNELLES => CE NE SERA PAS ÉCRASÉ S'IL YA DES MISES À JOURS…
- LA CONFIGURATION SE BASE SUR DES **UNITÉS** : ELLES ONT UN UN NOM ET UN TYPE
- PLUSIEURS UNITÉS PEUVENT ÊTRE GROUPÉES ENSEMBLE POUR FORMER UNE **CIBLE** OU **RUNLEVEL**
- LES **RUNLEVEL** (NIVEAUX D'EXÉCUTIONS) CORRESPONDENT À UN MODE DE FONCTIONNEMENT DU SYSTÈME (MODE GRAPHIQUE, NON GRAPHIQUE ETC.) QUI CORRESPOND À UN DÉMARRAGE D'UN CERTAIN NOMBRE DE SERVICES.
- CES RUNLEVELS DÉPENDENT DES DISTRIBUTIONS
- LES SERVICES SE MANIPULENT AVEC LA COMMANDE **SYSTEMCTL**
  - systemctl <action> <nom_du_service>.service

SYSTEMD : **TYPES D'UNITÉS**

- **SERVICE** : POUR UN SERVICE SYSTÈME ;
- **SOCKET** : POUR UNE SOCKET DE COMMUNICATION ENTRE PROCESSUS (DE TOUS TYPES : UNIX, INTERNET, FICHIER ETC.) ;
- **BUSNAME** : POUR LES LOGICIELS DE COMMUNICATION INTER-PROCESSUS (PAR EXEMPLE DBUS) ;
- **TARGET** : MACRO-UNITÉ QUI PERMET DE GROUPER PLUSIEURS UNITÉS (EXEMPLE : **multi-user.target** POUR DÉFINIR UNE CIBLE) ;
- **PATH** : POUR L'ACTIVATION D'UN SERVICE BASÉE SUR LA MODIFICATION DE FICHIERS OU DE RÉPERTOIRES (TYPIQUEMENT POUR LES FILES D'ATTENTE LORS DE L'IMPRESSION) ;
- **MOUNT** : POUR UN SYSTÈME DE FICHIERS (EXEMPLE : HOME.MOUNT), TOUT EN UTILISANT /etc/fstab ;
- **AUTOMOUNT** : POUR UN SYSTÈME DE FICHIERS MONTÉ À LA DEMANDE ;
- **DEVICE** : POUR UN PÉRIPHÉRIQUE ;
- **TIMER** : POUR L'ACTIVATION BASÉE SUR UNE DATE ;
- **SCOPE** : UTILISÉ PAR SYSTEMD LUI-MÊME POUR GÉRER DES GROUPES DE PROCESSUS, TYPIQUEMENT, PAR SESSION UTILISATEURS ;

SYSTEMD : **DÉMARRAGE, ARRÊT DE SERVICE**

- Démarrer un service : systemctl start application.service
- Arrêter un service : systemctl stop application.service
- Redémarrer un service lancé : systemctl restart application.service
- Recharger les fichiers de configuration d'un service : systemctl reload application.service
- Lancer au démarrage du système : systemctl enable application.service
- Ne pas lancer au démarrage du système : systemctl disable application.service
- Empêcher l'activation d'un service : systemctl mask application.service
- Envoyer un signal d'arrêt à tous les processus du service : systemctl kill application.service

SYSTEMD : **INFORMATION SUR UN SERVICE**

- Voir tous les services disponibles et leur statut : systemctl list-unit-files --type=service --all
- Vérifier si le service est démarré, arrêté : systemctl status application.service
- Voir si le service est actuellement démarré : systemctl is-active application.service
- Vérifier si le service sera up au démarrage du système : systemctl is-enabled application.service
- Vérifier qu'il y a eu un problème lors du démarrage : systemctl is-failed application.service
- Voir tous les services qui ont un problème : systemctl --failed --type=service

PLACE AUX TPS

04/03/2022

LAB6 SYSTEMD

PARTIE IV

SERVICE WEB

LOAD BALANCING

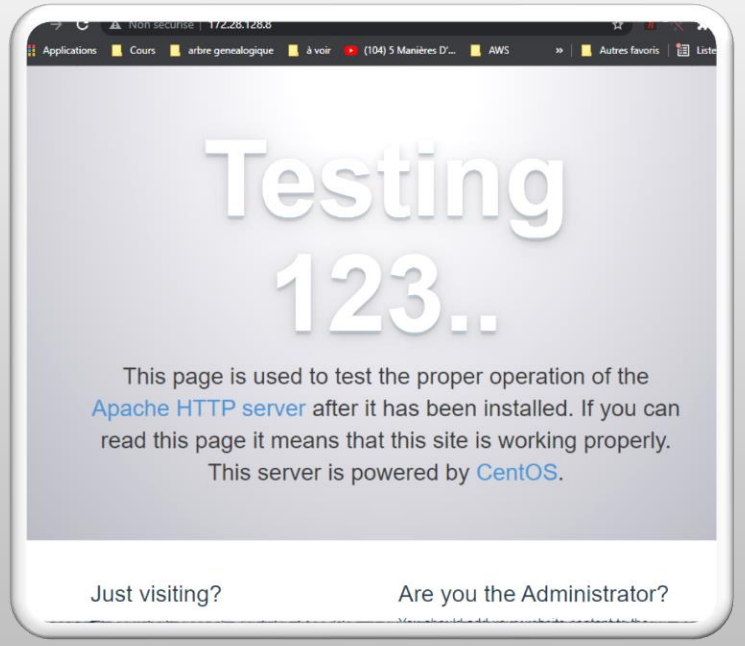
SERVICE DE PARTAGE DE FICHIER

SERVICE DATABASE

SERVICE WEB : APACHE

- C'EST UN SERVEUR HTTP PRODUIT PAR LA FONDATION APACHE
- C'EST LE SERVEUR WEB LE PLUS POPULAIRE SUR INTERNET
- IL EST DISPONIBLE SUR DE NOMBREUX OS (UNIX ET DERIVÉS, WINDOWS)
- SUR CENTOS, LE NOM DU PACKAGE EST HTTPD
- SA DOCUMENTATION OFFICIELLE : HTTP://HTTPD.APACHE.ORG/DOCS/
- IL DISPOSE DE NOMBREUX MODULES QUI ÉTENDENT SES FONCTIONNALITÉS
  - SUPPORT DU SSL/TLS
  - VIRTUAL HOSTING
  - SUPPORT DE LANGAGES DE PROGRAMMATION VARIÉS

APACHE : INSTALLATION



- Commande d'installation : yum install httpd
- Démarrage et activation au boot : systemctl enable --now httpd
- Port par defaut utilisés par le serveur :
  - http 80/tcp
  - https 443/tcp
- Test de fonctionnement :
  - curl http://<adresse_IP>/
  - Ou taper ceci dans le navigateur : http://<adresse_IP>/

APACHE : CONFIGURATION

Emplacement	Utilité
/etc/httpd	Répertoire principal de configuration
/etc/httpd/conf/httpd.conf	fichier principal de configuration, il décrit le comportement général du serveur
/etc/httpd/conf.d	emplacement des configurations secondaires. C'est là qu'on stocke les configurations de nos sites web
/var/log/httpd	logs de httpd
/var/www/html	emplacement des pages web affichées
/var/log/httpd/access_log	logs des demandes traitées par le serveur
/var/log/httpd/error_log	erreurs enregistrées par le serveur, souvent des refus d'accès
/var/www/error	emplacement des pages affichées en cas d'erreur

APACHE : VIRTUAL HOST

```
<VirtualHost 172.28.128.8:80>
  DocumentRoot /var/www/tp.linux.tp/html
  ServerName eni.tellnet.fr
  ErrorLog logs/tp.linux.fr-error_log
  CustomLog logs/tp.linux.fr-access_log common
</VirtualHost>

<VirtualHost 172.28.128.8:80>
  DocumentRoot /var/www/cours.linux.fr/html
  ServerName cours.linux.fr
  ErrorLog logs/cours.linux.fr-error_log
  CustomLog logs/cours.linux.fr-access_log common
</VirtualHost>
```

- L'IDÉE EST DE FAIRE CROIRE QU'IL EXISTE PLUSIEURS SERVEURS WEB QUI RÉPONDENT ALORS QU'EN RÉALITÉ IL N'EXISTE QU'UN SEUL SERVEUR PHYSIQUE
- IL EST PRÉFÉRABLE DE LES CONFIGURER DANS /ETC/HTTPD/CONF.D
- ON PEUT LE FAIRE DE 2 MANIÈRES
  - VHOST PAR NOM
    - ON A UNE SEULE IP, A LAQUELLE ON VA ASSOCIER +SIEURS NOMS DNS
  - VHOST PAR ADRESSE IP
    - ON A +SIEURS @ IP, ON AURA 1 IP POUR 1 VHOST

```
<VirtualHost 172.28.128.9:80>
  DocumentRoot /var/www/172.28.128.9
  ServerName 172.28.128.9
  ErrorLog logs/vhost2.example.com-error_log
  CustomLog logs/vhost2.example.com-access_log common
</VirtualHost>
```

PLACE AU TP : DÉPLOIEMENT DE SITE WEB (LAB 7.1)

- Mettre en place un serveur web apache
- Le serveur devra avoir deux vhost
- Le premier vhost hébergera le site : https://github.com/diranetafen/static-website-example.git
- Le deuxième héberge une simple page html écrite par vos soins
- Vous avez le choix du type de vhost à mettre en œuvre

SERVICE WEB : NGINX

- SE LIT ENGINE X, C'EST LE PRINCIPAL CONCURRENT DE APACHE
- IL A VOCATION A ÊTRE PLUS RAPIDE QUE APACHE SUR LES TÂCHES SUIVANTES :
  - SITE WEB BASIQUE
  - REVERSE PROXY
  - EQUILIBRAGE DE CHARGE
  - CACHE HTTP

NGINX : CONFIGURATION

Emplacement	Utilité
/etc/nginx	Répertoire principal de configuration
/etc/nginx/nginx.conf	fichier principal de configuration, il décrit le comportement général du serveur
/etc/nginx/conf.d	emplacement des configurations secondaires. C'est là qu'on stocke les configurations de nos sites web
/var/log/nginx/	logs de httpd
/usr/share/nginx/html	Emplacement du site web principal (par défaut) du serveur
/var/log/nginx/access.log	logs des demandes traitées par le serveur
/var/log/nginx/error.log	erreurs enregistrées par le serveur, souvent des refus d'accès
/var/www/error	emplacement des pages affichées en cas d'erreur

NGINX : INSTALLATION

- Commande d'installation : yum install nginx
- Démarrage et activation au boot : systemctl enable --now nginx
- Port par defaut utilisés par le serveur :
  - http 80/tcp
  - https 443/tcp
- Test de fonctionnement :
  - curl http://<adresse_IP>/
  - Ou taper ceci dans le navigateur : http://<adresse_IP>/

NGINX : CONFIGURATION MINIMALE

- **server { }** : config d'un site web
- **server_name** : nom de domaine
- **root** : définition dela racine du site web dans l'arborescence
- **location url_path { }** : configuration d'une sous partie du site

```
[root@web conf.d]# pwd
/etc/nginx/conf.d
[root@web conf.d]# cat monsite.conf
    server {
        server_name   www.monsiteinternet.com;
        listen        80;
        root   /usr/share/nginx/www.monsiteinternet.com;
        location /externes {
                # Directives de configuration spécifiques
        }
    }
```

NGINX : REVERSE PROXY

- La primitive **proxy_pass** est la clés
- Attention à ne pas oublier le "/" à la fin

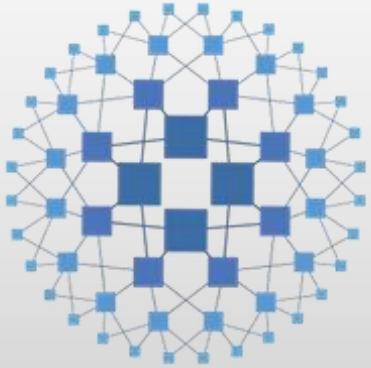
```
[root@web conf.d]# pwd
/etc/nginx/conf.d
[root@web conf.d]# cat monreverseproxy.conf
   server {
       server_name   www.monsiteinternet.com;
       listen        80;
       root   /usr/share/nginx/www.monsiteinternet.com;
       location /admin {
               proxy_pass http://127.0.0.1:8080/;
       }

       location /externes {
               proxy_pass http://web:8081/;
       }
   }
```

TP : SITE WEB DERRIÈRE UN PROXY (LAB 7.2)

- Mettre en place deux serveur web sur deux machines
- Le premier tournant sur un apache, le deuxième sur un nginx
- Le serveur apache heberge le site : https://github.com/diranetafen/static-website-example.git
- Le serveur nginx héberge ce que vous voulez
- Configurez un troisième serveur frontal, qui fera office de reverse proxy
- Ce serveur proxy tourne sur du nginx

LOAD BALANCING AVEC HAPROXY

- C'est une solution opensource permettant de faire de la haute disponibilité sur plusieurs serveurs
- Le nom du package est haproxy
- Son fichier de configuration est le /etc/haproxy/haproxy.cfg
- Une configuration minimaliste consiste a
  - Définir un frontend : point d'entrée de l'application
  - Définir un backend : les serveurs hebergeant l'application
  - Lier le frontend et le backend

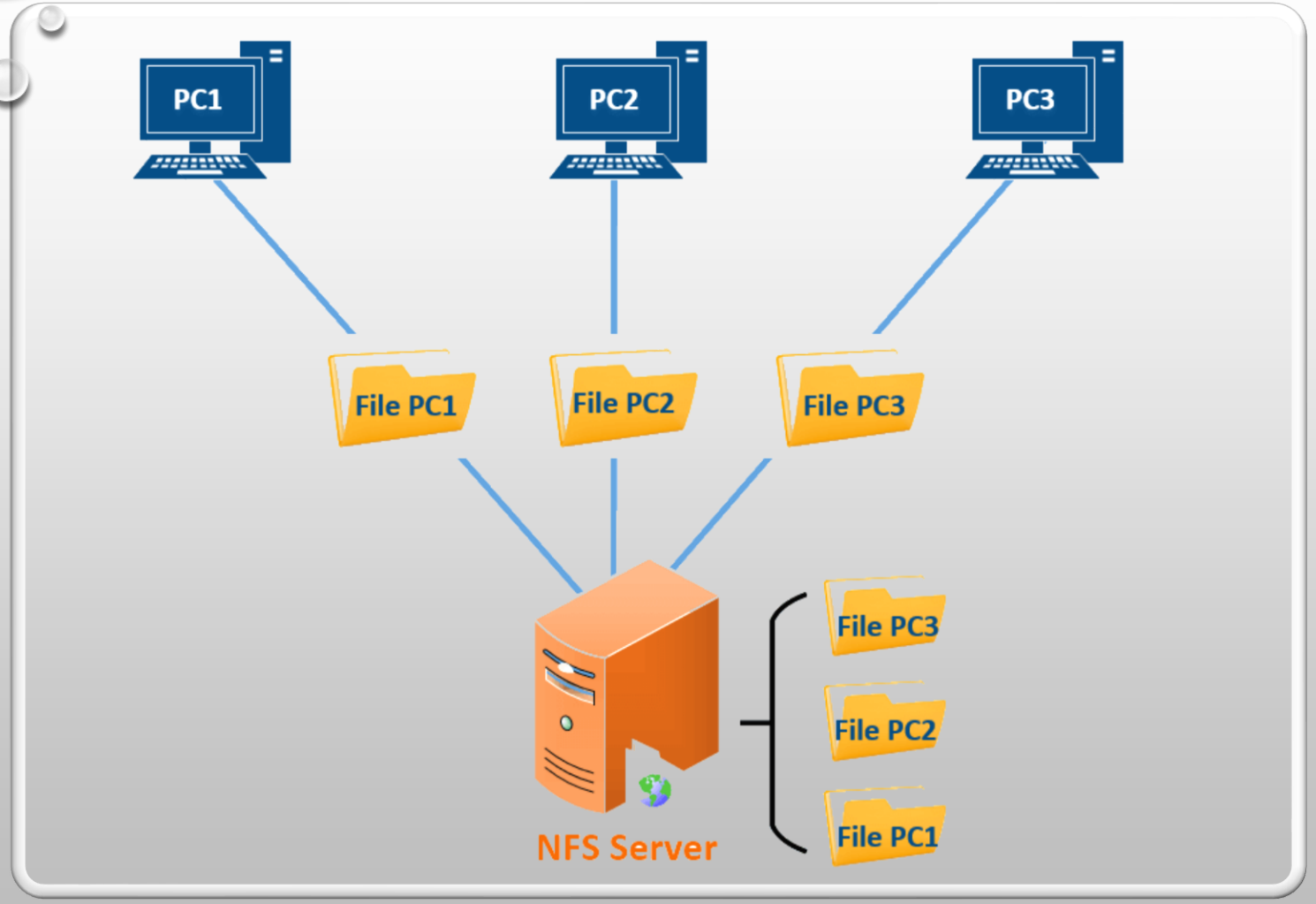


HAPROXY

```
frontend monsite
    bind *:8000

    use_backend static
    default_backend             static


backend static
    balance     roundrobin
    server      server1 web:80 check
    server      server2 web:8080 check
```

HAPROXY : EXEMPLE DE CONFIGURATION

LAB 7.3 DÉPLOYER UN HAPROXY EN FRONTAL DE VOS SERVEURS WEB



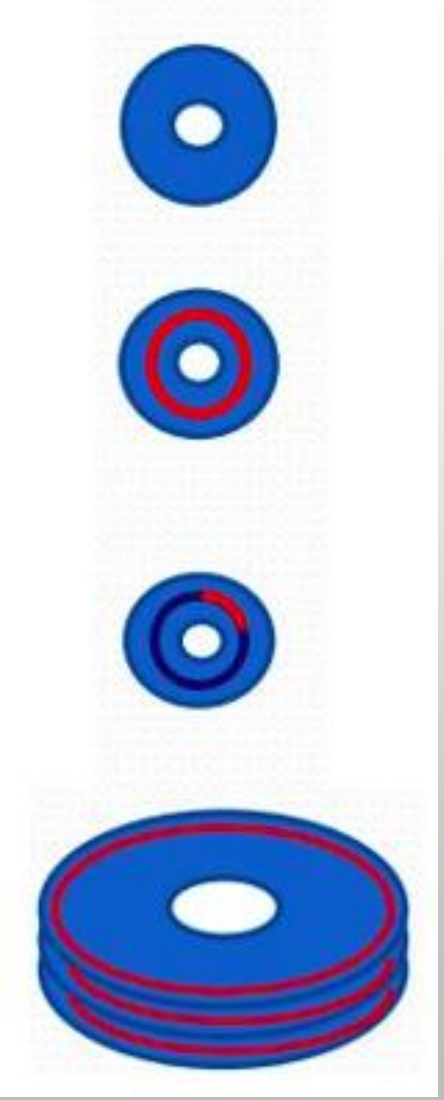
STOCKAGE : NFS

- il est question de mettre a disposition un espace de stockage partagé via le réseau

LAB8 PARTAGE NFS

PARTIE V

- Le disque dur
- Organisation du disque dur
- Nomenclature
- Points de montage
- Création de partitions avec fdisk
- Le LVM



LE DISQUE DUR

- IL EST CONSTITUÉ D'UN OU PLUSIEURS PLATEAUX
  - CHAQUE PLATEAU EST DIVISÉ EN PISTES (TRACKS)
  - CHAQUE PISTE EST DIVISÉE EN SECTEURS (SECTORS)
  - LE CYCLINDRE EST FORMÉ PAR LES PISTES DE MÊME RAYON SUR CHAQUE PLATEAU
- LA CAPACITÉ DU DISQUE DÉPEND DONC DE :
  - LA TAILLES DES SECTEURS
  - DU NOMBRE DE CYLINDRES

ORGANISATION DU DISQUE

- Le **MBR** (**M**aster **B**oot **R**ecord) d'une taille totale de **512 Octets** contient :
  - La table des partitions (4 descripteurs de fichiers sous de 16 Octets) de **64 Octets**
  - Le programme de boot qui charge le noyau du système (GRUB) de **446 Octets**
  - Une signature sur **2 Octets**

- Plusieurs types de partitions
  - **Principales** ou primaires
    - Maximum de **4** à cause des **4 descripteurs** de fichiers du MBR
    - Acceptent tout type de FS
  - **Etendue** ou secondaire
    - Un entonnoir pour les partitions logiques
    - Nécessitent au moins une partition principale
    - Logiques, elles sont contenues dans celle étendue et acceptent tout type de FS
  - **Active** : c'est celle qui contient le système d'exploitation

NOMENCLATURES

- SOUS LINUX LA NOMENCLATURE DES DISQUES NE SE FAIT PAS AVEC LES LETTRES COMME C'EST LE CAS POUR WINDOWS
- **H/S** : LA PREMIÈRE LETTRE INDIQUE SI LE DISQUE EST DE TYPE **IDE** OU **SCSI** (UN TYPE DE CONNEXION DIFFÉRENT À LA CARTE MÈRE). S'IL EST DE TYPE IDE, LA LETTRE EST UN « H », SI C'EST UN SCSI (OU UN S-ATA OU UN USB), LA LETTRE EST UN « S ».
- **D**: CETTE LETTRE NE CHANGE PAS, PROBABLEMENT MIS POUR DISK
- **A**: C'EST CETTE LETTRE QUI INDIQUE LES DIFFÉRENTS DISQUES DURS. HD**A** REPRÉSENTE LE PREMIER DISQUE DUR IDE, HD**B** LE SECOND, HD**C** LE TROISIÈME, ETC.
- LORSQU'ON CRÉE DES PARTITIONS, ON AJOUTE GÉNÉRALEMENT UN CHIFFRE REPRÉSENTANT LE NUMÉRO DE LA PARTITION. AINSI, SI ON A TROIS PARTITIONS SUR NOTRE DISQUE HDA, ELLES SERONT NOMMÉES HDA**1**, HDA**2**, HDA**3**…

POINT DE MONTAGE

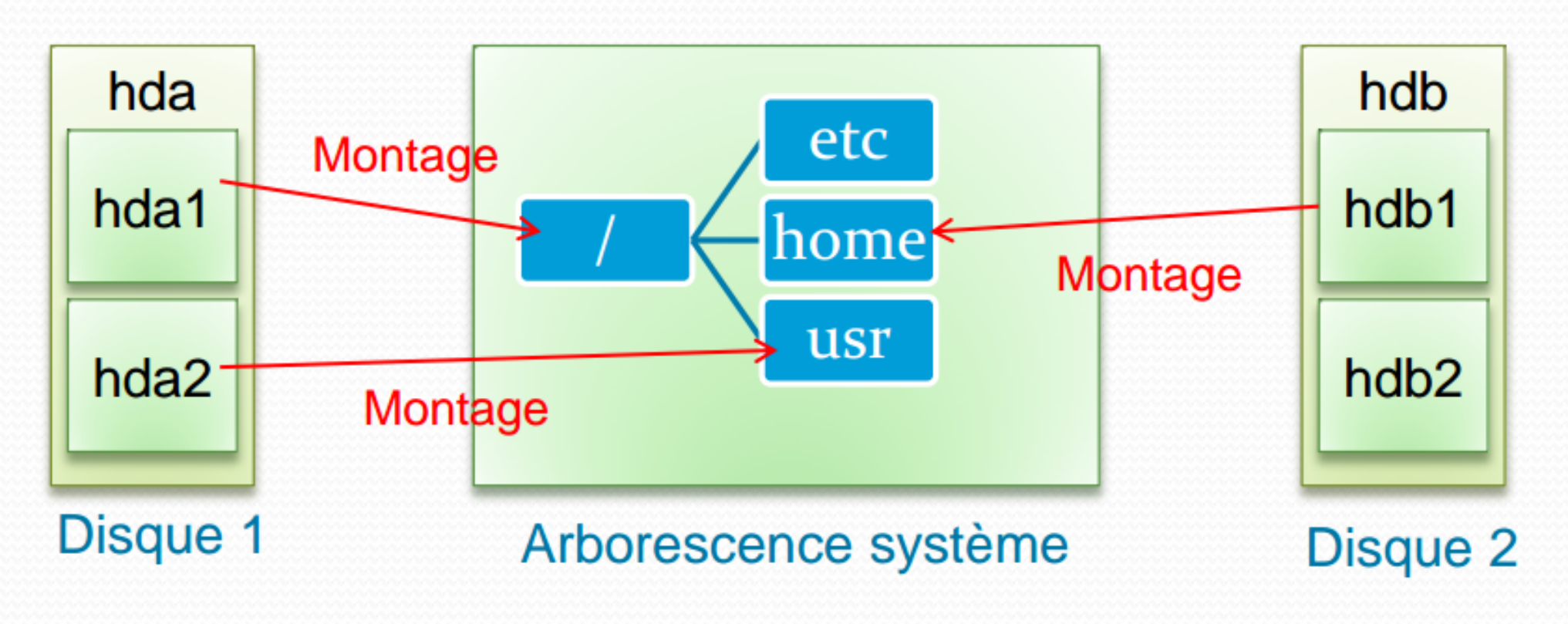
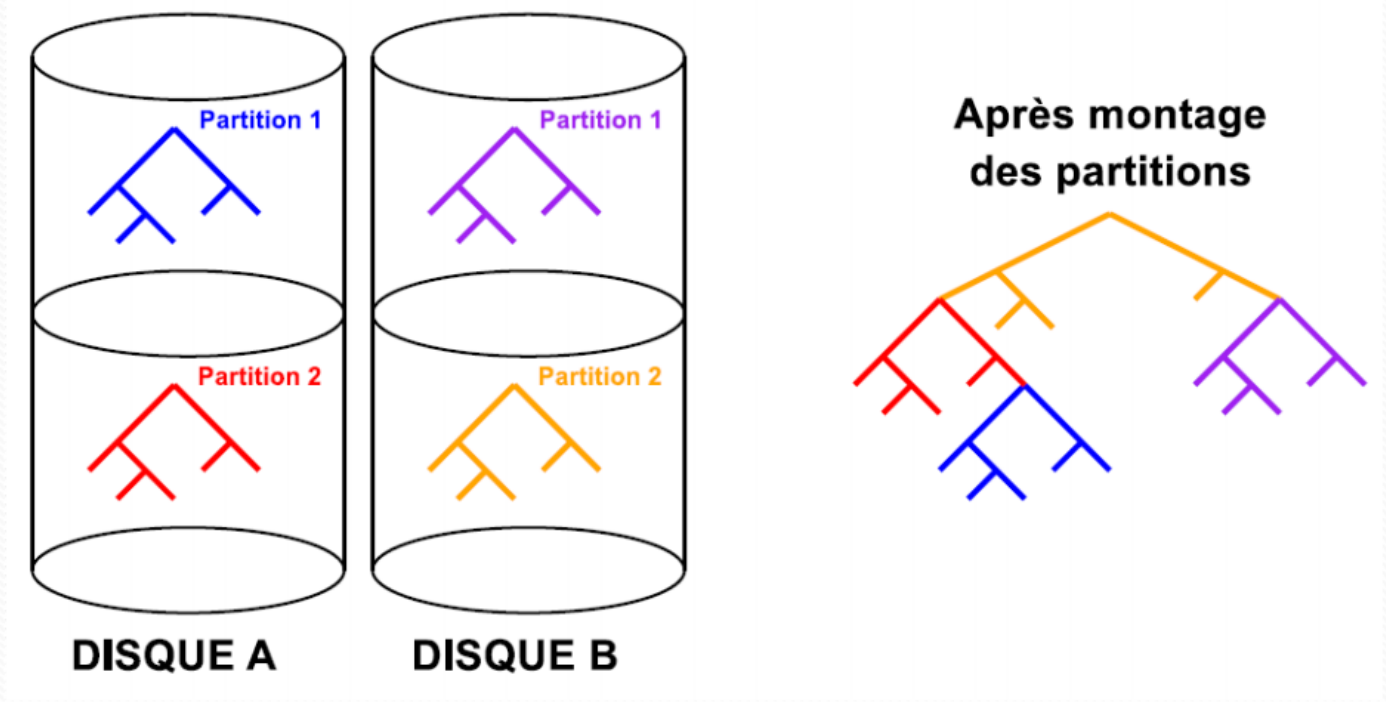


SCHÉMA DE PRINCIPE



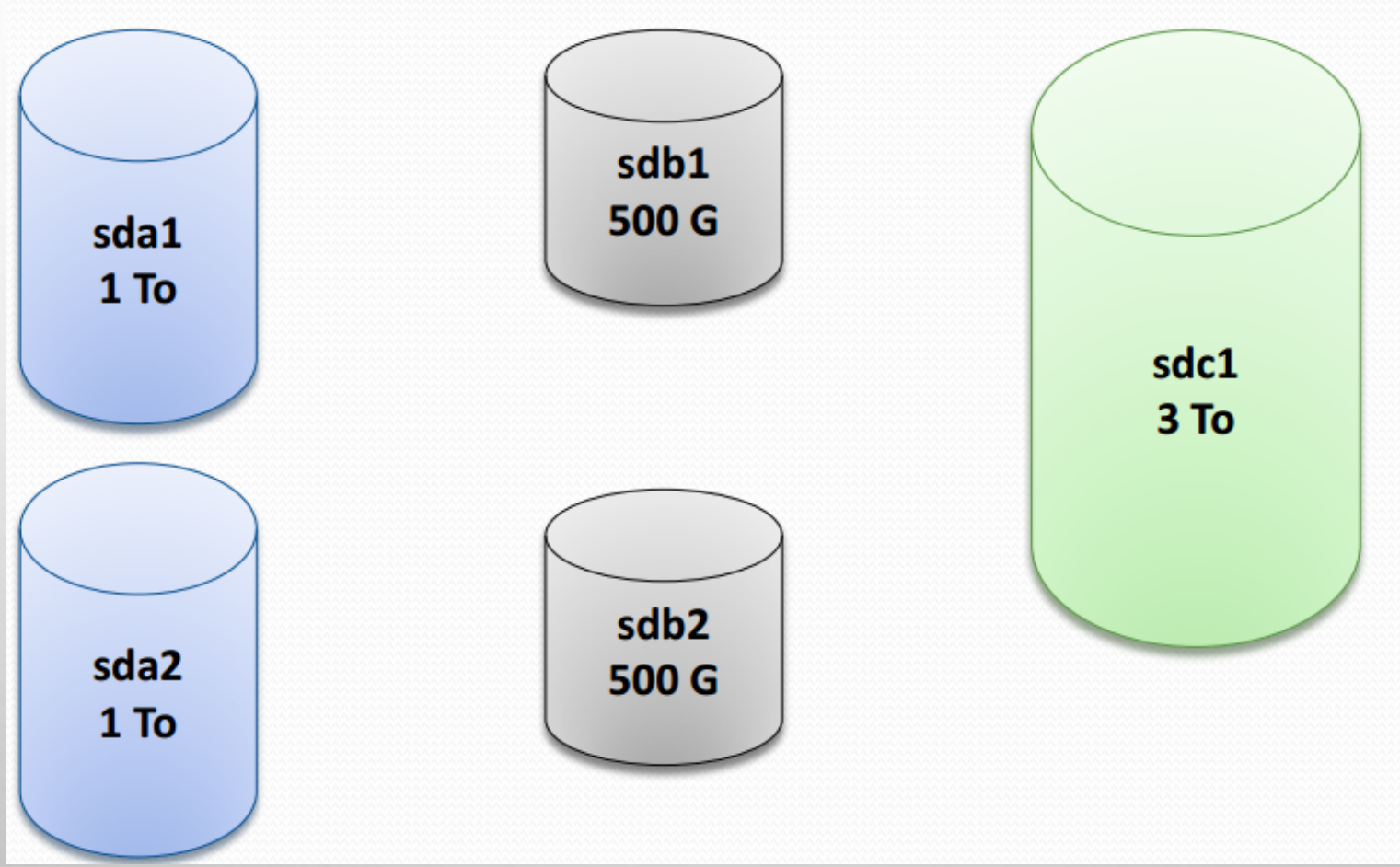
DISQUES : RECETTE DE CUISINE

- AFFICHER LA LISTE DES DISQUES : **FDISK –L**
- CRÉATION DE NOUVELLE PARTITION : **FDISK** "NOM DE LA PARTITION"
- MONTER LE DISQUE : **MOUNT** –T "TYPE DE FS" PARTITION MOINT_DE_MONTAGE
- DÉMONTER LA PARTITION : **UMOUNT** POINT_DE_MONTAGE
- VÉRIFIER L'INTÉGRITÉ DU SYSTÈME : **FSCK** "DISQUE"

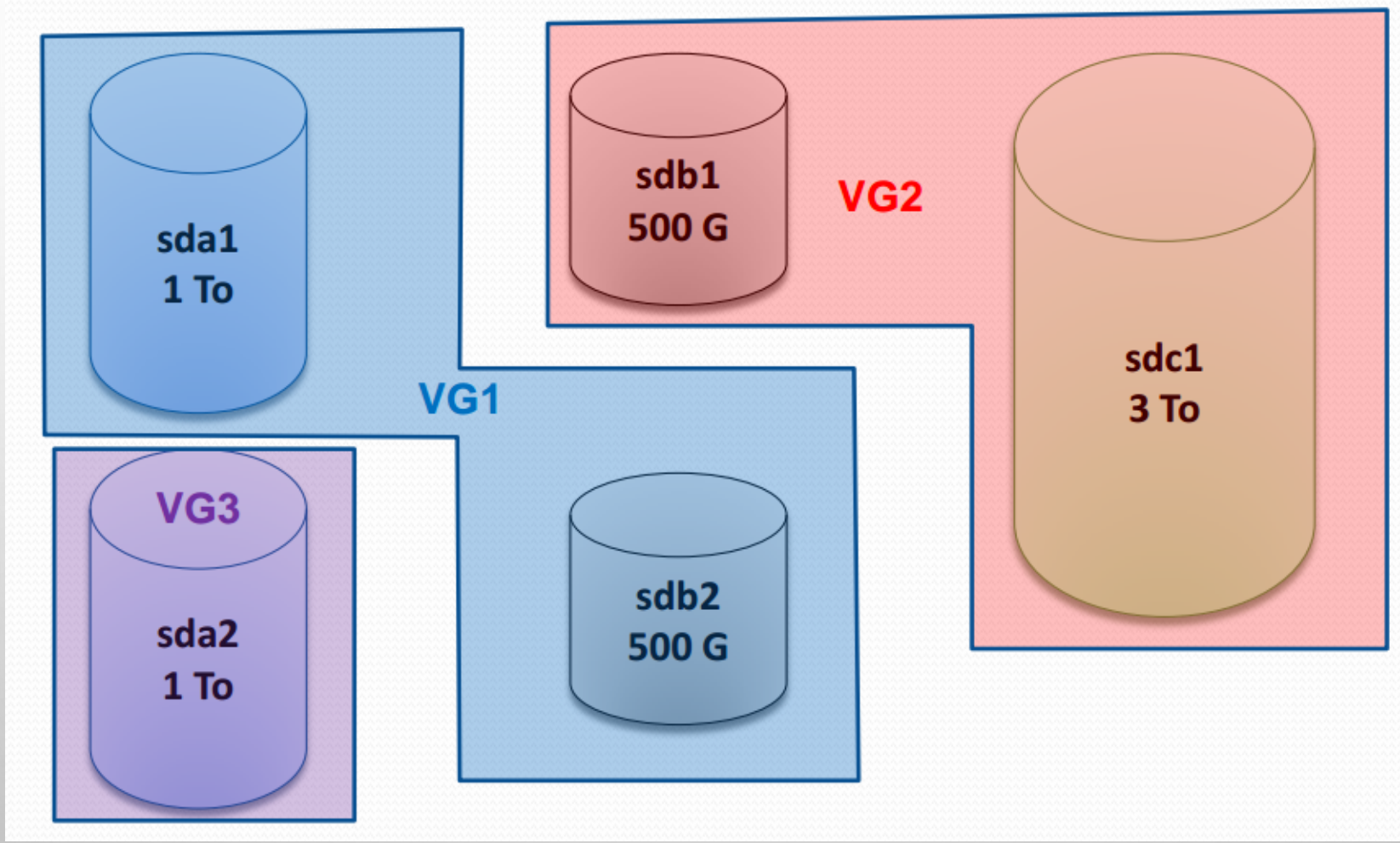
LE LVM : LOGICAL VOLUME MANAGER

- C'EST UN AGRÉGAT DE SOURCES DE STOCKAGE DISPARATES
- REDIMENSIONNEMENT À LA VOLÉE
- GESTION PLUS FINE DU STOCKAGE
- HIERARCHIE :
  - VOLUME PHYSIQUE OU **P**HYSICAL **V**OLUME (**PV**): DES PARTITIONS DE DISQUE ÉVENTUELLEMENT DIFFÉRENTS
  - GROUPE DE VOLUMES OU **V**OLUME **G**ROUP (**VG**): REGROUPEMENT DE PLUSIEURS **PV**
  - VOLUME LOGIQUE OU LOGICAL VOLUME (**LV**) ; CE QUI REÇOIT LE SYSTÈME DE FICHIER

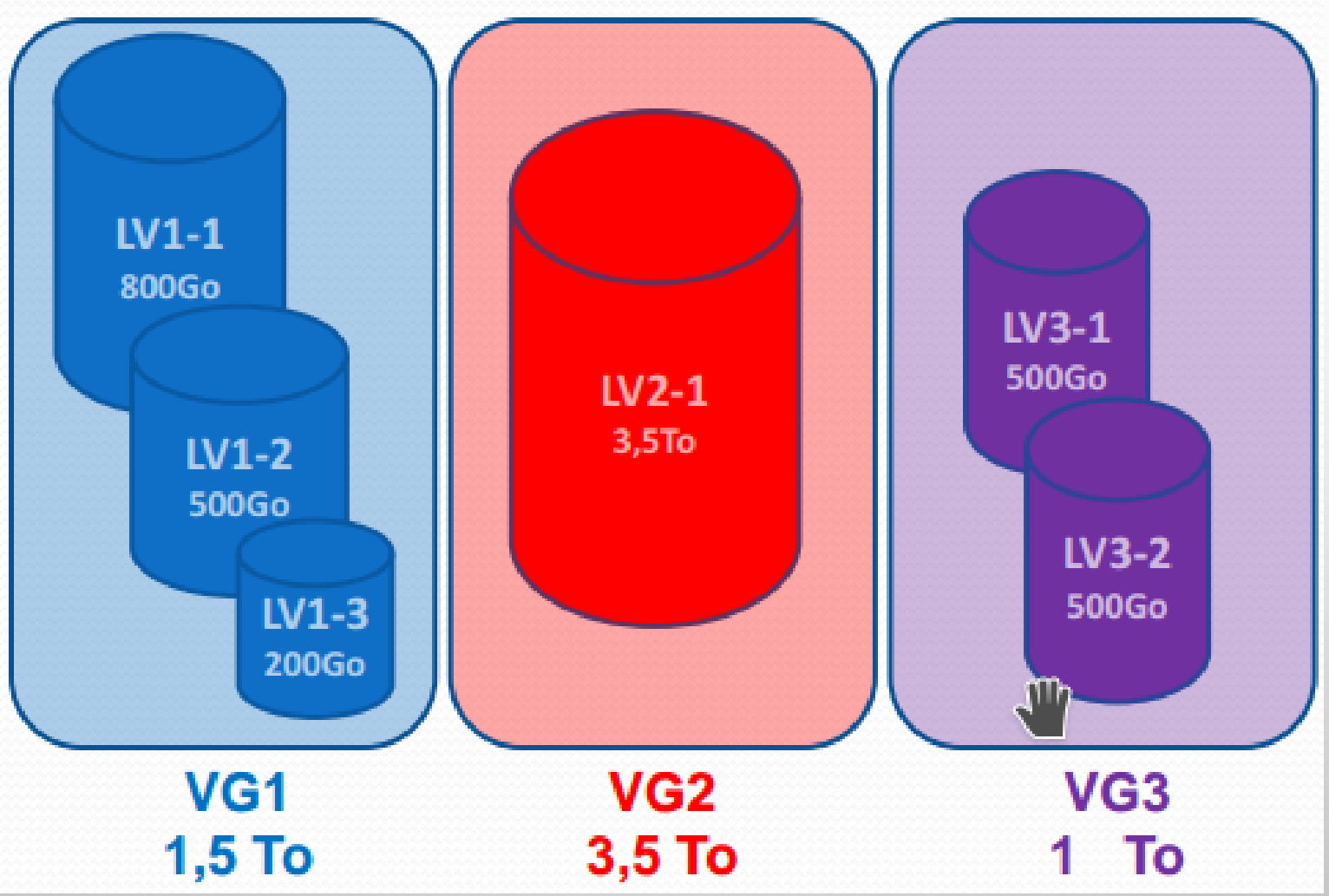
LES PV (PHYSICAL VOLUM)



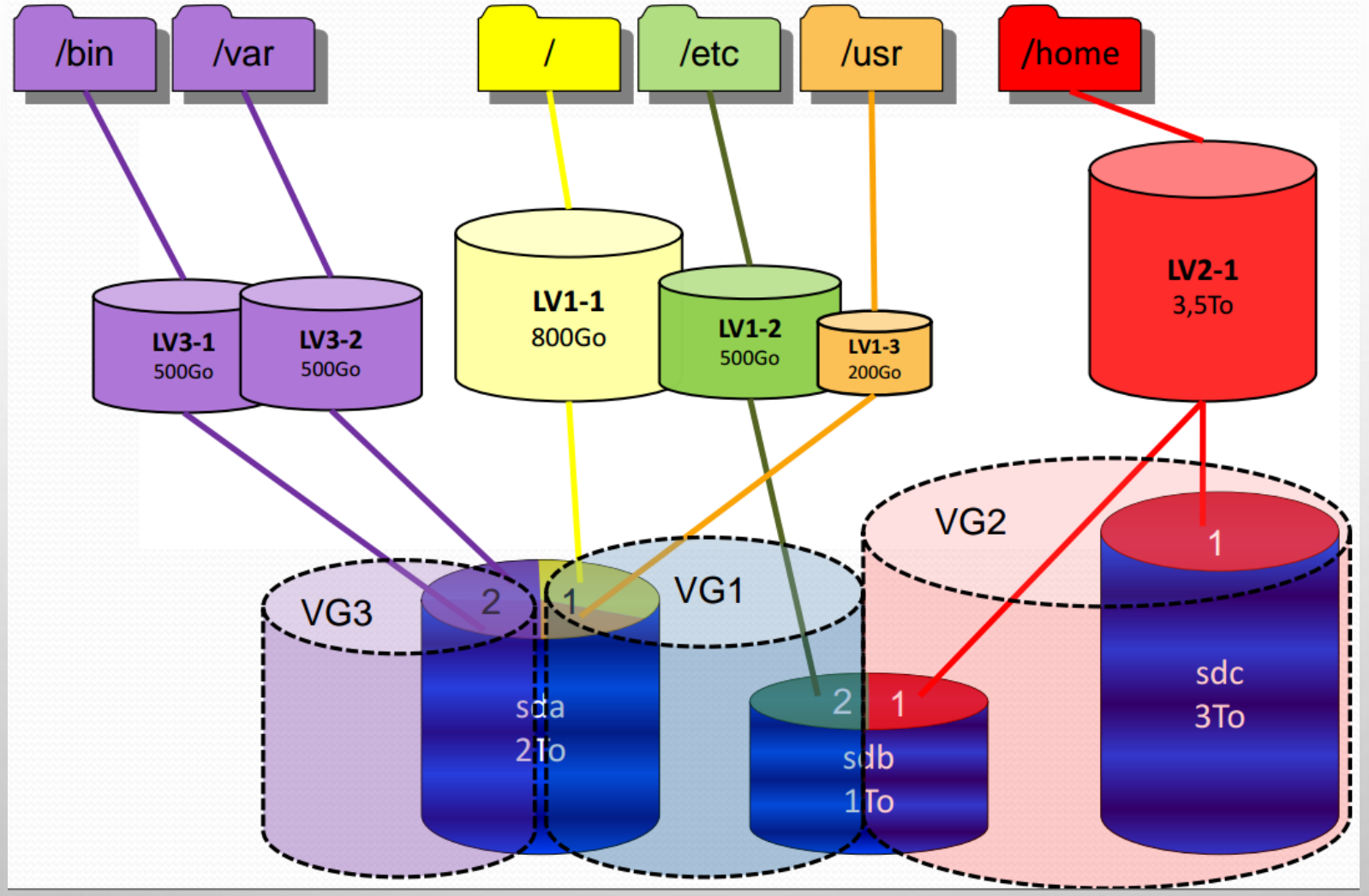
LES VG (VOLUM GROUP)



LES LV (LOGICAL VOLUME)



LVM ET POINT DE MONTAGE



PARTITIONNEMENT CLASSIQUE VS LVM

- PARTITIONNEMENT CLASSIQUE
  - PARTITION

    => FS

- LVM
  - Partition

    => PV

    => VG

    => LV

    => FS

LVM : RECETTE DE CUISINE

- CRÉER UN PV : **PVCREATE DISQUE**
  - PVCREATE /DEV/XVDB
- CRÉATION DU VG : **VGCREATE NOM_DU_VG DISQUE**
  - VGCREATE VG00 /DEV/XVDB4
- CRÉATION DE LV : **LVCREATE -L TAILLE –N NOM_DU_LV NOM_DU_VG**
  - LVCREATE -L 1G -N PREMIERLV VG00
- FORMATTAGE : MKFS –T TYPE CHEMIN_DU_LV
  - MKFS -T EXT4 /DEV/MAPPER/VG00-PREMIERLV
- MONTAGE DE LA PARTITION : **MOUNT**
  - MOUNT –A (IL VOUS DIRA LES POINTS DE MONTAGE MANQUANT)

QUELQUES COMMANDES

- **LVEXTEND** : LVEXTEND -L +500M /DEV/MAPPER/VG00-PREMIERLV
- **RESIZE2FS** : RESIZE2FS NOM_DU_LOGICAL_VOLUME
- **LVS** OU LVDISPLAY :
- **VGS** OU VGDISPLAY :
- **PVS** OU PVDISPLAY :
- **LVREDUCE**
- **LVREMOVE**
- **VGREMOVE**

LAB9 LES DISQUES

MERCI ET À BIENTÔT SUR EAZYTRAINING