Cour

Pare-feux

Définition rapide d’un pare-feu :
Un pare-feu est un système de sécurité informatique qui contrôle les connexions réseau entrantes et sortantes afin d’autoriser ou bloquer le trafic selon des règles définies. Il protège les équipements contre les accès non autorisés et les attaques.

Définition rapide d’un pare-feu OPNsense :
OPNsense est un pare-feu open source basé sur FreeBSD. Il permet de sécuriser un réseau grâce à des fonctionnalités comme le filtrage des paquets, le VPN, la détection d’intrusion et la gestion des règles de sécurité via une interface web simple.

Procédure de test des règles du pare-feu

1. Vérifier que la règle est bien activée dans OPNsense.
2. Identifier l’adresse IP source, destination et le port concerné.
3. Effectuer un test de connexion depuis un poste client :
   - ping
   - accès web
   - test de port
4. Vérifier dans les journaux (logs) du pare-feu si la connexion est autorisée ou bloquée.
5. Confirmer que le comportement correspond à la règle configurée.
6. Modifier la règle si nécessaire puis refaire les tests.

ACLs

Access Control List

Mini documentation : Les ACL sous Debian

1. Définition

Les ACL (Access Control List) permettent de gérer les permissions de fichiers et dossiers de manière plus précise que les droits Linux classiques.

Avec les permissions classiques, seuls :
- le propriétaire ;
- le groupe ;
- les autres utilisateurs

peuvent recevoir des droits.

Les ACL permettent d’ajouter des permissions spécifiques à plusieurs utilisateurs ou groupes différents.

---

2. Vérifier le support ACL

Installer les outils ACL :

apt install acl -y

Vérifier que le système supporte les ACL :

mount | grep acl

---

3. Commandes principales

Afficher les ACL :

getfacl fichier.txt

Ajouter une ACL à un utilisateur :

setfacl -m u:utilisateur:rwx fichier.txt

Ajouter une ACL à un groupe :

setfacl -m g:groupe:r-- fichier.txt

Supprimer une ACL :

setfacl -x u:utilisateur fichier.txt

Supprimer toutes les ACL :

setfacl -b fichier.txt

---

4. Exemple simple

Créer un fichier :

touch test.txt

Donner les droits lecture/écriture à l’utilisateur "user1" :

setfacl -m u:user1:rw test.txt

Afficher les droits :

getfacl test.txt

Résultat attendu :

user:user1:rw-

---

5. ACL par défaut sur un dossier

Créer un dossier :

mkdir partage

Ajouter une ACL par défaut :

setfacl -d -m u:user1:rwx partage

Toutes les futures créations dans ce dossier hériteront des permissions définies.

---

6. Avantages des ACL

- gestion plus précise des permissions ;
- accès personnalisés ;
- meilleure gestion des dossiers partagés ;
- administration simplifiée des utilisateurs.

Hash

Le **hash** (ou hachage) est le résultat d'une fonction mathématique à sens unique qui transforme un ensemble de données de taille variable en une **empreinte numérique de longueur fixe**, souvent appelée condensat, signature ou digest. Cette transformation est conçue pour être **unidirectionnelle**, ce qui signifie qu'il est théoriquement impossible de retrouver les données originales à partir du hash sans recourir à des méthodes de force brute ou des dictionnaires précalculés.

Les **fonctions de hachage** sont essentielles pour garantir l'**intégrité des données** et la **sécurité**, car toute modification, même minime, des données d'entrée produit un hash radicalement différent. Elles sont largement utilisées pour :

- **Stocker les mots de passe** de manière sécurisée sans les conserver en clair.
- **Vérifier l'authenticité** des fichiers téléchargés en comparant les empreintes.
- **Assurer la sécurité de la blockchain** et des signatures numériques

HSRP

Principe d’HSRP

HSRP (Hot Standby Routing Protocol) est un protocole propriétaire Cisco qui permet d’assurer la **continuité du réseau** en cas de panne d’un routeur.

Plusieurs routeurs travaillent ensemble et **partagent une seule adresse IP virtuelle** qui sert de **passerelle** pour les machines du réseau.

Fonctionnement

- Les routeurs du groupe HSRP communiquent entre eux régulièrement (messages UDP).
- Un seul routeur est actif à un moment donné :
  - **Routeur actif (Active)** : gère le trafic réseau.
  - **Routeur en attente (Standby)** : prêt à prendre le relais immédiatement si le routeur actif tombe en panne.

Priorité

- Chaque routeur a une **priorité (1 à 255)**.
- Plus la priorité est élevée, plus le routeur a de chances d’être actif.
- Par défaut : **100**.

Exemple :

- R1 = 105 → devient actif
- R2 = 104 → standby
- R3 = 103 → secours supplémentaire

IP virtuelle

- Une **IP virtuelle commune** est configurée (ex : `192.168.0.100`).
- Les clients utilisent **cette IP comme passerelle**, sans savoir quel routeur est actif.

Commandes principales

Sur chaque routeur :

- `standby 1 ip 192.168.0.100`
  → définit l’IP virtuelle du groupe
- `standby 1 priority X`
  → définit la priorité du routeur
- `standby 1 preempt`
  → permet à un routeur avec une meilleure priorité de reprendre la place de l’actif

---

Résumé simple

HSRP permet :
d’éviter une coupure réseau si un routeur tombe
d’avoir un routeur de secours automatique
d’utiliser une seule passerelle pour les clients

IP

IP est l'abréviation de **Internet Protocol**, un protocole de communication qui gère la transmission des données sur les réseaux. Une **adresse IP** (Internet Protocol Address) est le **numéro d'identification unique** attribué à chaque équipement (ordinateur, routeur, imprimante) connecté à un réseau, servant à localiser l'appareil et à acheminer les paquets de données vers leur destination.

Il existe deux versions principales de ce protocole : **IPv4**, la plus courante, qui utilise une notation décimale comme `192.168.1.2`, et **IPv6**, qui offre un espace d'adressage beaucoup plus vaste avec une notation hexadécimale. Les adresses IP peuvent être **publiques** (uniques mondialement, visibles sur Internet) ou **privées** (utilisées uniquement au sein d'un réseau local).

L'attribution de ces adresses se fait soit de manière **dynamique** (via le protocole DHCP, changeant lors de chaque connexion) soit de manière **statique** (fixe, souvent utilisée pour les serveurs). Le système de noms de domaine (**DNS**) traduit ensuite les noms de domaine lisibles (comme `www.wikipedia.org`) en adresses IP numériques pour permettre la connexion des utilisateurs.

TOUT LES PROTOCOL ET LEUR PORT et les truc commun lié

TCP : 22 = SSH

UDP : 53 = DNS

TCP : 80 = HTTP

TCP : 443 = HTTPS

ICMP : ANY = ping

UDP : 514 = ryslog

TCP : 3306 = requete mysql

STP

Spanning Tree, c’est quoi ?

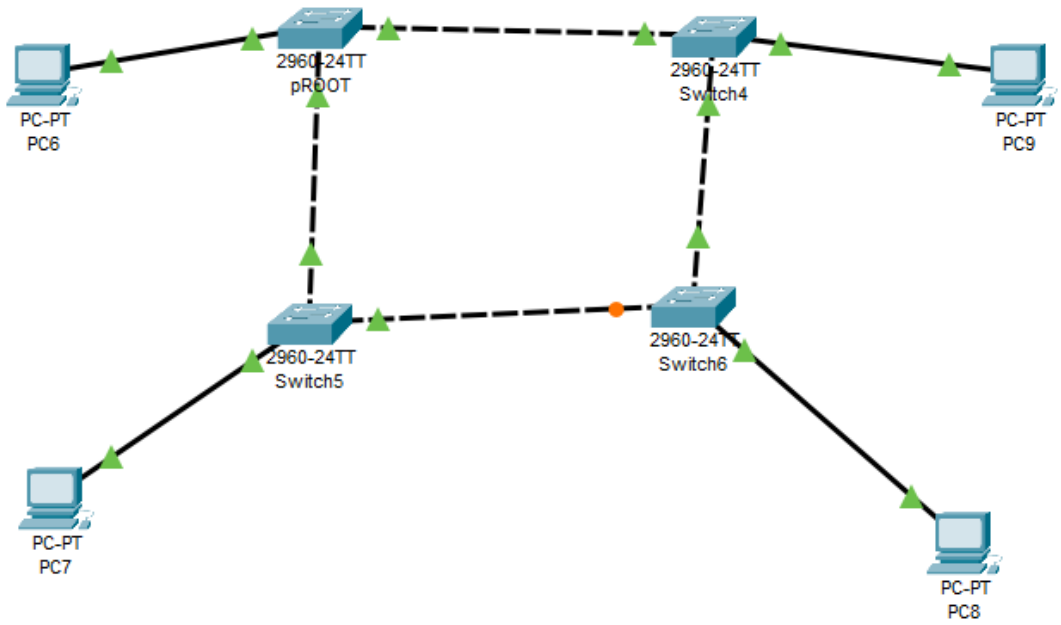
Le protocole **Spanning Tree** (que l’on appelle aussi STP) est conçu pour prévenir les boucles dans les réseaux locaux (LAN). Son principal objectif est d'éliminer ces boucles en identifiant les chemins redondants dans le réseau et en les désactivant.

Par ailleurs, il garantit également la redondance en maintenant des chemins alternatifs, assurant ainsi la résilience en cas de défaillance d’un lien ou d’un commutateur. Il y aura un chemin unique et certains ports seront bloqués, au niveau logique. Il permet également de s'assurer que les commutateurs disposent d'une vision cohérente et stable du réseau. En effet, les boucles réseau peuvent entraîner des problèmes tels que des tempêtes de diffusion, une dégradation des performances, voire un arrêt complet du réseau.

Base de la commande « show spanning-tree »

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp  << nous dit que STP est enable
  Root ID     Priority    32769
              Address     00D0.5846.69A7  <<< @ mac du root
              This bridge is the root <<< indique que c le root ( pas la si c pas le root)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.5846.69A7 <<<< @ mac de la machine
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

Switch#
```

Voici l’infrastructure de base :



Le switch root et celuis en haut a gauche

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.43AD.2110
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.43AD.2110
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

Switch#
```

Il a était désigner comme root car il est celuis avec l'@ mac la moins forte.

A présent j'ai changer la priorité avec la commande

```
Switch(config)#spanning-tree vlan 1 priority 28672
Switch(config)#
```

.

Désormais a cause de ce changement le STP a changé de root, le root n'est donc plus le meme.

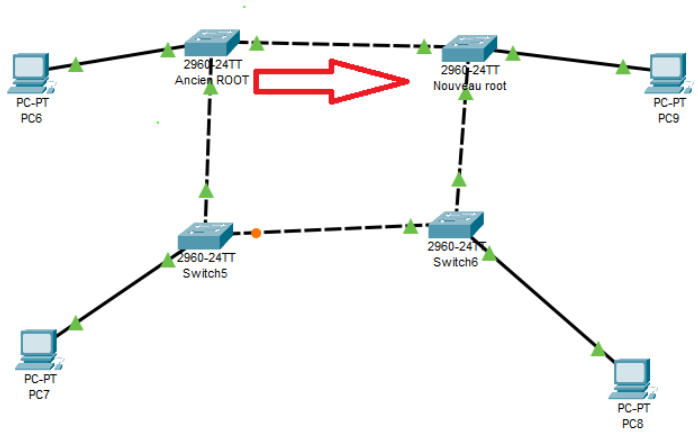
```
            Address     0001.6432.49BB
            Cost        19
            Port        1(FastEthernet0/1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
            Address     0001.43AD.2110
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p

Switch#
```

3

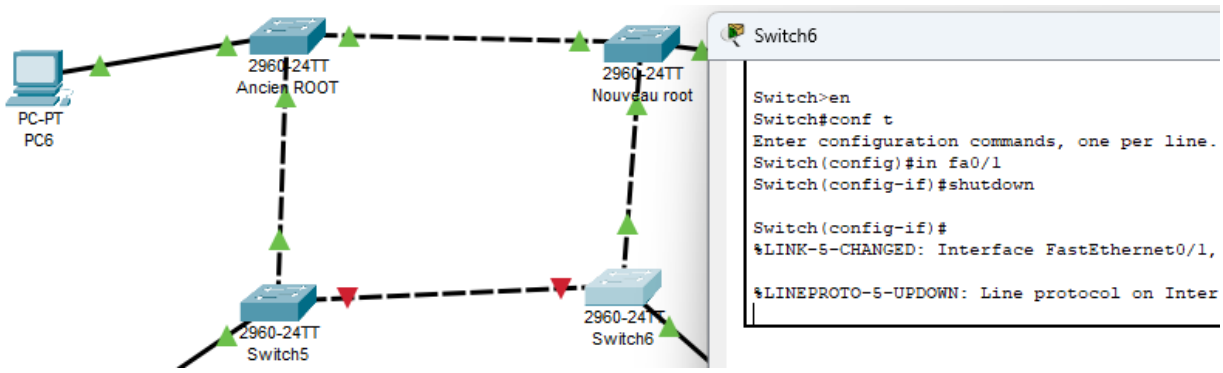
Celui la n’est plus root

Tandis que celuis ci l’est :

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    28673
             Address     0001.6432.49BB
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673  (priority 28672 sys-id-ext 1)
             Address     0001.6432.49BB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

Switch#
```



Pour tester , j’ai désactivé un port fonctionelle



Comme prévue le liens a était rompu mais les autre on pris le relais.

VOiP

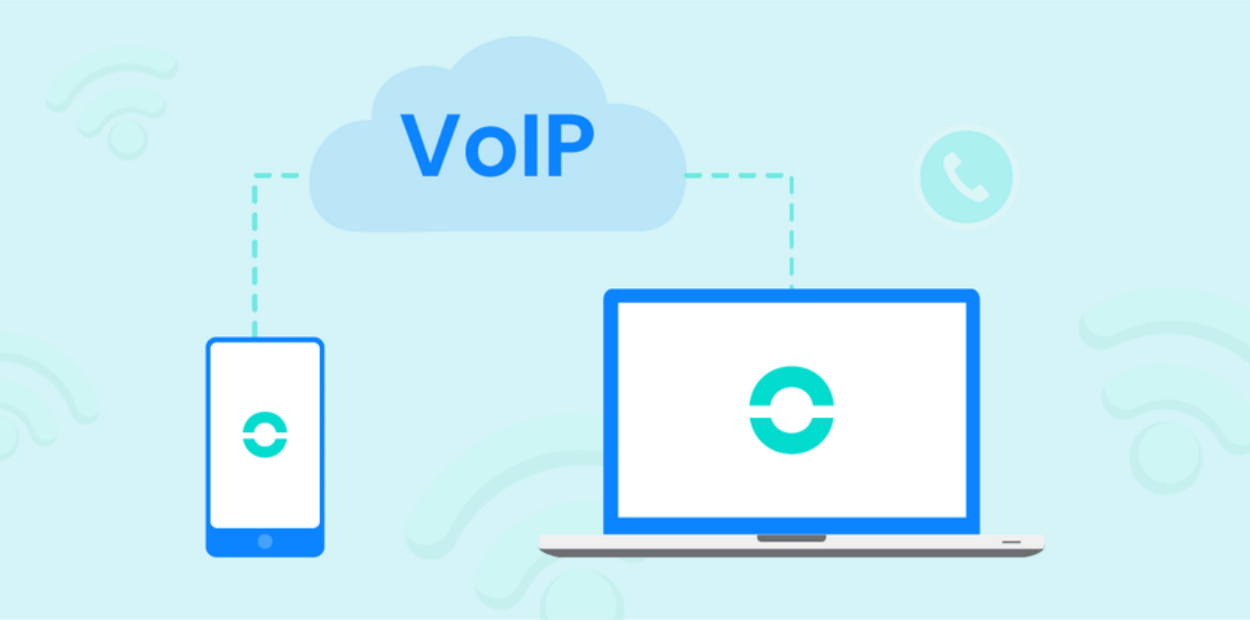
La VoIP ou VoixIP c’est un moyen de passer des appel via internet.

Avec la VoIP, votre voix est transformée en signaux électriques à l’aide d’un pilote audio. Puis, un logiciel appelé codec (qui compresse et décompresse les informations transmises) convertit ce signal en langage binaire – ou langage informatique.

Votre système d’exploitation peut alors décomposer ce code binaire en plusieurs informations sous forme de paquets (ou lot de données numérisées). Ces paquets de données sont transmis :

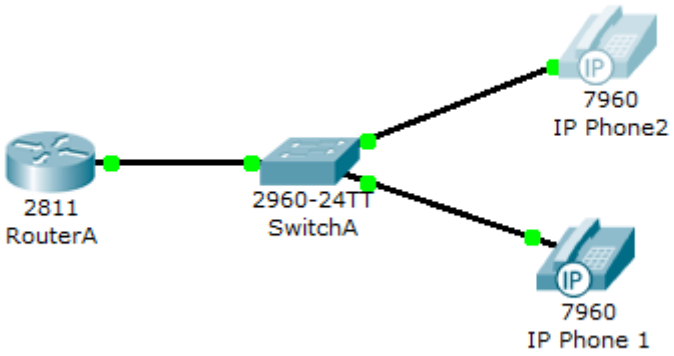
-depuis un pc vers un autre. La voix est transformé en packet et reconsitituer a l’arrivé.

La VoIP ne fonctionne pas uniquement avec 2 Téléphone IP. IL Peut fonctionner avec un seul téléphone et un tiers d’occupe de faire la «traduction » et donc etre acheminé vers une ligne plus classique.



Des logiciels de VoIP tels que Skype, Signal, Discord et WhatsApp[2],[3] gèrent aujourd'hui tous les flux multimédia (téléphonie, appels vidéo, messagerie instantanée et transferts de fichiers).

Comment faire (packet tracer)



Tâches 1 : Configurer l'interface FastEthernet 0/0 et le serveur DHCP sur RouterA (routeur 2811)

Configurez l'interface FastEthernet 0/0 avec l'adresse IP 192.168.10.1/24. N'oubliez pas d'activer l'interface avec la commande no shutdown !

```
RouterA>enable
RouterA#configure terminal
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip address 192.168.10.1 255.255.255.0
RouterA(config-if)#no shutdown
```

Le serveur DHCP est nécessaire pour fournir à chaque téléphone IP connecté au réseau une adresse IP et l'emplacement du serveur TFTP.

```
RouterA(config)#ip dhcp pool VOICE # sa crée un pool phcp avec le nom " voice "
RouterA(dhcp-config)#network 192.168.10.0 255.255.255.0 #DHCP = on définis le réseau etc
RouterA(dhcp-config)#default-router 192.168.10.1 #l'@ oar défault
RouterA(dhcp-config)#option 150 ip 192.168.10.1 # ?
```

Après avoir configuré le routeur ISR, attendez un instant et vérifiez que ‘IP Phone 1’ a reçu une adresse IP en plaçant votre curseur sur le téléphone jusqu'à ce qu'un résumé de configuration apparaisse.

Tâches 2 : Configurer le service de téléphonie Call Manager Express sur RouterA

Vous devez maintenant configurer le service de téléphonie Call Manager Express sur RouterA pour activer la VoIP sur votre réseau.

```
RouterA(config)#telephony-service #on met le routeur pour les tel
RouterA(config-telephony)#max-dn 5 #le max de numéro
RouterA(config-telephony)#max-ephones 5 #le max de téléphone
RouterA(config-telephony)#ip source-address 192.168.10.1 port 2000 #IP Address source
RouterA(config-telephony)#auto assign 4 to 6 #Automatically assigning ext numbers to buttons#
RouterA(config-telephony)#auto assign 1 to 5 #Automatically assigning ext numbers to buttons#
```

Tâche 4 : Configurer un vlan vocal sur SwitchA

Appliquez la configuration suivante sur les interfaces SwitchA. Cette configuration séparera le trafic vocal et de données dans différents vlan sur SwitchA. Les paquets de données seront transportés sur le vlan d'accès.

```
SwitchA(config)#interface range fa0/1 – 5 #Configure interface range#
SwitchA(config-if-range)#switchport mode access
SwitchA(config-if-range)#switchport voice vlan 1
```

Tâche 5 : Configurer le répertoire téléphonique pour le téléphone IP 1

Bien que ‘IP Phone 1’ soit déjà connecté à SwitchA, il a besoin d'une configuration supplémentaire avant de pouvoir communiquer. Vous devez configurer RouterA CME pour attribuer un numéro de téléphone à ce téléphone IP.

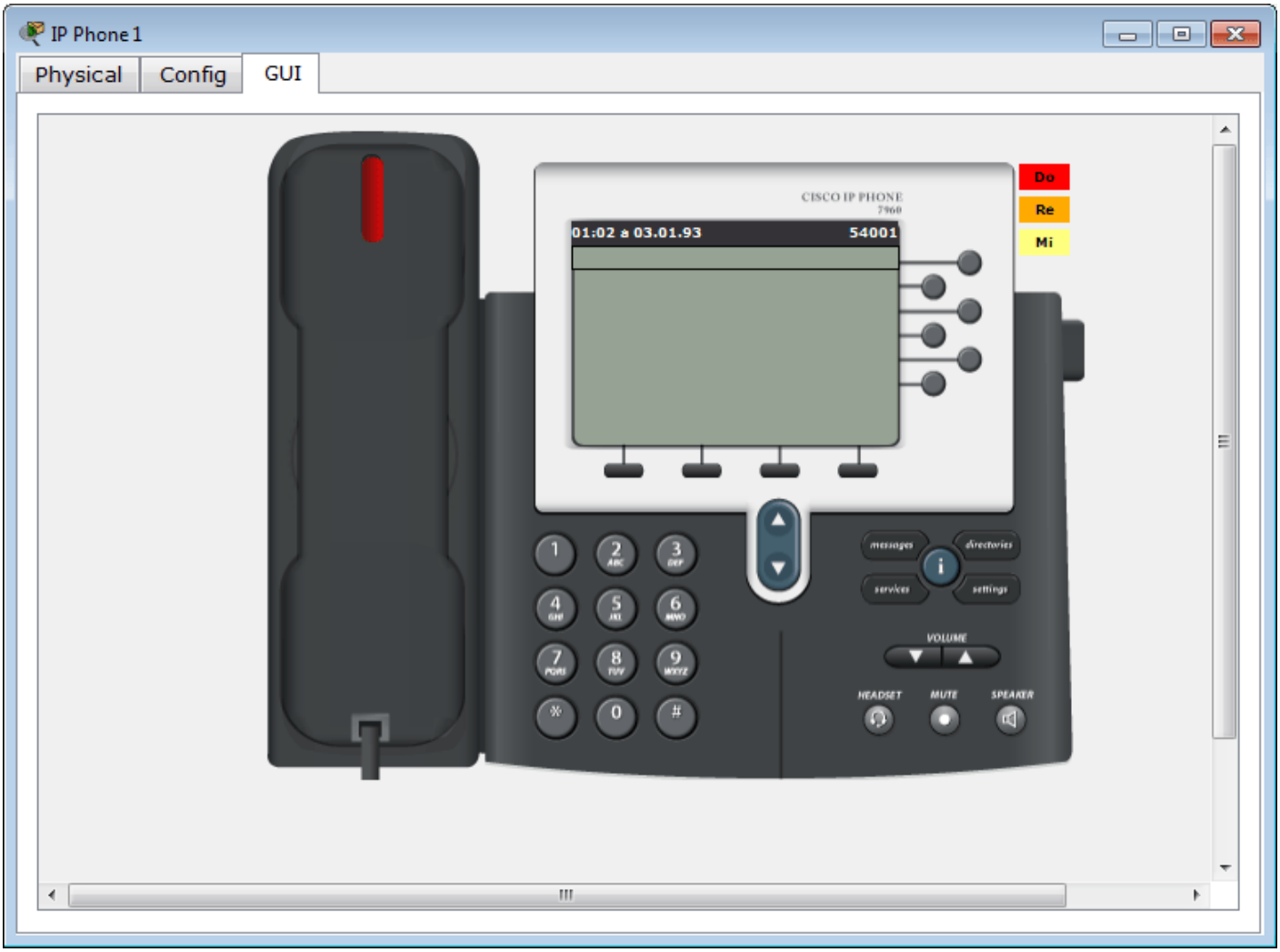
```
RouterA(config)#ephone-dn 1 #Defining the first directory entry#
RouterA(config-ephone-dn)#number 54001 #Assign the phone number to this entry#
```

Tâche 5 : Vérifier la configuration

Assurez-vous que le téléphone IP reçoit une adresse IP et le numéro de téléphone 54001 de RouterA (cela peut prendre peu de temps).

Numéro de téléphone IP 1 confondu avec l'adresse IP et le numéro de téléphone

Téléphone IP 1 configuré - Vue de face



Tâche 6 : Configurer le répertoire téléphonique pour IP Phone 2

Connectez le téléphone IP 2 à SwitchA et allumez le téléphone à l'aide de l'adaptateur secteur (onglet Physique).

```
RouterA(config)#ephone-dn 2 #Defining the first directory entry#
RouterA(config-ephone-dn)#number 54002 #Assign the phone number to this entry#
```

Tâche 7 : Vérifier la configuration

Assurez-vous que le téléphone IP 2 reçoit une adresse IP et le numéro de téléphone 54002 de RouterA (cela peut prendre peu de temps). Même procédure que la tâche n°5.

Composez le 54001 et vérifiez si le téléphone IP 1 reçoit correctement l’appel.

Active Directory - AD

Active Directory

Présentation :

Active dirrecory est un service d'annuaire dév par Microsoft pour les systéme Wind. IL permet d'identifier les utilisateur et ordinateurs d'un part informatique et de gérer leurs droit d'accés aux ressources.

Profil itinérant : garde toute la configuration de la personne peut importe le post.

Annuaire : une base de donnée spécialisé conçue pour stocker et orga les info sur les user , machine, services et ressource d'un réseau.

-retrouver rapidement une ressources

-gère l'authentification et autorisation

-centralisation de l'administration.

En recensant toute ces info : active directory constitue un noyau central :

-retrouve et accéder a n'importe quelle ressources recensée

-avoir une représentation global de l'ensemble des ressources et des droits/accés associé et constitue de ce fait un outils d'admin et de gestion centralisé du si.

Active Directory permet :

-gère de façon centralisé des réseau pouvant aller de quelque pc a des réseau d'entreprise réparti sur de site éloignée géographiquement.

Pour utilisé active directory : il faut

-un pc window server.

P**ar** sécurité : il doit u avoir 2 contrôleur de domaine :

Assurer une tolérance aux pannes

Répartition des charges.

Caractéristique :

AD est un outil destiné aux utilisateurs

IL constitue également un outil d'admin et de gestion du sys d'in

R2PARTITION :

-répartition de l'annuaire sur le réseau

-réplication : tolérance aux pannes et repartions des charges : toute modif d'annuaire est automatiquement copié sur tout les controleur de domaine d'un domaine.

-sécurisation de l'annuaire

Le mécanisme de rechercher et d'index : est basé sur le protocole LDAP qui permet de communiqué avec un annuaire.

Il définit comment client peut :

-Rechercher un utilisateur

-vérifier un mode de passe

-Obtenir les information d'un groupe

-Ajouter/modifier/supprimer des objets dans l'annuaire

-Ou tout autre type d'interaction avec l'annuaire.

AD utilise les systéme de nom de domaine DNS afin d'échanger des info avec n'importe quel annuaire qui utilise les protocole ldap Il faut donc un serveur DNS sur le réseau.

Protocole utilisé :

TCP/IP , dns , dhcp , kerberos , LDIF , sntp, LDAP.

Structure logique :

Un domaine est une structure logique qui regroupe logique des pc en partageant la meme base d'annuaire

L'annuaire est géré au niv du domaine.

Une forét de AD :

Une foret contient 1 a n arabes

Un arabe contient 1 a n domaine

Un domaine contient n unité d’organisation

Une unité d’orga contient n objet.

Unité d’orga :

Pour de trés grande orga, il peut y avoir une gestion de plusieurs domaines.

Sinon un seul domaine suffit, dépend des besoin de l’orga.

Les unité d’une orga :

Une unité d’orga est une structure hiérarchique logique (et non physique) créée dans un domaine pour représenter une strcuture géographique ou des services de l’entreprise. Les unité d’orga peuvent etre fondées sur :

-adminnistration ou les objet

-les zone géo

-les activité de l’entreprise

-les service de l’entre

-les projet.

Les OU

Les ou se présent comme des conteneurs (comme des dossier).

Les console d’admin permet de gérer tt.

Les groupe d’utilisateur permet de d’avoir des user avec les meme perm.

Il existe 2 groupe :

-les groupe de sécurité pour gérer l’accés aux ressources et que vous allez utilisé.

-Les groupe de distribution pour envoyer des message a plusieurs avec le logiciel de msg exchange.

Il faut que le DNS le la machine soit celle du domaine.

GPO :

Les stat de groupe ou global Policy Objects sont un outil essentiel d’AD , ce sont des paramètre applicable a des user, pc ou groupe d’user.

Ces stratégie se définissent au niv d’un site , d’un domaine ou d’un unité d’orga.

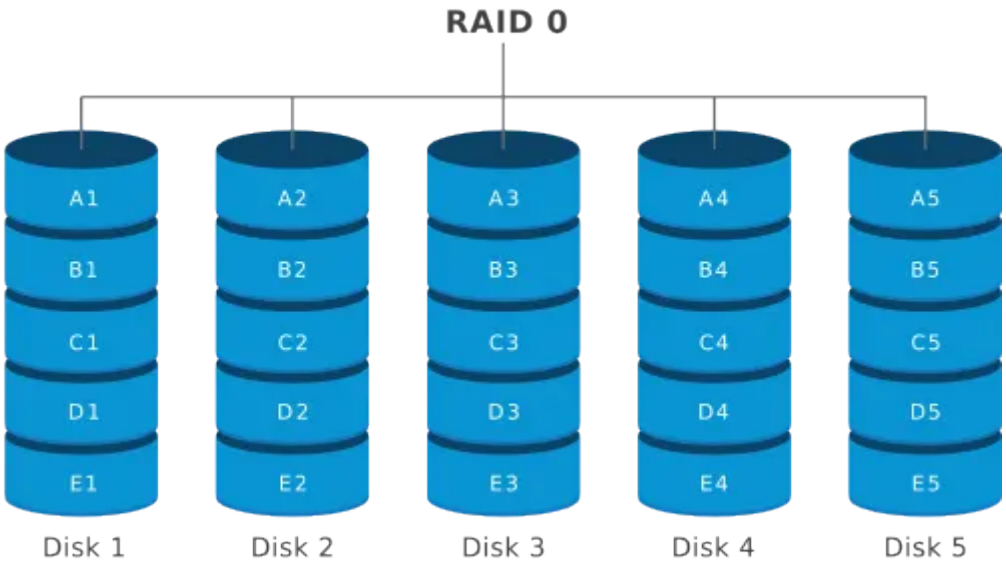
RAID

Le RAID (Redundant Array of Independent Disks) est une technologie de virtualisation du stockage qui consiste à regrouper plusieurs disques durs indépendants pour les présenter au système d'exploitation comme une seule unité logique. Cette méthode permet d'optimiser la performance, la sécurité ou la tolérance aux pannes en répartissant ou en dupliquant les données sur l'ensemble des disques de la grappe.

Le raid (redundant array of Independent Disks)

Sécurité de donné, permet de garder les donnée disponible en cas de panne.

RAID 0 :



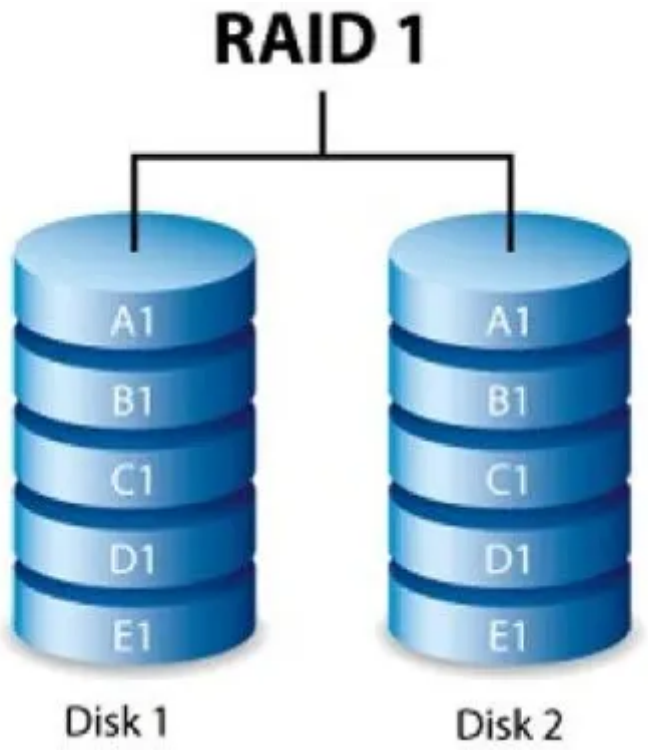
Le raid 0 c répartir les disques de la grappe, les blocks de données qui sont alternativement stocké sur les disques sans aucune redondance , Cela confére une plus grand rapidité au détriment de la fiabilité de l’ensemble

On l’utilise uniquement pour la rapidité, dans des contexte comme

Inconvénients : taille de la grappe limité par le plus petit disque (utilisé d disque de capacité identique)

On multiplie le nombre de disque utilisé et donc les chance de perte de donnée. Il faut donc prévoir une sauvegarde.

Raid 1 :



Le raid 1 consiste en l'utilisation d'un nombre de n disques redondants, chaque disque de la grappe contenant les même donnée.

Avantage : temps d'accès plus rapide , redondance d donnée.

Désavantage :

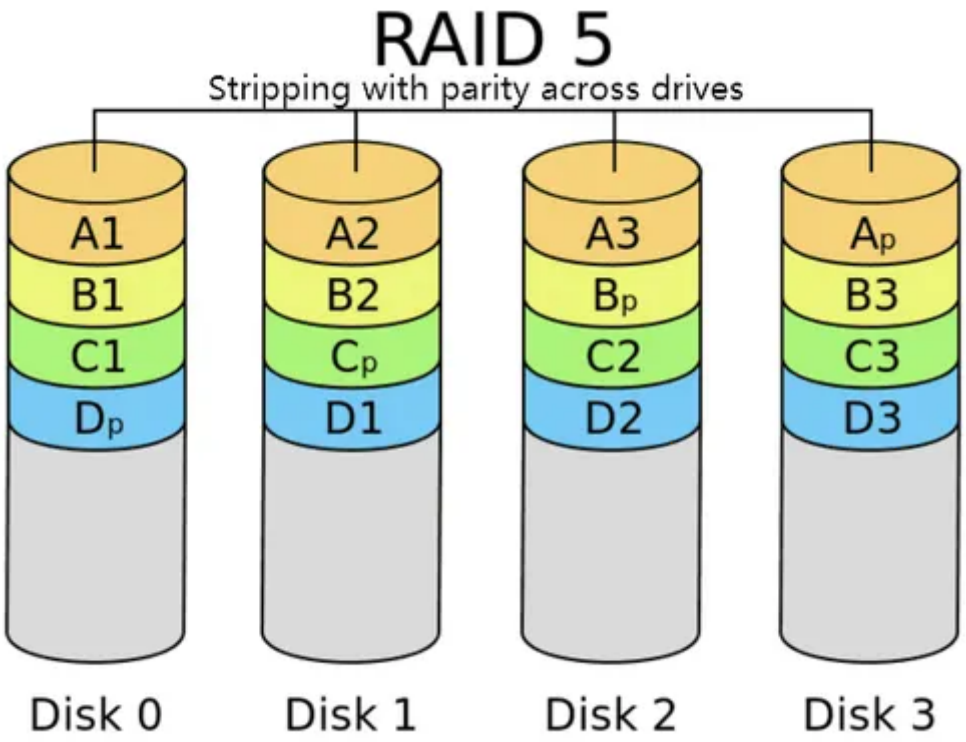
-Limité par le plus petit

-Aucune extension de volume totale de grappe possible. (faut tt changer si + de volume)

-Coûte cher.

Le raid 1 est surtout utilisé pour stocker des données très sensibles dans des petit infrastructure.

RAID 5 : 3 disque min



Le raid 5 combine la méthode du volume agrégé par bandes a une parité répartie.

C’est un système qui permet de reconstruire les donnée les autre disque en cas de panne.

Avantage :

-plus rapide

-Redondance

Inconvénient :

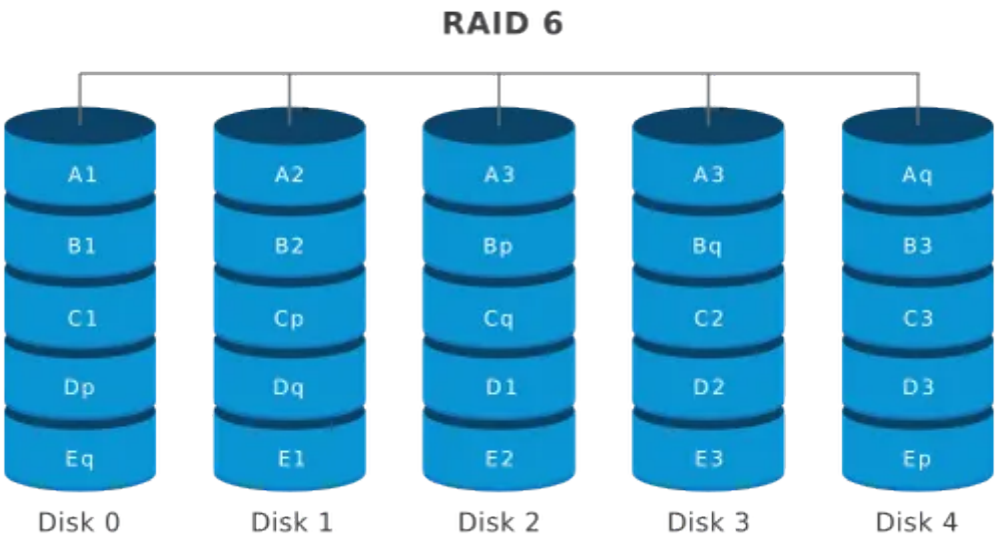
-Taille de volume limité

-capacité de redondance limité

-Reconstruction peut être longue

–Le temps d ‘écriture est ralenti par le calcule de la parité.

RAID 6 :

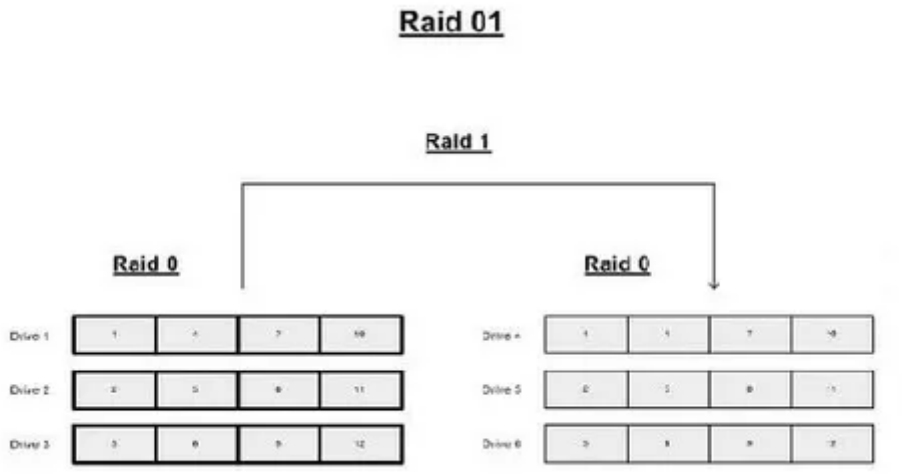


Le raid 6 fonctionne c comme le raid 5 mais il calcule plus de parité , souvent 2 de redondance.

Les niveau de raid :

Il est possible de combiner différents niveau de raid entre eux, pour crée des raid composer.

Raid 0+1 :



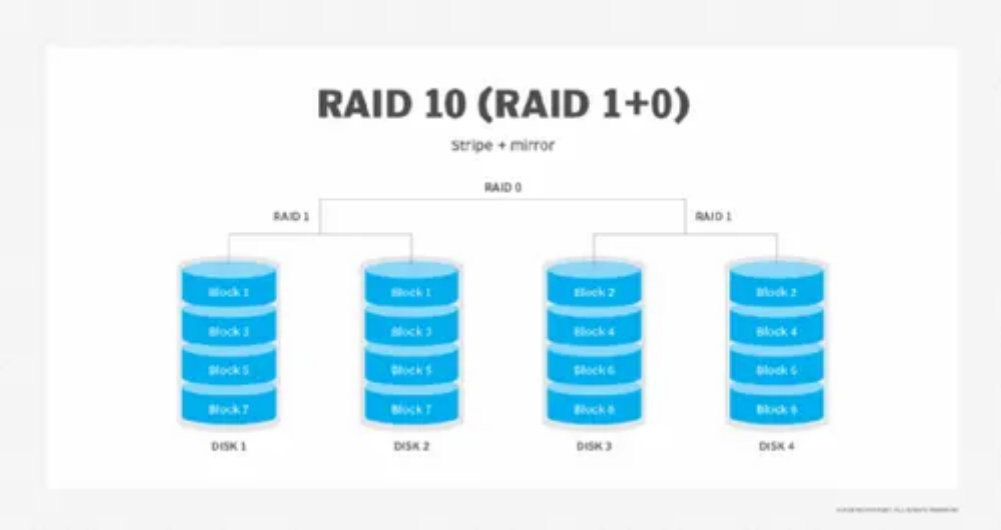
-très rapide

-redondance mauvaise

-coût élevé

-Reconstruction risqué

Raid 1+0



C’est un raid 0 et de raid 1

-Temps d’accès et d’écriture élevé

-Très bonne redondance

-Reconstruction rapide et fiable

-Coût élevé

Les raid les plus utilisé : raid 1, 5 et 1+0

2type de raid

Raid logiciel (géré souvent par l’os)

Raid matériel (meilleur perf, meilleur fiabilité, plus coûteux et dépendant du matérielles)

Aide site calcule pour un raid : Free raid calculator

10.123.33.231

Sauvegarde

La sauvegarde.

Def : dupliquer des donnée sur différent stockage , afin de la récupérer si l'un des support a un problème. Ces support doivent etre amovible.

Def :

L'enregistrement des données, qui est l'opération d'écriture des données sur un support d'enregistrement durable , tel qu'un disque magnétique ou SSD, disque optique, clé USB , bandes magnétique etc

L'archivage, qui consiste à enregistrer des données sur un support à des fins légales ou historiques.

Duplication du contenu des disques sur d'autre supports non amovibles (mirroring , raid) ne peut etre considérée comme un sauvegarde et ce , pour les raisons suivantes :

Le support n'est pas amovible ce qui ne permet pas le stockage du support dans un lieu tiers

La capacité de stockage des support embarqués est nécessairement limitée **(**capacité non extensible et pas capable de modifier le volume).

Une sauvegarde est une copie d'un fichier , ou d'un ensemble de fichier , transférée sur un support tel que des bandes, un CD, ou un disque externe. Elle doit etre conservé en lieu sur.

Un dispositif de sauvegarde est d'abord en avant tout caractérisé par l'amovibilité du support ou par le fait que le support soit distant géographiquement.

Incidents :

La sauvegarde régulière des données permet de restaurer les données partiellement ou en totalité en cas d'incident.

Il existe **2 type de sauvegardes** qui peuvent mener a une perte de données et donc a une restauration de sauvegarde.

Les incidents d'**origines externes** et les incidents **d'origines internes.**

Externe : Choc, vol , incendie , foudre etc

Interne : virus, erreur humaine manipulation (suppression, modif , manip) , problème lié au systéme d'exploitation, panne matérielle.

Que doit-on sauvegarde ?

La sauvegarde est un processus couteux et qu'il faut optimiser, une réflexion préalable sera donc de déterminer ce qu'il faut sauvegarder et à quel rythme.

Que doit-on sauvegarde ? =

- Le systéme d'exploitation pour permettre de retrouver l'environnement de travail sans devoir réinstaller et configurer manuellement tout le systéme d'exploitation et les logiciels.

- Les document de travaille et de profil individuel des utilisateurs ainsi que les documents partagés pour ne pas perdre tout le travail qui a été fait.

- Les donnée des application qui , dans la plupart des cas, sont mémorisées dans des bases de données.

- Les fichier des application Web , les fichier de configuration des services applicatifs et des équipements réseaux afin de pouvoir restaurer les services en cas de nécessité.

- sauvegarde des log. Les événement journalisés ou journaux de logs des services applicatifs et des équipements conformité RGPD.

Les différent type de sauvegarde.

3 type de sauvegardes :

-sauvegarde complète

-sauvegarde différentielle

-sauvegarde incrémentale

Les différente méthode de sauvegarde :

- les sauvegarde a chaud

- les sauvegarde a froid

Sauvegarde a chaud , également connue sous le nom de save dynamique , consiste a créer des save alors que le systéme ou l'application fonctionne toujours et sert activement les utilisateur. La save a chaud consiste a save les donnée lorsqu'elles sont dans un état actif et opérationnel. Les save a chaud sont généralement effectuées a l'aide d'un logiciel de sauvegarde spécialisé qui peut saisir les modifications apportées aux données en temps réel. La sauvegarde a chaud et la méthode la plus utilisé dans le monde pro.

Les avantage :

-interruption minimale

-Protection continue des données

-Récupération plus rapide.

Les inconvénients :

-Utilisation des ressources

-Complexité : la mise en œuvre est plus complexe,utilisation de logicielle annexe.

-Vulnérabilité a certain types de défaillances (défaillance systéme)

Sauvegarde a froid :

La sauvegarde a froid également connue sous le nom de sauvegarde statique, consiste a créer des sauvegardes lorsque le systéme ou l'application ne fonctionne pas ou se trouve dans un état de repos. Cela nécessite généralement d'arrêter tempo le systéme ou l'application pour garantir les cohérent pendant le processus de save.

Avantage :

- Cohérence des données

-Réduction de l'utilisation des ressources

- Protection contre certaines défaillances

Inconvénient :

- Temps d'arret

-actualité des données (peuvent ne pas capturer les données récente)

-Temps de récupération plus long.

La save complete :

Cette sauvegarde consiste ,a un moment donnée , a avoir une copie intégrale de toutes les données sélectionnée sur un support de save. Le volume de données save, qui est identique a celui des données peut etre compressé pour diminuer l'espace de stockage nécessaires.

A chaque save totale , l'intégralité des données sont a new cp sur le support de save.

Avantage :

-il suffit de prendre la dernière save

-Pas nécessaire de garder les save les plus anciennes.

Inconvénient :

-le temps de restauration est long

-le temps de sauvegarde est long

Sauvegarde différentielle :

Cette save consiste à réaliser une première save complète , puis les sauvegardes suivantes sont différentielles , c'est a dire que le logiciel de save vérifie quels sont les fichiers qui on été modifiés depuis la sauvegarde complète.

Tt les save différentielles suivante se feront tjs par rapport a la 1er sauvegarde.

Avantage :

-seuls les fichier modif depuis la save compléte sont save

-La save différentielle est plus rapide et utilise moins d'espace de stockage.

-La restauration nécessite la dernière save compléte et la dernière save différentielle

Inconvénient :

-le temps de save prendra + de temps a fur et a mesure

-Le temps de restauration vas +

La save incrémentale :

Cette save consiste a réalisé une première save compléte. Puis les save suivantes sont incrémentales c'est a dire que le logiciel de save vérifie quels sont les fichier qui on ete modifies ou crée depuis la save précédente , compléte ou incrémentale. De cette manière, seuls les fichiers modifié seront pris en compte dans cette save incrémentale.

Avantage :

-La save incrémentale est tres rapide et utilise un faible espace de stockage.

-Seul les fichier modifié sont « rajouté »

Inconvénients :

-La restauration est lente.

Plan de save

Le plan de save doit etre définit

Les personnes chargées de l’admin doivent garder une trace sous forme de rapports.

Un logiciel de sauvegarde permet alors la gestion de ces rapports.

Regle 3/2/1

La régle de save 3/2/1 est une strat de save des donnée :

Crée trois copies de vos données

Utilisez 2 périphériques de stockage différents.

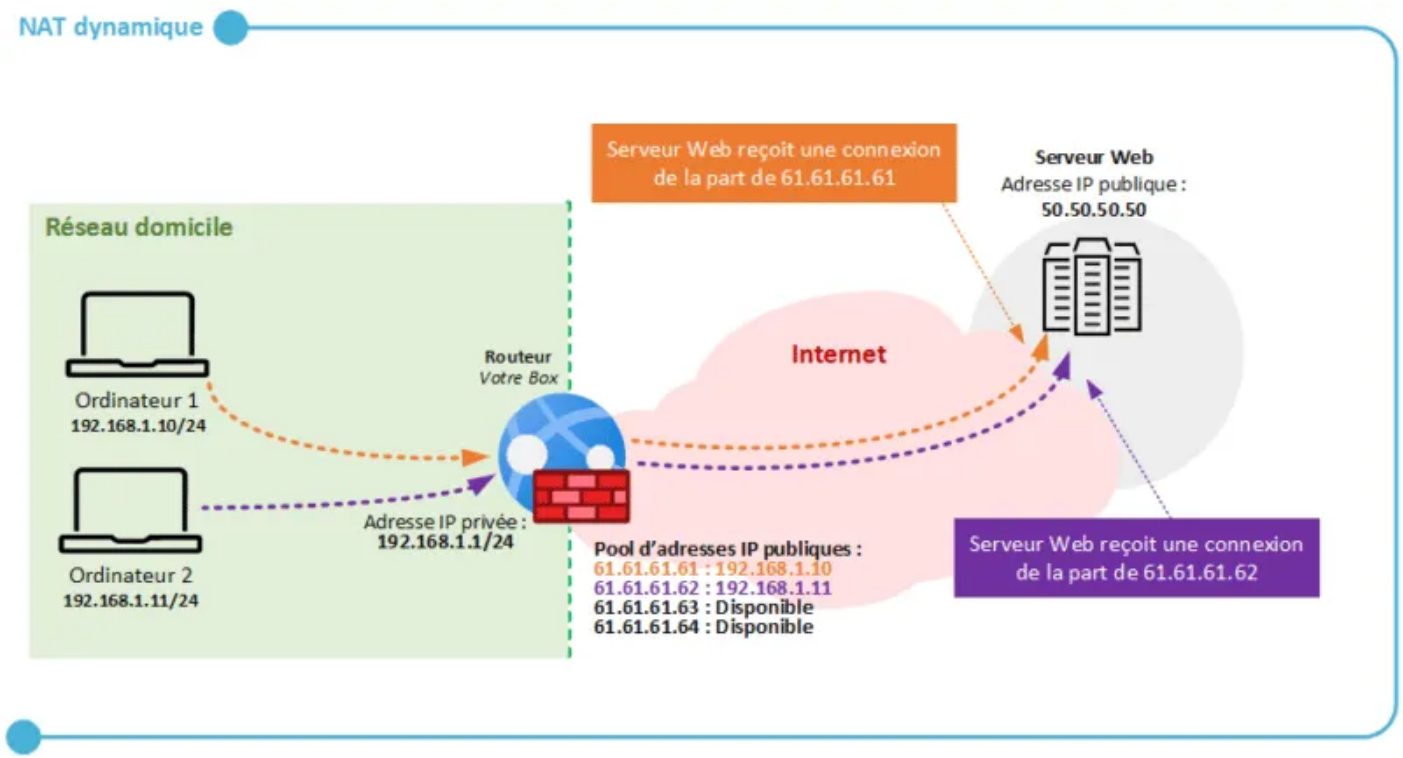
Vous conservez l’une des copies de save hors site.

NAT/PAT

Le NAT/PAT c'est quoi ?

Le **NAT (Network Address Translation)** et le **PAT (Port Address Translation)** sont des technologies réseau qui permettent de traduire les adresses IP privées d'un réseau local en adresses IP publiques pour accéder à Internet, palliant ainsi la pénurie d'adresses IPv4.

Le **NAT** assure une correspondance entre une adresse IP privée et une adresse IP publique, tandis que le **PAT** (aussi appelé NAT Overload) permet à **plusieurs appareils** de partager **une seule adresse IP publique** en utilisant des **numéros de port uniques** pour distinguer chaque connexion.



Comment mettre en place le NAT/PAT (exemple sur packet-tracer)

Le NAT (Network Address Translation) et le PAT (Port Address Translation) sont des technologies permettant à plusieurs appareils d'un réseau privé d'accéder à Internet en utilisant une ou plusieurs adresses IP publiques. Le NAT traduit les adresses IP privées en adresses IP publiques, tandis que le PAT, une variante du NAT, permet à plusieurs appareils de partager une seule adresse IP publique

3 : Orientation : en gros on dit quelle port et ou (in ou out du réseau)

```
Router(config)#int fa1/0
Router(config-if)#ip nat inside
Router(config-if)#exit
```

```
Router(config)#int f0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

ACL :

```
#access-list 20 permit 10.0.0.0 255.255.255.255
```

La commande access-list 20 permit 10.0.0.0 masque_générique configure une règle dans une liste de contrôle d'accès (ACL) sur un routeur Cisco. Elle permet d'autoriser le trafic provenant du réseau 10.0.0.0, en utilisant un masque générique pour définir la plage d'adresses IP concernée. Le masque générique indique quels bits de l'adresse IP doivent être vérifiés et lesquels peuvent

3.3 Configuration du NAT

```
#ip nat pool plage_nat 60.0.0.1 60.0.0.1 netmask 255.0.0.0
#ip nat inside source list 20 pool plage_nat overload
#exit
```

La commande ip nat pool plage_nat 60.0.0.1 60.0.0.1 netmask 255.0.0.0 définit un pool d'adresses NAT contenant une seule adresse IP publique, 60.0.0.1, avec un masque de sous-réseau 255.0.0.0, ce qui signifie que le pool couvre la plage d'adresses 60.0.0.0 à 60.255.255.255. Cette configuration crée un espace d'adresses globales utilisées pour la traduction des adresses sources internes.

3.4 Test du fonctionnement du NAT

```
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/0
Inside Interfaces: FastEthernet1/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 20 pool plage_nat refCount 0
 pool plage_nat: netmask 255.0.0.0
       start 60.0.0.1 end 60.0.0.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
Router#show ip nat translation
```

```
Router#show ip nat stat
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet1/0
Inside Interfaces: FastEthernet0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 20 pool plage_nat refCount 0
 pool plage_nat: netmask 255.0.0.0
       start 60.0.0.1 end 60.0.0.1
       type generic, total addresses 1 , allocated 0 (0%), misses 0
Router#
```

RouteurVPN(config)# **ip route 0.0.0.0 0.0.0.0 10.0.0.1**

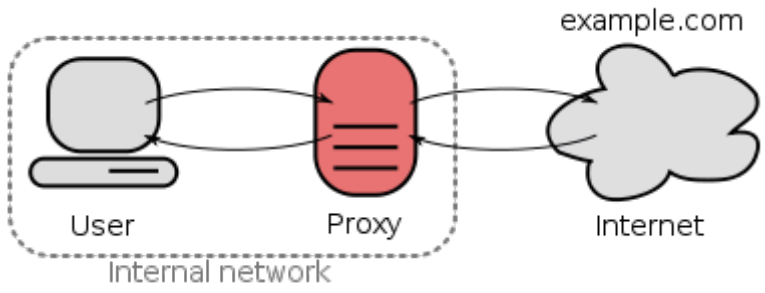
Ip /masque /prochain saut

PROXY

Proxy Opnsens

Proxy de mise en cache

Un proxy, ou mandataire, est un composant logiciel ou matériel qui agit comme intermédiaire entre un client (comme un ordinateur ou un smartphone) et un serveur cible sur Internet.Son rôle principal est de relayer les requêtes du client vers le serveur cible en utilisant sa propre adresse IP, sans que le client et le serveur ne soient directement connectés. Ce mécanisme permet de masquer l'identité du client, car le serveur cible perçoit les requêtes comme provenant du proxy.



OPNsense est équipé d'un proxy de mise en cache directe (transparent) complet. Un proxy de mise en cache réduit la bande passante et améliore les temps de réponse grâce à la mise en cache et réutilisation de pages Web fréquemment demandées. Les listes de contrôle d'accès peuvent être utilisées pour l'authentification des utilisateurs et/ou comme filtre Web (basé sur les catégories).

Gestion de projet

Définition d’un projet :

ISO : organisme qui s’occupe de faire des normes dans le monde

Un projet :

Vise un objectif donnée

Il est unique

Est provisoire

Périmètre :

Définit les éléments constitutif d’un projet

Contrainte :

Budget, délais, considération matérielles et techniques, communication.

Les enjeux

bénéfice/perte potentielle

Risques :

Événement a venir , incertains, et dommageables pour le projet

Estimation de la probabilité des conséquence :

-organisationnels, techniques, financier , humains , juridiques

Jalon :

Événements au cours du projet dont la date est connue.

Livrables :

Production attendues d’une activité au processus : 3 type de livrables :

-livrable projet

-livrable de gestion

-livrable produit.

Cout :

-directs (rh matos)

-indirecte (communication)

Date cible :

Date a la quelle le produit doit etre livré.

Acteur d’un projet :

Individu ou groupe ayant :

-un intérêt

-une influence

-une responsabilité

= Partie prenantes internes ou externes au projet.

Maître d’ouvrage (parton/le gars qui commande)

Commanditaire

Définit les objectifs

Exprime les besoins

Valide les résultat

Maître d’oeuvre (le maçon) :

Responsable de la réalisation

Propose des solutions techniques

Met en œuvre conformément aux exigence du Maître d’ouvrage.

Chef de projet :

Dirige , garanti les délais

Équipe projet :

Membres impliqués dans le projets

Sponsor :

Finance le projet ou du service issu de projet.

Externe :

Client :

Bénéficie du projet

Fournisseur :

Il fournis

Régulateur :

S’assurent que le projet respecte les nomes légales et industrielles

Utilisateurs finaux :

Ceux qui vont utilisé le truc qui a était fait.

Cartographie des acteurs :

Identifie les parties prenantes :

Analyser leur influence et intérêt,

Positionner les acteurs sur la matrice

Définir des stratégie de gestion adaptés

-acteur clée : implication régulière et gestion active

-Acteurs impliqués : consultation régulière

-acteurs a informé : communication continue

-acteurs a surveillé : veille

Outil et méthode de gestion d’un projet :

Spécifique :

Définition claire de l’objectif

Mesurable :

Définition des critère mesurable pour suivre les progrès

Atteignable :

Objectif réalisable compte-tenue des ressources disponible.

Réaliste :

Pragmatique et pertinent par rapport aux capacité et au contexte

Temporalisé :

Définition d’une échéance.

Traditionnelle (ou fonctionnelle)

Organisation divisée en fonction spécialisées.

Avantage :

-rôle et responsabilité claires

-gestion optimisé pour chaque fonction

Inconvénients :

-prise de décision lente

-manque de flexibilité

-communication entre les fonctions.

Par projet :

Organisation centrée sur les projets

Avantages :

Autonomie du CdP ,

Gestion efficace des ressources dédiées au projet

Flexibilité et réactivité

Inconvénients :

Dépendance aux projets :

Manque de coordination entre les projets

Exculisivité des ressources = cout élevé

Réaffections des ressources après un projet.

Gestion du patromoine informatique

Gestion du Patrimoine Informatique

Définition :

Quels enjeux ?

Permet a une organisation de :

-connaître l’ensemble des actifs,

-prévenir les défaillances,

-Répondre aux demandes des utilisateurs,

-Réduire les coûts de fonctionnement.

Qu’est que le patrimoine informatique ?

-matérielle « terminal » (ordi , serveurs etc)

-logiciels (système d’exploitation, application)

-Données (base de données , fichiers)

-Réseau (Infrastructure réseau, équipement réseau)

Gestion du patrimoine :

Processus global , complet et indispensable pour repondres aux exigences de performance de réactivité et de sécurité

Regroupe la fonction d’inventaire mais aussi l’ensemble des taches visant a entretenir, développer et optimiser l’ensemble des ressources informatique de l’entreprise.

Réaliser un inventaire

-identifier et relever les caractéristique

-catégoriser

-évaluer l’état

-sécuriser les accès

-Tenir a jour

Type de licences

-Licence propriétaire ? / licence open-sources ?

-Licence par utilisateur ? par poste ? par serveur ?

Gestion :

-suivi

-conformité

-renouvellement et lise a jour.

Maintenance

-planification des maintenances

-gérer les incidents

-mises a jour des systèmes et des logiciels

-save de données

Investir

-prévoir le renouvellement des actifs ,

-assurer la formation des utilisateurs

Gérer

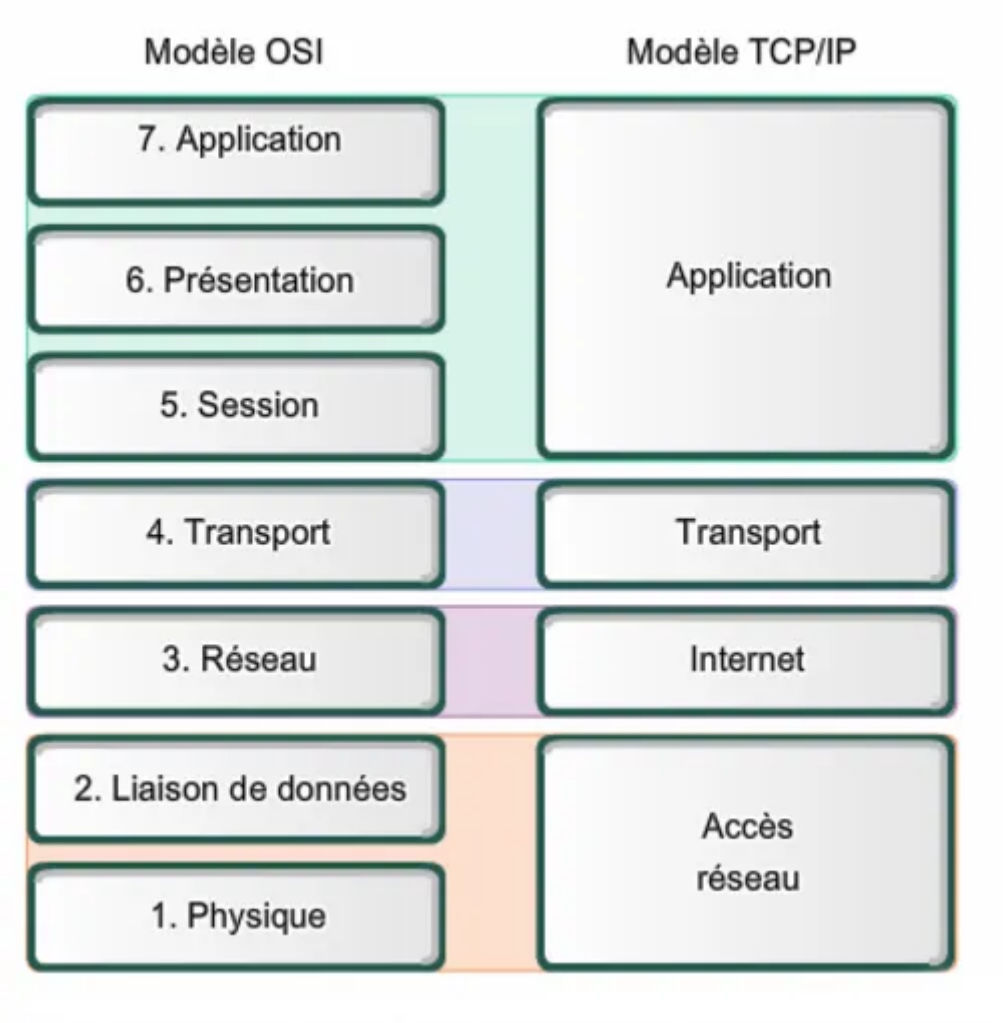
-les déploiements

-les prestataires

-la documentation

Modéle OSI

Le **modèle OSI** (Open Systems Interconnection), ou *modèle d'interconnexion de systèmes ouverts*, est un cadre conceptuel normalisé par l'**ISO** (Organisation internationale de normalisation) en **1984** (norme ISO 7498). Il décrit la communication entre systèmes informatiques en réseau à travers **7 couches hiérarchiques**, chacune ayant un rôle spécifique. Ce modèle permet d’assurer l’interopérabilité entre équipements et logiciels de différents constructeurs en standardisant les fonctions réseau.



HA/SLA

HA/SLA

HA COUR

TP – Haute Disponibilité (HA)

Table des matières - Définitions d’éléments servant à la HA - Mise en place d’une haute disponibilité sur un serveur web - Prérequis - Installation de Corosync et de Pacemaker

Définitions d’éléments servant à la HA

1) Qu’est-ce que la haute disponibilité ? La haute disponibilité (HA) est le fait qu’un système puisse être accessible au plus proche de 100 % du temps, donc avec le moins d’interruption possible. La haute disponibilité désigne aussi la capacité d’un système à rester accessible et fiable presque 100 % du temps. Un système hautement disponible doit pouvoir résister à des interruptions, qu’il s’agisse de temps d’arrêt planifiés ou de sinistres à grande échelle.

Un système HA répond généralement à deux critères clés : - Il doit rester disponible quasiment en permanence. - Il doit satisfaire un ensemble d’attentes prédéfinies de la part des utilisateurs.

2) Pourquoi mettre en place la haute disponibilité ? La HA permet à des utilisateurs d’un service qu’il soit accessible au plus proche de 100 % du temps et permet donc d’assurer la non interruption d’une activité ayant besoin d’accéder en continu à un système.

3) Qu’est-ce que “SLA” ? Le SLA, pour Service Level Agreement ou accord de niveau de service, est le taux de disponibilité d’un service en pourcentage et sur une année.

C’est un contrat formel entre un fournisseur de services informatiques (interne ou externe) et un client (entreprise ou utilisateur final), qui définit : - les niveaux de service attendus - les engagements de performance - les méthodes de mesure de ces performances

4) En quoi cela concerne la haute disponibilité ? Le SLA concerne la haute disponibilité car il permet d’établir la complexité du système d’HA à mettre en place, selon si on souhaite une disponibilité de 99.9 %, 99.99 %, 99.999 %, etc. La SLA est en partie basée sur la haute disponibilité car si le site est indisponible, il n’y a plus de disponibilité.

5) Qu’est-ce que la réplication ? La réplication est le fait qu’un élément soit recopié à l’identique pour que la copie serve à remplacer ce dernier en cas de problème. C’est une duplication d’un serveur ou d’un service à des fins de haute disponibilité.

6) Qu’est-ce qu’un cluster ? Un cluster est un groupe d’éléments regroupés qui fonctionnent ensemble. Un cluster informatique est un groupe d’ordinateurs ou de serveurs indépendants, interconnectés, qui fonctionnent comme un seul système cohésif.

7) Qu’est-ce que Corosync ? Corosync est un service permettant de gérer des clusters de machines et de gérer leur accessibilité. C’est un service qui permet de faire fonctionner la haute disponibilité.

Dans le cadre de la HA : - Il gère le serveur maître et les serveurs secondaires - En cas de panne, un serveur secondaire prend le relais

Fonctionnement : - Chaque serveur envoie régulièrement un message appelé heartbeat - Ces messages passent par un lien Corosync - Si le serveur maître ne répond plus, un vote est organisé

En cas d’absence de majorité : - Un Quorum permet de trancher

8) Qu’est-ce qu’une IP virtuelle ? Une adresse IP virtuelle est une adresse IP non liée à une interface physique mais à un service ou un cluster. Elle permet à plusieurs machines d’être accessibles via une seule adresse IP.

9) Qu’est-ce qu’une IP failover ? Une IP failover est une adresse IP pouvant être transférée rapidement d’un serveur à un autre sans interruption de service.

Elle permet : - un basculement rapide - la continuité de service - la redondance en cas de panne

10) Fonctionnement de l’IP Failover dans la HA (IP failover utilisée pour basculer rapidement vers un serveur de secours en cas de panne)

11) Qu’est-ce que Pacemaker ? Pacemaker est un logiciel open source de gestion de cluster haute disponibilité. Il permet de :

- démarrer, arrêter et superviser les ressources
- garantir la continuité des services

Il fonctionne souvent avec Corosync, qui gère la communication entre les nœuds.

12) Qu’est-ce qu’une ressource (Pacemaker) ? Une ressource est un service ou un élément que le cluster doit gérer pour assurer la haute disponibilité. Exemples : serveur web (Apache, Nginx), base de données, etc.

13) Qu’est-ce qu’un script OCF ? Un script OCF (Open Cluster Framework) est un script utilisé comme agent de ressource. Il permet :

- de démarrer / arrêter un service
- de surveiller son état

14) Qu’est-ce qu’un CIB ? (CIB mentionné mais non défini dans les textes)

Mise en place d’une haute disponibilité sur un serveur web

Prérequis Il faut : - un serveur LAP avec un service web (ex : GLPI) - un VHOST configuré (nom de domaine + IP) - un serveur de base de données fonctionnel

Reprendre à : « Installation de GLPI à partir de l’interface web »

Installation de Corosync et de Pacemaker

1. Installer les paquets : apt install corosync pacemaker pcs

2. Cloner le serveur ou en créer un second avec les mêmes services

3. Générer une clé : corosync-keygen

4. Copier la clé vers le serveur esclave : scp /etc/corosync/authkey root@:/etc/corosync/authkey

Configuration de Corosync

Modifier le fichier : /etc/corosync/corosync.conf

Dans le bloc totem : - ajouter : secauth: on - modifier : cluster_name - ajouter : transport: udpu

Dans le bloc nodelist :

- Ajouter un node pour le serveur maître :
  - ring0_addr : IP du serveur maître
  - name : nom
- Ajouter un node pour le serveur esclave avec ses informations

HA installation

SSH

Syntaxe SSH

ssh exemple@IP

ssh = base la commande

exemple : nom de l'utilisateur choisit

@ = @

ip = l'ip de la machine

Par défault ssh n'autorise pas root.

Si vous avez cette erreur :

```
caribou@fedora:~$ ssh jules@192.168.110.5
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:csefUI+e7zFyZGAJWMnu0TnGYbFUhNa2tY8zg8Hkeao.
Please contact your system administrator.
Add correct host key in /home/caribou/.ssh/known_hosts to get rid of this messag
e.
Offending ECDSA key in /home/caribou/.ssh/known_hosts:4
Host key for 192.168.110.5 has changed and you have requested strict checking.
Host key verification failed.
caribou@fedora:~$
```

Faire :

ssh-keygen -R IP

IP = l'ip de la machine sur laquelle vous souhaiter vous connecté.