Maquette

stage 2022 / 2023

Maquette

sommaire

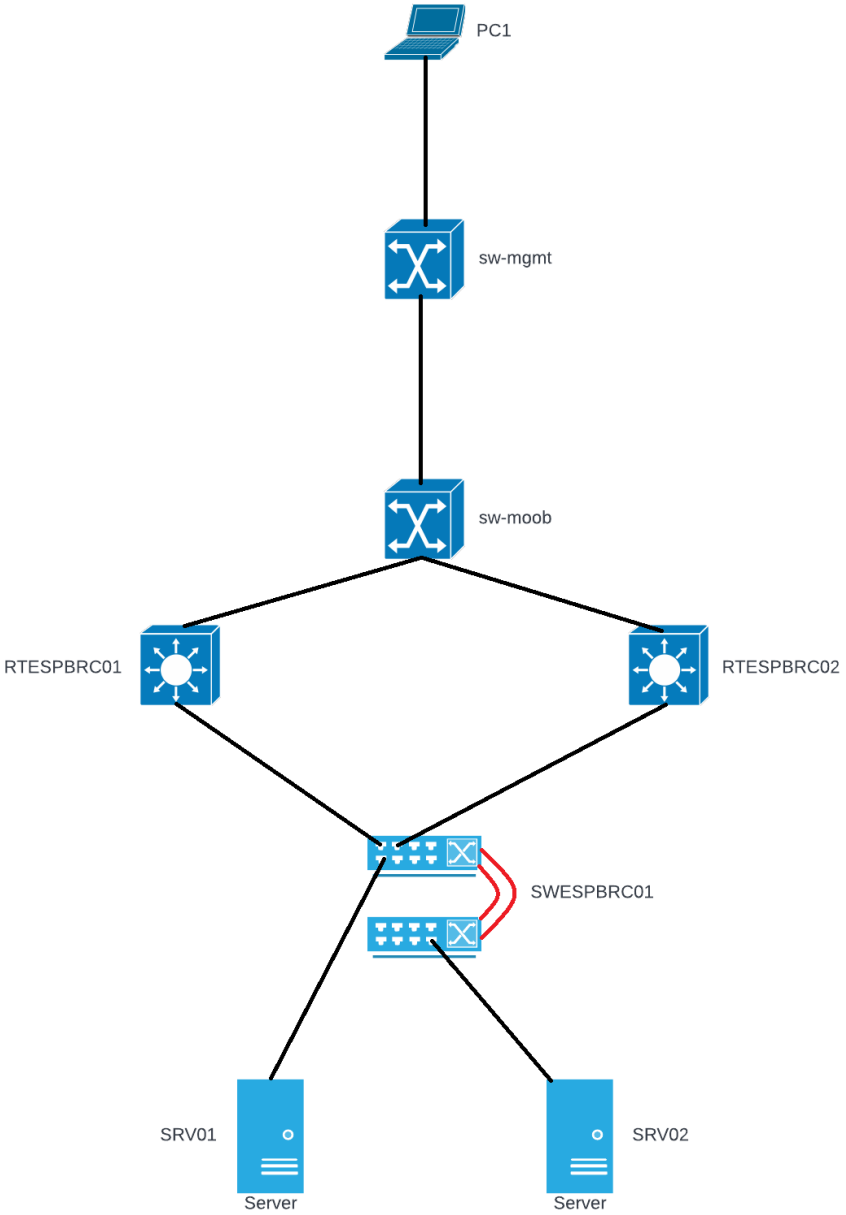
Maquette

Préparation

Objectifs

Créer une infrastructure réseau permettant de connecter des VM sur ESX à des serveurs sur une autre ESX

schéma réseau



Maquette

Notions

Notions réseau		
protocoles et notions	**réalisation**	**Niveau OSI**
DNS	- nom de domaine - nom d'hôte - désactiver la recherche DNS	5/6/7
HTTP/HTTPS	- désactiver les accès web HTTP et HTTPS	7
authentification port console et accès distant	mise en place d'un Id et mdp pour l'accès - au mode console (lin con 0) - au mode privilège - à distance (line vty 0 15) chiffrer les mots de passes stockés en clair dans la configuration	5/6/7
accès ssh	- création d'une clé RSA pour chiffrer les communications - configuration ssh version 2	5/6/7
spanning-tree	- mise en place du rapid pvst - choisir les priorités par vlan	2
VLAN / interfaces VLAN	- administration des différents vlan et des interfaces vlan, adresse ip et description	2/3
HSRP	- choix de la version HSRP (ici v2) - ip virtuelle - définition de la priorité pour choisir le rôle du routeur dans la topologie - preempt pour le routeur actif - authentification des équipements pour les communications HSRP avec key-string - tracking de port pour décrémenter la priorité HSRP quand le port est down	3
Etherchannel et liens trunk	- application du protocol sur 2 ports entre les 2 switchs L3 et création d'un port channel - liens trunks entre le stack et les switchs L3 et sur le port channel	3

Maquette

VLAN maquette							
nom	n° int vlan	ip	VIP	RTESPBRC01	RTESPBRC02	SWESPBRC01	SWITCH-MOOB
IDRAC	10	192.168.10.0 /24	.254	.252	.253		
Admin	20	192.168.20.0 /24				.251	
vMotion	50	192.168.50.0 /24					
Stockage	60	192.168.60.0 /24					
Interco	100	192.168.100.0 /24					.1
Livebox	200	192.168.200.0 /24	.105	.100	.110		.1
Etage	90	192.168.90.0 /24					

Notions ESX / SRV / VM	
protocoles et notions	**réalisation**
ESX	installation des VM sur 2 ESX une serveur et une client
serveur DHCP	étendues par vlan
serveur DNS	enregistrement AAA et CNAME
serveur AD	ajout d'uo et d'utilisateur
VM client	ajout dans le domaine AD

matériels

- deux switchs 3750 stackés
- deux switchs L3
- deux ESX

Configuration

Cours

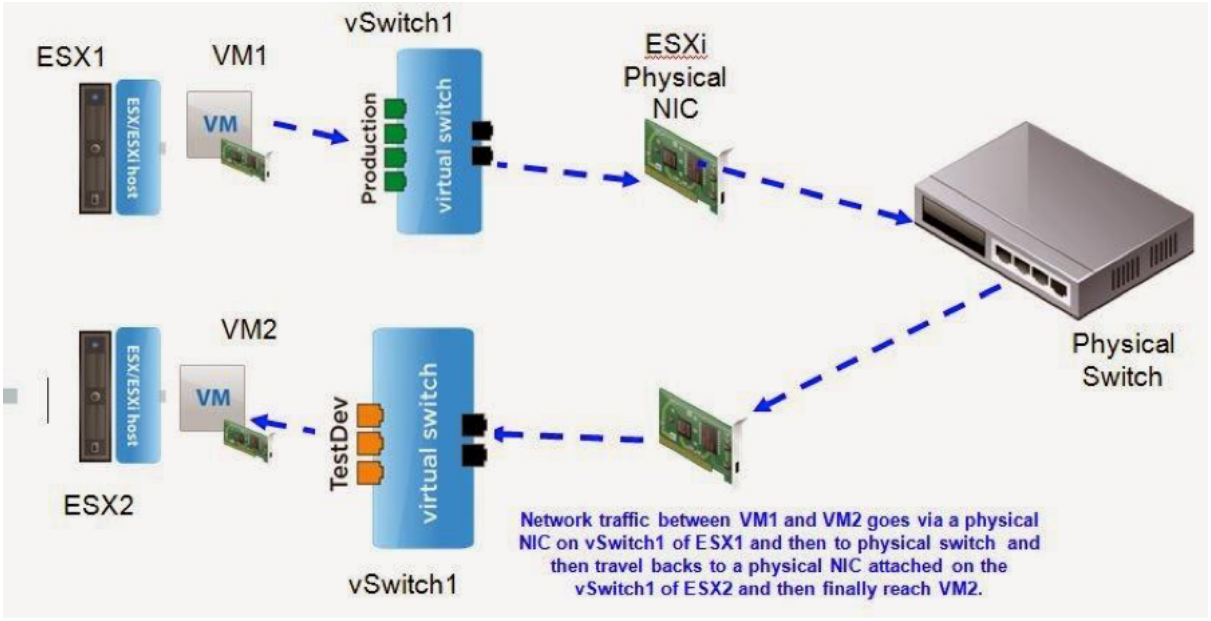
Qu'est-ce qu'un port SFP

Les ports SFP sont utilisés avec des connecteurs à facteur de forme réduit (SFF), ils offrent une vitesse élevée pour un module compact. Ces ports permettent d'autoriser les liaisons fibres comme cuivre en ajoutant le module SFP cuivre ou SFP fibre.
ce dispositif est enfichable à chaud cela signifie que l'on à pa besoin d'éteindre ou de redémarrer l'équipement pour retirer ou ajouter un module SFP

Maquette

Distance et portée des ports	
type de câble	portée
SFP cuivre	100 m
SFP fibre optique	2000m et +

ESX



VMNIC et PNIC virtual-machine / physical network interface card
les vNIC sont des cartes réseau virtuelles (une machine virtuelle en dispose d'au moins une)

interface PCI
peripheral component interconnect est un standard de bus local qui permet la connection des cartes d'extension sur la carte mère d'un ordinateur

port IDRAC9 (integrated dell remote access controller)

configurer iDRAC9
https://www.dell.com/support/kbdoc/fr-fr/000177212/dell-poweredge-configurer-l-ip-r%c3%a9seau-de-l-idrac9-et-du-lifecycle-controller

port vMOTION
VMotion est la technologie inventée par VMware permettant de déplacer une VM en fonctionnement d'un serveur hôte ESX à un autre de façon totalement transparente. Le système d'exploitation et l'application ne subissent aucun arrêt de service.
permet la migration à chaud d'un ESX à l'autre et sans interruption de service

port réservés (well known 0 - 1023)

- 368 :
- 370 :

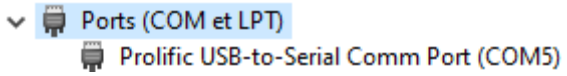
Première connection sur le switch

La **première connection** s'effectue sur le port **console** du switch on utilise un câble USB/RJ45 afin de connecter physiquement l'ordinateur au switch, puis on utilisera le logiciel window "**putty**" pour le terminal de connection

schéma sw port console

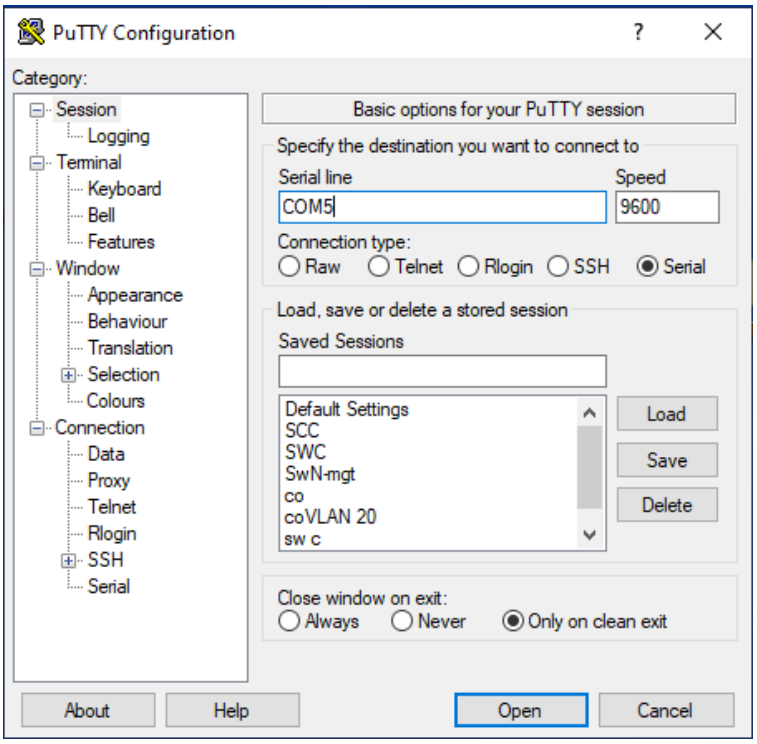
Avant de lancer putty on doit récupérer le numéro de port COM sur lequel notre cable USB/RJ45 est branché

WIN > gestionnaire de périphériques > Ports (COM et LPT) >
agrandir le menu déroulant et **récupérer** le numéro COM (ex COM5)



utiliser putty

une fois le n° port COM récupéré, on peut lancer putty



Une fois connecté on accède à une console dans le mode **sans privilèges**

Maquette

```
switch>
```

Afin de pouvoir **modifier la configuration du switch** il faut passer en **mode privilège puis configuration.**
dans le mode privilège on peut passer que certaine commandes comme “show” afin de voir les configurations appliquées

```
switch>enable
switch#configure terminal
```

Redondance vers les serveurs

- 1 port sur chaque switch du stack
- même numéro de port pour le même rôle sur chaque switch

n° de port	
dizaine	unité
serveur	rôle

	ports						
	service	serveur 1	serveur 2	serveur 3	serveur 4	Vlan	ID (unité)
switch 1 SWESPBRC01	IDRAC	1/0/11	X	1/0/31	1/0/41	10	1
	Management	1/0/12	1/0/22	1/0/32	1/0/42	20	2
	v Motion	1/0/13	1/0/23	1/0/33	1/0/43	50	3
	Stockage	1/0/14	1/0/24	1/0/34	1/0/44	60	4

	ports						
	service	serveur 1	serveur 2	serveur 3	serveur 4	Vlan	ID (unité)
switch 2 SWESPBRC02	IDRAC	X	2/0/11	X	X	10	1
	Management	2/0/12	2/0/22	2/0/32	2/0/42	20	2
	v Motion	2/0/13	2/0/23	2/0/33	2/0/43	50	3
	Stockage	2/0/14	2/0/24	2/0/34	2/0/44	60	4

Maquette

switch 1 SWESPBRC01	service	serveur 5	serveur 6
	IDRAC	1/0/1	1/0/15
	Management	1/0/2	1/0/16
	v Motion	1/0/3	1/0/17
	Stockage	1/0/4	1/0/18

switch 2 SWESPBRC01	service	serveur 5	serveur 6
	IDRAC	X	X
	Management	2/0/2	2/0/15
	v Motion	2/0/3	2/0/16
	Stockage	2/0/4	2/0/17

port channel serveur 1	
n°	ports
po12	1/0/12 - 2/0/12
po13	1/0/13 - 2/0/13
po14	1/0/14 - 2/0/14

port channel serveur 2	
n°	ports
po22	1/0/22 - 2/0/22
po23	1/0/23 - 2/0/23
po24	1/0/24 - 2/0/24

port channel serveur 3	
n°	ports
po32	1/0/32 - 2/0/32
po33	1/0/33 - 2/0/33
po34	1/0/34 - 2/0/34

port channel serveur 4	
n°	ports
po42	1/0/42 - 2/0/42
po43	1/0/43 - 2/0/43
po44	1/0/44 - 2/0/44

Configurer un switch

effacer la configuration start et redémarrer le switch
sert à effacer toute la configuration présente sur le switch dans la NVRAM
à noter il y a **3 mémoires différentes sur le switch**

RAM (Random Access Memory)	volatile	running configuration
NVRAM	non volatile	startupconfiguration
Flash	non volatile	IOS

- `erase startup-config`
- `reload`

On pourrait penser que le switch est totalement vidé de toute configuration or ce n'est pas le cas il reste les vlan qui ont été créés dans le fichier vlan.dat
supprimer le fichier vlan.dat

- `delete flash:vlan.dat`

enregistrer la configuration
copier la configuration en cours dans le fichier de configuration de démarrage, sans cette commande si le switch s'éteint ou qu'on redémarre on perd toute la configuration
c'est une manière de sauvegarder la configuration

- `copy running-config startup-config`
- `[appuyer-sur-entrée]`
- `wr`

changer le nom d'hôte
le nom d'hôte ne contient pas d'espace, utiliser le '-' ou le '_'

- `hostname [new-name]`

définir un mot de passe pour l'accès au mode privilège
password : permet de créer un mot de passe qui sera stocké en clair dans le fichier de configuration
secret : permet de créer un mot de passe qui sera crypté dans le fichier de configuration

- `enable password [mdp]`
- `enable secret [mdp]`

chiffrer tous les mots de passes qui sont en clair dans le fichier de configuration

- `service password-encryption`

créer un utilisateur et mot de passe pour l'accès au switch
username : nom d'utilisateur
privilège :

- niveau 0 : Comprend les commandes disable (désactiver), enable (activer), exit (quitter), help (aide), et logout (déconnexion).

- niveau 1 : niveau normal sur Telnet; comprend toutes les commandes user-level (niveau de l'utilisateur) pour l'invite router>.

- niveau 15 : Comprend toutes les commandes enable-level (niveau d'activation) pour l'invite router#.

secret : mot de passe

- `username [ID] privilège [0,1,15] secret [mdp]`

désactiver la résolution DNS

- `no ip domain lookup`

définir un message du jour / authentification à l'ouverture du switch
motd : message of the day
login : à l'authentification
les messages sont délimités par des '$'

- `banner login $ [message] $`

définir un nom de domaine
le nom de domain est à créer obligatoirement pour administrer les connections ssh par la suite sur l'équipement

```
ip domain-name
```

mise en place de ssh

création d'une clé rsa pour chiffrer les échanges ssh
general keys : spécifie le type de clé, ici une paire de clé par défaut vas être créé
modulus : spécifie la taille de la clé IP

```
crypto-key generate rsa general-keys modulus 2048
ip ssh version 2
```

connection au port console

login : met en place l'authentification avec le mdp que l'on vient de créer
login local : utilise le mdp de "enable secret" (mdp pour le passage en mode privilège)

```
line con 0
password [mdp]
login / login local
```

administration de l'accès à distance

vty : virtual teletype permet les sessions d'accès à distance au switch
0 15 : on à 16 sessions possibles en simultané
input ssh : autoriser les entrées ssh, la prise de contrôle à distance en ssh
output none : se connecter en ssh depuis cet équipement à un autre

```
line vty 0 15
transport input ssh
transport output none
login local
```

désactiver les connections web

l'accès en HTTP et HTTPS avec server et secure-server est désactivé

```
no ip http server
no ip http secure-server
```

Création des VLAN et nommage

```
- vlan [vlan-number]
- name [vlan-name]
```

création d'une interface VLAN
Les interfaces vlan sont la continuité des sous interfaces sur les routeurs, on les utilise sur les switchs L3 qui peuvent router les adresses IP.
Tout comme une sous interface, l'interface vlan sert de passerelle pour sortir du réseau.

```
- conf t
- interface vlan [vlan-number]
```

Mise en place du rapid-pvst

le rapid-pvst fonctionne comme le spanning-tree à la seule différences que les ports convergent plus vites, il y a une réduction des délais de convergences et d'envois de BPDU entre les équipements

Il est possible de changer les priorités par vlan afin de forcer l'élection du root bridge.
c'est le switch avec la priorité la plus basse qui est élu root bridge
La priorité en spanning-tree est un incrément de 4096 et va de 0 à 61440
par défaut elle est à 32768

```
- spanning-tree mode rapid-pvst
- spanning-tree vlan [vlan-number(s)] priority
  [incrément-of-4096]
```

sur les interfaces access (de terminaison) comme vers un PC, il est judicieux de désactiver le spanning-tree afin que la convergence des ports se fasse plus rapidement (supprimer la phase d'envoie de BPDU pour ce port car inutile)

```
- spanning-tree portfast
- spanning-tree bpduguard enable
```

Enfin pour apporter de la sécurité au processus spanning-tree on peut activer le BPDU guard, qui a pour rôle de désactiver les ports en err-disabled si des BPDU sont reçus sur ce port.
Concrètement cela permet d'empêcher un attaquant de prendre la place du Root Bridge

Etherchannel

```
- int range gi1/0/X - X
- channel-protocol lacp
- channel-group [group-number] mode active
- ex
- int po[group-number]
- no switchport
- switchport mode …
```

Configuration de l'Authentification HSRP MD5 avec une key chain
pour cette étape il faut au préalable avoir configuré HSRP sur la topologie

```
- key chain [keychain-name]
- key [integer]
- key-string [mdp]
```

```
choisir un nom
la clé doit être un entier
définir un mdp
```

aller sur les interfaces qui sont configurées en HSRP

```
- standby [standby-group] authentication md5 key-chain
  [keychain-name]
```

tracking de port

```
- track 50 int gi 1/0/X line-protocol
- standby X track 50
ou
- standby X track gi1/0/X [priority-decrement]
```

permettre au switch d'effectuer le routage d'adresse ip L2 → L3

```
- ip routing
```

Rôle DHCP sur switch L3 ou routeur
définir une pool DHCP

- spécifier les adresses à ne pas délivrer pour encadrer celles à délivrer
  ex : pour définir une pool de 50 à 100 on exclu de 1 à 49 puis de 101 à 254

```
- ip dhcp excluded-address [adresse-début] [adresse-fin]
- ip dhcp excluded-address [adresse-début] [adresse-fin]
```

voir les détails DHCP

```
- sh ip dhcp pool
```

configurer le routage statique

```
- ip route [ip_destination][masque][passerelle]
```

route par défaut

```
- ip route 0.0.0.0 0.0.0.0 [passerelle]
```

interface vlan

```
- int vlan[n°-de-vlan]
```

default gateway

```
- ip default-gateway [ip-passerelle]
```

nat

```
   vers l'interieur
- int gi 1/0/X
- ip nat inside

vers l'exterieur
- int gi 1/0/X
- ip nat outside
```

🔺 **warning**

```
- exemple general
```

Sources

cours

- Connexion au switch (clemanet.com)

vmotion

- https://www.etudier.com/dissertations/Vmotion/585439.html#:~:text=1)%20D%C3%A9finition%20%3A,subissent%20aucun%20arr%C3%AAt%20de%20service.

installation de vcenter

- https://pixelabs.fr/installation-vmware-vcenter-server/

commandes cisco

- https://www.numelion.com/commandes-commutateurs-cisco.html