Administration

Samuel "Big Boss" Monroe

30 Mai 2015

Table des matières

Chapitre 1

Avant-Propos

Et oui ma biche, c'est le challenge, l'examen sans cours, l'examen de la mort.

Maintenant, grâce à moi, tu as entre les mains ton ticket pour la grande dis mon asti. Voici le cours condensé d'Administration des Réseaux, le cours pour les gouverner tous et dans les ténèbres les lier.

Chapitre 2

Structure

1 Environnements et besoins

Comme vu en sécurité, il est nécéssaire de classer les assets sur base de leurs besoins en termes de **CIA**, Confidentiality, Integrity, Availability.
L'analyse de ces besoins vont forcer le concepteur réseau à séparer ces assets dans différentes zones spécifiques, afin que ces besoins soient satisfaits et qu'un certain niveau de sécurité soit disponible.

1.1 Production

Dans un environnement de production, ou **Core Business**, on retrouve typiquement deux zones distinctes :

— **Trusted Zone** : Zone de confiance, dans laquelle on va placer les machines qui nécéssitent un plus haut degré de sécurité, tels que les serveurs de Data, et qui ne sont pas accessibles directement depuis l'extérieur.

— **Demilitarized Zone** : C'est typiquement une zone "tampon", qui est placée entre une **Trusted Zone** et une zone **Untrusted** telle que l'Internet.
Cette zone contient généralement les services et devices accessibles directement par internet, tels que les serveurs HTTP, DNS et Mail, mais qui nécéssitent tout de même un certain degré de protection.

1.2 Autres environnements

On trouve également les environnements **Office/Corporate** qui sont des réseaux isolés internes à une entreprise, et également de **Test** et **Development** dont le nom indique bien leur but.

2 Plan d'adressage IP

Comme vu dans tout les cours de réseaux depuis la deuxième, un plan d'adressage IP doit être conçu pour pouvoir d'une part prévoir l'évolution de ce réseau tout en ne gaspillant pas d'adresse, et d'autre part pour pouvoir identifier aisément les machines présentes dans ce réseau.
Il faut également un moyen de pouvoir regrouper certaines machines logiquement, même si la topologie physique est totalement différente. Ceci sera accompli via des VLAN.

3 Plan de nommage - Naming Convention

Le nommage des serveurs est une tradition commune dans le réseau, afin de pouvoir se référer à ces machines plus aisément que sur base de l'adresse IP.

Donner un petit surnom sympathique lorsqu'on a 4 serveurs est une option envisageable, mais lorsqu'on doit réfléchir à une infrastructure comptant des dizaines de serveurs de toutes sortes, il faut envisager un plan de nommage logique.

Ce plan de nommage devrait pouvoir tenir compte de l'évolutivité du réseau, afin que l'on puisse intégrer de nouvelles machines sans devoir renommer toutes les autres.
Il devrait également permettre d'obtenir des informations utiles décrivant la cible, pour permettre une recherche aisée.

Voici quelques bonnes pratiques de nommage :

— **Décomposable** : Le nommage devrait être composé de combinaisons d'acronymes représentant tous de l'information, par exemple les serveurs mails devraient porter MX ou MAIL dans leur nom complet. Ensuite avec un autre set de caractères, on pourrait obtenir d'autres informations. Attention toutefois que donner trop d'informations pourrait aussi faciliter la vie d'un hacker.

— **Séquences de caractères pour chaque composant d'information** : On pourrait établir que chaque nom de serveur ou machine commence par trois caractères qui donne le pays où il est localisé, etc...

— **Nombre consistant de caractères pour tout les noms**

4 Elements constitutifs d'un réseau, design et stratégie

Typiquement on a dans un réseau des **Firewalls**, **Switches**, **Routers** et **Serveurs** ainsi que des **Machines utilisateurs**.

Le design de ce même réseau doit répondre à certains besoins afin de pouvoir le maintenir et pouvoir assurer le service :

— La complexité du réseau doit être en phase avec l'expertise de l'équipe IT
— Faut-il du Power over Ethernet (POE) ?
— De quelle bande-passante a-t-on besoin ?
— Quel niveau de redondance doit-être assuré ?

Il est question aussi du design de la topologie logique et phyique, comment il faudra organiser les zones et le placement des machines dans celles-ci, à quels niveau se trouvent les FireWalls et pour quels buts ?

Chapitre 3

Les Réseaux

1 Concepts réseaux utilisés pour connectivité Intra et Inter Datacenter

2 Types de réseaux

2.1 LAN

Local Area Network : Le LAN est un réseau local, définit par sa taille phyique plus que par sa connectivité, où il représente généralement un réseau à l'échelle d'une habitation voir d'un site d'entreprise.

2.2 WAN

Wide Area Network : Réseau étendu, couvrant une large zone géographique telle qu'un pays ou un continent. Internet est le plus grand WAN.

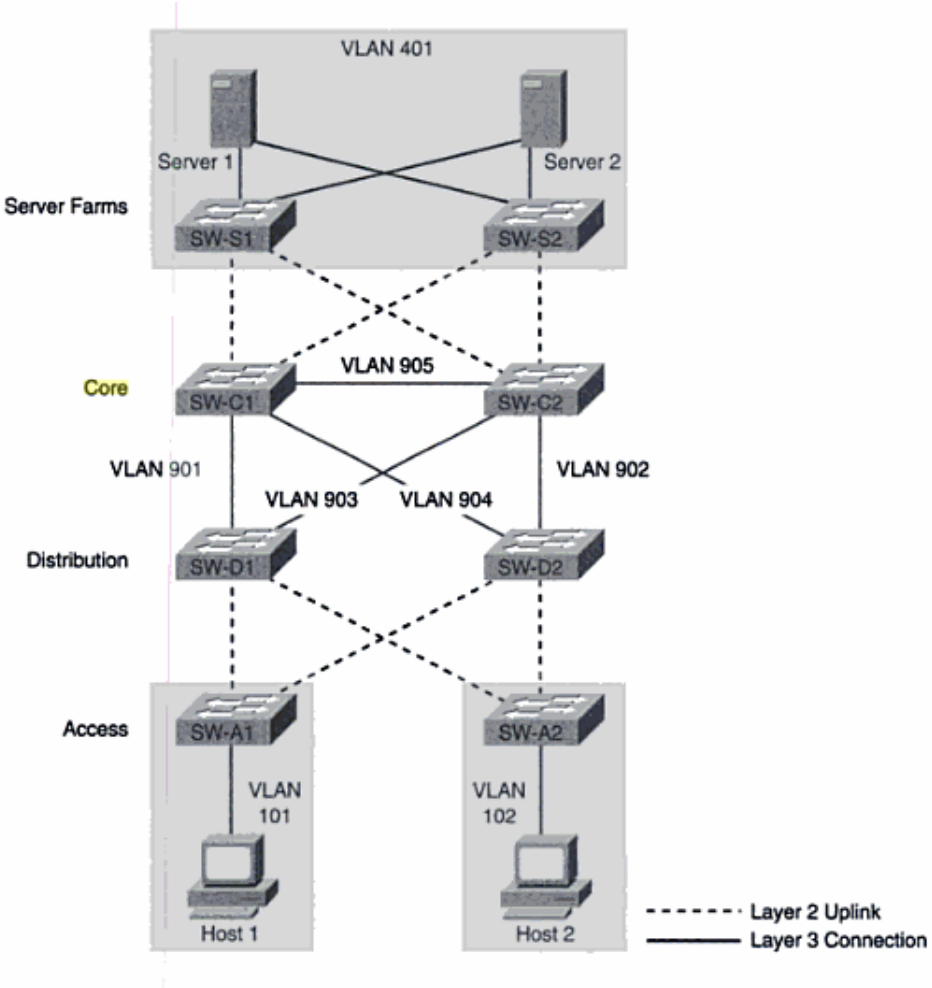
2.3 SAN

Storage Area Network : Le SAN est un réseau spécialisé dans la mutualisation de ressources de stockages. Les baies de stockage n'apparaissent pas comme des volumes partagés sur le réseau, comme un NAS.
Chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur, ces unités logiques (**Logical Unit Number**) doivent être définies précisément pour que les machines aient accès aux bonnes ressources.

3 LAN

3.1 Three Tiers Models

Typiquement, Cisco définit un LAN en trois **Tiers** de base que l'on va définir juste après, juste avant un petit schéma montrant le modèle trois tiers.



Core Layer

Cette couche propose des services à haut débit et à haute redondance de forwarding pour déplacer les paquets entre la couche de distribution et différentes autres régions du réseau.

Les **Core Devices** sont des switches et des routers parmis les plus puissants en termes de transmission.

En entreprise, le Core gère les connexions ayant le plus haut débit, tel l'ethernet 10Gigabit.

Distribution - Aggregation Layer

Cette couche est la plus intelligente du modèle. On y trouve la gestion du routage, du filtrage et du QoS.

Access Layer

C'est à cette couche que se connectent les serveurs et stations utilisateurs.
La couche d'accès est souvent une couche de switching de couche 2 uniquement.

3.2 Blocks supplémentaires

Ces deux blocks supplémentaires sont associables au modèle en trois tiers en venant s'ajouter dessus :

Server Farm Block

Relié au Core, ce bloc rassemble les serveurs.

Edge Block

Relié au Core, c'est là qu'on trouvera un ensemble de FireWalls et une DMZ pour assurer la connectivité aux ISP (Internet Service Provider).

4 SAN

Nous avons définit précédemment ce qu'était un SAN, attardons-nous maintenant sur des éléments plus spécifiques à ce type de réseau.

Avant de commençer, précisons que SAN utilise le protocole iSCSI (Small Computer System Interface) basé sur le protocole IP et destiné à relier les installations de stockage de données.

4.1 Initiators & Targets

Commençons par l'**Initiator**. Typiquement, c'est un ordinateur faisant partie d'un domaine SCSI intitie les connexions vers un device de stockage de données qui lui sera la cible.
L'initateur est un end-point, qui initie une session via une commande SCSI.

Le **Target** est un endpoint qui n'initie pas les sessions, mais écoute dans l'attente d'une commande d'un initiateur, auquel il répondra par le transfert de données souhaité.
Le target fournit aux initiateurs des **LUNs** afin qu'il puisse demander une lecture ou une écriture, qu'on définira juste après.

4.2 Storage Arrays

C'est en fait les rangées de disques qui sont connectés au réseau de stockage, et donc au SAN.

4.3 SAN Switches / WWN / Port Zoning

Le **SAN Switch** est un Switch (Fibre Channel ou Ethernet) qui va analyser les headers des paquets et déterminer l'origine et la destination de celui-ci, afin de l'envoyer vers le bon système de stockage.
Il est conçu pour fournir une latence ainsi qu'une perte très faibles sur les transmission de données.

Le **World Wide Name** est un identifiant unique dans un réseau SAN, comparable à l'adresse MAC sur les cartes réseaux classiques.

Enfin, le **Zoning sur Port ou WWN** est le fait de fournir des plus petits ensembles de machines à partir du SAN afin de réduire l'interférence, augmenter la sécurité ou simplifier la gestion.
On peut comparer cela au VLAN (qui existe en SAN en tant que VSAN), à la différence qu'un port peut être membre de plusieurs zones (pas en VSAN).

4.4 RAID Groups, LUNs & Storage Groups

Un **RAID** ou Redundant Array of Independant Disk est un ensemble de disques physiques composant une seule unité logique à des fins de redondance ou et de performances.

Le **LUN** ou Logical Unit Number est un identifiant qui désigne un ou plusieurs éléments de stockage physiques ou virtuels.

Un **Storage Group** peut être un ensemble de LUNS, aussi appelé Pool of Storage.

4.5 No drop environnement

Ce type d'environnement assure un niveau de perte le plus réduit possible.

5 High Availability

Le concept de High Availability ou Haut Disponibilité consiste en le fait d'assurer la disponibilité de l'information et des processus adaptés afin de réduire les erreurs et d'accélérer la reprise d'activité en cas d'interruption.

Ceci est notamment assuré via la mise en place de Dark Fibre, qui consiste en de la fibre optique non alimentée par une source lumineuse, ainsi que via des systèmes synchrones avec un round-trip-time de 10ms.

6 Disaster Recovery

Assure la remise en route des services et la disponibilité de l'information après une défaillance informatique importante par le basculement vers une infrastructure secondaire capable de prendre en charge les besoins informatiques nécéssaires à la survie de l'entreprise.

Ces infrastructures sont caractérisées par des systèmes pouvant être asynchrones et à des longues distances, disposant d'un RTO **Recovery Time Objective** qui est le délai de rétablissement d'un service le plus bas possible, ainsi que d'un RPO **Recovery Point Objective** qui désigne la durée maximum d'enregistrement qu'il est acceptable de perdre lors d'une panne.
Le RPO définit en d'autres termes les objectifs de sauvegarde.

7 Inter Site Link

Les liens entre plusieurs sites sont possible via plusieurs technologies :

7.1 Dark Fibre

Contrairement à la Dark Fibre définie précédemment, celle-ci est une fibre louée à l'état brut au client, c'est le client qui gère les équipements actifs aux extrémités de la fibre et aucun équipement actif de l'opérateur n'est utilisé pour la transmission.

7.2 MPLS/Switches Connection

Multi**P**rotocol **L**abel **S**witching est un mécanisme de transport de données basé sur des étiquettes ou "labels", qui sont apposés sur les paquets à l'entrée du réseau et retiré en sortie.
Ceci permet de créer des liens entre deux sites via ce mécanisme.

7.3 VPN

Le VPN permet d'étendre une liaison locale directe à travers le réseau internet, via deux servers VPN qui vont agir comme passerelle sur chacun des sites.

8 Connection Internet

Parlons à présent des moyens de connexion à Internet pour une entreprise.

8.1 ISP/FAI

Les ISP sont des Fournisseurs d'Accès à Internet, moyenant facturation, ils fournissent un accès à l'internet.

8.2 Carrier Tier 1

Ce sont les carrier possédent les accès direct à Internet et composant donc le backbone de l'Internet.

Chapitre 4

Datacenter

Un Datacenter est un site physique où se trouvent regroupés et interconnectés les différents équipements constituant une infrastructure IT d'une entreprise afin de délivrer des services à des utilisateurs.

1 Interne

Les Datacenters internes le sont souvent pour des raisons historiques, placés dans les caves de bâtiments ou dans des locaux qui ne fournissent pas toujours les besoins que nécéssite une telle infrastructure. Les problématiques que nous allons lister ci-après ont conduits à tendre vers une externalisation de ces Datacenters.

1.1 Problématiques

Les problèmes d'un datacenter interne concernent en premier lieu l'évolution de ses besoins tels que l'électricité, la climatisation l'espace disponible à la mise en place de serveurs supplémentaires.

Ensuite, en termes de besoins CIA : Ces serveurs doivent être régulés, leur conformité doit être assurée (**compliance**), des audits annuels doivent être menés sur ceux-ci.

2 Externe

2.1 Composantes

— Climatisation précise et stables
— FIltration de l'air (poussières)
— Distribution électrique
— Alimentation d'urgence UPS
— Alerte incendie
— Extinction automatique des incendies via gaz inerte (Azote, Argon)
— Plancher surélevé
— Conduites pour les câbles
— Surveillance par caméra de 3 mois minimum (obligation légale)
— Sécurité physique non-stop
— Connectivité vers l'extérieur

2.2 Racks

Les racks sont aussi appelés baies, et sont des armoires généralement dotées de rails qui recoivent les serveurs en lames.

Typiquement, un rack de 42U peut accueillir 42 serveurs en lame de 1U chacun, 1U faisant 4,45 centimètres.

Une baie possède trois zones :

1. TOP : Assure la connectivité au réseau (path pannel, etc)
2. BETWEEN : Equipements
3. BOTTOM : Alimentation et refroidissement

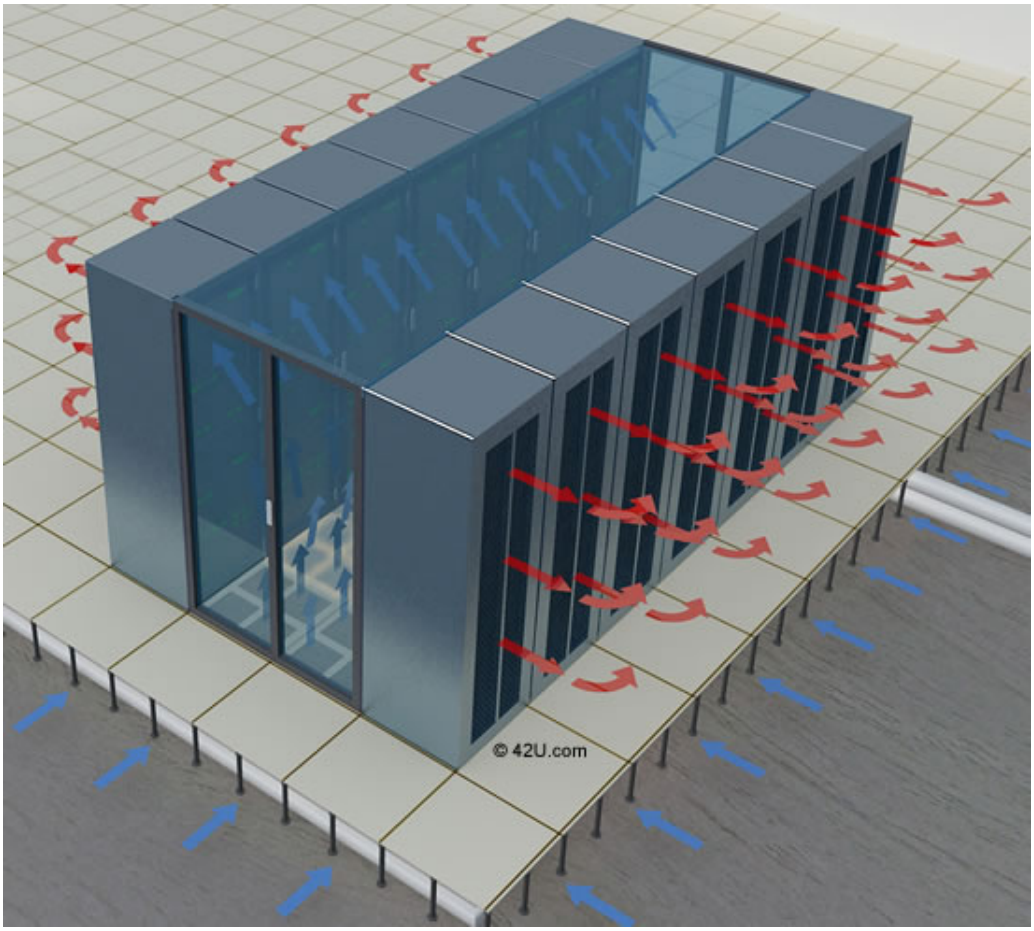
2.3 Problématique

Climatisation

Une des problématiques concerne la climatisation que requiert le datacenter.
Il faut éviter le risque de surchauffe, et limiter au maximum la consommation énergétique pour des raisons économiques et écologiques.
De plus, il faut limiter le mélange air froid et air chaud, qui n'est pas optimal et génère un gaspillage d'énergie.

Cold Corridor

Une solution à ces problème est le **Cold Corridor**, qui consiste à isoler l'air froid de l'air chaud, afin de ne pas mélanger ceux-ci :



Autres problèmes

On pointera aussi des besoins en termes de **Sécurité**, **Localisation**, et d'indépendance vis-à-vis des opérateurs télécoms.

2.4 Tiers Levels

Plusieurs niveaux décrivent les caractéristiques des datacenters afin de pouvoir classifier ceux-ci.

— **T1** : Server Room basique, règles basiques, pas de redondance au niveau énergétique.
Disponibilité de 99,671%, 28,8h d'indisponibilité par an.

— **T2** : Redondance partielle, souvent au niveau énergétique et connectique.
Disponibilité de 99,741%, 22,7h d'indisponibilité par an.

— **T3** : Redondance quasi totale, maintenance sans impact sur les services.
Disponibilité de 99,982%, 1,6h d'indisponibilité par an.

— **T4** : Redondance à 100%.
Disponibilité de 99,995%, 26,3 minutes d'indisponibilité par an.

L'objectif majeur est le **Five 9s**, dans lequel le taux de disponibilité est total avec redondance à tous les niveaux pouvant pallier à quasi toutes les pannes et les maintenances. Disponibilité de 99,999%, ou 5,3 minutes d'indisponibilité par an.

2.5 Cloud

Serveur loué à la demande selon les besoins techniques.
On retrouve trois types de Cloud :

— **IAAS** : Ou Infrastructure As A Service, cela peut-être par exemple une VM avec les ressources désirées avec un usage non limité, typiquement les VPS.

— **PAAS** : Pour Platform, qui constitue une couche supplémentaire et offre un certain niveau de spécialisation, par exemple hébergement web.

— **SAAS** : Pour Software, logiciel spécialisé disponble via le Web (Gmail, etc).

2.6 Private Cloud

Cloud interne à l'entreprise, nécéssite des aspects sécurités et son positionnement derrière un Fire-Wall.
Gestion interne du firewall.

2.7 Hybrid Cloud

Environnement cloud qui utilise du cloud privé et des services cloud publiques via orchestration de ces deux plateformes.
Peut fournir plus de flexibilité et d'options de déploiement de données.

Chapitre 5

Virtualisation

1 Problématique

Les Ressources sont sous-utilisées sur les serveurs physiques.
Le CPU, la mémoire et le réseau sont utilisés à seulement 20% et utilisent quasi la même quantité d'électricité que des serveurs utilisés à 80% ou plus.

L'extensibilité des ressources sont limitées et couteuses dans un datacenter, de plus le déploiement de nouvelles machines physiques est lent et fastidieux.

2 Solution aux problèmes

La virtualisation permet de résoudre certains de ces problèmes.
Elle permet la **consolidation** (Physical 2 Virtual), la flexibilité via déploiement rapide et à la demande.

Ceci offre également des copies et déplacements faciles (démos sans risques, tests, etc), ainsi que des scénarions de **Disaster Recovery** via copies également.

3 Hyperviseur

Logiciel capable de faire tourner des machines virtuelles, on distingue deux types :

— **Classe 1** : Native ou "Baremetal", qui tourne en tant que système d'exploitation directement sur le matériel et le contrôle pour le partager entre les guests.

— **Classe 2** : Hosted, le logiciel fonctionne au-dessus d'un système d'exploitation.

4 Virtual Machine or Guest OS

C'est une machine software qui tourne des programmes comme une machine physique normale, en tant que logiciel la VM est composée de plusieurs fichiers :

— **NVram** : Bios de la machine virtuelle
— **Vmx** : Configuration de la machine virtuelle (Nom, mémoire, cpu)
— **Vmdk** qui est le contenu du disque dur de la machine virtuelle, il peut être :

  — Fixe : Aussi appelé **thick provisionning**, la totalité du disque est réservée et allouée dès la création de la VM sur disque physique.
  — Dynamique : Aussi dit **thin provisionning**, seul l'espace réellement utilisé par la VM est écrit sur disque physique et peut augmenter jusqu'à une certaine limite.

Il faut surveiller la sur-allocation.

5 Environnement VMWare

Voici une liste des caractéristiques principales d'un environnement VMWare :

— **vSwitch** : Switch virtuel fonctionnant de manière similaire à un switch Ethernet physique.
— **dvSwitch** : Switch offrant accès aux machines virtuelle pour l'ensemble des datacenters
— **vCenter Server** : Serveur de gestion centralisé d'un datacenter virtuel
— **vMotion** : Module permettant de migrer des VM à chaud sans interruption des services.
— **DRS** : Distributed Resources Scheduler, groupement des hosts en clusters afin de balancer les besoins en ressources et optimiser les performances.
— **EVC** : Enhancer vMotion Compatibility, garanti que tout les hôtes d'un cluster présenteront les mêmes caractéristiques CPU définies sur les VM, permet aussi d'éviter les échecs de migration.
— **HA** : High Availability, fournit la disponibilité requise par nombre d'application tournant sous machine virtuelle, indépendammant de l'OS ou de l'application qui le fait fonctionner.
HA fournit une protection et récupération effective contre les problèmes hardware ou OS.

— **FT** : Fault Tolerence, fournit une disponibilité continue pour les applications dans des cas de panne serveur en créant une instance miroir de la machine virtuelle.
— **Snapshot** : Capture de l'état entier de la machine au moment T, comprend le contenu de la machine virtuelle, tout les paramètres et l'état des disques. Utilisés pour créer des points de restauration.

— **Template** : Copie parfaite d'une VM existante à partir de laquelle il est possible de cloner, convertir ou déployer plus de machines virtuelles.

Chapitre 6

Windows Server

1 Installation d'un nouvel OS

Nous allons passer en revue les différents moyen qui exitent afin d'installer un nouveau système d'exploitation.

On a d'abord le moyen classique du **CD-ROM**.
Ensuite l'**image ISO** qui est installable via des remote consoles tels que KVM, HP iLO ou Dell Drac.

Encore, il existe le **PXE Boot** (Preboot Execution Environment), qui consiste en un démarrage depuis le réseau et récupération d'une image d'OS se trouvant sur un serveur.
Ceci est fait via configuration du BIOS afin d'utiliser soit la combinaison DHCP/BOOTP en UDP sur les ports 67/68, ou bien via TFTP sur le port UDP 69.
L'exécution se fait via chargement de l'image dans la RAM.

Enfin il y a le système via **Automatisation**.
Ce système est une combinaison de PXE et de WDS (Windows Deployement Server), et suit les étapes suivantes :

1. Chargement par PXE d'une version miniature de Windows
2. Un menu de configuration s'ouvre et permet de sélectionner le servername, les paramètres réseaux, les packages optionnels ou encore le partitionnement.
3. Sysprep, un utilitaire Microsoft utilisé pour le déploiement d'OS Windows permet d'éviter ls problèmes de clonage. Il va effectuer une reconnaissance du matériel, gérer les pilotes des périphériques, etc...

2 Windows Server 2008

On retrouve deux types d'installations possibles pour cet OS :

1. **Core** : L'installation est minimale, elle réduit les problèmes de sécurité et simplifie la gestion. Elle évite également les charges supplémentaires. Cependant, cette installation a un nombre limité de rôles :

   — Active Directory Domain Service (AD DS)
   — DHCP
   — DNS
   — File Server
   — Print Server
   Sa gestion est effectuée via PowerShell.

2. **GUI** : Installation complète via une interface utilisateur.

3 Partitionnement

L'évaluation des tailles des espaces diques avant d'effectuer le partitionnement est indispensable. Cela dépend également de la RAM et de la nécéssité de SWAP, pour lequel il faut prévoir au moins 1,5x la taille de la RAM.

4 Registry

C'est le base de registre Windows, une base de données des OS Windows qui contient toutes les données de configuration du système d'exploitation ainsi que des programmes installés.

La commande **regedit** permet la consulation et la modification de cette base de données avec les risques en découlant.

5 Gestion des serveurs

La gestion de serveurs windows s'effectue sur plusieurs points :

5.1 Rôle Serveur

C'est un programme qui permet à un ordinateur de devenir serveur en remplissant une fonction spécifique pour des utilisateurs ou d'autres ordinateurs du réseau.
Le serveur a pour fonction primaire de fournir un service à des utilisateurs ainsi qu'un accès à des ressources.
Les rôles principaux sont Active Directory, DNS, DHCP, File Server, Print Server, Terminal Server et Web Server.

5.2 Rôles Services

L'installation d'un rôle implique celle d'un ou de plusieurs services, ainsi le DNS n'a qu'une seule fonction et donc un seul service.
Le rôle de Web Server par exemple va impliquer plusieurs services, telle un serveur de bases de données.

5.3 Fonctionnalité

La **Feature** est un programme qui permet d'augmenter la fonctionnalité d'un ou de plusieurs rôles et ou de l'améliorer.
Par exemple la feature **Failover Clustering** permet d'augmenter la disponibilité ou redondance du Role Service installé sur un serveur.

Chapitre 7

Domain et Active Directory

Nous avons vu dans le chapitre précédent que des serveurs Windows pouvaient être affectés à des **Server Roles** spécifiques. Un rôle relativement répandu au sein des entreprises est celui de **Domain Controller**.

1 Domain Controller

Le Domain Controller est dans la suite Active Directory, un serveur qui est responsable de l'autorisation des hôtes à accéder à certaines ressources via autentification etc.

Lorsque le premier Domain Controller est créé dans une organisation, se créent dans le même processus le premier domaine (collection d'objets), la première forest (instance complète de l'AD), le premier site (objet), ainsi que l'installation de l'AD.
Un Domain Controller va stocker les données de l'annuaire et gérer les interactions entre utilisateurs et domaine, y compris les processus d'ouverture de session, l'autentification et les recherches d'annuaires.

2 Domain

Un domaine est une base de données stockées sur les Domain Controller permettant l'administration des utilisateurs et ordinateurs déployés au sein de l'entreprise.
Elle a une forme d'organisation hiérarchique et peut-être composée de sous-domaines (Domain Trees), le tout formant une **Forst**.

3 Active Directory

Tout domaine possède son Active Directory, c'est-à-dire un service d'annuaire basé sur LDAP (Lightweight Directory Access Protocol) référençant n'importe quel objet constitutif du domaine (utilisateurs, ordinateurs, imprimantes, groupes de users).
Il s'agit d'une structure arborescante d' **Orgabisation Unit** dans lesquelles résident ces objets, eux-mêmes constitués d'attributs associés à une valeur.

4 FSMO

Flexible **S**ingle **M**aster **O**peration est un certain type de Domain Controller qui joue un rôle de **maître** unique pour la réplication entre Domains Controllers.
Il permet entre autre la compatibilité de Domain Controllers de générations différentes, la synchronisation des hrologes entre les différents DC, etc.

5 GPO

Les **G**roup **P**olicy **O**bject sont des stratégies de groupe permettant la gestion centralisée de la configuration des systèmes d'exploitation, des applications, ou des paramètres des utilisateurs dans un environnement **Active Directory**.
Les entreprises peuvent par exemple restreindre les actions et les risques potentiels en verrouillant le panneau de configuration, en désactivant certaines applications, ou en forçant le changement du mot de passe à intervalle strict.

Chapitre 8

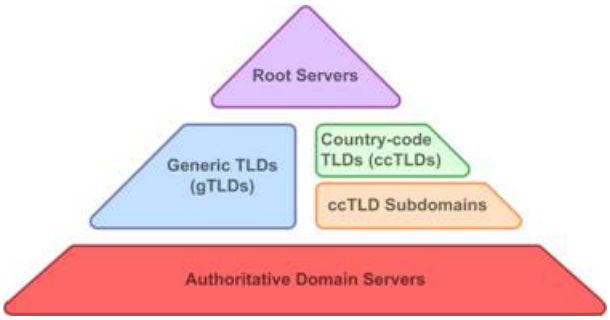
Services Réseaux

Nous allons lister ici un ensemble de services que peuvent proposer les serveurs et détailler quelque peut leurs spécificités.

1 DNS

Domain **N**ame **S**ystem est un service de traduction des noms de domaines en information de types machine, telle que l'adresse IP. Il fonctionne sur le port TCP/UDP **53**.

DNS fonctionne de manière hierarchique :



Un fichier de zone DNS possède plusieurs types d'entrées dits **records** :

— **A/AAAA record** : Correspondent aux ipv4/v6
— **CNAME** : Canonical Name, spécifie un nom de domaine alias d'un autre domaine
— **MX** : Mail Exchange, Record pointant sur un serveur Mail
— **PTR** : Pointer records, utilisés pour mapper une ip à un nom de domaine, système inverse aux A records
— **NS** : Name Server record

La **Forward Lookup Zone** consiste à utiliser un nom de domaine pour trouver l'IP correspondante, et c'est le système inverse pour le **Reverse Lookup Zone**.

Un **F**ully **Q**ualified **D**omain **N**ame est un nom de domaine qui révèle la position absolue d'un noeud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine. Il se termine par un point final par convention.

Le **Host File** est un fichier utiliser par l'OS, il permet d'associer des noms d'hôtes à des adresses IP.

2 DHCP

Dynamic **H**ost **C**onfiguration **P**rotocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station (Adresse, Masque, Gateway, DNS).

Il tourne sur le port UDP **67** en server, et **68** en client.
Il fonctionne de la manière suivante :

— L'ordinateur équipé de carte réseau mais sans ip envoie en **broadcast** un datagramme pour le port 67 de tout serveur écoutant : **DHCP DISCOVER**
— Tout server ayant reçu le datagramme envoie une offre au client sur le port **68**, c'est un **DHCP OFFER**
— Le client retient l'offre et diffuse sur le réseau un datagramme de requête content l'ip proposée , c'est une **DHCP REQUEST**
— Le serveur établit un datagramme d'accusé de réception **DHCP ACK**.

Cette attribution des paramètres IP fonctionne sur base d'un bail d'une certaine durée.

Les serveurs DHCP sont configurés de manière a posséder un certain **pool** d'adresses qu'il peut offrir.

3 Web Server

Le Web Server est un serveur stockant et diffusant du contenu web par l'éxécution de requêtes HTTP, il est souvent associé à un serveur FTP.

— TCP 80 HTTP
— TCP 443 HTTPS
— TCP 20/21 FTP

4 File Server

Un **File Server** permet le partage de données sur un réseau, principalement via les protocoles suivants :

4.1 CIFS

Le Common Internet File System, anciennement SMB, est un protocole permettant le partage de ressources sur des réseaux locaux.

Il tourne sur le port 445 et permet aussi de partager des imprimantes.

4.2 NFS

Network **F**ile **S**ystem est un protocole qui permet à un ordinateur d'accéder à des fichiers via le réseau.

Il tourne sur le port TCP 2049.

5 Mail Server

Le Mail Server est un serveur de mailing, on retrouve principalement trois protocoles liés à son implémentation :

5.1 SMTP

Le protocole **Simple Mail Transfer Protocol** est un protocole de communication utilisé pour transférer le courrier mail d'un client SMTP vers les serveurs de messagerie électronique.

Celui-ci tourne sur les ports TCP 25 par défaut, et le port TCP 587 en SSL.

Le serveur est indiqué sur le serveur DNS par un MX record.

Les serveurs SMTP doivent être sécurisés afin d'éviter que celui-ci serve d'**open relay**, un relai ouvert pour les spammeurs.
Le problème de SMTP est le manque d'indentification des expéditeurs, qui peuvent donc utiliser votre serveur mal protégé pour diffuser leurs spams.

5.2 POP3

Post **O**office **P**rotocol **v3** permet la récupération du courrier électronique situé sur un serveur de messagerie électronique.
POP se connecte au serveur de messagerie, s'authentifie, récupère le courrier, peut effacer le courrier sur le serveur. Ceci est accomplissable via les commandes HELLO, USER, PASS, LIST, RETR, DELE, QUIT.

POP tourne sur :

— **TCP 110** par défaut
— **TCP 995** en mode sécurisé SSL

5.3 IMAP

Internet **M**essage **A**ccess **P**rotocol **v4** permet d'accéder à ses courriers mails directement sur les serveurs de messagerie.
Son fonctionnement est opposé à POP qui extrait les messages du serveur mail, IMAP effectue une synchronisation avec le serveur afin de créer des copies locales des mails et permettre d'éviter des pertes.

Il fonctionne sur les ports 143 par défaut et 993 en SSL.

Les opérations sont effectuables Online ou Offline, ce protocole est utilisé pour la mise en place des **WebMails**.

Chapitre 9

Sécurité

Nous allons dans ce chapitre aborder quelques points concernant la sécurité dans les réseaux :

1 Hardening & Stripping

C'est un processus visant à sécuriser un système en réduisant la surface d'attaque possible sur le système.
On va pour cela réduire à l'indispensable les services et applications qui tournent sur le système, ainsi qu'élimiter les utilisateurs et droits non indispensables à la gestion du serveur.
Le but est d'obtenir un système qui fournit que les fonctionnalités requises.

2 Audit

L'**audit** est l'identification est l'évaluation des risques associés aux activités informatiques d'une entreprise ou d'une administration.
L'audit se base sur un cadre réglementaire du secteur d'activité du pays ou sur les référentiels de bonnes pratiques existants.

3 Vulnerability Scan

Ce scan est une application permettant l'identification des vulnérabilités dans un système d'exploitation, une application ou un réseau.
Le but est de pointer et corriger les failles de sécurités avant leur exploitation par un pirate.

4 Penetration Testing

Ceci consiste en la simulation d'une attaque informatique sur le réseau d'une entreprise en vue d'évaluer la sécurité des systèmes.
Le **Pentest** tente de détecter les failles, mais également des les exploiter afin d'en évaluer les risques potentiels.

Chapitre 10

Monitoring

1 Principes et Objectifs

Le **Monitoring** consiste en la détection de pannes, le plus rapidement possible afin de pouvoir réduire le temps d'intervention.

Il aide également à résoudre des problèmes complexes en fournissant des informations pertinantes (logs), mais permet aussi de fournir une analyse de l'utilisation des ressources à long terme (Capacity Management).

Ce monitoring peut être **actif** ou **passif**.

2 Protocoles

Ce monitoring est accomplissable via un ensemble de protocoles et de services qui y sont liés :

— **ICMP** : Internet Control Message Protocol, utilisé pour véhiculer des messages de contrôle (ping)
— **WMI** : Windows Management Instrumentation, est un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle des ressources systèmes via un ensemble d'interface.
— **SSH**
— **SNMP**

3 SNMP

SNMP est un protocole utilisé dans le monitoring dont nous allons plus amplement parler ici.

Simple **N**etwork **M**anagement **P**rotocol est un protocole qui permet aux admin réseaux de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

3.1 Polling

Le **Polling** consiste en du monitoring actif où des requêtes sont envoyées à intervalles réguliers pour obtenir une valeur particulière.
Utilise **UDP** sur le port 161, utilisé pour créer une vue générale de tout le réseau.

Généralement un script est configuré pour comparer les valeurs du polling avec des valeurs espérées et détecter une anomalie.

Permet aussi de configurer des appareils en **WRITE MODE**.

3.2 Traps

Le mode **Traps** est du monitoring passif, il consiste à configurer un agent pour qu'il émette une alerte vers un autre agent appelé **trap host** en cas d'anomalie de monitoring.
Utilise **UDP** sur le port 162.

Utilisé pour des évènements spécifiques tels qu'une panne matérielle ou un changement de statut d'un équipement réseau.

3.3 MIB

Les **M**anagement **I**nformation **B**ases sont des fichiers textes qui décrivent les informations disponibles via SNMP sur l'appareil supervisé.

3.4 OID

Les **O**bjects **ID**entifiers sont des suites de nombres séparés par des points dont la séquence permet de naviguer au sein de la structure hierarchisée de la MIB.

3.5 Community String

En SNMPv2, des mots de passes sont utilisés pour s'authentifier auprès de l'appareil supervisé.

Ces mots de passes sont envoyés en clair, sauf si la version 3 est utilisée.

La Community String définit les droits possibles sur l'apareil supervisé.