UNIVERSITE DE DOUALA


FACULTE DES SCIENCES

Mathématiques et Informatique

COURS

D'ADMINISTRATION SYSTEME ET RESEAUX

Licence 3 Informatique

SSR 366

Par :

Dr NFONGOURAIN MOUGNUTOU R.

Année Académique 2023/2024

Plan du cours

Objectifs

- Connaitre le rôle et les exigences de l'administration des systèmes et réseaux
- S'initier à la pratique d'administration des systèmes et réseaux sous différents SEs

I.Introduction à l'administration

L'administration réseau, (de même que l'administration système) est une discipline qui ne s'enseigne pas, par contre elle s'apprend et le but de ce cours est de fournir un minimum d'éléments pour permettre d'orienter cet apprentissage. L'administration réseaux et systèmes ne s'enseigne- donc pas, parce ce sont des domaines bien trop vastes et qui évoluent trop rapidement pour que quiconque puisse le dominer de la tête et des épaules. De plus, le nombre de matériels et de logiciels est trop important pour qu'on puisse en faire une étude sérieuse. Chaque entreprise fait ses choix dans ce domaine et les administrateurs auront généralement à s'y plier. Le but d'un réseau informatique est d'assurer le transport des données de manière automatique. Il faut donc tendre vers les 100 % de disponibilité et arriver à minimiser l'impact des incidents et les interventions d'urgence par les protocoles permettant une gestion centralisée (DHCP, LDAP), les matériels redondants, les matériels de secours, le système de surveillance, etc. Le champ d'application étant plutôt étendu, nous nous limiterons à quelques technologies fondamentales, applicables aux réseaux IP dans l'environnement OSI et TCP/IP. Nous n'aborderons pas du tout la configuration des équipements actifs (*routeurs, commutateurs, etc.)*

I.1 Définition et finalités

L'administration de réseaux informatique (*ou Network management*) se réfère aux activités, méthodes, procédures comme la surveillance du réseau et aux outils de mise en œuvre par l'administrateur réseaux ayant trait à l'exploitation, l'administration, la maintenance et la fourniture des réseaux informatiques. La gestion des réseaux informatiques constitue un problème dont l'enjeu est de garantir au meilleur coût, non

seulement la qualité du service rendu aux utilisateurs mais aussi la réactivité dû aux changements et à l'évolution rapide du secteur informatique. Cette gestion des réseaux se définit comme étant l'ensemble des moyens mis en œuvre (*connaissances, techniques, méthodes, outils, ...)* pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût, de qualité et de matériel. La qualité de service se décline sur plusieurs critères pour le futur utilisateur, notamment la disponibilité, la performance (temps de réponse), la fiabilité, la sécurité… L'administration des réseaux est couramment classée en trois :

Supervision

La supervision consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes. Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des réseaux afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels. Plus le système est important et complexe, plus la supervision devient compliquée sans les outils adéquats. Une grande majorité des logiciels de supervision sont basés sur *le protocole SNMP* qui existe depuis de nombreuses années. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information ;
- Visualiser l'architecture du système ;
- Analyser les problèmes ;
- Déclencher des alertes en cas de problèmes ;
- Effectuer des actions en fonction des alertes ;
- Réduire les attaques entrantes.

La tâche de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée.

Administration

L'administration désigne plus spécifiquement les opérations de contrôle du réseau avec la gestion des configurations et de sécurité. De façon générale, une administration de réseaux a pour objectif d'englober un ensemble de techniques de gestion mises en œuvre pour :

- Offrir aux utilisateurs une certaine qualité de service;
- Permettre l'évolution du système en incluant de nouvelles fonctionnalités;
- Rendre opérationnel un système

Exploitation

De nos jours, les systèmes d'exploitation à savoir les systèmes UNIX, MacOs et Windows gèrent tous l'aspect de l'exploitation des réseaux, les procédures, et les fonctions associées. Un système d'administration réseau est une collection d'outils pour la supervision et le contrôle du réseau qui sont intégrés dans le sens qu'ils impliquent :

- Une interface opérateur unique avec un puissant, mais convivial ensemble de commandes pour exécuter toutes les tâches d'administration réseau ;
- Un nombre minimal d'équipements séparés qui sont le plus souvent des composants matériels et logiciels requis pour l'administration réseau, et incorporés dans les équipements utilisateurs existants.

I.2 Profile de l'administrateur réseau et système

Tout administrateur est un utilisateur ayant des privilèges spéciaux et des devoirs. L'administrateur système est en charge des serveur et l'administrateur réseau quant à lui doit exploiter gérer et maintenir la fourniture des réseaux informatique.

L'administration d'un réseau suppose l'existence d'un système d'information décrivant le réseau de l'entreprise et recensant toutes les données et événements relatifs à chaque constituant du réseau administré.

L'environnement de travail de l'administrateur réseau exige qu'il soit un spécialiste d'une pluralité technique, d'une flexibilité et de compétences humaines tout à fait particulières. En effet, les administrateurs réseau travaillent dans des environnements très variés, comprennent les grandes entreprises, les petites et moyennes entreprises, des institutions académiques et de formation, des organisations gouvernementales, du domaine de la santé ou à but non lucratif. La sensibilité et les défis des aspects centraux de l'administration varient d'un environnement à l'autre.

Les objectifs de l'administration des réseaux pour un administrateur :

- Supervision du fonctionnement des réseaux ;
- Optimisation pour l'utilisation des ressources ;
- Détection et prévision des erreurs ;
- Signalisation des pannes ;
- Calculs de facturations à l'utilisation des ressources ;

L'administrateur réseau est responsable de ce qui peut se passer dans un réseau c'est ainsi que les rôles d'un administrateur réseau consiste à :

- Mettre en place et maintenir l'infrastructure du réseau (organisation, ...) ;
- Installer et maintenir les services nécessaires au fonctionnement du réseau ;
- Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures) ;
- S'assurer que les utilisateurs n'outrepassent pas leurs droits ;
- Gérer les « logins » (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...) ;
- Gérer les systèmes de fichiers partagés et les maintenir

Pendant que la tâche d'administration réseau se réfère aux activités, méthodes, procédures ayant trait à l'exploitation, l'administration, la maintenance et la fourniture des réseaux informatiques, celle de l'administrateur système concerne les serveurs et systèmes informatiques.

II. Les fondamentaux des réseaux : rappels

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services. La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

II.1 Les éléments d'un réseau

II.1.1 Point de vue matériel

Quelque équipements/composants réseau

Nous présenterons les principaux composants des réseaux tels que les commutateurs, les routeurs et les pare-feu. De nombreux autres composants ne seront pas présentés car ne sont plus utilisés de nos jours.

Commutateur

Les commutateurs permettent d'accélérer les transferts au sein du réseau. Le bus interne (backplane) assurant la liaison dispose d'une bande passante suffisante, correspondant à la vitesse des ports et à leur nombre, pour relier simultanément tous les ports.

Le commutateur maintient une table de routage par port, ce qui permet de décider à quel port il doit transmettre une trame. Cette table peut être gérée de manière entièrement automatique, les stations devant s'identifier auprès du port à l'émission et le commutateur se contentant de mémoriser l'information. Si une station n'a encore rien émis, elle ne figure pas dans la table et le commutateur expédie la trame sur tous les

ports, comme lors d'une diffusion générale. On se rapproche alors du fonctionnement d'un concentrateur.

Il existe des commutateurs adaptés à différents types d'applications et qui, par conséquent, s'intègrent à différents niveaux du modèle OSI. Les commutateurs de couche 2 utilisent l'adresse physique de la trame ethernet pour la commutation. Parfois, certains moyens de communication récents tels que Voice over IP (système vocal sur l'Internet) exigent une bande passante que seul un commutateur peut assurer.

Les commutateurs de couche 3 relient les ordinateurs en fonction de leur adresse IP. Autrement dit, ils peuvent assurer la tâche des routeurs. Pour les applications où la durée d'acheminement des trames est critique, un commutateur de couche 3 peut apporter un gain appréciable de rapidité par rapport à un routeur. Cela ne concerne toutefois que les réseaux locaux, la capacité en mémoire des commutateurs ne leur permettant pas de gérer des tables de routage de la taille de celles couramment exploitées avec un routeur. De même, ce type de commutateurs n'est pas adapté à la gestion de réseaux complets car la commutation se fait sur la base de l'adresse IP complète et ils ne savent pas la subdiviser en adresse de réseau et adresse de machine. Enfin, ils ne peuvent échanger entre eux leur table de routage, si bien qu'une transmission intelligente de données en cas de panne de réseau est impossible.

Les commutateurs de couche 4 peuvent analyser l'application à l'origine des données. Le nom peut prêter à confusion car il ne s'agit pas de la couche 4 OSI, les différents protocoles n'implémentant pas la totalité des couches. Cette couche 4 correspond plutôt à une poursuite cohérente du développement des commutateurs. Selon l'application utilisée, ils peuvent proposer une qualité de service à l'utilisateur. Celui-ci décide d'une priorité pour les données d'une application et, par conséquent, de la bande passante dont elle disposera. Cela correspond à un gain de vitesse pour l'application. Parfois, seul un commutateur de niveau 4 autorise purement et simplement l'utilisation d'une application. Citons l'exemple d'applications multimédias pour lesquelles la garantie d'une bande passante minimale est la condition nécessaire à une projection fluide de

films ou la retransmission d'un son de haute qualité. La figure suivante illustre un commutateur.

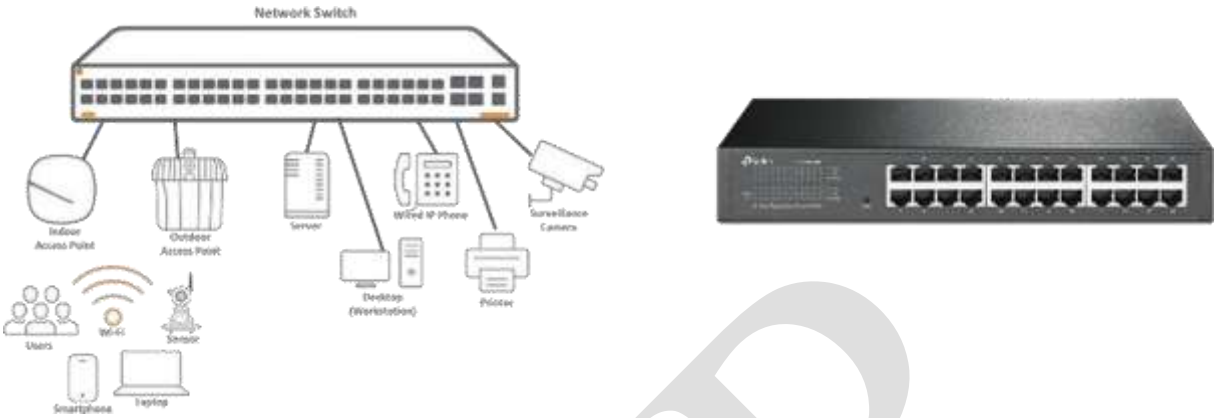


Figure 1 : Exemple de commutateur

Routeur

Les routeurs sont indépendants du matériel, c'est-à-dire qu'ils peuvent être équipés de cartes réseau de n'importe quelle architecture. Cela signifie aussi qu'ils peuvent relier des réseaux de types différents. Un routeur permet, par exemple, de relier un réseau ethernet et un réseau token ring, une ligne WAN ou FDDI ou encore un autre type de réseau. On distingue les routeurs monoprotocoles des routeurs multiprotocoles. Un routeur monoprotocole ne gère qu'un seul protocole, par exemple IP, indépendamment des interfaces réseau employées ou du fait que sa tâche consiste à effectuer des liaisons LAN/LAN, WAN/WAN ou LAN/WAN. Les routeurs monoprotocoles actuellement les plus courants sont les routeurs IP, exploités plus spécialement dans les réseaux d'entreprises ou les liaisons Internet.

Il existe différents algorithmes de routage. L'un s'appelle shortest path first (« d'abord le chemin le plus court »). La distance au réseau cible est évaluée en sauts au moyen des tables de routage, un saut correspondant à un passage par un routeur. Cet algorithme privilégie le chemin passant par un nombre minimal de routeurs. Un autre algorithme s'appelle open shortest path first (« d'abord le chemin libre le plus court »). Extension du premier, l'algorithme vérifie également si la voie proposée est libre. Un autre algorithme s'appelle lowest cost first (« d'abord le chemin le moins cher »). Cette

méthode du chemin le plus économique est particulièrement importante dans le cas des WAN. Une table s'ajoute à partir de laquelle il est possible de définir le coût d'un transport par un certain chemin.

Selon l'application, un routeur contiendra également un pare-feu (firewall) pour protéger le réseau d'accès extérieurs ou un moyen d'établir automatiquement une connexion avec un fournisseur d'accès Internet. Il existe donc des routeurs RNIS, ADSL et ATM qui comportent des mécanismes de filtrage.

Figure 2 : Exemple de routeur

L'interconnexion

Pour que la communication réseau soit opérationnelle, il faut tout d'abord interconnecter les matériels entre eux. Ceci est souvent effectué à travers une interface filaire, par exemple un câble connecté à une carte réseau ou à un modem. L'interface air peut également être exploitée, à travers des communications non filaires, en utilisant l'infrarouge, le laser ou les ondes radio.

Il existe différents médias de transport pour les réseaux.

- les **câbles coaxiaux** utilisés dans les réseaux locaux en bande de base ou pour la transmission urbaine et interurbaine à moyen et haut débit ;
- les **fils de cuivre** en paire torsadée utilisés pour la transmission locale en bande de base ou pour de faibles fréquences et sur de courtes distances ;
- les **paires torsadées** blindées utilisées en réseau local ou urbain pour des transmissions numériques ;

- les **fibres optiques** utilisées dans les réseaux locaux à haut débit, sur les liaisons interurbaines et sur les liaisons d'abonnés des réseaux publics numériques ;

- les **supports hertziens** (ondes radioélectriques) pour les applications urbaines et interurbaines de télécommunication (réseaux cellulaires ou boucle locale WiMAX par exemple) ainsi que pour les réseaux locaux sans fil (WLAN au standard WiFi) ou encore l'interconnexion des équipements personnels de type smartphone ou appareil photo (WPAN au standard Bluetooth) ;

- **les liaisons satellitaires** de télécommunication et de télédiffusion. Le tableau suivant résume les caractéristiques principales des supports usuels pour des transmissions en bande de base.

La paire torsadée est abordé dans le cadre de ce cours est constituée de paires de fils torsadés entre eux. C'est, à l'heure actuelle, le support privilégié des réseaux reposant sur ethernet. Ce câble est constitué de paires de fils électriques (en général, 4 paires pour la réseautique informatique). Ces câbles sont normalisés et catégorisés. Actuellement, la catégorie 5e s'impose.

La catégorie 5 (cat. 5) : permet un transfert de données jusqu'à 100 Mbps. La catégorie 5e (e pour enhanced, soit amélioré ou perfectionné) est conçue pour accepter le Gigabit Ethernet.

Pour ce qui est du blindage : il permet l'atténuation des perturbations électromagnétiques. L'UTP – Unshielded Twisted Pair ou câble UTP : paire torsadée non blindée, c'est le câble le plus utilisé en raison de son faible coût et de sa facilité de mise en œuvre. La STP ou SUTP – Screened Unshielded Twisted Pair : paire torsadée à blindage global, offrant une meilleure protection contre les parasites électromagnétiques. La FTP – Foiled Twisted Pair : paire dite à écran protecteur, puisqu'elle est protégée par une fine feuille d'aluminium.

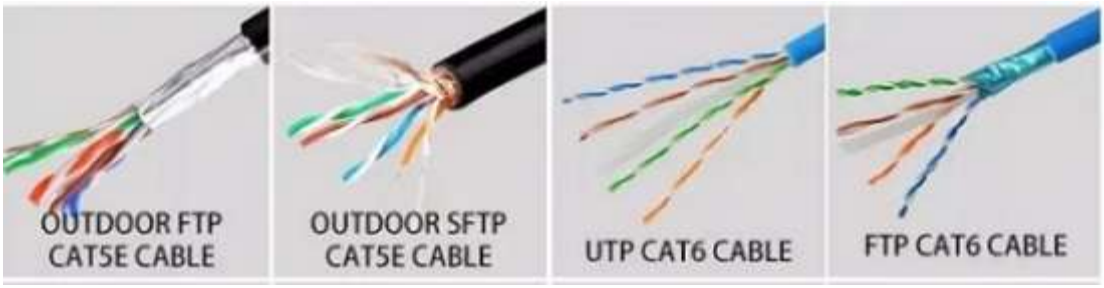


Figure 3 : Exemple de câble Cat 5E

Il existe deux normes de câblage. EIA 568 B est conseillée car répandue en Europe et la EIA 568 A répandue aux États-Unis. Ce qui est impératif, c'est de câbler chaque extrémité du câble de la même manière.

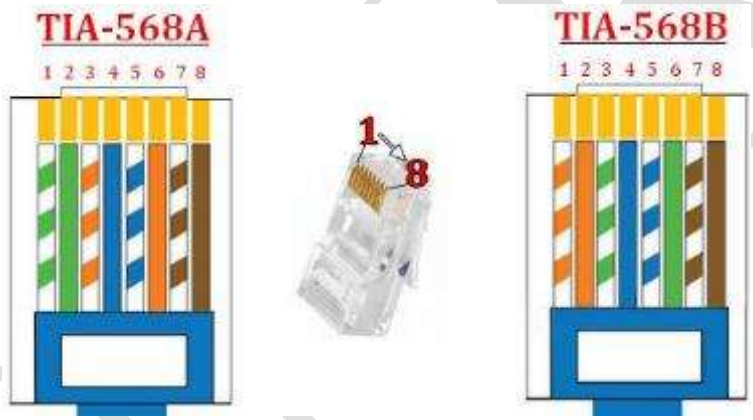


Figure 4 :Les normes de câblages des paire torsadés

Les protocoles de communication

En plus du matériel, qui assure la connectivité et l'échange des signaux sur le support, physique ou non, il est nécessaire d'utiliser des règles de communication. Ces protocoles permettent de donner un sens au signal qui circule entre les postes, et de gérer l'accès au support partagé.

Protocole	Port d'écoute
HTTP	TCP 80
HTTPS	TCP 443
TELNET	TCP 23
SSH	TCP 22
SMTP	TCP 25
POP3	TCP 110
FTP	TCP 21, TCP 20
TFTP	UDP 69
DNS	UDP 53
DHCP	UDP 67, UDP 68
NTP	UDP 123
RIP	UDP 520

Figure 5 : Quelques protocoles et ports associés

II.1.2 Les ressources

L'objectif premier des réseaux est la mise en commun de ressources, assurant notamment le partage de l'information. En informatique, celle-ci existe sous différentes formes : Fichiers, Documents, et Données.

Un ensemble de services réseaux apporte les fonctionnalités désirées. Ils sont fédérés, bien souvent, par le système d'exploitation réseau, qui fait remonter l'information vers des applications spécifiques aux services gérés.

Les services de fichiers

Les premières formes d'informations manipulées à travers les applications réseaux sont les fichiers. Ils sont stockés dans des arborescences de dossiers (Windows), de répertoires (UNIX/Linux) ... Un fichier contient des informations, de différentes formes présentées de manière libre, non structurée. Les services de fichiers effectuent quatre fonctions essentielles : le stockage, transfert et la copie, synchronisation, et sauvegarde et l'archivage...

Les services de gestion électronique de documents

Les documents informatiques contiennent des informations semi-structurées, c'est-à-dire sans organisation prédéfinie, mais dont le contenu peut être exploité électroniquement (recherche de mots-clés...). Ils peuvent parfaitement être issus de documents papiers scannés et prendre la forme de fichier (ou non).

Secondant ceux de services de fichiers, les applicatifs de gestion électronique de documents (GED) permettent un traitement de l'information sous cette forme spécifique. L'organisation est plus précise que la simple arborescence de fichiers et l'exploitation est plus proche de l'information contenue. La notion de fichiers et leur manipulation devient transparente pour l'utilisateur. Grâce aux services de GED, la donnée informatique, sous forme d'écrits, de sons, de vidéo, d'images de graphiques..., est accessible à travers le réseau. Elle peut l'utiliser pour circuler, à travers des cheminements prévus par des procédures (workflow).

Le terme gestion électronique d'information et de documents existants (GEIDE) désigne, complémentairement, la récupération des archives de l'entreprise, sous format électronique. Ces informations numérisées sont ensuite gérées dans une telle application. La scénarisation de l'information papier est désormais courante et les outils sont devenus très performants (reconnaissance de texte, de photos, de plans...).

Services de base de données

Les bases de données autorisent l'utilisation d'informations électroniques sous forme structurée. Leur but est double :

- Proposer la saisie de renseignements dans un schéma prédéfini (par exemple dans les champs d'un formulaire) ;
- Permettre l'exploitation optimale de ceux-ci, classés dès la saisie.

Le stockage des données s'effectue le plus souvent au sein de bases centralisées. Des applicatifs dédiés permettent l'accès aux informations et leur exploitation (statistiques, recherches...).

Il existe plusieurs familles de systèmes de gestion de bases de données. Par exemple, la gestion des systèmes de fichiers est souvent assurée par un tel service. Les annuaires informatiques reposent également sur une base de données, optimisée en lecture. Le langage standard pour effectuer des requêtes de lecture et d'écriture dans de telles bases est LDAP (Lightweight Directory Access Protocol).

La manipulation de données sous forme de tables, qui peuvent être dépendantes les unes des autres, est le propre des systèmes de gestion de bases de données relationnelles (SGBDR), ou Relational DataBase Management System (RDMS). La programmation de requêtes standard s'effectue ici en langage SQL (Structured Query Language).

Services de stockage et de sauvegarde

Les entreprises gèrent désormais des quantités d'informations (fichiers, documents et données) de plus en plus importantes. Le stockage des données et leur mise à disposition aux utilisateurs est devenu une problématique à part entière.

De nouvelles solutions, qui permettent réellement de dédier des espaces de stockage ou de sauvegarde performants et suffisants, sont donc apparues. Quelque peu onéreux à leur début, ces systèmes ont su évoluer et sont dorénavant également intéressants pour des entreprises de petite taille.

Un serveur NAS s'intègre au réseau existant de l'entreprise, au même titre que les autres serveurs (application, base de données...). Il fournit des services comparables à ceux d'un serveur de fichiers, mais reste généralement dédié.

Ainsi, il n'a pas besoin d'un processeur puissant ni de beaucoup de mémoire vive. Par contre, il embarque un espace de stockage très conséquent, sécurisé par des solutions de type RAID, dont nous reparlerons plus loin.

Son système d'exploitation peut être spécifique, tel que le propose Microsoft avec « Windows Storage ». Gérant plusieurs protocoles de communication, un serveur NAS sécurise l'accès aux ressources et assure un accès à travers le réseau, indépendamment du type de client.

Cette technologie présente différents avantages :

- Coût d'achat inférieur à un serveur de fichiers traditionnel ;
- Augmentation de la sécurité des données liée aux redondances matérielles associées ;
- Mise en œuvre simplifiée et réduction du temps d'administration des serveurs ;
- Serveur universel au sein d'un réseau hétérogène.

Par extension, un serveur NAS peut servir de destination de sauvegarde et remplacer une unité à bandes. En effet, sa connexion directe au réseau de l'entreprise permet de le placer dans un bâtiment éloigné des autres serveurs, sécurisant ainsi les données sauvegardées sans manipulation de média amovible.

Une autre exploitation possible de serveurs NAS peut être la mise en place de deux unités dans deux salles informatiques distantes. Par synchronisation permanente de leurs données, la redondance de l'information est ainsi assurée à un coût très raisonnable. Si l'un des serveurs tombe en panne, les utilisateurs peuvent continuer de travailler en allant chercher les données sur celui restant opérationnel.

Les services d'application

Ils permettent, non seulement le partage des données, mais aussi celui de la puissance de traitement. L'objectif principal est la spécialisation des serveurs en inter-réseau, de manière à répartir au mieux les tâches sur les machines les plus appropriées.

II.1.3 Point de vue logiciel

D'un point de vue logiciel, les ordinateurs reliés à un réseau sont répartis en deux catégories, en fonction des actions qu'ils effectuent sur celui-ci.

Un *client* est demandeur de services. Ce peut être, par exemple, un poste de travail utilisateur demandeur de services d'applications, de fichiers, d'impression... Ces services sont offerts par une entité logicielle qualifiée de *serveur*.

Système d'exploitation réseau

Le système d'exploitation réseau est un système complexe constitué de différentes couches logicielles (protocoles de communication, couche application...). Il permet à plusieurs personnes interconnectées (physiquement) de travailler avec les mêmes ressources.

Il fournit un contrôle d'accès au réseau (sécurité de connexion, sécurité d'accès aux ressources), tout en coordonnant les accès simultanés (en gérant bien souvent des files d'attente pour tous les périphériques exclusifs).

En évoluant, les systèmes d'exploitation réseau ont acquis un certain nombre de capacités complémentaires. Par exemple, tous les logiciels Windows offrent des services de fichiers, d'impression et d'hébergement/distribution de site Web, sans installation de logiciels tiers. Bien sûr, les possibilités offertes par les versions destinées aux utilisateurs finaux sont bien inférieures.

C'est souvent le système d'exploitation réseau (NOS - Network Operating System) ou SER (Système d'Exploitation Réseau) qui va dicter l'architecture du réseau. Comme exemple de système d'exploitation, on distingue les systèmes organisés autour d'un serveur de ceux basés sur une architecture d'égal à égal.

- **Poste à poste** : Dans le cas où tous les postes ont un rôle identique et sont à la fois clients pour des ressources et serveurs pour d'autres, on parle de réseau d'égal à égal, de pair à pair (peer-to-peer), ou encore de poste à poste. Dans ce type de structure, regroupant en général peu de postes, les ressources, les opérations de sécurité, les tâches d'administration sont réparties sur l'ensemble du réseau. Le contrôle centralisé est donc rendu impossible. Chaque utilisateur est souvent administrateur de son propre poste. Ce type d'organisation suppose que les utilisateurs ne soient pas complètement néophytes pour pouvoir travailler dans un environnement correctement structuré.
- **Réseau centralisé** : Chaque utilisateur dispose d'un nom et d'un mot de passe qu'il doit fournir au moment de l'ouverture de session sur le réseau, en vue d'être

authentifié. La base de données des utilisateurs du réseau est centralisée. Un autre inconvénient est que l'on ne peut pas centraliser la gestion des utilisateurs sur une base de données unique du réseau, c'est-à-dire que l'on ne peut pas contrôler l'accès aux ressources en fonction des noms d'utilisateurs. Il est ainsi possible de contrôler l'accès aux ressources en utilisant une sécurité au niveau utilisateur : c'est-à-dire que des permissions sont individualisées pour chaque utilisateur pour chacune des ressources disponibles. Il est ainsi beaucoup plus facile de savoir qui fait quoi et à quel moment. Un utilisateur particulier est nommé administrateur. Il a pour fonction de gérer l'ensemble des ressources du réseau. C'est l'utilisateur qui a le plus de pouvoir sur l'ensemble du réseau

II.2 Concepts généraux des réseaux

Un réseau est constitué d'équipements appelés nœuds. En fonction de leur étendue et de leur domaine d'application, ces réseaux sont catégorisés.

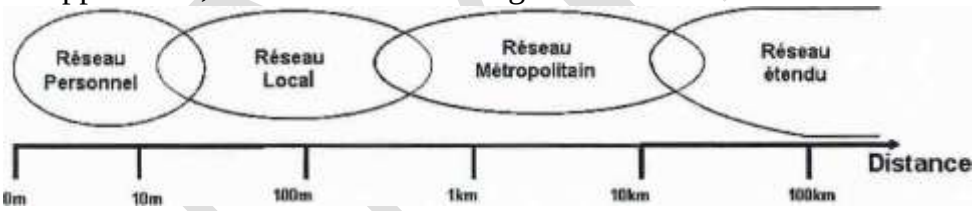


Figure 6 : Types de réseaux informatiques

Le réseau personnel

La plus petite étendue de réseau est nommée en anglais Personal Area Network (PAN). Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le Personal Operating Space (POS). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

Le réseau local

De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français réseau local d'entreprise (RLE), relie entre eux

des ordinateurs, des serveurs... Il est couramment utilisé pour le partage de ressources communes, comme des périphériques, des données ou des applications.

Le réseau métropolitain

Le réseau métropolitain, ou Metropolitan Area Network (MAN), est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments, distants de quelques dizaines de kilomètres.

Le réseau étendu

Les étendues de réseaux les plus conséquentes sont classées en WAN, acronyme de Wide Area Network. Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est le réseau public Internet, dont le nom provient de cette qualité : Inter Networking, ou interconnexion de réseau.

II.2.1 Normes et protocoles

Un aspect important dans l'ouverture des réseaux a été la mise en place d'un modèle de référence, le modèle OSI. Celui-ci définit un modèle en sept couches réseau, présentes sur chaque station qui désire transmettre. Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes. Même si le modèle OSI est très peu implémenté, il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant réseau. Ainsi, paradoxalement aujourd'hui, TCP/IP est mis en œuvre partout et même lorsque l'on parle de ce protocole on l'associe aux couches du modèle OSI (postérieur de 10 ans au modèle TCP/IP).

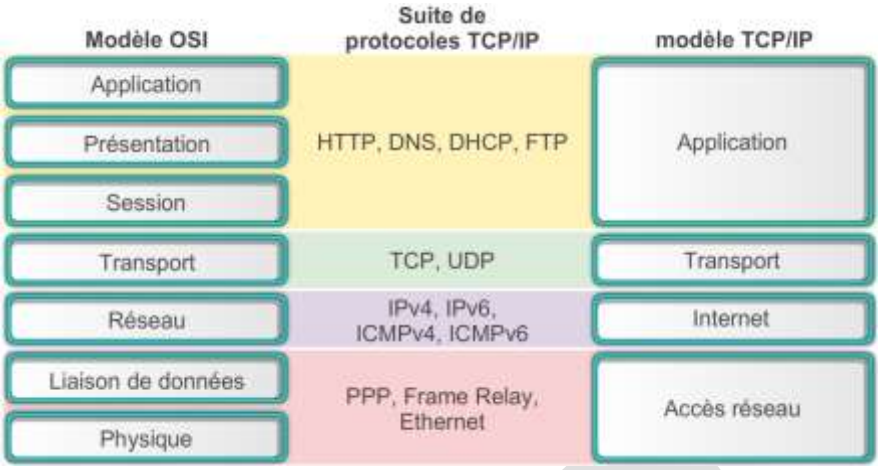


Figure 7 : Modèles OSI vs TCP/IP

La **couche Physique**. Elle a pour rôle la transmission bit à bit sur le support, entre l'émetteur et le récepteur, des signaux électriques, électromagnétiques ou lumineux, qui codent des données numériques (0 ou 1). Des matériels comme les modems (modulateur/démodulateur), les répéteurs ou la connectique des cartes réseaux, RJ45 par exemple, se placent à ce niveau.

La **couche Liaison** (ou Liaison de données). C'est au niveau de cette couche que les données numériques sont traduites en signal. Les bits de données sont organisés en trames. Un en-tête est créé dans lequel on peut identifier l'émetteur et le destinataire par leur adresse physique. Au niveau de cette couche est ajouté un code de redondance cyclique (CRC - Cyclic Redundancy Code) qui permet de détecter certains problèmes de transmission. Ainsi, le destinataire d'une trame recalcule la somme et la compare avec celle qui a été transmise. S'il y a une différence, la trame est rejetée.

La **couche Réseau.** C'est au niveau de cette couche qu'est géré le choix du meilleur chemin (lorsqu'il en existe plusieurs) pour atteindre le destinataire. Alors que l'adresse physique sert à identifier un périphérique local, une adresse logique permet de référencer un composant de manière globale.

La **couche Transport**. Il s'agit du cœur du modèle OSI. Au niveau de cette couche, différents mécanismes sont mis en œuvre pour établir un mode connecté, c'est-à-dire un moyen de s'assurer que les informations ont toutes été transmises et sans problème. Un

premier niveau de connexion consiste à accuser réception systématiquement de tous les paquets reçus, et cela, dans un délai suffisant (deux fois la durée aller et retour normalement nécessaire), faute de quoi le paquet est retransmis, car il est considéré comme égaré.

La **couche Session**. Cette couche gère également un mode connecté. C'est à son niveau que sont gérés les points de synchronisation, permettant ainsi, par une sauvegarde de contextes et de sous-contextes, une reprise en cas d'incident.

La **couche Présentation.** Elle assure la mise en forme des données : paramètres internationaux, pages de codes, formats divers… Cette couche peut également exploiter des fonctions de chiffrement et de compression.

La **couche Application.** Cette couche assure l'interface de communication avec l'utilisateur, à travers des logiciels adéquats. Elle gère également la communication entre applications, comme pour le courrier électronique.

II.2.2 Architectures réseaux

Aujourd'hui, les réseaux sont constitués d'ordinateurs et de systèmes d'exploitation hétérogènes. Ils sont très souvent interconnectés à travers l'Internet. La répartition de puissance est désormais multiple, à travers des architectures comprenant différents étages (tiers). La puissance de traitement au niveau de l'utilisateur est utilisée

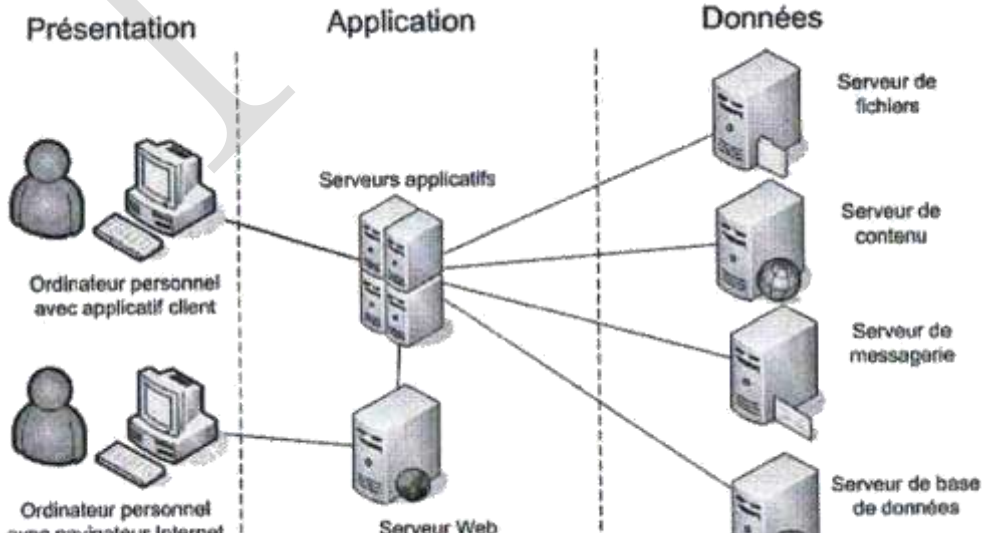


Figure 8 : Architecture 3tiers

essentiellement pour la mise en forme des informations reçues, quand une couche intermédiaire gère les applications. Celles-ci sont devenues indépendantes des données, réparties sur un à plusieurs autres niveaux. Le schéma suivant représente une architecture à trois étages (3 tiers) ou 3/3.

Avec l'utilisation d'une infrastructure SAN, cette architecture peut même contenir un étage supplémentaire et, par exemple, devenir 4 tiers.

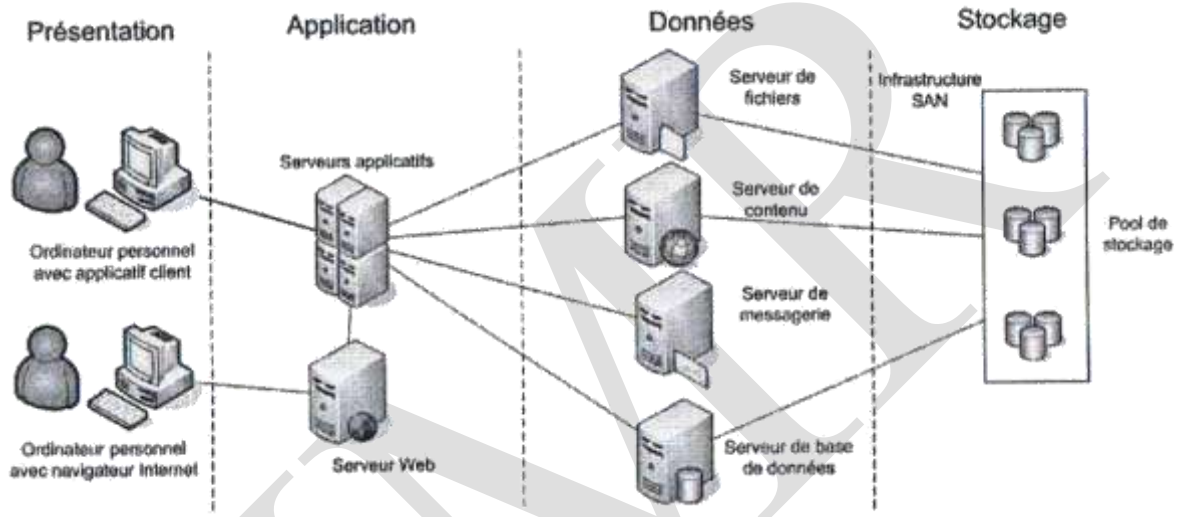


Figure 9 : Architecture 4tiers

L'architecture réseau un donc un élément crucial dans une infrastructure réseau, il désigne aussi bien les **technologies**, les **services** associés et les **protocoles** (langages) mis en œuvre qui vont permettre d'acheminer les messages entre les différents éléments du réseau. Il doit également répondre aux besoins croissant des utilisateurs tel que la tolérance au pannes, l'évolutivité, la sécurité et la QoS.

Tolérance au pannes

Même lorsqu'on met en place une infrastructure réseau fiable et robuste, de multiples aléas peuvent survenir. Piratage, brusque montée en charge, accident matériel, catastrophe naturelle, erreur humaine… Tous ces facteurs sont susceptibles d'entraîner des pannes et de peser sur la productivité des entreprises. Un réseau informatique à haute disponibilité offre un bon niveau de fiabilité grâce à la tolérance aux pannes.

La haute disponibilité d'un réseau informatique peut être assuré via des techniques telles que :

- load balancing (répartition de charge): distribuer intelligemment les flux sur plusieurs équipements, de sorte à éviter leur surcharge
- clustering (regroupement en grappes): mettre en commun plusieurs équipements, tels que des serveurs, qui fonctionnent comme un seul et même système.
- failover (basculement): rediriger une requête d'un serveur à un autre, lorsque le premier est confronté à une panne.

Evolutivité et QoS

Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.

La qualité de servite désigne les mécanismes utiliser pour contrôler le trafic et assurer la performance des applications. Vous pouvez hiérarchiser le trafic au sein de votre réseau à l'aide d'une configuration QoS personnalisée. En principe, le contrôle du trafic réseau sortant d'une interface est plus aisé que le contrôle du trafic réseau entrant. L'exemple que nous allons traiter ici concerne directement la gestion de la bande passante. Cette gestion se fera via des files d'attente basées sur du *Class Based Queueing* (CBQ). CBQ est une file d'attente permettant de stocker d'autres files en fonction des classes pré-déterminées. La figure suivante illustre Réservation ou limitation de bande passante (CBQ) pour le trafert de fichier en FTP et sur One Drive.

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
Type: CBQ						
MOD_WAN_Q	CBQ	10 Mbits	unlimited	10 Mbits	20 Mbits	Microsoft OneDrive Queue
FTP_WAN_Q	CBQ	10 Mbits	20 Mbits	10 Mbits	20 Mbits	File transfer Queue

Figure 10 : Définition d'une file d'attente CBQ

Sécurité

En matière de sécurité des réseaux, deux points doivent être pris en considération : **la sécurité de l'infrastructure réseau** et la **sécurité du contenu.** Pour assurer une protection optimale, les FW professionnels ont recourt à deux modes de protection qui agissent de façon cohérente et complémentaire.

- ✓ **Protections automatiques:** Les protections automatiques protègent l'activité système et réseau au niveau du poste Client.
- ✓ **Protection par règles,** La protection par règles permet de définir une politique spécifique à chaque entreprise. L'administrateur est responsable de la mise en place de cette politique en indiquant de manière explicite les droits et les interdictions d'accès aux ressources du poste Client.

La figure suivante illustre la définition d'une règle de filtrage. Dès que les éléments du paquet correspondent à une règle dans un niveau, l'action de la règle (bloquer ou autoriser) est appliquée et le paquet n'est plus confronté aux règles suivantes.

Status	Action	Source	Destination	Dest. port	Protocol	Security
on	pass	LAN_Clients	WAN_FTP_Server	ftp		IPS

Figure 11 : Exemple de règle de filtrage dans les FW SNs

III. Exploitation des réseaux

Le domaine informatique est confronté au même problème. Un environnement réseau doit disposer d'informations sur les utilisateurs, les ordinateurs, les adresses IP, les imprimantes... La liste est longue, et une préoccupation majeure est de centraliser ces

informations pour éviter les redondances, amenant à des confusions éventuelles, du travail supplémentaire pour les mises à jour et des risques majeurs de perte par absence de sauvegarde. Les annuaires ont été conçus pour tenter de résoudre ces problèmes

III.1Services d'annuaire

Un service d'annuaire diffère d'un simple répertoire, en ce sens qu'il contient des données, plus des services permettant aux utilisateurs d'accéder à ces données. Étant à la fois un outil d'administration et un outil pour l'utilisateur final, un service d'annuaire doit satisfaire aux besoins suivants :

- Accès à tous les serveurs, à toutes les applications et à toutes les ressources par le biais d'une ouverture de session unique (l'utilisateur n'accède effectivement aux ressources que s'il dispose des autorisations adéquates).
- Réplication multimaître. Toutes les données sont distribuées sur l'ensemble du système informatique et répliquées sur plusieurs serveurs.
- Recherches de type « pages blanches », par exemple pour faire une recherche à partir d'un nom ou d'un type de fichier.
- Recherches de type « pages jaunes », par exemple pour rechercher toutes les imprimantes du troisième sous-sol ou tous les serveurs du site Lyon.
- Suppression de la dépendance vis-à-vis des emplacements physiques, à des fins d'administration. Cela signifie qu'il doit être possible de déléguer l'administration de l'annuaire, partiellement ou complètement.

III.1.1 Notions

Un annuaire est un ensemble d'informations, dont les principales caractéristiques sont les suivantes :

- **Optimisation pour la consultation**. Un annuaire est souvent confondu avec une base de données. Une différence majeure tient à l'optimisation en consultation d'un annuaire, alors qu'une base de données doit fournir des performances semblables en écriture et en lecture.
- **Modèle de stockage distribué**. Un annuaire peut répartir ses données sur plusieurs serveurs, avec une organisation hiérarchique ou non. Cette façon de stocker les informations permet une délégation des responsabilités ; par exemple, l'administrateur d'un serveur DNS gère seul les domaines dont il a la charge, et les informa¬tions sont accessibles dans le monde entier. Elle permet également d'assurer la tolérance aux pannes et la répartition de charge, car la même information peut être accessible à plusieurs endroits.
- **Extensibilité des informations stockées**. Un annuaire stocke des données dont la structure peut être étendue sans perdre les entrées déjà définies. Par exemple, on peut ajouter dans les informations d'un domaine Internet des enregistrements de type serveur, permettant d'interroger le DNS pour trouver une machine assurant un service particulier. C'est ce qui est mis en oeuvre dans Active

Directory pour que toute machine du domaine puisse localiser les contrôleurs de domaine.

- **Recherche avancée**. Un annuaire fournit des mécanismes de recherche permettant d'extraire une partie des informations, en fonction de critères plus ou moins détaillés. Par exemple, le système DNS est employé par les serveurs de messagerie pour obtenir la liste des MX (Mail Exchanger) d'un domaine, c'est-à-dire les serveurs SMTP à qui envoyer les mails pour le domaine considéré.

Services d'annuaire et X.500

X.500 est une norme de services d'annuaire, créée par l'ITU (*International Telecommunications Union*). Cette même norme est également publiée par la commission ISO/IEC (*International Standards Organization/International Electrotechnical Commission*). X.500 définit le modèle de données employé par les services d'annuaire. Dans ce modèle, toutes les données d'un annuaire sont stockées dans des rubriques (entrées), dont chacune appartient à au moins une classe d'objet. Les données proprement dites d'une rubrique sont définies à l'aide d'attributs contenus dans cette rubrique. La norme X.500 d'origine de 1988 se concentrait principalement sur les protocoles à implémenter. DAP (*Directory Access Protocol*) spécifie comment les applications des utilisateurs accèdent aux informations de l'annuaire. DSP (*Directory Service Protocol*) propage entre les serveurs d'annuaire la requête d'un utilisateur si le serveur local ne peut répondre à cette requête.

III.1.2 Active directory

Aucun service d'annuaire existant n'implémente entièrement la norme X.500, mais tous les services d'annuaire, en particulier Active Directory, s'appuient sur ses spécifications fondamentales.

Active Directory permet d'administrer, depuis un même emplacement, toutes les ressources publiées : fichiers, périphériques, connexions d'hôte, bases de données, accès web, utilisateurs, autres objets quelconques, services, etc. Active Directory emploie le protocole DNS comme service de localisation, organise les objets des domaines dans une hiérarchie d'unités organisationnelles (OU, *organizational unit*) et permet de regrouper plusieurs domaines au sein d'une arborescence. Exit les concepts de contrôleur principal de domaine (PDC) et de contrôleur secondaire de domaine (BDC).

Terminologie et concepts d'Active Directory

Certains des termes utilisés pour décrire des concepts d'Active Directory existant déjà depuis un certain temps dans d'autres contextes, il est important d'en connaître la signification dans le contexte spécifique d'Active Directory.

Attribut

Un *attribut* est un élément de données qui décrit un certain aspect d'un objet. Un attribut se compose d'un type et d'une ou plusieurs valeurs. « Numéro de téléphone » est un exemple de type d'attribut, dont la valeur pourrait être « 33-2-37519964 ».

Objet

Un *objet* est un ensemble particulier d'attributs qui représente quelque chose de concret, par exemple un utilisateur, une imprimante ou une application. Les attributs contiennent des données qui décrivent l'entité identifiée par l'objet d'annuaire. Les attributs d'un utilisateur sont, par exemple, le nom, le prénom et l'adresse de messagerie. La classification de l'objet indique quels sont les types d'attributs utilisés. Par exemple, les objets classifiés comme « utilisateurs » permettent d'employer des types du genre « nom de famille », « numéro de téléphone » et « adresse de messagerie », alors que la classe d'objets « entreprise » permet d'employer des types du genre « nom de la société » et « secteur d'activité ». Un attribut peut prendre une ou plusieurs valeurs, selon son type.

Dans Active Directory, chaque objet possède une identité unique. On peut déplacer ou renommer les objets, mais leur identité est invariable. En interne, les objets sont référencés par leur identité et non par leur nom. L'identité d'un objet est un GUID (*Globally Unique IDentifier*), assigné par le DSA (*Directory System Agent*) lors de la création de l'objet. Le GUID est stocké dans un attribut, *objectGUID*, commun à tous les objets. Vous ne pouvez ni modifier, ni supprimer l'attribut *objectGUID*. Quand vous stockez dans un magasin externe (par exemple, dans une base de données) une référence à un objet Active Directory, utilisez de préférence *objectGUID* qui, contrairement au nom, ne change jamais.

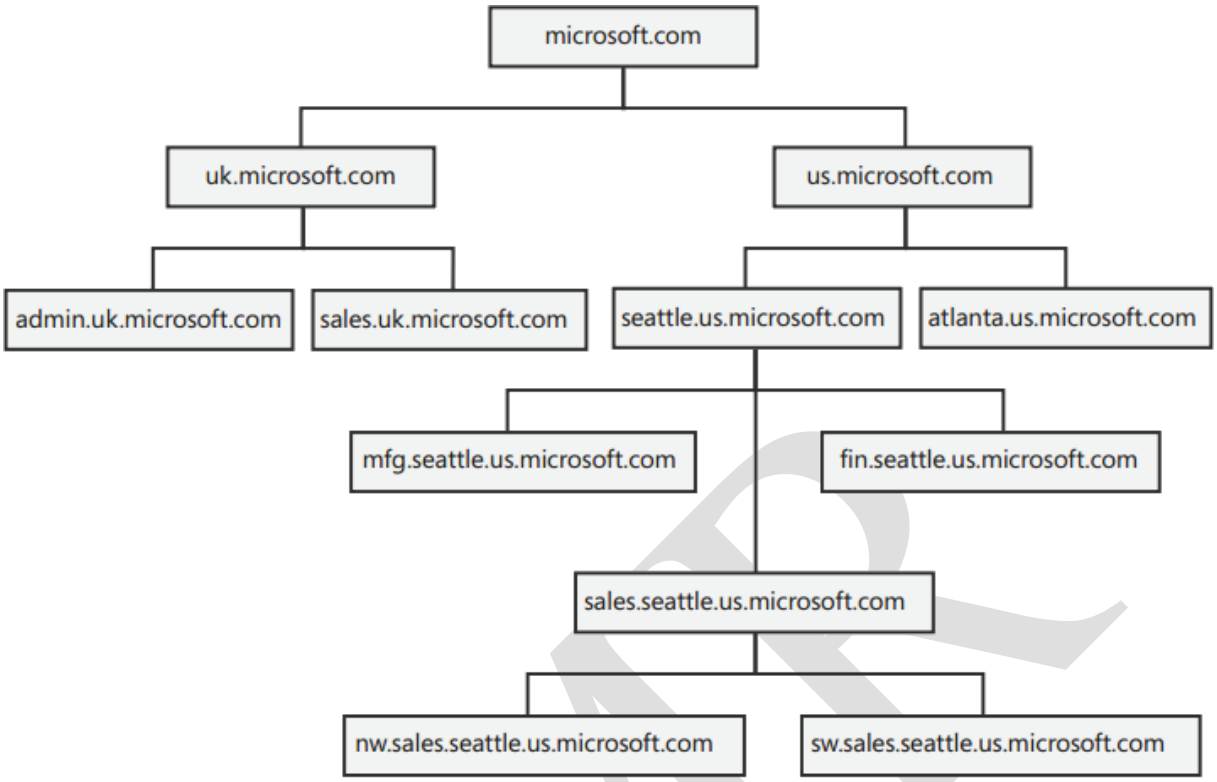
Conteneur

Un *conteneur* ressemble à un objet en ce sens qu'il possède des attributs et qu'il fait partie de l'espace de noms d'Active Directory. Toutefois, contrairement à un objet, un conteneur ne correspond à rien de concret. C'est simplement une enveloppe, qui renferme des objets et d'autres conteneurs.

Arborescence et sous-arborescence

Dans Active Directory, une *arborescence* étend le concept d'arborescence de répertoires. C'est une hiérarchie d'objets et de conteneurs qui montre les relations entre les objets, c'est-à-dire les chemins par lesquels on passe d'un objet à un autre. Les points terminaux d'un arbre sont, en général, des objets.

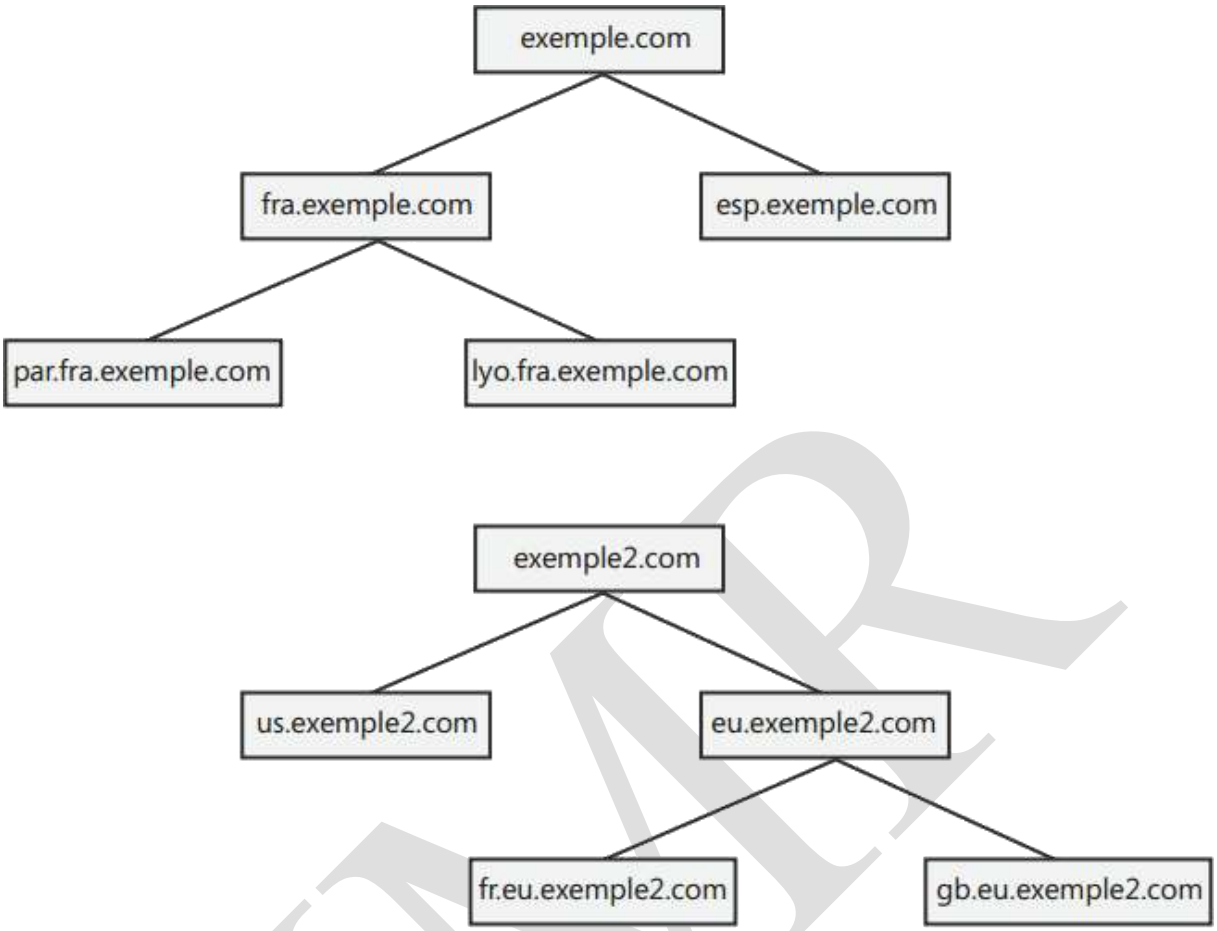
Une sous-arborescence est un sous-ensemble non isolé de l'arborescence, contenant tous les membres de chacun des conteneurs qu'il renferme.



Une arborescence et des sous-arborescences

Forêts

Un espace de noms en forêt, comme celui de la figure suivante, est un regroupement d'arborescences pour l'essentiel égales, sans que l'espace de noms ne possède de racine unique. L'espace de noms en forêt convient particulièrement à une organisation qui présente plusieurs secteurs d'activité, chacun disposant de son propre nom identifiable. Il s'agit généralement de grandes sociétés et en particulier celles qui se développent par le biais de l'acquisition. Elles ne possèdent en général pas de groupe central et unique qui gère la totalité de l'organisation et chacune des divisions a ses propres identité et infrastructure.



Une forêt est un regroupement d'arborescences individuelles qui n'appartiennent pas à un espace de noms contigu.

Nom unique

Chaque objet, dans Active Directory, possède un *nom unique* (DN, *distinguished name*). Le nom unique identifie le domaine contenant l'objet, ainsi que le chemin complet utilisé pour atteindre l'objet à travers la hiérarchie des conteneurs. Par exemple, CN=Charlie Russel, OU=Ingénierie, DC=monentreprise, DC=com est un nom unique, lequel spécifie que l'objet utilisateur « Charlie Russel » appartient à l'OU Ingénierie qui, elle-même, appartient au domaine monentreprise.com

Schéma

Schéma est un terme très fréquemment employé dans le contexte des bases de données. Dans celui d'Active Directory, le schéma correspond à tout ce qui constitue l'annuaire Active Directory : les objets, les attributs, les conteneurs, etc. Active Directory possède un schéma par défaut qui définit les classes d'objets les plus courantes : utilisateurs, groupes, ordinateurs, unités organisationnelles, stratégies de sécurité et domaines. Le schéma d'Active Directory est susceptible de modifications dynamiques : une application peut compléter le schéma en y ajoutant de nouveaux attributs et de nouvelles classes, puis utiliser ces ajouts dans la foulée. La modification du schéma repose sur la

création d'objets de schéma ou la modification des objets de schéma stockés dans l'annuaire. Les objets de schéma sont protégés par des ACL, afin que seules les personnes habilitées (membres du groupe Admins du schéma) puissent modifier le schéma

Unités d'organisation

Le concept d'unité d'organisation a été introduit pour la première fois dans Windows 2000. Elle possède certaines des caractéristiques d'un domaine, mais sans sa charge de ressources. L'OU est comprise dans un domaine et agit comme un conteneur d'objets du service d'annuaire. Elle forme une branche de l'espace de noms LDAP (*Lightweight Directory Access Protocol*) continu, mais pas nécessairement de l'espace de noms DNS et elle peut également contenir d'autres OU. Ainsi, le domaine *entr.microsoft.com* peut contenir d'autres domaines, comme *finance.entr.microsoft.com*, et des unités d'organisation telle que l'unité « rh » de *entr.microsoft.com*. Ici, le nom LDAP serait « OU=rh,DC=finance,DC=entr,DC=microsoft,DC=com » mais le nom DNS resterait *entr.microsoft.com*, sauf si on le modifie explicitement.

L'OU établit une frontière administrative appropriée et vous pouvez déléguer des droits et des privilèges d'administration à des utilisateurs d'une OU sans compromettre le reste du domaine. Cependant, une OU ne requiert pas de contrôleur de domaine séparé et elle n'intervient pas dans la réplication.

Domaines

L'unité fondamentale du service d'annuaire Active Directory de Windows Server 2008 est le domaine, exactement comme dans Windows Server 2003 et Microsoft Windows NT 4. Tous les objets du réseau existent comme partie du domaine et la stratégie de sécurité y est uniforme. Contrairement à Windows NT, la sécurité dans Windows 2000, Windows Server 2003 et Windows Server 2008 repose sur la version 5 de Kerberos et les relations d'approbation sont transitives. Cela signifie que si le domaine A approuve le domaine B et que si le domaine B approuve le domaine C, le domaine A approuve également le domaine C

III.1.3 LDAP

LDAP (Lightweight Directory Access Protocol) a été conçu comme une adaptation TCP/IP du protocole DAP pour l'interrogation des annuaires X.500 sur les postes clients. X.500 est un ensemble de normes, qualifié de lourd, qui s'appuie sur le modèle des sept couches du protocole OSI. LDAP génère un trafic réseau très réduit, offrant moins de possibilités que X.500, d'où le qualificatif "léger".

LDAP est devenu en 1995, un annuaire natif (standalone LDAP) sous l'im¬pulsion d'une équipe de l'université du Michigan (logiciel U-M LDAP).

LDAP est aujourd'hui en version 3 et est défini par dix documents de base et documents complémentaires. Les RFC 4510 à 4519 ont remplacé en juin 2006 les anciennes

versions : RFC 3377, RFC 2251 à 2256, RFC 2829 et RFC 2830, qui apparaissent en référence un peu partout et que vous continuerez à rencontrer pendant un certain temps.

LDAP emploie une approche client/serveur classique, en mode connecté avec le protocole TCP, sur le port 389 par défaut. Contrairement à la plu¬part des protocoles Internet, le codage utilise BER (Basic Encoding Rule) au lieu d'une transcription ASCII classique.

Le principe de BER est de transformer les entités décrites dans la norme avec la notation ASN.1. Il permet des transferts rapides sur le réseau. En revanche, l'analyse par un oeil humain des paquets transmis sera relative¬ment difficile, car elle nécessite de connaître les conventions de codage et de les appliquer pour comprendre le message.

Par exemple, le type de message 3 signifie Search Request et il appa¬raît dans le paquet sous là forme d'un code d'opération 63 en hexadécimal ! On est loin de la lisibilité du protocole HTTP, où les requêtes et les réponses sont immédiatement compréhensibles. Ne comptez pas utiliser la com¬mande telnet pour déboguer les problèmes de connexion ou de protocole LDAP.

Pour définir ce qu'est le service LDAP, on peut retenir les caractéristiques suivantes.

- Un service de publication d'annuaire
- Un protocole d'accès aux annuaires de type X.500 ou Lightweight Directory Access Protocol
- Un dépôt de données basées sur des attributs ou un «genre» de base de données
- Un logiciel optimisé pour les recherches avancées et les lectures
- Une implémentation client/serveur
- Un mécanisme extensible de schémas de description de classes d'objets

Les entrées (Directory Service Entry) d'un annuaire LDAP sont distribuées suivant une arborescence (Directory Information Tree) hiérarchisée que l'on peut voir comme un système de fichiers avec ses répertoires et ses fichiers. Au sommet de l'arborescence on trouve un nom de racine (Domain Component) ou suffixe.

L'adresse d'une entrée de l'annuaire LDAP est appelée : distinguished name ou dn. En reprenant l'exemple d'arborescence ci-dessus, les adresses des différentes entrées sont notées comme suit.

- dn: dc=lab,dc=stri
- dn: ou=lab1,dc=lab,dc=stri dn: ou=lab2,dc=lab,dc=stri
- dn: cn=etu1,ou=lab1,dc=lab,dc=stri dn: cn=etu2,ou=lab1,dc=lab,dc=stri dn: cn=etu3,ou=lab2,dc=lab,dc=stri dn: cn=etu4,ou=lab2,dc=lab,dc=stri

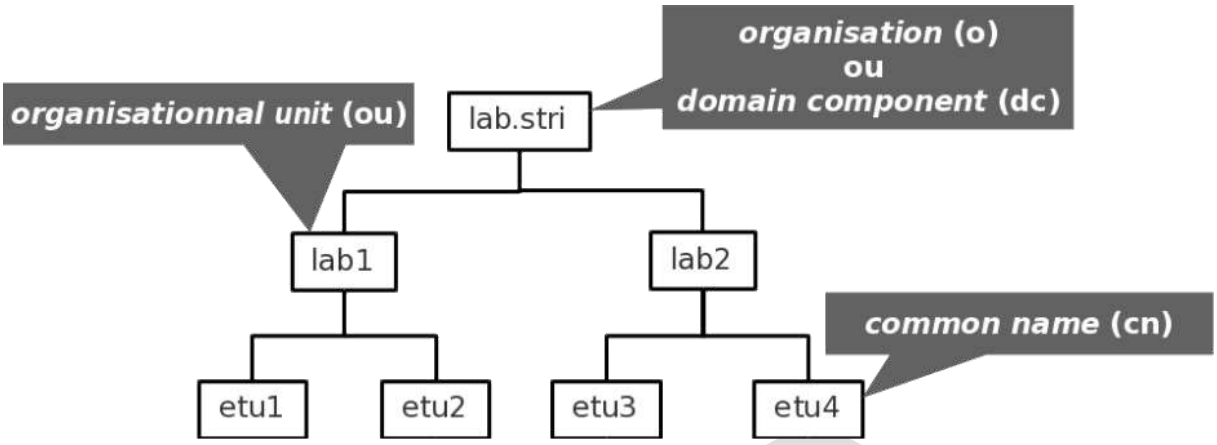


Figure 12 : Arborescence élémentaire LDAP

LDAP vs OpenLDAP ?

III.1.4 OpenLDAP

OpenLDAP est une implémentation libre, open-source du protocole LDAP. Parce qu'il s'agit d'une itération commune, gratuite et accessible à tous, OpenLDAP est parfois appelé simplement "LDAP". Cependant, c'est plus qu'un simple protocole : il s'agit d'un logiciel d'annuaire LDAP léger.

OpenLDAP peut être utilisé sur n'importe quelle plateforme. Contrairement à d'autres implémentations qui offrent des caractéristiques plus robustes comme une interface graphique et souvent une suite d'autres protocoles et fonctionnalités (souvent payants), OpenLDAP est une option LDAP très ciblée, personnalisable et supportant toutes les principales plateformes informatiques. Si la flexibilité peut sembler être un avantage (et c'est souvent le cas), elle peut rendre le logiciel plus difficile à utiliser. Ceci, associé à son manque d'interface, signifie que sa mise en œuvre et sa gestion peuvent nécessiter une expertise importante.

OpenLDAP et Active Directory

Microsoft Active Directory (AD) est un service d'annuaire qui stocke les données des comptes d'utilisateurs et de périphériques dans un emplacement central pour l'accès aux réseaux, appareils, applications et fichiers basés sur Windows.

AD est plus riche en fonctionnalités qu'OpenLDAP : il comprend une interface graphique et des fonctionnalités de configuration plus robustes, comme les objets de stratégie de groupe pour les périphériques Windows. Alors qu'OpenLDAP utilise uniquement le protocole LDAP, AD utilise également d'autres protocoles. D'ailleurs, LDAP n'est pas le protocole principal d'AD ; il exploite plutôt une implémentation du Lightweight Directory Access Protocol propriétaire de Microsoft et utilise principalement Kerberos, le principal protocole d'authentification propriétaire de Microsoft.

Si AD peut sembler plus robuste dans l'ensemble, le fait qu'OpenLDAP se concentre exclusivement sur le protocole LDAP lui confère une profondeur bien supérieure à celle d'AD.

Bien sûr, la différence de coût reflète la notion d'une plus grande variété de fonctionnalités et la nature commerciale des solutions Microsoft : OpenLDAP est gratuit, et AD ne l'est pas. AD nécessite une licence, et parce qu'il fonctionne sur un équipement préinstallé, les coûts du matériel et de la maintenance d'AD peuvent s'accumuler.

Alors qu'AD offre plus de capacités en dehors du protocole LDAP, OpenLDAP est plus flexible et personnalisable en termes d'implémentation. Lorsqu'elles envisagent ces deux solutions, les entreprises doivent décider si elles sont plus intéressées par la flexibilité (OpenLDAP) ou la facilité d'utilisation (AD).

Pour certaines organisations, OpenLDAP est une meilleure option. Plus précisément, pour les entreprises utilisant des systèmes et des applications basés sur Linux ainsi que des équipements réseau et des systèmes de stockage NAS et SAN, LDAP est souvent le protocole favori. De plus, les organisations qui utilisent des centres de données ou une technologie d'infrastructure en cloud en tant que service trouvent l'utilisation d'un serveur OpenLDAP souvent beaucoup plus efficace qu'Active Directory

III.2 Protection et environnement réseau

Dans les entreprises, on utilise l'informatique pour stocker des données parfois sensibles. Il est important d'en assurer la protection, que ce soit lors des stockages ou dans leur mise à disposition.

III.2.1 Disponibilité

La disponibilité permet d'assurer un service en toutes circonstances. Elle nécessite la mise en œuvre de solutions de fiabilisation des services ainsi que des stockages. Les principes de confidentialité sont importants, qui protègent la visibilité des données. Les calculs d'intégrité permettent, quant à eux, de préserver des pertes d'information.

La fiabilisation lors du stockage

- **Redondance des données**. Il est possible de mettre en œuvre une redondance de moyens pour assurer une tolérance de panne à travers une duplication des données sur les disques durs. Certaines des solutions Redundant Array of

Inexpensive Disks (RAID), ou ensemble redondant de disques indépendants, le permettent.

- **Système de fichiers transactionnel**. Ce système de transaction est soit explicitement mis en place au niveau du système de fichiers (comme sur Novell Netware), soit implicitement ; c'est, par exemple, le cas avec Linux (Ext3) et Windows (NTFS).

III.2.2 Redondance

1. **Redondance des données**

Tolérance de panne

On peut la définir comme une configuration matérielle ou logicielle qui permet de prévenir d'une ou plusieurs pannes susceptibles de nuire au bon fonctionnement du système, de retarder ou perturber un utilisateur ou un processus.

Pour les disques durs, bien qu'elle existe sous forme logicielle, la tolérance de panne matérielle est particulièrement utilisée. Elle permet le remplacement à chaud (hot plug), c'est-à-dire, sans extinction de l'ordinateur. Parmi les solutions offrant une tolérance de panne, on peut citer :

- RAID 1, ou miroir (mirroring), dans lequel les opérations d'écriture et de lecture ont lieu simultanément sur deux disques ;
- RAID 2, autre dispositif de miroir ne sollicitant qu'un disque lors des opérations de lecture ;
- RAID 3, agrégats par bandes avec parité sur un disque dédié ;
- RAID 5, agrégats par bandes avec parité répartie sur l'ensemble des disques ;
- RAID 5+1, combinaison de disques en agrégats par bandes avec parité, mis en miroir ;
- RAID 0 + 1, combinaison de stripping (agrégat par bande) et de miroir...

Toutes les solutions RAID n'incluent pas de la tolérance de panne. Ainsi, le mode RAID 0, qualifié d'agrégats par bandes (stripping) sert essentiellement à accélérer les opérations d'écriture, en répartissant les données sur plusieurs disques, de manière transparente pour l'utilisateur.

2. Redondance serveurs

Les solutions de redondance serveur permettent deux fonctionnalités qu'il est nécessaire de distinguer : la tolérance de panne et la répartition de charge.

Ces deux fonctions peuvent tout de même être mises en œuvre simultanément. Elles autorisent ce qu'on appelle la haute disponibilité, en offrant un service continu aux utilisateurs, même en cas de problème ou de surcharge.

La tolérance de panne

Dans ce cas, plusieurs instances d'un système d'exploitation serveur adapté sont exécutées sur des serveurs distincts. On parlera de cluster à *n* nœuds pour identifier une solution mettant en œuvre *n* occurrences d'exécution d'un même système d'exploitation. Cette tolérance de panne permet de maintenir le service aux utilisateurs. Par contre, il est nécessaire que les données restent disponibles et à jour, quel que soit le serveur défaillant.

Si ces informations sont maintenues sur les disques durs locaux des serveurs, une synchronisation continue (réplication) peut être mise en œuvre. Sinon, il est possible de déporter les données sur une baie de stockage partagée (infrastructure NAS).

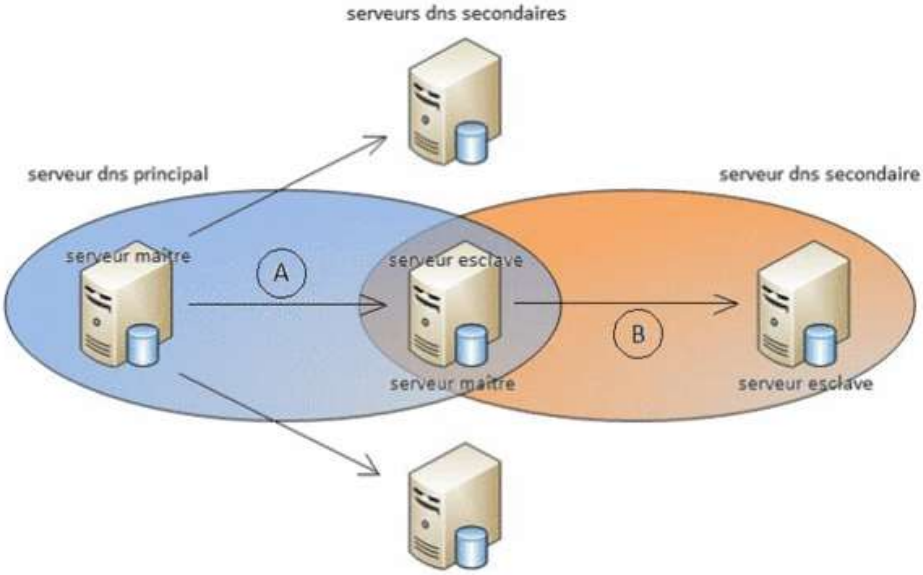


Figure 13 : Tolérance aux pannes

Dans un tel système de redondance de serveurs, tous ne répondent pas obligatoirement aux demandes des utilisateurs. Un tel fonctionnement est d'ailleurs réservé aux solutions les plus évoluées. Souvent, un seul serveur offre de manière permanente ses services aux utilisateurs (serveur actif) et un second reste près à prendre le relais en cas de défaillance du premier (serveur passif).

La réparation de charge réseau

Le Network Load Balancing (NLB) ne correspond pas à proprement parler à une solution matérielle, en ce sens que l'on peut utiliser des ordinateurs non dédiés à un rôle de serveurs. Il est ainsi possible, avec des PC mis en réseau, de mettre en œuvre une telle solution. L'équilibre de charge réseau permet ainsi de fournir une solution à haute disponibilité évolutive. Elle convient parfaitement pour servir des sites Web, par exemple.

Une telle fonction permet d'adapter les performances liées à l'application, en distribuant ses requêtes de clients sur les serveurs présents dans le cluster. Ainsi, lorsque le trafic augmente, il est possible d'ajouter des serveurs supplémentaires au cluster.

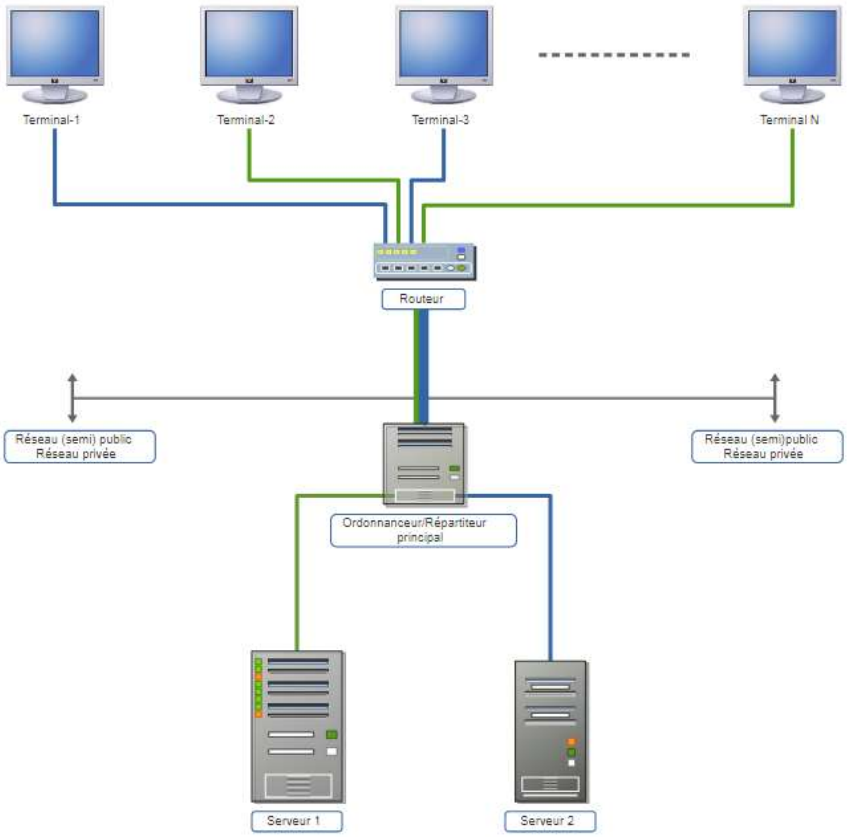


Figure 14 : Répartition de charge

III.2.3 Stratégie de sauvegarde

Pour tout fichier créé ou modifié, le système d'exploitation positionne un bit d'archive ou met à jour la date de dernière modification. À partir de là, il est possible de déterminer quels sont les fichiers qui doivent être sauvegardés. L'entreprise va déterminer une stratégie de sauvegardes qui va permettre de répondre à plusieurs questions :

- Quels sont les fichiers à sauvegarder ?
- Quels types de sauvegardes ?
- Quand effectuer les sauvegardes ?
- Sur combien de supports ?
- Est-il plus important de sauvegarder rapidement ou de restaurer rapidement ?
- Combien de bandes doit-on utiliser, de quelle manière (rotation des bandes) ?

La sauvegarde complète

Lors d'une sauvegarde complète, l'attribut d'archive du fichier est réinitialisé, pour mémoriser le fait qu'il a été enregistré. Si la date est utilisée, celle de dernière sauvegarde est mémorisée, de façon à pouvoir différencier les fichiers qui ont été sauvegardés des autres (date de dernière modification).

La sauvegarde incrémentale

Ce type de sauvegarde marque les fichiers comme ayant été enregistrés. Elle est souvent effectuée quotidiennement, prenant en compte les modifications de la journée. Une stratégie hebdomadaire consiste, par exemple, à effectuer une sauvegarde complète le vendredi et une sauvegarde incrémentale les autres jours.

Une telle stratégie minimise la durée quotidienne de sauvegarde. En revanche, lors d'une restauration complète jusqu'au jeudi, par exemple, il faut restaurer la bande du vendredi,

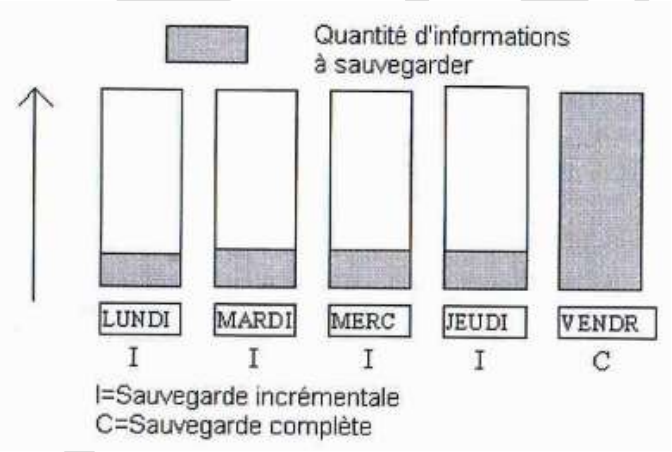


Figure 15 : Exemple N°1 d'une stratégie de sauvegarde

plus les quatre bandes correspondant à chaque jour de la semaine.

La sauvegarde différentielle

Cette sauvegarde (souvent quotidienne) ne réinitialise pas les attributs d'archive des fichiers, pour préciser qu'ils ont été enregistrés. De ce fait, à chaque nouvelle sauvegarde différentielle, les modifications précédentes, plus celles du jour, sont prises en compte. Cette stratégie minimise le temps de restauration puisqu'elle ne nécessite que deux bandes (la complète plus la dernière différentielle). En revanche, la sauvegarde quotidienne est de plus en plus longue chaque jour.

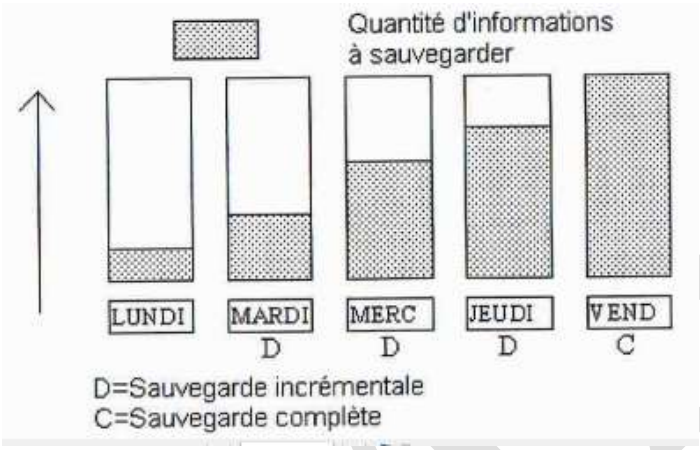


Figure 16 : Exemple N°2 d'une stratégie de sauvegarde

III.3 Supervision des réseaux informatiques

Le métier d'administrateur devient de plus en plus complexe, d'où l'importance pour l'équipe de gagner en temps et en efficacité grâce à un bon outil de supervision. Les systèmes d'information sont tous différents de par leur taille, leur nature, leur criticité. Ils ont cependant pour point commun d'être le théâtre d'incidents, à un moment ou à un autre. Un des rôles des administrateurs est justement de gérer cela. Ils doivent concevoir l'architecture du système d'information de telle manière qu'une panne ait un impact minimal sur le reste du système. Ils doivent aussi gérer les éventuels problèmes – ce qui reste une part importante de leur charge de travail.

III.3.1 Introduction et ambigüité

La supervision consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes. Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir

réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des réseaux afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils adéquats. Une grande majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information ;
- Visualiser l'architecture du système ;
- Analyser les problèmes ;
- Déclencher des alertes en cas de problèmes ;
- Effectuer des actions en fonction des alertes ;
- Réduire les attaques entrantes.

La tâche de l'administrateur est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée.

Monitoring, supervision et métrologie

La supervision est un sujet présent dans tous les systèmes d'information à partir d'une certaine taille. Le monitoring s'est le fait de "surveiller" , ou "garder un oeil sur" . Cependant, le fait de surveiller quelque chose revient à connaître sont état actuel mais aussi l'historique de ses états passés, par l'intermédiaire de valeurs (UP/DOWN) et de données chiffrées (des pourcentages par exemple). C'est ici que l'on retrouve une distinction entre deux notions que sont la supervision et la métrologie. La métrologie, dans laquelle on retrouve la notion de mètre/métrique, est le fait d'obtenir, de garder et de tracer la valeur numérique d'une charge. Par exemple le pourcentage de CPU utilisé sur un serveur, le nombre de personnes connectées sur une site web, le trafic sortant et

entrant sur un switch. Bien souvent, la métrologie permet tout simplement de tracer des graphiques, bien connus dans le domaine du monitoring.

La métrologie est donc le fait de récupérer la charge (chiffrée), permettant de tracer son évolution dans le temps. Elle est donc caractérisée non pas par le fait de récupérer une valeur à l'instant T, mais de pouvoir afficher et tracer l'évolution d'une charge, construite par un ensemble de métrique récupérées dans le temps.

La supervision, en revanche, est le fait de récupérer l'état d'un service à l'instant T. la supervision vise à répondre à la question "Le service est-il joignable ?". Au sens strict du terme, aucune valeur numérique n'entre en compte, et l'aspect historique de charge ne fait donc pas partie de la supervision. L'exemple le plus frappant est Nagios qui, par défaut, ne possède aucune fonctionnalité permettant de tracer des graphiques ou obtenir l'historique de la charge d'un service/serveur. Une "extension" de la supervision porte sur le fait de récupérer une valeur chiffrée comme une charge mémoire et de lui appliquer un seuil d'alerte. Dans ce cas, aucun historique n'est gardé mais l'on est capable d'obtenir et de surveiller non plus des états, mais des valeurs numériques. La supervision se caractérise d'ailleurs aussi par son système d'alerte, conséquence directe de la vision "à l'instant T". On peut alors avertir l'administrateur si un système passe de UP à DOWN et inversement. Au contraire, dans le concept pur de la métrologie, le système d'alerte n'est pas pris en compte car la récupération des valeurs/charges n'est pas forcément faite à l'instant T.

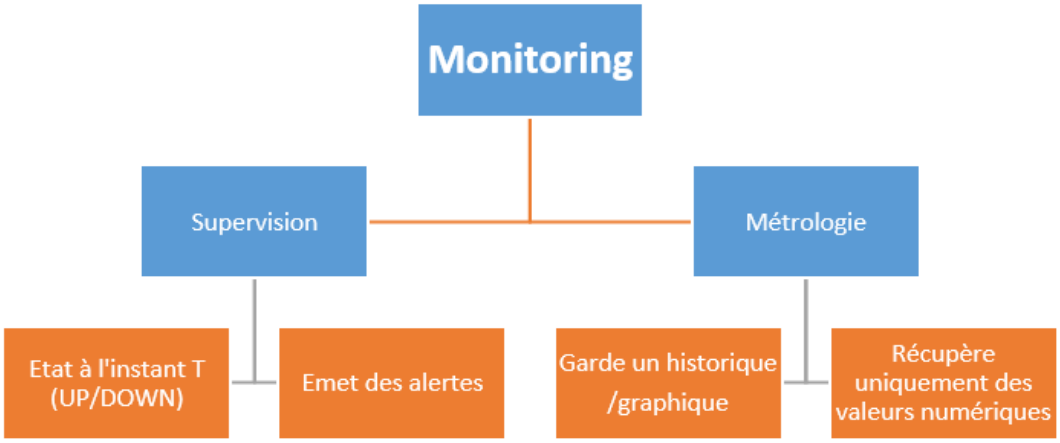


Figure 17 : Monitoring, supervision et métrologie

Avec le temps, supervision et métrologie tendent à complètement se confondre dans les solutions proposées. Ainsi, lorsque l'on cherche à récupérer une information, on parle alors de monitoring. On est maintenant capable d'appliquer de la supervision sur la métrologie, pour faire plus claire, on va appliquer des alertes sur des seuils de charge.

III.3.2 Principe et fonctionnement

Pour résumer, la supervision va dépendre de l'activité de l'entreprise mais aussi de son besoin. On trouve rarement un même type de supervision d'une entreprise à l'autre.

Mais cela reste abstrait. Concrètement on supervise les serveurs, les switchs, les routeurs, les téléphones IP, les caméras IP, les badgeuses, les sondes, la bande passante, le CPU, la mémoire, les disques, les processus, les services, le bon déroulement des actions (backups, transferts, consolidation).

On distingue différents types de supervision.

- La supervision technique. Elle va consister à surveiller le réseau, l'infrastructure et les machines du système d'information (Processeur, Mémoire, Stockage)
- La supervision Applicative. Elle va consister à surveiller les applications et les processus métiers.

- Contrat de service. Elle va consister à surveiller le respect des indicateurs, afin de voir si on respecte bien les contraintes que nous impose par exemple un contrat avec un client
- La supervision Métier. Elle va consister à surveiller les processus métiers de l'entreprise

Fonctionnement

La supervision peut se résumer à cette formule : *Informations* + *Traitement* = *Supervision*

La principale source d'informations va être Snmp (Simple network management Protocol), c'est un protocole qui permet le management d'équipement. Snmp est présent sur quasiment tous les équipements réseaux, ainsi que tous les systèmes d'exploitation. Il permet d'obtenir, de positionner des informations et de remonter des alarmes.

Sur chaque équipement on trouve un agent Snmp. Cet agent gère les informations relatives à l'équipement et sont stockées dans une base de données propre : la MIB (Management Information Base). On positionne un manager Snmp sur l'unité qui va servir de console d'administration.

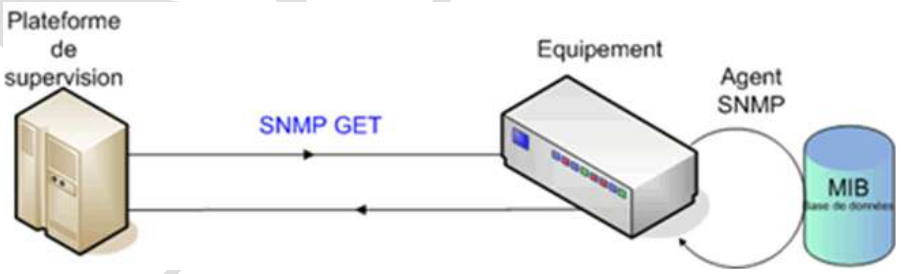


Figure 18 Fonctionnement de la supervision

Le manager va interroger l'agent qui va fouiller dans la mib pour positioner ou donner une valeur voulue. L'agent peut de lui même remonter une information au manager via une trap. Si une carte réseau tombe, l'agent pourra en informer le manager sans que celui-ci en ai fait la demande. Ce protocole permet donc d'obtenir des informations variées sur un équipement à superviser. Il existe aussi d'autres sources d'informations comme l'analyse des logs, des scripts sur les machines qui vont analyser des choses

précises, et des scripts positionnés sur la machine de supervision et qui vont interroger les machines à superviser à distance. Ces moyens permettent donc d'obtenir de l'information. Mais il faut un outil de supervision pour pouvoir les exploiter et, justement, faire de la supervision.

Figure 19 : Modèle de management agent

On se retrouve avec 4 types d'opérations différentes :

- get-request / get-response : l'administrateur interroge une variable particulière de la MIB.
- get-next-request / get-response : l'administrateur interroge toute une table de la MIB.
- set-request / get-response : l'administrateur met une valeur à jour dans la MIB.
- trap : l'agent prévient l'administrateur qu'un événement particulier s'est produit.

Ces opérations utilisent les protocoles OSI classiques pour le transfert d'information. C'est par exemple le CMIP utilise les primitives de service suivantes (CMISE : Common Management Information Service Element) :

- Get : il est utilisé par le gérant pour lire la valeur d'un attribut ;
- Set : fixe la valeur d'un attribut ;
- Event : permet à un agent de signaler un événement ;
- Create : génère un nouvel objet ;
- Delete : permet à l'agent de supprimer un objet.

III.3.3 Les logiciels de supervision

SNMP est un protocole situé entre la couche 4 et la couche 7 du modèle OSI. Il s'appuie sur le protocole de télécommunication UDP (User Datagram Protocol). Le paquet UDP est encapsulé dans un paquet IP (Internet Protocol). UDP est plus simple à utiliser que TCP (Transmission Control Protocol) car il fonctionne en mode non connecté. Le mode non connecté n'oblige pas les deux entités à établir une connexion entre elles avant de transférer des données puis de mettre fin à leur connexion. En revanche, UDP ne permet pas de savoir si les datagrammes sont bien arrivés et s'ils sont arrivés dans un ordre différent de celui d'émission.

Cette architecture SNMP fonctionne sur un modèle client-serveur. Le client correspond à la station de gestion de réseau, souvent appelée Manager ou encore Network Management Station (NMS) par certains éditeurs. Les serveurs correspondent aux agents SNMP qui enregistrent en permanence des informations les concernant dans leur MIB. La station interroge les MIB des différents agents pour récupérer les informations qu'elle souhaite.

Choix d'une licence

En ces périodes où les budgets des services informatiques fondent comme neige au soleil, la gestion des licences est de plus en plus contraignante. Les demandes des utilisateurs augmentent et conduisent à une accumulation de licences. Les outils de supervision ne font pas exception à cette règle. On peut, dans certains cas, arriver à ces situations où seuls les environnements critiques sont supervisés, faute de moyens pour acquérir les licences nécessaires aux autres environnements. Cette situation est dommageable à la qualité du service fourni aux utilisateurs l'outil risque par exemple de ne pas être utilisé pour signaler un problème sur un environnement de test avant mise en production. L'utilisation d'un outil open source est tout indiquée dans ce genre de situation.

De très bonnes performances

Les systèmes d'information varient en architecture mais aussi en taille. La solution de supervision choisie doit être performante afin d'être en mesure de gérer un nombre important d'éléments. Il serait dommage de se restreindre à cause des piètres performances de l'outil. Bien évidemment, toute solution a ses limites, ne serait-ce qu'en raison des limitations des serveurs. L'outil doit dans l'idéal proposer des méthodes de répartition de charge sur plusieurs serveurs.

Transparence du mécanisme de remontée d'alerte

Un autre besoin des administrateurs est de savoir comment est recueillie l'information. Les alertes qu'ils ne comprennent pas ne peuvent guère leur inspirer confiance. S'ils savent précisément comment est récupérée l'information, ils la prendront immédiatement en considération. Ils pourront même essayer de l'améliorer. C'est tout l'intérêt des solutions open source !

Les logiciels de supervision dits « Open Source », les plus utilisées sont :

- le logiciel NAGIOS ;
- le logiciel CACTI ;
- le logiciel CENTREON

IV. Administration systèmes

IV.1 Pratique sous Windows

Comprendre les capacités d'un système d'exploitation vous permet de tirer profit efficacement de ce système d'exploitation. En comprenant comment exploiter complètement votre système d'exploitation et en comprenant le fonctionnement des outils disponibles pour gérer ces fonctionnalités, vous fournirez une valeur ajoutée supérieure à votre organisation.

Chaque organisation possède ses propres exigences. Une organisation située dans une zone dotée d'une connectivité Internet limitée devra compter davantage sur les serveurs locaux qu'une organisation qui dispose d'une connexion haut débit. Dans une organisation, il est important que, même dans l'éventualité de problèmes de connectivité Internet, le travail puisse continuer. La productivité sera affectée si la défaillance de la

connexion Internet de l'organisation signifie que soudainement personne ne peut accéder à ses fichiers et imprimantes partagés.

Les serveurs déployés localement forment la colonne vertébrale d'un réseau organisationnel et fournissent les ressources suivantes aux clients :

- Services d'infrastructure. Les serveurs fournissent aux clients les ressources d'infrastructure, y compris les services DNS (Domain Name System) et DHCP (Dynamic Host Configuration Protocol). Ces services permettent aux clients de se connecter et de communiquer avec d'autres ressources. Sans ces services, les clients ne pourraient pas se connecter entre eux ni à des ressources distantes, telles que les ressources hébergées via un cloud computing.
- Fichiers et imprimantes partagés. Les serveurs fournissent un emplacement centralisé qui permet aux utilisateurs de stocker et de partager des documents. Les serveurs hébergent également des ressources telles que les imprimantes partagées, qui permettent aux groupes d'utilisateurs de tirer profit plus efficacement des ressources. Sans ces ressources centralisées, déployées localement, le partage et la sauvegarde de fichiers de manière centralisée constitueraient un processus plus long et plus complexe. Il serait possible d'héberger certaines de ces informations via un cloud computing, mais il ne semble pas vraiment raisonnable d'envoyer un travail à une imprimante située dans une pièce voisine via un serveur hébergé à un emplacement distant.
- Applications hébergées. Les serveurs hébergent des applications. Les clients accèdent à ces applications pour accomplir différentes tâches, telles qu'accéder à leur courrier électronique ou déployer en libre-service des applications de bureau. Dans certains cas, ces ressources peuvent être déployées via un cloud computing. Dans de nombreux cas, ces ressources doivent être hébergées localement pour des raisons liées aux performances, au coût et à la réglementation. Le fait qu'il soit plus judicieux d'héberger ces ressources localement ou via un cloud computing dépend des spécificités de l'organisation elle-même.
- Accès au réseau. Les serveurs fournissent des ressources d'authentification et d'autorisation aux clients dans le réseau. L'authentification au niveau d'un serveur permet à un utilisateur et à un client de prouver leur identité. Même lorsqu'un grand nombre de serveurs d'une organisation sont situés dans un cloud public ou privé, les personnes doivent encore disposer d'une certaine forme d'infrastructure locale d'authentification et d'autorisation.
- Déploiement d'applications, de mises à jour et de systèmes d'exploitation. Les serveurs sont souvent déployés localement pour faciliter le déploiement d'applications, de mises à jour et de systèmes d'exploitation sur les clients dans le réseau organisationnel. En raison de l'utilisation intensive de la bande passante, ces serveurs doivent être à proximité des clients auxquels ils fournissent ce service

IV.1.1 Vue d'ensemble Windows server

Il existe plusieurs éditions différentes de Windows Server parmi lesquelles choisir. Ces éditions permettent aux organisations de sélectionner une version de Windows Server qui répond au mieux à leurs besoins, plutôt que de payer pour des fonctionnalités dont elles n'ont pas besoin. Lors du déploiement d'un serveur pour un rôle spécifique, les administrateurs système peuvent faire des économies substantielles en sélectionnant l'édition appropriée. Le tableau ci-dessous répertorie les éditions de Windows Server 2012.

Par exemple Windows Server 2012 Standard fournit l'ensemble des rôles et des fonctionnalités disponibles sur la plateforme Windows Server 2012. Il prend en charge jusqu'à 64 sockets et jusqu'à 4 téraoctets (To) de mémoire vive (RAM). Il inclut deux licences d'ordinateur virtuel. Par contre Windows Server 2012 Foundation est Conçu pour les gérants de PME, prend en charge seulement 15 utilisateurs, ne peut pas être joint à un domaine et inclut des rôles serveur limités. Prend en charge un cœur de processeur et jusqu'à 32 Go de RAM.

L'*installation minimale* est une option d'installation utilisée pour Windows Server, qui peut contenir des variantes de l'interface graphique utilisateur selon les exigences. L'installation minimale peut être gérée localement à l'aide de Windows PowerShell ou d'une interface de ligne de commande, plutôt qu'en utilisant des outils basés sur l'interface graphique utilisateur, ou à distance à l'aide de l'une des options de gestion à distance. L'installation minimale est l'option d'installation par défaut utilisée lors de l'installation de Windows Server.

IV.1.2 Rôles et fonctionnalités

Pour planifier correctement comment vous allez utiliser Windows Server pour prendre en charge les exigences de votre organisation, vous devez être pleinement conscient des ***rôles*** qui sont disponibles dans le cadre du système d'exploitation. Chaque version de Windows Server présente un ensemble différent de rôles. Lorsque de nouvelles versions de Windows Server sont mises sur le marché, certains rôles sont améliorés et d'autres sont abandonnés. Windows Server prend en charge les rôles serveur, certains sont répertoriés dans le tableau ci-dessous

Rôle	Fonction
AD CS	Permet de déployer des autorités de certification et les services de rôle associés.
AD DS	Banque centralisée d'informations sur les objets réseau, y compris les comptes d'utilisateur et d'ordinateur. Utilisé pour l'authentification et l'autorisation.
ADFS	Fournit la prise en charge de l'authentification unique (SSO) via le Web et de la fédération des identités sécurisée.
Active Directory Lightweight Directory Services (AD LDS)	Prend en charge le stockage des données spécifiques aux applications pour les applications orientées annuaire qui ne requièrent pas l'infrastructure complète des services de domaine Active Directory.
Active Directory Rights Management Services (AD RMS)	Permet d'appliquer des stratégies de gestion des droits pour empêcher tout accès non autorisé à des documents sensibles.
Serveur d'applications	Prend en charge la gestion et l'hébergement centralisés d'applications métier distribuées à hautes performances, telles que celles créées à l'aide de Microsoft .NET Framework 4.5.
Serveur DHCP	Configure les ordinateurs clients dans le réseau avec les adresses IP temporaires.
Serveur DNS	Fournit la résolution des noms pour les réseaux TCP/IP.
Serveur de télécopie	Prend en charge l'envoi et la réception de télécopies. Permet également de gérer les ressources de télécopie dans le réseau.
Services de fichiers et de stockage	Prend en charge la gestion du stockage des dossiers partagés, du système de fichiers distribués (DFS) et du stockage réseau.

Quand vous déployez un rôle, Windows Server configure automatiquement les aspects de la configuration du serveur (tels que les paramètres du pare-feu), pour prendre en charge le rôle. Windows Server déploie également automatiquement et simultanément les dépendances des rôles.

Les ***fonctionnalités*** Windows Server sont des composants indépendants qui prennent souvent en charge les services de rôle ou prennent en charge le serveur directement. Par exemple, la Sauvegarde Windows Server est une fonctionnalité car elle fournit

uniquement la prise en charge de la sauvegarde pour le serveur local ; ce n'est pas une ressource que d'autres serveurs du réseau peuvent utiliser. Windows Server inclut plusieurs fonctionnalités. Certaines sont présentés dans le tableau ci-dessous.

Fonctionnalité	Description
Fonctionnalités .NET Framework 3.5	Installe les technologies .NET Framework 3.5.
Fonctionnalités .NET Framework 4.5	Installe les technologies .NET Framework 4.5. Cette fonctionnalité est installée par défaut.
Service de transfert intelligent en arrière-plan (BITS)	Permet le transfert asynchrone des fichiers pour garantir que d'autres applications réseau ne sont pas affectées défavorablement.
Chiffrement de lecteur BitLocker® Windows	Prend en charge le chiffrement de disque complet et de volume complet, ainsi que la protection d'environnement de démarrage.
Équilibrage de la charge réseau	Permet la distribution du trafic avec équilibrage de la charge entre plusieurs serveurs qui hébergent la même application sans état.

Windows PowerShell introduit le concept de cmdlet (prononcez « commande-let »), un outil en ligne de commandes simple et d'usage unique intégré au shell. Les cmdlets s'emploient séparément, mais elles s'avèrent plus efficaces combinées. Windows PowerShell propose plus d'une centaine de cmdlets de base qu'il est possible de combiner pour automatiser des tâches complexes. Vous pouvez même rédiger vos propres cmdlets afin de personnaliser vos scripts.

IV.1.3 Gestionnaire de serveur et services

La configuration correcte d'un serveur peut vous permettre d'éviter des problèmes ultérieurs substantiels. Windows Server 2012 fournit plusieurs outils permettant d'effectuer des tâches d'administration spécifiques, dont chacune est appropriée à un ensemble spécifique de circonstances. L'interface de gestion de Windows Server 2012 améliore également votre capacité à effectuer les tâches d'administration sur plusieurs serveurs simultanément.

Le Gestionnaire de serveur est le principal outil graphique que vous utilisez pour gérer les ordinateurs exécutant Windows Server 2012. Vous pouvez utiliser la console du Gestionnaire de serveur pour gérer le serveur local et les serveurs distants. Vous pouvez également gérer les serveurs sous forme de groupes. En gérant les serveurs sous forme de groupes, vous pouvez effectuer rapidement les mêmes tâches d'administration sur

plusieurs serveurs exécutant le même rôle ou membres du même groupe. Vous pouvez utiliser la console du Gestionnaire de serveur pour effectuer les tâches suivantes sur des serveurs locaux et des serveurs distants :

- ajouter des rôles et des fonctionnalités ;
- lancer des sessions Windows PowerShell ;
- afficher des événements ;
- effectuer des tâches de configuration de serveur.

Types de démarrage

Les services utilisent l'un des types de démarrage suivants :

- Automatique. Le service démarre automatiquement au démarrage du serveur.
- Automatique (début différé). Le service démarre automatiquement après le démarrage du serveur.
- Manuel. Le service doit être démarré manuellement, soit par un programme, soit par un administrateur. • Désactivé. Le service est désactivé et ne peut pas être démarré.

REFERENCES

Olaf Kirch, Terry Dawson. Administration réseau sous Linux, Édition 2, Editions ENI (2000).

Nicolas Bonnet. Windows Server 2012 R2 les bases indispensables pour administrer et configurer votre serveur, Editions ENI (2014).

Sébastien Rohaut. Linux - maitrisez l'administration du système (2e édition), *Editions ENI* (2009)

François Pignet. Réseaux informatiques: supervision et administration, *Editions ENI* (2007)