L'installation et l'administration de serveurs et de services en réseau

. 1. Installation du réseau local

➢ *Planification de la structure physique du réseau.*

Implantation des postes de travail, implantation des serveurs, segmentation du réseau, choix de câblage, choix et implantation du matériel d'interconnexion (hub, switch, routeurs).

Topologie : l'architecture physique du réseau (étoile, en bus, en anneau).

Câblage : Organisation et répartition de l'ensemble des médias de transmission utilisés par le réseau (câbles cuivre, fibres optiques, Wifi,...) ainsi que des locaux techniques qui recevront le matériel d'interconnexion.

Protocole : c'est l'ensemble des règles qui régissent la communication inter-ordinateur (ex: Ethernet, TCP/IP).

Matériel d'interconnexion : ensemble des matériels permettant de segmenter le réseau, de relier les câbles.

Ex : répéteur, concentrateur (hub), pont, commutateur (switch), routeur.

➢ *Installation et configuration du matériel réseau*

✔ *Câblage*

Types de Câbles : cuivre paire torsadée, fibre optique , WiFi (réseau sans fil)

Architecture de câblage : on distingue le câblage horizontal de distribution (vers la prise utilisateur) et le câblage vertical d'interconnexion (entre les locaux techniques)

Norme de câblage : définit les caractéristiques d'un câblage informatique ainsi que les performances minimales des différents câble informatiques. Actuellement la norme de câblage informatique pour le câblage générique des locaux d'utilisateurs est ISO 11801 V2 et sa publication date de 2002.

✔ *Locaux techniques*

Ces locaux sont équipés d'**armoires de brassages** ventilées contenant :

- les **baies de brassages** (barrettes de prises RJ45) dans lesquelles arrivent tous les câbles du réseau.
- les **éléments d'électronique active** : matériel d'interconnexion : commutateurs, routeurs...
- les **serveurs**
- **le matériel de sécurisation** (onduleur, climatiseur, alarme incendie, caméra de surveillance,...)

✔ *Le brassage*

L'opération de brassage consiste à **connecter** l'ensemble des prises des baies de brassage venant du câblage terminal sur des ports des commutateurs par l'intermédiaire de câbles courts appelés **cordons de brassage**.

➢ *Installation des serveurs*

Les serveurs du réseau vont permettre aux utilisateurs de **partager** des données, des applications et des périphériques (essentiellement les imprimantes).

✔ *Planification de la structure logique du système*

- Déterminer le **nombre et la répartition des serveurs** (serveur d'authentification, serveur de fichiers, serveur d'impression, serveur de sauvegardes, serveur Web, serveur de messagerie, serveur d'accès distant, etc.)
- Déterminer la **structure d'organisation** choisie (gestion centralisée ou répartie des utilisateurs et des ressources). Ex : sous NT choix de la structure de domaines, sous Windows 2000 : répartition des utilisateurs en unités organisationnelles.
- Déterminer le **plan d'adressage IP**.

✔ *Choix de la configuration matérielle*

- Processeur rapide, biprocesseur pour un serveur d'application
- Contrôleur RAID, Disques SCSI Hotplug
- Alimentation redondante
- Lecteur de bandes, ou disque dur externe pour sauvegarde

✔ *Choix du système d'exploitation réseau*

Le système d'exploitation doit être multitâche, multi-utilisateur, et doit fournir des services de base :

- Gestion de la **sécurité des données** (permissions sur les ressources, cryptage des mots de passe, surveillance)

- Gestion des **services réseaux** de base : gestion de protocoles réseaux, DHCP, service de nom DNS, accès distant
- Gestion de la **tolérance aux pannes** (protection contre les sinistres, RAID, sauvegardes)

➢ *Déploiement des serveurs*

- **Installation** du système.
- Configuration du protocole réseau **TCP/IP**,.
- Configuration des **services** : Authentification (ex : Active Directory, Ldap), Routage, DHCP, Nommage (DNS), serveur de fichier (permissions, partages), Messagerie, SGBD....

➢ *Installation et configuration des postes clients*

L'installation peut être **automatisée** par différents outils : installation réseau, télé-distribution d'image disque (norton ghost, partimage sous Linux).

➢ *Installation et configuration des périphériques*

Imprimantes réseau, scanner, copieur, traceur, système de visioconférence...

. 2. Administration des serveurs et services

2.1 ***Gestion des utilisateurs et des ressources***

➢ *Services réseau (DHCP, DNS)*

Contrairement aux services applicatifs fournis par les serveurs de fichiers, ou les serveurs web, les services réseau ne sont pas directement fournis aux utilisateurs, mais permettent de faire fonctionner les ordinateurs en réseau.

Le serveur DHCP (Dynamic Host Configuration Protocol) permet d'attribuer automatiquement la configuration IP aux ordinateurs du réseau.

Le serveur DNS (Domain Name System) renvoie aux ordinateurs du réseau l'adresse IP associée à un nom de domaine.

➢ *Serveur d'authentification*

Pour que seuls les membres autorisés de l'entreprise accèdent aux ressources du réseau, chaque utilisateur du réseau dispose d'un « **login** » ou compte utilisateur, associé à un **mot de passe** qui lui est personnel et secret. Pour accéder aux ressources, il doit s'**authentifier** auprès du serveur, c'est-à-dire valider son nom et son mot de passe.

L'administrateur crée les comptes utilisateurs, forme les utilisateurs à une **politique de sécurité** des mots de passe, surveille et résout les anomalies (mot de passe oublié, compte verrouillé).

Exemples : annuaire LDAP, Active Directory , protocoles d'authentification sécurisés (Radius, Kerberos,...)

➢ *Serveur de fichiers*

Un serveur de fichier met à la disposition des utilisateurs en général un **répertoire personnel,** u **répertoire public** (modèles de documents utilisés dans l'entreprise, documentations,...) ainsi que des répertoires par **groupe de travail, par équipe, par projet.**

L'accès aux fichiers et répertoires est contrôlé par l'intermédiaire de **droits d'accès** qui définissent les permissions de lecture, écriture en fonction du login de l'utilisateur. L'administrateur attribue ces permissions, et surveille (audite) le système pour s'assurer qu'aucun utilisateur n'accède frauduleusement à des données.

Exemple : partage de fichier sous Windows, serveur Samba sous Linux, serveur FTP

➢ *Serveur d'impression*

Le serveur d'impression (Exemple : serveur CUPS sous Linux) permet de **centraliser le contrôle et la maintenance des imprimantes**. Les imprimantes sont en général des imprimantes **réseaux** (connectées directement au réseau par l'intermédiaire d'une carte réseau) et peuvent être regroupées en **pool d'impression.** Les documents envoyés à l'impression sont placés dans des files d'attente.

L'administrateur installe et configure les imprimantes, définit des **droits d'accès** aux imprimantes et les quotas d'impression en fonction des utilisateurs, gère les **priorités dans les files d'attente et** corrige les erreurs

➢ *Proxy*

Le serveur proxy permet de partager et d'**accélérer l'accès à internet** grâce au **cache** centralisé dans lequel sont stockées les ressources d'internet (pages web, fichiers téléchargés images, ...). Il permet également de **contrôler l'accès** aux protocoles d'internet en fonction du login. Exemple : Squid (Linux)

Serveur Web

En général, le serveur Web (protocole http) de l'**intranet** héberge en général des applications non sensibles : consultation de documentation produits, informations sur l'entreprise, sur le comité d'entreprise, pages personnelles des employés. Mais de plus en plus, des applications clients serveur stratégiques sont développées avec une interface Web, suivant l'**architecture à trois niveaux** (serveur Web, serveur d'application, serveur de bases de données).

Exemples : Apache (Linux), IIS (NT / 2000)

Serveur de messagerie

Les protocoles de messagerie d'internet sont de plus en plus utilisés en intranet et tendent à remplacer les protocoles des systèmes de messagerie propriétaires (Exchange, Lotus notes). Les dernières versions de ces logiciels ont d'ailleurs totalement intégré les protocoles SMTP et POP3.

Exemples : Exchange (Windows), Postfix, Exim (Linux)

Serveur de bases de données

Les **données de l'entreprise** (données commerciales, données comptables, financières, gestion du stock, etc.) sont enregistrées et gérées dans une base de données. Le serveur de base de données regroupe une ou plusieurs bases de données de l'entreprise gérée au travers d'un **SGBDR** (SQL Server, Oracle, Informix, ...). Les **permissions** sur les différents composants de la base de données (**tables, requêtes, vues**,...) sont contrôlées directement par le SGBDR dans lequel sont définis les utilisateurs de la base. L'administration de la base de données est un métier à part entière qui consiste à configurer et maintenir les droits d'accès aux interfaces de consultation et de modification de la base.

L'accès des utilisateurs à la base se fait généralement par l'intermédiaire d'un **logiciel client** qui communique avec le serveur de bases de données ou au travers d'une **application client serveur spécifique**. Cette solution est entièrement propriétaire, et limitée au réseau d'entreprise. A cause du développement d'Internet, ce modèle client serveur classique est de plus en plus **remplacé par des interfaces Web,** permettant d'accéder aux bases de données via un **navigateur** classique (le client universel) et des pages interactives, dans un intranet (interne à l'entreprise) ou un extranet (entreprise associée à ses clients et fournisseurs), ou bien sur internet (commerce électronique). Il existe différentes architectures suivant la répartition physique des serveurs (serveur Web, serveur d'applications, serveur(s) de bases de données).

Exemples : MS SQL Server; PostGreSQL et MYSQL sous Linux

Serveur d'applications

Le serveur d'application **gère l'accès des clients aux applications partagées et distribuées** sur plusieurs serveurs. Ceci peut aller d'applications classiques de **gestion d'entreprise** (paye, comptabilité, gestion commerciale), jusqu'à des applications web de **commerce électronique**, par exemple.

Un véritable serveur d'application doit pouvoir **orchestrer des transactions** impliquant de nombreux utilisateurs et serveurs. Dans le modèle client serveur classique, le serveur d'application se place entre le client et le serveur de bases de données. Dans les nouvelles architectures d'applications Web (commerce électronique), le serveur d'application se place entre le serveur Web (IIS, Apache,...), qui reçoit les requêtes des clients, et le serveur de bases de données proprement dit.

Le serveur d'application permet de **supporter la montée en charge** (augmentation des accès clients), la **sécurité**, et la f**iabilité des transactions** (système de **rollback** en cas d'interruption de la transaction).

Exemple : TomCat sous Linux

Serveur de terminaux

Permet d'**ouvrir une session à distance** sur un serveur à partir d'un terminal (PC ou une station de travail) et de lancer des applications résidant sur le serveur.

Telnet et SSH (sécurisé) permettent d'ouvrir une session à distance en mode texte.

Terminal server (sous Windows ou Linux) est un environnement multi-session en mode graphique dans lequel des clients distants ont un accès complet à des applications installées sur le serveur. Il est beaucoup utilisé pour les applications bureautiques, et permet de recycler les vieux PC tout en utilisant un environnement graphique et des applications récentes. La maintenance des applications est centralisée ce qui facilite l'administration.

Exemples : Microsoft TSE, Citrix, Linux Terminal Server Project (LTSP)

Virtualisation de serveur : hyperviseur

La virtualisation de systèmes d'exploitation est une technique consistant à faire fonctionner en même temps, sur un seul ordinateur, plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts. C'est une méthode faisant fonctionner un ou des systèmes d'exploitation invités dans des machines virtuelles, au-dessus d'un système d'exploitation hôte.

La virtualisation peut-être réalisée par une application fonctionnant à l'intérieur d'un système d'exploitation (ce sont des système de virtualisation complète comme par exemple VirtualBox, VirtualPC, VMWare Server/Workstation) ou par un

hyperviseur, noyau système très léger et optimisé pour gérer les accès des noyaux d'OS invités à l'architecture matérielle sous-jacente (Xen, ESX, HyperV)

L'intérêt de la virtualisation est de réduire les couts d'exploitation des serveurs en mutualisant les ressources (économies d'électricité, climatisation, optimisation de l'utilisation de la RAM et du processeur) mais aussi d'améliorer la sécurité. Les machines virtuelles peuvent être sauvegardées, et rapidement déployées sur d'autres serveurs physique en cas de problème.

- *Stockage en réseau : NAS, SAN*

Le serveur de stockage en réseau NAS (Network Attached Storage) permet de centraliser le stockage des données afin d'en mutualiser l'accès au travers du réseau et d'en faciliter la gestion. Les fichiers sont stockées sur le serveur NAS et rendues accessible aux clients (postes de travail ou serveurs d'application) par l'intermédiaire des protocoles de partage de fichiers courants (CIFS/SMP, NFS, FTP).

Dans le cas du SAN, les baies de stockage n'apparaissent pas comme des volumes partagés sur le réseau. Elles sont directement accessibles en mode bloc par le système de fichiers des serveurs. En clair, chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur.

Le stockage SAN est basé sur la Fibre Channel, topologie indépendante et multi-couches fonctionnant en série et se comportant exactement comme une liaison téléphonique. Le SAN est un réseau de stockage ouvert et évolutif qui relie, à des baies de stockage, des serveurs/stations et postes de travail, par ailleurs reliés au réseau d'entreprise. Ceci permet le partage centralisé des données via des « switches » intelligents Fibre Channel. Pour information, les SAN peuvent ainsi être connectés à des milliers de serveurs pour constituer des systèmes de calcul évolutifs et surpuissants présents au sein des laboratoires de recherche dans les domaines industriels, environnementaux, militaires, financiers,… que l'on appelle GRID.

Les ressources de stockage ainsi mutualisées (SAN ou NAS) donnent la possibilité de mettre en œuvre des fonctions de réplication (copie de données entre deux baies) et de snapshot (duplication d'un volume pour l'utiliser sur un autre serveur ou pour le sauvegarder par exemple). Ces fonctions permettent de sécuriser les données (implantation physique dans des locaux distants) et d'optimiser la disponibilité des applications. Ces fonctions sont réalisées de façon transparente pour les serveurs, et la réplication et la copie de données n'affectent pas les ressources du serveur, puisqu'elles sont réalisées au niveau des contrôleurs SAN ou des serveurs NAS.

2.2 ***Sécurité, tolérance aux pannes.***

La sécurité d'un serveur de réseau est primordiale, puisque c'est de son bon fonctionnement que dépend l'accès aux ressources du réseau. Le fonctionnement du serveur doit être assuré sans interruption (continuité du service, haute disponibilité). Pour cela, il faut s'assurer de la protection contre le piratage (parefeu), contre les virus, contre les sinistres (incendies, inondations, coupure de courant), de la sécurité des données (sauvegardes) et de la disponibilité des services (tolérance aux pannes).

- *Parefeu*

Le firewall (Parefeu ou coupe feu) permet de **protéger le réseau des accès pirates de l'extérieur**, par le filtrage des paquets (datagrammes IP).

Exemples : Netfilter (Linux), Internet Security, Winroute, Outpost (windows)

- *Antivirus*

La **lutte contre les virus** est encore plus **indispensable en réseau** qu'en monoposte. En effet, un virus entré par une disquette sur un poste du réseau peut affecter la totalité des machines (serveurs et postes clients). Il est donc nécessaire que chaque ordinateur soit protégé par un **antivirus remis à jour fréquemment**. Pour faciliter et réduire le coût de maintenance antivirus du parc informatique, il existe des solutions logicielles permettant le **déploiement et la mise à jour distante** de l'antivirus, et la **surveillance centralisée** sur un serveur.

Exemple : Trend OfficeScan (Windows), Clamav (linux)

- *Protection contre les sinistres*

Alarme incendie, local séparé et fermé, surveillance vidéo, porte blindée, ...

- *Sécurité électrique*

L'**arrêt brutal d'alimentation électrique** dans un réseau, aussi bien sur les serveurs, que sur les éléments d'interconnexion réseau (hub, commutateur), peut provoquer des **dégâts matériels** et des pertes de données irrémédiables.

Double alimentation : Un serveur possède généralement deux alimentations, avec un système qui permet à la deuxième de prendre le relais en cas de panne de la première alimentation

Onduleur : L'onduleur est un matériel qui fournit une alimentation électrique de secours en cas de panne du secteur ou de micro-coupure électrique. Un onduleur permet de protéger plusieurs serveurs, et matériels réseau (routeur, commutateurs, Hubs) à la fois. En cas de panne, l'onduleur continue à alimenter les équipements connectés pendant un certain temps, et envoie un message provoquant l'arrêt correct des serveurs si la panne dure trop longtemps.

➢ *Sauvegardes*

Les données importantes de l'entreprise doivent être sauvegardées **quotidiennement**, sur des **supports archivés** au fur et à mesure, pour pouvoir être **restaurées en cas de perte** (virus, panne de disque dur, erreur de manipulation).

Il existe différents types de supports pour les sauvegardes, qui se distinguent par le coût de l'octet enregistré. Le CDRom est plutôt utilisée pour la sauvegarde de postes clients. Les baisses importantes de prix et les derniers progrès en matière de **supports optiques** (DVD) et de **disques durs amovibles** permettent à ces technologies d'aborder la sauvegarde de serveur. Cependant, le support le plus adapté reste sans conteste la **bande magnétique** montée en cartouche, à accès séquentiel. Il existe plusieurs standards : DAT, DLT,LTO. Un **robot** de sauvegarde permet de charger automatiquement les cartouches.

Les supports de sauvegarde, cartouches magnétiques, disques durs, supports optiques doivent être conservés dans un **local séparé**, et même dans un bâtiment différent de celui des serveurs pour se protéger du risque de vol ou d'incendie.

L'administrateur réseau doit définir la **stratégie de sauvegarde**, par exemple : sauvegarde complète hebdomadaire le samedi à 20h, et sauvegarde différentielle quotidienne à 21h du lundi au vendredi avec roulement des bandes sur deux semaines. Puis il doit tous les jours changer et stocker les bandes, et vérifier que la sauvegarde s'est déroulée sans erreur grâce au journal de sauvegarde.

Le serveur de sauvegarde peut sauvegarder ses propres disques et également les disques durs des autres serveurs et clients connectés. La sauvegarde doit évidement être **automatisée** grâce à des fichiers de commandes programmés pour être exécutées aux heures ou le serveur est peu sollicité (soirée, nuit). Certains logiciels de sauvegarde permettent de sauvegarder le système pour pouvoir restaurer un serveur complet (système et données) en cas de panne.

Exemples : Ntbackup (Windows), Rdiff-backup(linux).

➢ *Redondance des données : RAID*

L'inconvénient majeur de la sauvegarde des fichiers système sur bande est qu'un cas de panne du système, le serveur doit être arrêté pendant le temps de la restauration, et donc le serveur étant indisponible, sa fonction n'est plus assurée, ce qui est problématique pour un **serveur stratégique** (serveur d'authentification, de bases de données, d'applications). Par conséquent dans ce cas, le serveur dispose d'un dispositif assurant la haute disponibilité des données en cas de panne de disque dur.

La redondance des données peut-être assurée en local sur une serveur grâce au système appelé RAID (Redondant Array Of Inexpensive Disks : en français : ensemble redondant de disques bon marché). La **redondance des données** sur plusieurs disques durs assure la **continuité du service** en cas de panne d'un des disques. Attention : le RAID n'assure pas la sauvegarde des données mais la tolérance aux pannes, il existe donc en complément d'un système de sauvegarde des données.

Il existe plusieurs niveaux de RAID mais seuls les RAID 1 et 5 assurent une tolérance aux pannes correcte.

RAID 1 : mise en miroir de disque

- Enregistrement simultané sur deux disques : double la capacité nécessaire.
- En cas de panne il faut casser le miroir, changer le disque puis recréer le miroir.
- Mirroring ou duplexing (deux contrôleurs)

RAID 5 :

- Nécessite trois disques au moins : capacité supplémentaire de 1 disque
- Enregistrement des données par bandes sur l'ensemble des disques avec contrôles de parités répartis.
- En cas de panne, le disque défaillant est reconstruit sur un disque neuf.

Le système RAID est en général réalisé avec un ensemble de disques dur extractibles à chaud (hotplug), ce ui permet de les changer en cas de panne sans arrêter le serveur.

Il existe aussi des système RAID réseau de type miroir. Les données sont écrites simultanément sur les disques de deux serveurs différents. Exemple : DRBD qui assure la synchronisation permanente de deux disques durs situés sur deux ordinateurs différents au travers du réseau.

➢ *Redondance de serveurs : cluster*

Une autre façon d'assurer la continuité d'un service est de fournir un même service par plusieurs serveurs redondants.. La redondance de serveur permet une répartition de la charge sur plusieurs serveurs physique, et donc améliore les temps de réponse. Un cluster (grappe de serveurs) est un groupe de serveurs indépendants fonctionnant comme un seul et même système. Un client dialogue avec un cluster comme s'il s'agissait d'une machine unique. les clusters sont utilisés pour minimiser l'impact d'une panne de serveur sur la disponibilité d'une application. Cela nécessite la mise en œuvre de disques partagés, par exemple dans le cadre d'un réseau de stockage SAN.

- *Anticiper les sinistres : Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)*

Un plan de reprise d'activité (en anglais Disaster Recovery Plan ou DRP) permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

Le plan de continuité d'activité permet quand à lui de poursuivre l'activité sans interruption du service en cas de sinistre, grâce à la redondance d'infrastructure et à la réplication de données sur plusieurs sites.

. 3. Exploitation du réseau

- *Gestion de parc informatique*

L'inventaire et la maintenance du parc informatique ainsi que l'assistance aux utilisateurs sont facilités par des outils adaptés de gestion de parc, comme OCS inventory (inventaire automatisé de parc) GLPI (outil de helpdesk permettant la signalisation et le suivi des pannes). Ces outils exploitent de manière automatique les fichiers systèmes des ordinateurs et centralisent les informations dans une base de données exploitée par une interface web. L'administrateur du parc informatique a donc une vision complète et centralisée des caractéristiques de tous les ordinateurs du réseau (système d'exploitation, configuration matérielle, périphériques, configuration réseau, logiciels installés, etc...).

- *Gestion des performances et des configurations des serveurs*

Surveillance des performances du système, grâce à des **outils d'analyse de charge** du processeur, des disques, de la mémoire etc.

Evolution de la configuration du serveur (ajout de processeur, augmentation de la RAM, ajout de disque,...)

- *Surveillance, et correction des erreurs*

Surveillance du bon fonctionnement du système grâce à des **fichiers journaux** qui répertorient les évènements (ex : observateur d'événement sous NT).

Correction des erreurs : redémarrages de services, modification de la configuration.

- *Gestion des sauvegardes / restaurations de données*

Changement des bandes, vérification du bon déroulement de la sauvegarde, restaurations en cas de besoin.

- *Surveillance de trafic*

Une des tâches fondamentales de l'administrateur est de **surveiller le trafic réseau** pour détecter les nœuds bloquants, où le taux élevé de trafic est proche de la **saturation**. Cette surveillance se fait grâce à des **outils d'analyse de trames** (sniffers en anglais). Ils permettent de mesurer le trafic en différents points du réseau, pour mettre en évidence les saturations et goulots d'étranglement, mais aussi de capturer, décoder et analyser les trames pour donner un diagnostic clair du problème.

Exemples : moniteur réseau (windows), Ethereal (linux)

- *Supervision SNMP*

SNMP (simple Network Management Protocol) est le standard de fait dominant en matière de **protocole de supervision technique des équipements connectés au réseau** (adaptateurs, concentrateurs/hubs, ponts, commutateurs, routeurs, onduleurs, modems, ...). Le logiciel de supervision SNMP interroge périodiquement (polling) la base d'information de chaque équipement SNMP connecté au réseau et met à jour une base de données dans laquelle est enregistrée la **cartographie complète du réseau** avec chacun de ses nœuds. Les outils de supervision SNMP permettent non seulement de **configurer à distance** tous les équipements SNMP du réseau, mais également de **surveillance** (détection d'incidents, dépassement de seuil).

L'inconvénient de SNMP est, d'une part, que le polling (interrogation) engendre un trafic réseau important, et d'autre part, qu'il n'est pas encore complètement normalisé, ce qui pose des problèmes de compatibilité. Pour contourner ce problème, les plates-formes ouvertes de supervision SNMP peuvent être enrichies par le développement de modules logiciels complémentaires permettant la prise en compte d'équipements nouveaux. Les plates-formes ouvertes les plus connues sont : HP Openview, SystemView, Spectrum, ISM – Open Manager.

- *Assistance aux utilisateurs, télé-maintenance*

Outils de **prise en main à distance** : Laplink, PCAnywhere, Winvnc, ssh.

- *Déploiement et configuration de clients à distance*

Une des tâches les plus fastidieuses de l'administrateur réseau est la **maintenance des postes clients**. Elle est facilitée par l'utilisation de logiciels permettant de gérer **à distance** l'installation et la configuration des stations clientes. Certains outils permettent de stocker l'image disque compressée de chaque station cliente sur un serveur, et de pouvoir la restaurer automatiquement en cas de problème (Norton Ghost, partimage).

D'autres permettent de déployer automatiquement une application sur un ensemble de postes au travers du réseau (WPKG, MSI par GPO)