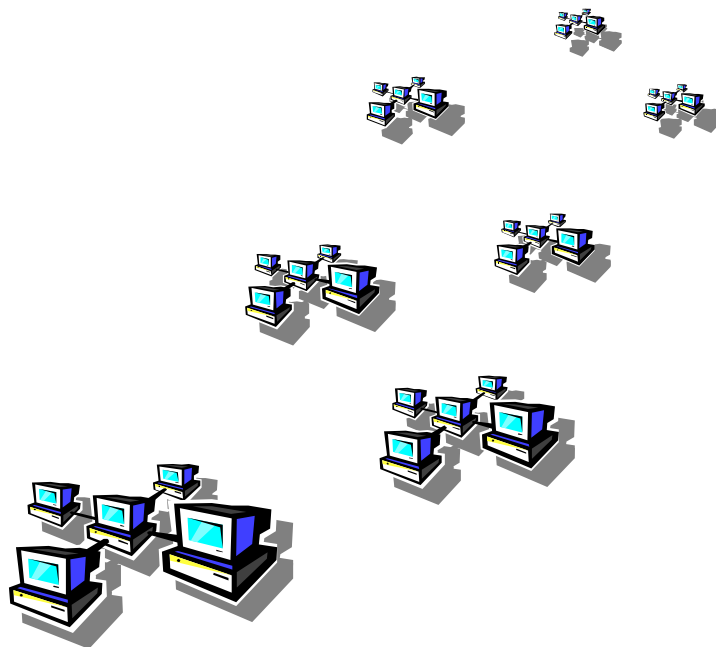


Administration de systèmes

Windows NT·2000·XP·2003



Sommaire

Introduction	2
Eléments logiques et physiques du réseau.....	5
Annuaire et domaine.....	6
Les utilisateurs et les administrateurs.....	6
Les clients et les serveurs.....	8
Types de clients	9
Types de serveur.....	9
Clients et serveurs dans un domaine Windows	11
Les systèmes d'exploitation Windows	12
Versions.....	13
Outils d'administration	14
Les consoles MMC	14
Consoles standards.....	14
Consoles personnalisées.....	15
Administration distante.....	17
Avec les MMC.....	17
Avec Terminal Services.....	17
Avec Telnet	17
Outils de base.....	18
Gestionnaire de sécurité.....	18
Observateur d'événements.....	20
Services	23
Dossiers partagés	24
Utilisateurs et ordinateurs Active Directory.....	25
Gestion des comptes d'ordinateur	29
Ajout de clients et de serveurs membres au domaine	29
Gestion des comptes d'utilisateur	31
Groupe global.....	31
Groupe local	32
Groupe universel	33
Imbrication de groupes	33
Partage de ressources	34
Dossiers partagés.....	34
Publication dans Active Directory	35
Partages administratifs	35
Serveurs d'impression	37
Installation côté serveur.....	37
Installation côté client	39
Planification et priorités	39
Gestion de la file d'attente	41
Racines DFS	43
Sécurité des données.....	44
Confidentialité et intégrité.....	44
Autorisations NTFS	44
Audit	49
Cryptage	50
Disponibilité.....	52
Configurations RAID.....	52
La sauvegarde	53
Réparation d'un système.....	55
Outils de gestion matérielle	58
Gestion des périphériques et des pilotes.....	58
Gestion des disques	59
Surveillance des performances.....	60
Moniteur système.....	61

Journalisation des performances	61
Les stratégies de groupe	63
Qu'est ce qu'une stratégie ?	63
Types de stratégies	65
Stratégies pour la configuration de l'environnement de l'utilisateur	65
Stratégies pour la configuration des ordinateurs	65
Stratégie de sécurité.....	66
Stratégies de déploiement logiciel	66
Application d'une stratégie	66
Stratégie résultante.....	70
Modèles applicables aux stratégies.....	70
Architecture des GPO	70
Architecture en couches	70
Filtrage par groupes de sécurité	71
Documentation des stratégies	71
Installation & migration	72
Installation	72
Configuration minimale pour Windows 2000	72
Mise à niveau ou nouvelle installation ?	72
Méthodes d'installation	73
Création de contrôleurs de domaine	77
Scénarios de migration	78
Etude préalable.....	78
Choix du système d'annuaire.....	79
Etapas de migration d'un domaine.....	80
Mode mixte, mode natif	81
La gestion d'Active Directory	82
Structure de l'annuaire.....	82
Domaine Windows 2000.....	82
Modes de domaine.....	83
Arborescence	83
Forêts.....	83
Structure d'UO	84
La base de données Active Directory	84
Interfaces et normes prises en charge.....	85
Emplacement.....	86
Sauvegarde et restauration	86
Réplication.....	87
Intrasite	87
Intersite	88
Modifications de l'annuaire : rôle des serveurs	89
Serveurs de catalogue global	89
Rôles de niveau forêt.....	90
Rôles de niveau domaine	90
Administration de serveurs	91
Terminal Server	91
Installation et configuration	91
WTS en mode administratif.....	92
WTS en mode application.....	92
Administration des connexions	92
Serveur Web (Internet Information Server).....	93
Fonctionnalités principales	93
Serveur Web public, serveur Intranet.....	94
Configuration de base	96
Options de configuration.....	100
Services Web intégrés	102





Introduction

Les tâches principales d'administration système sont indépendantes de la plate-forme. Si certains systèmes d'exploitation réseau (NOS¹) se distinguent par leurs fonctionnalités avancées, leur stabilité ou leur ergonomie, tous fournissent les mêmes services de base. Cette introduction a pour but de délimiter la fonction d'administration système et ne concerne donc pas uniquement les systèmes Windows.

Eléments logiques et physiques du réseau



Avec l'évolution des systèmes informatiques à base de mainframes vers des réseaux de PC, le rôle de l'administrateur réseau et celui de l'administrateur système ont fini par se confondre. En effet, la distinction entre infrastructure matérielle et logiciels s'est gommée. Lorsqu'on emploie maintenant le terme de réseau, on veut le plus souvent parler du système informatique dans son ensemble. Complexe et à plusieurs niveaux, ce système comporte de nombreux éléments étroitement liés.

Eléments physiques :



-  réseau physique : câblage et équipements intermédiaires (routeurs, commutateurs...),
-  ordinateurs de type poste de travail, de bureau ou portables,
-  ordinateurs de type serveur,
-  périphériques : imprimantes, scanners, équipements de sauvegarde, tours de CD...

La gestion de ces éléments physiques amène à les convertir en éléments logiques indépendants de la structure matérielle.

Eléments logiques :

-  **ressources** : les ressources sont les données, applications ou périphériques qui peuvent être partagés pour être mis à disposition de tout le réseau et dont l'accès doit être contrôlé.
-  **droits** : un droit détermine une action qu'un utilisateur peut effectuer ou non, par exemple ouvrir une session sur un serveur, modifier la configuration, changer l'heure du système...

¹ Network Operating System

-  **autorisations** : l'autorisation concerne l'accès à une ressource : autorisé en lecture seule, autorisé en modification, non autorisé...
-  **comptes et groupes de comptes**: les comptes représentent les utilisateurs et certains ordinateurs. Les comptes sont rassemblés en groupes pour optimiser leur gestion. C'est au groupe de comptes que l'on va allouer des droits et des autorisations.

Annuaire et domaine

Comme on peut le constater ci-dessus, les éléments logiques et physiques d'un réseau sont nombreux. Il est donc indispensable d'avoir un annuaire central listant les objets existants et leur emplacement. Cet annuaire est le plus souvent composé d'une base de données ainsi que de services permettant de l'exploiter à partir de n'importe quel point du réseau.

On doit au minimum trouver les comptes des utilisateurs dans un annuaire de réseau mais des versions plus évoluées tendent à inscrire tous les éléments, y compris les ressources, avec un grand niveau de détail.

Un système d'exploitation réseau se doit de fournir un annuaire complet et ergonomique. Novell a conquis l'essentiel de son marché grâce à ses services d'annuaire (NDS¹) et, si l'annuaire de NT 4.0 (SAM²) était assez basique, celui de Windows 2000 (AD³) est en grande partie responsable de son succès.

Les NOS Windows qualifient de **domaine** l'ensemble des objets qui sont référencés dans un annuaire. On parlera de domaine NT 4.0 ou de domaine Active Directory, selon l'annuaire utilisé.

Les utilisateurs et les administrateurs

Dans un réseau, on distingue systématiquement ceux qui utilisent le réseau de ceux qui gèrent le réseau. Un respect strict de la distinction entre ces deux rôles contribue grandement à améliorer la sécurité du système tout en diminuant les coûts de maintenance.

¹ Novell Directory Service

² Security Account Manager





³ Active Directory

Les utilisateurs

L'utilisateur, comme son nom l'indique, se sert des ressources du réseau. Pour lui, l'ordinateur est un outil de travail mais sa spécialité n'est pas l'informatique. La complexité du réseau doit donc lui être autant que possible masquée. L'utilisateur doit recevoir une formation sur les logiciels qu'il utilise et être informé des règles de gestion du réseau, notamment la politique de sécurité.

Les utilisateurs ne doivent pas avoir à disposition des logiciels qui ne leur sont pas réellement nécessaires et ne doivent pouvoir accéder qu'aux données relatives à leurs fonctions dans l'entreprise.






Toujours dans un souci d'efficacité et de rentabilité, il est conseillé de gérer aussi souvent que possible les utilisateurs par groupe et, sauf exception, d'éviter les opérations relatives à un seul utilisateur. On opérera des regroupements sur les critères suivants :



-  **emplacement** : l'utilisateur se connecte-t-il localement seulement ou est-il mobile ?
-  **poste occupé** : quelle(s) fonction(s) l'utilisateur exerce-t-il et quelles sont les implications concernant les ressources du réseau ?
-  **compétence** : quel est le niveau de compétence informatique de l'utilisateur ? Peut-on ou doit-on lui laisser une certaine autonomie dans la gestion de son environnement de travail informatique ?
-  **cas spéciaux** : l'utilisateur est-il un consultant externe ? Un employé temporaire ? Un cadre supérieur ?

Les administrateurs

Selon la taille du réseau, il peut y avoir un ou plusieurs administrateurs mais chacun possède généralement sa propre zone d'autorité. L'administrateur a tout pouvoir sur les ressources du réseau et doit être un professionnel qualifié.

Les tâches suivantes relèvent de la responsabilité de l'administrateur :

-  gestion quotidienne du réseau : surveillance, dépannage, assistance aux utilisateurs
-  sauvegardes
-  tests et déploiement des mises à jour, correctifs et nouveaux logiciels
-  documentation du réseau
-  mise à niveau matérielle : choix de fournisseurs et de matériels, voire de logiciels

-  gestion des utilisateurs et des ressources : partages et restrictions d'accès
-  gestion des licences et conformité légale du système



En résumé, l'administrateur est responsable du bon fonctionnement et de la sécurité du système informatique, du matériel au logiciel.

Selon la taille de l'organisation, l'administrateur peut aussi gérer la base de données et assumer toute autre tâche informatique (formation, développement...).

A l'opposé, dans une organisation importante, certains rôles ne relèveront plus de l'administrateur comme la maintenance, l'assistance aux utilisateurs, l'installation de matériels, etc.

Les opérateurs

Le rôle des opérateurs se situe à mi-chemin entre l'utilisateur et l'administrateur. Il peut s'agir :

-  d'utilisateurs que leurs fonctions appellent à remplir certains rôles informatiques comme la création de comptes d'utilisateurs ou les sauvegardes.
-  d'administrateurs dont le champ d'activité est restreint à certaines tâches (gestion des imprimantes par exemple) ou à certains serveurs.

Enfin, il est possible de déléguer tout ou partie des tâches d'administration d'un groupe d'objets déterminé. Cet administrateur délégué reste subordonné à l'administrateur principal.



Les clients et les serveurs

Un client est un système qui demande une opération à un autre système. Tous les systèmes d'exploitation permettant la connexion à un réseau sont en même temps des clients et des serveurs. Cependant, certains systèmes sont davantage conçus pour demander des services et d'autres pour en fournir ; c'est sur cette conception spécialisée que l'on distingue habituellement les OS¹ serveurs des OS clients.

¹ Operating System – système d'exploitation

Types de clients




Le terme « client », en fonction du contexte, peut désigner :

-  un ordinateur servant de poste de travail à un utilisateur
-  un programme conçu pour utiliser des ressources fournies par d'autres ordinateurs que celui sur lequel le programme s'exécute

Dans le premier cas, on caractérise l'usage principal de la machine, mais la machine peut néanmoins jouer un rôle mineur de serveur, par exemple lorsqu'elle possède un répertoire partagé. Le terme « client » est un raccourci couramment employé par les ASR1 mais c'est un abus de langage.

Dans le second cas, il ne s'agit plus d'un ordinateur mais d'un logiciel dont le rôle se limite effectivement à consommer des services. La dénomination est exacte. Elle implique qu'un PC de bureau peut héberger plusieurs clients. On qualifie souvent ces clients en ajoutant le nom de l'application ou du protocole pour lesquels ils sont conçus : client web, client FTP, client WAP, client SAP, client Terminal Server...

D'un point de vue physique, les clients d'un réseau d'entreprise sont généralement :

-  des ordinateurs de bureau (*desktop*) ou portables (*laptop*)
-  des terminaux, ne possédant que les périphériques d'entrée et de sortie (le plus souvent, un écran et un clavier)
-  des ordinateurs de poche de type agenda électronique (PDA²) ou téléphone mobile (*smartphone*³)

Types de serveur















Le terme « serveur » est sujet à la même double interprétation que le terme « client ». Il peut s'agir d'une machine jouant principalement le rôle de serveur ou du programme répondant aux demandes des logiciels clients. Dans ce dernier cas, le terme le plus précis est « service ». On donne cependant souvent à la machine le nom du rôle qu'elle joue, c'est-à-dire celui d'un de ses services.

Comme un serveur peut exécuter autant de services que sa mémoire et sa puissance de calcul le permettent, les rôles listés ci-après pourraient être joués par un seul ordinateur, si l'on faisait abstraction des considérations liées à la sécurité et à la maintenance.

¹ Administrateur Système et Réseau

² Personal Digital Assistant – assistant électronique personnel

³ téléphone « intelligent » pouvant exécuter des logiciels web, bureautique, etc.

-  **Serveur de fichiers** : met à disposition de l'espace de stockage et ne fournit que les services permettant d'écrire, ouvrir, déplacer (etc.) des fichiers sur un volume non-local.
-  **Serveur d'impression** : gère des imprimantes (connectées au serveur ou en réseau) partagées, c'est-à-dire destinées à être utilisées par plusieurs clients.
-  **Serveur d'application** : exécute une application capable de répondre aux demandes d'ordinateurs clients. Toutes les applications d'architecture client/serveur exécutent leur partie serveur sur un serveur d'applications.
-  **Serveur de base de données** : il s'agit d'un serveur d'application supportant une base de données client/serveur de type Oracle.
-  **Serveur Web** : fournit des services employant le protocole HTTP à des clients Web, c'est à dire des navigateurs Internet. Le contenu véhiculé peut être des pages statiques (HTML) ou dynamiques (ASP, PHP). Un serveur FTP est souvent associé au serveur Web, afin d'autoriser la copie de fichiers (téléchargement).
-  **Serveur de terminal** : exécute des sessions utilisateurs pour le compte de clients légers.
-  **Serveur de démarrage / d'installation** : le serveur de démarrage fournit le système d'exploitation des clients sans disques tandis que le serveur d'installation fournit les fichiers permettant à un ordinateur d'installer un système.
-  **Serveur DNS** : exploite le fichier de zone contenant les mappages nom d'hôte-adresse IP et répond aux demandes de résolution des clients.
-  **Serveur WINS** : inscrit dynamiquement les noms NetBIOS et répond aux demandes de résolution des clients.
-  **Serveur DHCP** : fournit une configuration IP (adresse + masque de sous-réseau) à un client démarrant sans configuration.
-  **Serveur de certificats** : délivre et vérifie les certificats X. 509 utilisés dans les infrastructures à clés publiques (PKI)
-  **Serveur d'accès distant** : gère des périphériques d'accès distant et prend en charge de l'établissement de la connexion de clients distants sur liaisons téléphoniques.
-  **Serveur d'authentification** : possède les informations permettant d'authentifier un utilisateur, généralement un fichier crypté contenant la liste des utilisateurs et leur mots de passe.
-  **Serveur de sauvegarde** : gère les lecteurs et les bibliothèques de supports amovibles et exécute l'application de sauvegarde.

Cette liste ne présente que les termes les plus courants et n'est pas exhaustive.

Clients et serveurs dans un domaine Windows

Tous les systèmes ne sont pas égaux dans un domaine Windows : des distinctions existent en fonction du système d'exploitation et du rôle joué par un ordinateur. Certains systèmes, jugés peu sûrs, pourront seulement être authentifiés à l'aide du compte de leur utilisateur alors que d'autres possèdent leur propre compte. Les fonctionnalités des seconds sont plus étendues et autorisent notamment l'authentification hors connexion.

Contrôleurs de domaine

Un domaine est une zone d'autorité administrative. Tous les membres d'un domaine partagent les mêmes informations de sécurité. Ces informations sont contenues dans un annuaire qui est répliqué sur plusieurs serveurs. Ces serveurs emploient leur copie de l'annuaire afin d'authentifier les utilisateurs et de contrôler l'accès aux ressources : ce sont les contrôleurs de domaine (DC¹).

Un contrôleur ne peut appartenir qu'à un seul domaine à la fois.

NT 4.0

Il existe dans chaque domaine un unique contrôleur de domaine primaire (PDC²) qui possède la seule copie en lecture/écriture de l'annuaire et plusieurs contrôleurs de domaine secondaires (BDC³) qui possèdent des copies en lecture seule et sont chargés de l'authentification. Un DC NT 4.0 doit être entièrement réinstallé s'il doit changer de rôle ou de domaine.

W2003

La base de données peut contenir des types d'objets supplémentaires mais le fonctionnement des DC est identique.

Serveurs membres

Ces systèmes serveurs NT, 2000 ou 2003 ne jouent pas le rôle de contrôleurs et offrent d'autres services aux utilisateurs du domaine. Ils sont membres du domaine, c'est-à-dire qu'ils possèdent un compte permettant de les authentifier, tout comme des utilisateurs. Comme ces comptes ne peuvent être créés que par un administrateur du domaine, on contrôle ainsi quels ordinateurs peuvent se connecter au domaine. Un serveur membre ne peut avoir de compte que sur un domaine à la fois.

Serveurs autonomes

Les serveurs autonomes sont également des systèmes serveurs Windows NT-2K-2003 mais ils ne possèdent pas de compte sur le domaine, soit parce qu'il n'y a pas de do-

¹ Domain Controller

² Primary Domain Controller

³ Backup Domain Controller