Logiciel

DPS7000/XTA

Guide utilisateur

Sécurité sur le système DIANE

47 F2 02EL 00

Logiciel
DPS7000/XTA
Guide utilisateur
Sécurité sur le système DIANE

Sujet :	Guide conçu pour apporter des réponses aux demandes spécifiques de renforcement de la sécurité sur les systèmes Diane/Windows DPS7000/XTA
Observations :	Les recommandations contenues dans ce document ne doivent être appliquées qu'avec l'autorisation et sous le contrôle de l'organisation de support de Bull.
Version du logiciel :	N/A
Logiciel/Matériel requis :	Concerne les systèmes Diane/Windows DPS7000/XTA
Date :	Juillet 2003

Bull S.A. CEDOC
357 Avenue PATTON
B.P. 20845
49008 ANGERS Cedex 01
FRANCE

47 F2 02EL 00

47 F2 02EL 00

Préface

Objectifs

Ce document est destiné aux clients qui souhaitent avoir des informations sur la sécurité pour le système Diane (DPS7000/XTA) .

Cette sécurité comprend plusieurs aspects : droits NTFS , les services indispensables pour le fonctionnement du système et sa maintenabilité, les groupes et comptes utilisateurs, le partage NetBios et l'utilisation d'un antivirus .

Les réponses à ces différents points ont fait l'objet d'une validation dans les conditions de sécurité maximum.

Les effets provoqués par l'arrêt des différents services sont décrits dans le document *Windows 2000 Services* en Annexe B.

Table des matières

Sécurité sur le système DIANE

1 Les droits NTFS 1
1.1 Partition C 1
1.2 Partition E 1
1.3 Partition F 2
2 Les services installés sur la machine DIANE 2
2.1 Services utilisés par ESMPRO 2
2.2 Services sur système 180Rc4 2
2.3 Services relatifs à ECC (Emc Control Center). 3
2.4 Service relatif au driver Emulex V2.20a12 3
2.5 Service relatif à PowerPath 3
2.6 Services relatifs à Navisphere 6.X 3
2.7 Service WEB 4
2.8 Service FTP de Microsoft 4
2.9 Interop7Adm 4
2.10 Navisphere Agent 5
2.11 NetOp Helper ver. 6.50 (2000271) 5
2.12 Telnet 5
2.13 V7000 Administration 5
2.14 V7000 System Control 5
2.15 Autres services 5
3 Les comptes utilisateurs 6
3.1 Compte utilisateur GTS 6
3.2 Compte utilisateur IUSR-DIANE-013 (IUSR-<<system name>>) 6
3.3 Compte utilisateur TsinternetUser 6
3.4 Compte V7000Engine 6
4 Les groupes utilisateurs. 7
4.1 Groupes utilisateurs "replicator" et "backup operator" 7
4.2 Groupes NetopActivity. 7

5 Le partage NETBIOS. 7
6 Antivirus Norton 7
6.1 Livraison Anti-virus 7
6.2 Modes d'utilisation 8
6.3 Recommandations sur l'utilisation de Norton Antivirus 9
6.4 Performances 9
7 Sécurité d'exploitation des fichiers Gcos : 10

A. Tableau des services

B. Windows 2000 Services

B.1 Introduction B-1
B.2 Windows 2000 Services B-2

Sécurité sur le système DIANE

1 Les droits NTFS

1.1 Partition C

- Les répertoires **ESM** et **DMI** sont utilisés par ESMPRO . Ils sont créés en suivant la procédure standard d'installation du produit.
- Pour le répertoire **DRIVERS**, les droits peuvent être limités au contrôle total pour le groupe **administrator** et le groupe **V7000BULLSERVICES**.

1.2 Partition E

- La protection des disques GCOS7 est validée à partir du répertoire GCOS_DISK qui est placé après le point de montage afin de permettre l'utilisation de l'espace disque non alloué aux disques GCOS7 (demande client).
- Une protection peut-être placée sur la partition E: mais avec un droit modify/write pour le groupe **V700BULLSERVICES** :
  - Administrator -> Full control
  - EveryOne -> Liste folder / Read
  - V7000BullServices -> Modify/write

  Dans ce cas, il faut mettre en place par « Disk Manager » de Windows 2000 les mêmes droits sur les volumes (point de montage des disques externes) car il n'y a pas héritage des droits à ce niveau.

  Note : la mise en place de cette protection exclut l'utilisation de l'espace disque non alloué à gcos7 par d'autres utilisateurs ou applications .

1.3 Partition F

Partition de manœuvre : contrôle total à tout le monde.

2 Les services installés sur la machine DIANE

Les services suivants sont utilisés par le système Diane.

(Les logons de ces services ne doivent pas être modifiés)

2.1 Services utilisés par ESMPRO

Ces services sont utilisés par ESMPRO (surveillance et remontée d'événements liés au fonctionnement de la plate-forme :équivalent au téléalarme sur les systèmes Artémis). **Ces services doivent être conservés impérativement.**

Alert Manager ALIVE(S) Service

Alert Manager Main Service

Alert Manager Socket(S) Service

ESM Common Service

ESM DMI Component Provider Service

ESM Storage Service

ESM System Management Service

ESMFSService

ESMLANService

WIN32SL

2.2 Services sur système 180Rc4

Ces services sont présents sur un système 180Rc4 avec Director Agent. **Ces services doivent être conservés impérativement.**

Director Remote Control Service

Director Support Program

IBM Active PCI Alert Service

IBM Advanced System Management Remote Mouse

TME10RC

2.3 Services relatifs à ECC (Emc Control Center).

Ces services doivent être conservés impérativement.

EMC Control Center Master Agent

EMC storapid

EMC symapisrvEMC - Executes remote WideSky API functions over TCP/IP connectionsSymmetrix Integration Utilities Provides support for volume locking functionality

2.4 Service relatif au driver Emulex V2.20a12

Ce service doit être conservé impérativement

Emulex HBAnyware Remote Management

2.5 Service relatif à PowerPath

Ce service doit être conservé impérativement

EMC PowerPath Service 3.0.2

2.6 Services relatifs à Navisphere 6.X

Ces services doivent être conservés impérativement

NaviGovernor

Navisphere Agent

IIS Admin Service:

2.7 Service WEB

L'installation d'interop7 met les modules clients d'interop dans les pages WEB de Diane pour faciliter leurs téléchargements sur les systèmes clients distants.

L'installation INTEROP7 teste la présence de IIS sur Diane :

- si présent les pages WEB sont mises à jour,
- si absent les fichiers sont simplement chargés sur Diane dans C:\Program Files\Bull\Interop7\<GCOS_NAME>\STD\Web.

Un message signale pour information l'absence de IIS.

Le client est ensuite invité à faire par FTP depuis le système Diane le transfert du module client INTEROP vers le bon serveur.(dans ce cas le service FTP serveur n'est pas utilisé mais le FTP client)

- pour VIPPLET : le serveur VIPPLET peut être installé sur un autre système que le diane.

2.8 Service FTP de Microsoft

Le service FTP serveur de Microsoft peut être supprimé. Cela ne perturbe pas le FTP avec Gcos7.

Attention :

- **Si l'on veut supprimer le service IIS, il faut le désinstaller (panneau de configuration / Add Remove Program / Add Remove Windows) avant d'installer INTEROP7.**
- **il ne faut pas se contenter d'invalider le service IIS (‘disable’).**
- **Si les services d’Interop7 ont été installés avec IIS présent ,il faut les désinstaller (panneau de configuration / Add Remove Program) avant de désinstaller IIS .**

Dans ces conditions interop7 peut être installé et fonctionne sans problème.

2.9 Interop7Adm

Administration des serveurs d'interop7. **Ce service doit impérativement être conservé**.

2.10 Navisphere Agent

Ce service gère les disques EMC/CLARIION. **Ce service doit impérativement être conservé.**

2.11 NetOp Helper ver. 6.50 (2000271)

Netop permet à la maintenance de contrôler le système à distance en cas de besoin (équivalent à la RMS sur les sytèmes Artémis). A la différence de TSE il permet le contrôle de la session ouverte sur la console locale . Le mécanisme GUEST/GATEWAY/HOST permet ,avec la station de maintenance (BULLMAINT), de n'avoir qu'un seul point d'entrée sur le site (une seule ligne téléphonique). C'est un service qui peut être lancé manuellement à la demande sous le contrôle de l'opérateur (Toutes les opérations effectuées à distance sont visibles sur l'écran local).

2.12 Telnet

Telnet est utilisé par OPENSAVE (solution 2AI) . Il permet de se connecter à distance sur le windows de Diane, puis par cndsa , de se connecter sur GCOS7 Diane. Ce service peut être arrêté lorsque la solution OPENSAVE n'est pas installée sur le site.

2.13 V7000 Administration

Administration du V7000. **Ce service doit impérativement être conservé** .

2.14 V7000 System Control

Moteur V7000. **Ce service doit impérativement être conservé .**

2.15 Autres services

Les autres services correspondent à une installation par défaut de Windows 2000.Le tableau en annexe A donne les services qui peuvent être invalidés et ceux qui doivent être conservés (Voir en annexe 2 le document Windows 2000 services pour une présentation générale de chaque service et une description des effets

produits par leur arrêt.Pour plus de renseignements voir aussi http://www.microsoft.com/windows2000/server).

3 Les comptes utilisateurs

3.1 Compte utilisateur GTS

Le service Alerte Manager Main Service (module d'ESMPRO) est lancé pour le compte de GTS pour permettre le report des événements traités par ESMPRO vers un fichier partagé de la station de maintenance (BULLMAINT). Cet utilisateur peut être modifié, mais doit avoir le droit d'écriture dans le fichier partagé. Lorsque l' agent GTS sera installé sur le diane , il reportera les événements vers la station par un protocole RSF. Ce compte pourra alors être supprimé.

3.2 Compte utilisateur IUSR-DIANE-013 (IUSR-<<system name>>)

Le service IIS (serveur FTP/ serveur web) utilise cet utilisateur pour les connexions anonymes

Ce compte peut être supprimé / désactivé si le service IIS est invalidé ou si l'on supprime les connexions anonymous.

3.3 Compte utilisateur TsinternetUser

Ce compte est utilisé par terminal service. Terminal service peut être désinstallé s'il n'est pas utilisé. Dans ce cas **ce compte peut être supprimé / désactivé.**

3.4 Compte V7000Engine

Ce compte a été créé dans le groupe administrator pour donner des droits au service V7000 System Control . Il est créé sans possibilité de se connecter, le password est crypté dans le code V7000. **Ce compte doit impérativement être conservé.**

4 Les groupes utilisateurs.

4.1 Groupes utilisateurs "replicator" et "backup operator"

Ces groupes ne peuvent pas être supprimés mais ils **sont vides de tout utilisateur.**

4.2 Groupes NetopActivity.

Ce groupe est utilisé par le produit NetOp. **Ce compte doit impérativement être conservé**.

5 Le partage NETBIOS.

Le partage Netbios **peut être supprimé**.

6 Antivirus Norton

6.1 Livraison Anti-virus

Norton Anti Virus Corporate Edition est l'antivirus livré et validé par BULL sur les systèmes DPS7000/XTA. Ce logiciel, livré avec le système DIANE par l'usine d'Angers, permet une protection de la plate forme contre les risques d'infection . La licence Norton anti-virus a une validité de 1 an . Ensuite il est à la charge du client de souscrire un nouveau contrat auprès de Symantec pour l'obtention d'une prolongation de la nouvelle licence. La mise à jour des définitions virales doit être effectuée par le client. (http://www.symantec.com/avcenter). Elle comporte une phase de téléchargement depuis une station disposant d'un accès internet puis une phase de transfert du fichier sur le Diane (pour raison de sécurité) .

6.2 Modes d'utilisation

L'antivirus Norton peut être utilisé en 2 modes :

Mode « Norton Antivirus actif en mode Protection temps réel ».

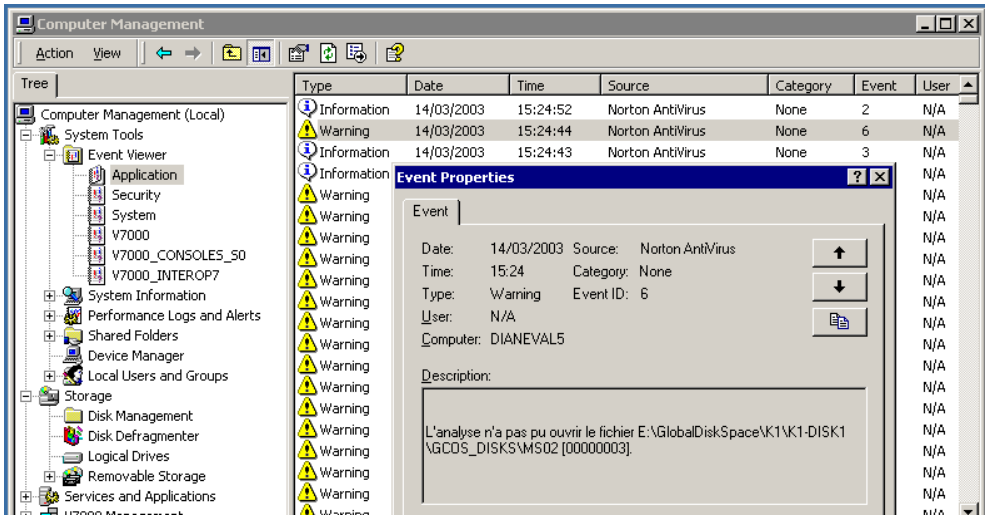
Dans ce mode l'antivirus surveille toute intrusion de virus sur la plate forme . Dans ce mode il n' y a pas de scan manuel ou programmé de l'ensemble des fichiers (Gcos et Windows) du système.

Dans ce mode il n'a pas été constaté d'impact sur les performances de la plate forme et la consommation CPU est faible.

Mode « Norton antivirus actif en mode Scan »

Dans ce cas un scan des fichiers de la plate forme est lancé manuellement ou par programmation .

Dans ce mode et lorsque l'application V7000 est opérationnelle les fichiers Gcos ne peuvent être scannés (voir copie d'écran) du fait qu 'ils sont protégés par un niveau de sécurité Windows qui permet à l'application V7000 d'utiliser en exclusivité les fichiers Gcos. Les droits d'accès V7000 appliqués aux fichiers Gcos s'appliquent aussi lorsque V7000 n'est pas opérationnel. Ce niveau de protection élevé des fichiers Gcos contribue à la sécurisation et à la fiabilité du système Diane.



6.3 Recommandations sur l'utilisation de Norton Antivirus

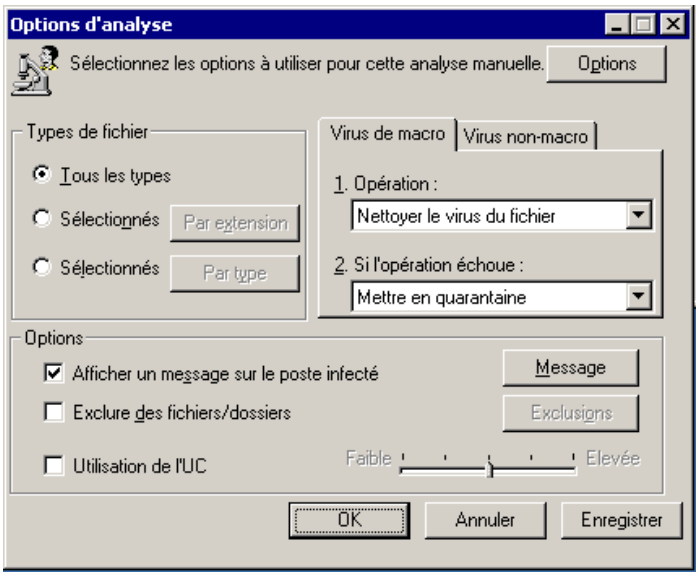
L'utilisation des outils de réparation en cas d'infection par un virus doit être effectuée en suivant les recommandations d'utilisation fournies par Norton Corporate.

6.4 Performances

Pour réduire l'impact que pourrait avoir le scan disque des fichiers Windows sur les performances de la plate forme il est recommandé de paramétrer l' analyse antivirus différée grâce aux options qui permettent de limiter la consommation UC (voir schéma) du programme Norton Anti Virus.

Cette programmation du taux d'occupation de l' UC s'effectue au travers :

analyse programmée -> Nouvelle analyse programmée -> option d'analyse



D'autre part l' impact sur les performances est dépendant de l'activité sur la machine pendant ces opérations. Il est possible de programmer à l' avance un scan des disques dans une période ou l'activité système sera plus faible.

7 Sécurité d'exploitation des fichiers Gcos :

Si une anomalie se produisait sur la plate forme Dps7000/XTA entraînant un arrêt brutal de l'environnement Windows , V7000 et GCOS, cette anomalie serait apparentée à un System Check sur une plate forme du type Artémis.

En d'autres termes sur un DPS7000/Xta un redémarrage GCOS du type Restart/Warm permet d'activer les mécanismes de recovery GCOS et donc de rétablir la cohérence des fichiers d'exploitation évitant d'avoir les fichiers dans l'état FLNAV.

A. Tableau des services

Cette liste n'est pas exhaustive car les services présents dépendent de la version de certains drivers ,de l'état technique de windows (service pack) et des produits installés etc ….

Name	**Description**	**Status**	**Startup Type**	**Log On As**	
Alert Manager ALIVE(S) Service			Manual	LocalSystem	Ce service doit être conservé
Alert Manager Main Service		Started	Automatic	.\gts	Ce service doit être conservé
Alert Manager Socket(S) Service			Manual	LocalSystem	Ce service doit être conservé
Alerter	Notifies selected users and computers of administrative alerts.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Application Management	Provides software installation services such as Assign, Publish, and Remove.	Started	Manual	LocalSystem	Ce service peut être invalidé
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.		Manual	LocalSystem	Ce service peut être invalidé

COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Started	Manual	LocalSystem	Ce service doit être conservé
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Started	Automatic	LocalSystem	Ce service peut être invalidé
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Distributed File System	Manages logical volumes distributed across a local or wide area network.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.		Manual	LocalSystem	Ce service peut être invalidé

Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.	Started	Automatic	LocalSystem	Ce service peut être invalidé
DNS Client	Resolves and caches Domain Name System (DNS) names.	Started	Automatic	LocalSystem	Ce service peut être invalidé
ESM Common Service		Started	Automatic	LocalSystem	Ce service doit être conservé
ESM DMI Component Provider Service			Manual	LocalSystem	Ce service doit être conservé
ESM Storage Service		Started	Automatic	LocalSystem	Ce service doit être conservé
ESM System Management Service		Started	Automatic	LocalSystem	Ce service doit être conservé
ESMFSService		Started	Automatic	LocalSystem	Ce service doit être conservé
ESMLANService			Disabled	LocalSystem	Ce service doit être conservé

Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.	Started	Automatic	LocalSystem	Ce service doit être conservé
Fax Service	Helps you send and receive faxes		Manual	LocalSystem	Ce service peut être invalidé
File Replication	Maintains file synchronization of file directory contents among multiple servers.		Manual	LocalSystem	Ce service peut être invalidé
FTP Publishing Service	Provides FTP connectivity and administration through the Internet Information Services snap-in.	Started	Automatic	LocalSystem	Ce service peut être invalidé
IIS Admin Service	Allows administration of Web and FTP services through the Internet Information Services snap-in.	Started	Automatic	LocalSystem	**Ce service ne doit pas être invalidé mais désinstallé avec le panneau de contrôle.** **Si Interop7 a été installé avec IIS présent Il faut désinstaller interop7 avant de désinstaller IIS et refaire l'installation d'interop7 sans IIS.**

Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.		Manual	LocalSystem	Ce service peut être invalidé
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.		Manual	LocalSystem	Ce service peut être invalidé
Interop7Adm	Allows to start, stop and to get the state of the Interop7 servers	Started	Automatic	LocalSystem	Ce service doit être conservé
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.		Disabled	LocalSystem	Ce service peut être invalidé
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Started	Automatic	LocalSystem	Ce service peut être invalidé

Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.		Disabled	LocalSystem	Ce service peut être invalidé
License Logging Service	Tracks Client Access License usage for a server product.	Started	Automatic	LocalSystem	Ce service doit être conservé
Logical Disk Manager	Logical Disk Manager Watchdog Service	Started	Automatic	LocalSystem	Ce service doit être conservé
Logical Disk Manager Administrative Service	Administrative service for disk management requests	Started	Manual	LocalSystem	Ce service doit être conservé
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Navisphere Agent		Started	Automatic	LocalSystem	Ce service doit être conservé
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.		Manual	LocalSystem	Ce service doit être conservé
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.		Manual	LocalSystem	Ce service peut être invalidé

NetOp Helper ver. 6.50 (2000271)		Started	Automatic	LocalSystem	Ce service doit être conservé
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.	Started	Manual	LocalSystem	Ce service doit être conservé
Network DDE	Provides network transport and security for dynamic data exchange (DDE).		Manual	LocalSystem	Ce service peut être invalidé
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE		Manual	LocalSystem	Ce service peut être invalidé
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.		Manual	LocalSystem	Ce service peut être invalidé
Performance Logs and Alerts	Configures performance logs and alerts.		Automatic	LocalSystem	Ce service doit être conservé
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Started	Automatic	LocalSystem	Ce service doit être conservé

Print Spooler	Loads files to memory for later printing.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.	Started	Automatic	LocalSystem	Ce service peut être invalidé **Attention : Si ce service est invalidé « disable » le service IIS ne peut pas être activé**.
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.	Started	Manual	LocalSystem	Ce service peut être invalidé
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.		Manual	LocalSystem	Ce service peut être invalidé
Remote Access Connection Manager	Creates a network connection.		Manual	LocalSystem	Ce service peut être invalidé
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Started	Automatic	LocalSystem	Ce service doit être conservé

Remote Procedure Call (RPC) Locator	Manages the RPC name service database.		Manual	LocalSystem	Ce service doit être conservé
Remote Registry Service	Allows remote registry manipulation.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Removable Storage	Manages removable media, drives, and libraries.	Started	Automatic	LocalSystem	Ce service doit être conservé
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.		Disabled	LocalSystem	Ce service peut être invalidé
RunAs Service	Enables starting processes under alternate credentials	Started	Automatic	LocalSystem	Ce service peut être invalidé
Security Accounts Manager	Stores security information for local user accounts.	Started	Automatic	LocalSystem	Ce service doit être conservé
Server	Provides RPC support and file, print, and named pipe sharing.	Started	Automatic	LocalSystem	Ce service doit être conservé
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.		Manual	LocalSystem	Ce service peut être invalidé

Smart Card Helper	Provides support for legacy smart card readers attached to the computer.		Manual	LocalSystem	Ce service peut être invalidé
SNMP Service	Includes agents that monitor the activity in network devices and report to the network console workstation.	Started	Automatic	LocalSystem	Ce service doit être conservé
SNMP Trap Service	Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on this computer.		Manual	LocalSystem	Ce service doit être conservé
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.	Started	Automatic	LocalSystem	Ce service doit être conservé
Task Scheduler	Enables a program to run at a designated time.	Started	Automatic	LocalSystem	Ce service peut être invalidé

TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Started	Automatic	LocalSystem	Ce service peut être invalidé
TCP/IP Print Server	Provides a TCP/IP-based printing service that uses the Line Printer protocol.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.	Started	Manual	LocalSystem	Ce service peut être invalidé
Telnet	Allows a remote user to log on to the system and run console programs using the command line.		Manual	LocalSystem	Ce service peut être invalidé

Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.	Started	Automatic	LocalSystem	Ce service peut être invalidé
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.		Manual	LocalSystem	Ce service peut être invalidé
Utility Manager	Starts and configures accessibility tools from one window		Manual	LocalSystem	Ce service peut être invalidé
V7000 Administration	Administration of V7000 GCOS7 virtual machine.	Started	Automatic	LocalSystem	Ce service doit être conservé
V7000 System Control	Engine of V7000 GCOS7 virtual machine.	Started	Automatic	.\V7000Engine	Ce service doit être conservé
Win32SL		Started	Automatic	LocalSystem	Ce service doit être conservé
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files.		Manual	LocalSystem	Ce service doit être conservé

Windows Management Instrumenta-tion	Provides system management information.	Started	Automatic	LocalSystem	Ce service doit être conservé
Windows Management Instrumenta-tion Driver Extensions	Provides systems management information to and from drivers.	Started	Manual	LocalSystem	Ce service doit être conservé
Windows Time	Sets the computer clock.		Manual	Ce service peut être invalidé	Ce service peut être invalidé
Workstation	Provides network connections and communications.	Started	Automatic	LocalSystem	Ce service doit être conservé

B. Windows 2000 Services

Pour plus de renseignements voir aussi :
http://www.microsoft.com/windows2000/server

Abstract

This reference article summarizes all of the approximately 100 services in the Windows® 2000 Server family of operating systems, presenting them in alphabetical order. It provides general information on how each service is related to functioning of the operating system, and describes the major effects of disabling each service.

B.1 Introduction

This reference article summarizes all of the approximately 100 services in the Windows® 2000 Server family of operating systems, presenting them in alphabetical order. It provides general information on how each service is related to functioning of the operating system and describes the major effects of disabling each service.

A service is a process or set of processes that adds functionality to Windows by providing support to other programs. The default installation of each version of Windows 2000 Server provides a core set of services and configurations designed to suit most needs, while offering users some flexibility.

Every service in Windows 2000 has three states, which users can control with the Microsoft Management Console (MMC) Snap-in:

- **Disabled**. These services are installed but not currently running.
- **Set to manual**. These services are installed but will start only when another service or application needs its functionality.
- **Set to automatic**. These services are started by the operating system after device drivers are loaded at boot time.

B.2 Windows 2000 Services

Alerter—notifies selected users and computers of administrative alerts. If this service is turned off, applications that use the NetAlertRaise or NetAlertRaiseEx APIs will be unable to notify a user or computer (by a Message Box from the Messenger service) that the administrative alert took place.

Application Management—provides software installation services, such as Assign, Publish, and Remove. This service (known as appmgmts) processes requests to enumerate, install, and remove applications deployed via a corporate network. When you press the Add button in Add/Remove Programs on a computer joined to a domain, the applet calls in to the service to retrieve the list of your deployed applications.

The service is also called when you use Add/Remove Programs to install or remove an application, and in cases when a component, such as the shell or COM, makes an install request for an application to handle a file extension, COM class, or progid that is not present on the computer. The service is started by the first call made to it—it does not terminate once started. If the service is disabled, users will be unable to install, remove, or enumerate applications deployed in the Microsoft Active Directory™ service through IntelliMirror® management technologies. **See also** Windows Installer.

Boot Information Negotiation Layer (BINL)—provides the ability to install Windows 2000 Professional on (Pre Execution Environment) PXE remote boot-enabled client computers. The BINL service, the primary component of Remote Installation Services (RIS), answers PXE clients, checks Active Directory for client validation, and passes client information to and from the server. The BINL service is installed when you either add the Remote Installation Services component from Add/Remove Windows Components, or select it when initially installing the operating system.

If turned off, PXE clients requesting RIS installations will fail to get a reply. If BINL is no longer needed on the system, the proper way to discontinue its use would be to use Add/Remove Windows components to remove the Remote Installation Services component. IF turned off, Remote Installation Services will fail to allow client machines to install the OS remotely.

Certificate Services—creates, manages, and removes X.509 certificates for applications such as (Secure/Multipurpose Internet Mail Extensions) S/MIME and (Secure Sockets Layer) Cliff this service is stopped, certificates will not be created. If this service is disabled, any services that explicitly depend on it will fail to start.

Clipbook—enables the Clipbook Viewer to create and share "pages" of data to be viewed by remote computers. This service depends on the NetDDE/Network Dynamic Data Exchange (DDE) service to create the actual file shares that other

computers can connect to, while the Clipbook application and service allow users to create the pages of data to share.

This service is turned off by default, and it is only started when a user starts the Clipbook. If you disable or remove the service, Clipbrd.exe will time out on startup and notify the user that it cannot be started and remote access is not available. However, Clipbrd.exe can still be used to view the local Clipboard (where data is stored when a user highlights text and then goes to the Edit menu and selects Copy, or types Ctrl+C).

Cluster Service—defines a cluster as a group of independent computer systems, referred to as nodes, that work together to provide a unified computing resource. There are two different types of cluster solutions in the Windows platform that support different application styles: Server Clusters and (Network Load Balancing) NLB clusters. Server clusters provide a highly available environment for long-running applications such as database or file servers by providing failover support with tightly integrated cluster management.

Network load balancing clusters provide a highly available and highly scalable environment for applications that have no long running state such as front-end web servers by load balancing client requests among a set of identical servers. This service applies to the server clusters and is the essential software component that controls all aspects of the server cluster operation and manages the cluster database. Each node in a cluster runs one instance of the cluster service

COM+ Event System—provides automatic distribution of events to subscribing (Component Object Model) COM components. COM+ Events extend the COM+ programming model to support late-bound events or method calls between the publisher or subscriber and the event system. Instead of repeatedly polling the server, the event system notifies interested parties as information becomes available.

COM+ Events handles most of the event semantics for the publisher and subscriber. Publishers offer to publish event types, and subscribers request event types from specific publishers. Subscriptions are maintained outside the publisher and subscriber and are retrieved when needed. This simplifies the programming model for both. The subscriber does not need to contain the logic for building subscriptions—building a subscriber is as easy as building a COM component. The life cycle of the subscription is separate from that of either the publisher or the subscriber. Subscriptions can be built prior to either the subscriber or publisher being made active.

If the service is turned off, System Event Notification (SENS) stops working: Login and logoff notifications will not occur. Other inbox applications, such as Volume Snapshot service, will not work correctly.

Computer Browser—maintains an up-to-date list of computers on your network, and supplies the list to programs that request it. The Computer Browser

service is used by Windows-based computers that need to view network domains and resources. Computers designated as browsers maintain browse lists, which contain all shared resources used on the network. Earlier versions of Windows applications, such as My Network Places, the NET VIEW command, and Windows NT® Explorer, all require browsing capability. For example, opening My Network Places on a computer running Windows 95 displays a list of domains and computers, which is accomplished by the computer obtaining a copy of the browse list from a computer designated as a browser.

There are several different roles a computer may perform in a browsing environment. Under some conditions, such as failure or shutdown of a computer designated for a specific browser role, browsers—or potential browsers—may change to a different role of operation. Windows NT assigns the following special roles to computers running the Computer Browser service:

- **Domain Master Browser.** Used only in domain environments. By default, the primary domain controller (PDC) for a domain operates in this role. The domain master browser collects and maintains the master browse list of available servers for its domain, in addition to any names for other domains and workgroups used in the network. It also distributes and synchronizes the master browse list for master browsers on other subnets that have computers belonging to the same domain.
- **Master Browser.** Collects and maintains the list of available network servers in its subnet. The master browser fully replicates its listed information with the domain master browser to obtain a complete browse list for the network, and distributes it to backup browsers located on the same subnet.
- **Backup Browser.** The backup browser receives a copy of the browse list from the master browser for its subnet, and distributes it to other computers upon request.
- **Potential Browser.** Capable of becoming a backup browser when instructed to by the subnet's master browser, the potential browser operates similarly to a non-browser under normal conditions.
- **Nonbrowser.** A nonbrowser is configured so it cannot become a browser, and it does not maintain a browse list. It can operate as a browse client, requesting browse lists from other computers operating as browsers on the same subnet. When the Computer Browser service is turned off there is no mechanism to discover other computers to populate the My Network Places, and so on.

DHCP Client— `Dynamic Host Configuration Protocol Client` manages network configuration by registering and updating IP addresses and Domain Name Server (DNS) names. You do not have to manually change the IP settings when a client, such as a roaming user, travels throughout the network. The client is automatically given a new IP address regardless of the subnet it reconnects to—as long as a DHCP server is accessible from each of those subnets.

There is no need to manually configure settings for DNS or Windows Internet Name Service (WINS). The DHCP server can give these settings to the client, as long as the DHCP server has been configured to issue such information. To enable this option on the client, simply select the Obtain DNS Server Address Automatically option button. There are no conflicts caused by duplicate IP addresses. If this service is turned off you will not be able to obtain an IP address. You will have to configure a static IP address. **See also** DHCP Server.

DHCP Server—using the Dynamic Host Configuration Protocol (DHCP), this service allocates IP addresses and allows the advanced configuration of network settings such as DNS servers, WINS servers, and so on to DHCP clients automatically. If the DHCP Server service is turned off, DHCP clients will not receive IP addresses or network settings automatically. **See also** DHCP Client.

Distributed File System (DFS)—manages logical volumes distributed across a local or wide area network. DFS is a distributed service that integrates disparate file shares into a single logical namespace. This namespace is a logical representation of the network storage resources that are available to users on the network. If the DFS service is turned off, users will be unable to access network data through the logical namespace; in order to access the data, users will need to know the names of all the servers and shares in the namespace, and access each of these targets independently.

Distributed Link Tracking (DLT) Client—maintains links between the NTFS file system files within a computer or across computers in a network domain. The DLT Client service ensures that shortcuts and (Object Linking and Embedding) OLE links continue to work after the target file is renamed or moved. When you create a shortcut to a file on an NTFS v5 volume, distributed link tracking stamps a unique object identifier (ID) into the target file, known as the link source. Information about the object ID is also stored within the referring file, known as the link client.

Distributed link tracking can use this object ID to locate the link source file in any combination of the following scenarios that occur within a Windows 2000 domain:

- The link source file is renamed.
- The link source file is moved to another folder on the same volume or to a different volume on the same computer.
- The link source file is moved from one NTFS volume to another within the same domain. (The NTFS volumes must be on computers running Windows 2000. The NTFS volumes cannot be on removable media.)
- The computer containing the link source file is renamed.
- The shared network folder containing the link source file is renamed.
- The volume containing the link source file is moved to another computer within the same domain.

Distributed link tracking also attempts to maintain links even when they do not occur within a domain, such as cross-domain, within a workgroup, or on a single computer that is not connected to a network. Links can always be maintained in these scenarios when a link source is moved within a computer, or when the network shared folder on the link source computer is changed. Typically, links can be maintained when the link source is moved to another computer, though this form of tracking is less reliable over time.

Distributed link tracking uses different services for client and server:

- The DLT Client service runs on all Windows 2000-based computers. In non-networked computers, the Client service performs all activities related to link tracking.
- The DLT Server service runs on Windows 2000 Server domain controllers. The server service maintains information relating to the movement of link source files. Because of this service and the information it maintains, links within a domain are more reliable than those outside a domain. For computers that run in a domain, the DLT Client service takes advantage of this information by communicating with the DLT Server service.

Note: The DLT Client service monitors activity on NTFS volumes and stores maintenance information in a file called Tracking.log, which is located in a hidden folder called System Volume Information at the root of each volume. This folder is protected by permissions that allow only the system to have access to it. The folder is also used by other Windows services, such as Indexing Service.

If the DLT Client service is disabled, you won't be able to track links. Likewise, users on other computers won't be able to track links for documents on your computer. **See also** DLT Server.

`Distributed Link Tracking (DLT) Server`—stores information so that files moved between volumes can be tracked for each volume in the domain. The DLT Server service runs on each domain controller in a domain. This service enables the DLT Client service to track linked documents that have been moved to a location in another NTFS v5 volume in the same domain

If the DLT Server service is disabled, links maintained by the DLT Client service may be less reliable, especially over time. The "NtfsDisableDomainLinkTracking" policy should be enabled in the File system policy group to prevent DLT clients from repeatedly trying to reach the disabled service. **See also** DLT Client.

`Distributed Transaction Coordinator`—coordinates transactions that are distributed across multiple computer systems and/or resource managers, such as databases, message queues, file systems, or other transaction-protected resource managers. The Distributed Transaction Coordinator is necessary if transactional components are going to be configured through Component Services (COM+). It is also required for transactional queues in Message Queuing (MSMQ) and

Microsoft SQL Server™ operations that span multiple systems. Disabling this service prevents these transactions from occurring.

DNS Client—resolves and caches (Domain Name Server) DNS names. The DNS client service must be running on every computer that will perform DNS name resolution. An ability to resolve DNS names is crucial for locating domain controllers in Active Directory domains. Running the DNS client service is also critical for enabling location of the devices identified using DNS names. If the DNS client service is disabled your computers may not be able to locate the domain controllers of the Active Directory domains and internet connections. The computers with disabled client service will not be able to locate the devices identified using DNS names; for example a Web server identified using DNS name www.example.com. **See also** DNS Server.

DNS Server—enables DNS name resolution by answering queries and update requests for Domain Name Server (DNS) names. Presence of the DNS servers is crucial for locating devices identified using DNS names and locating domain controllers in Active Directory. If there is no DNS authoritative for a particular portion of the namespace, then locating devices in that portion of the namespace will fail. Not having the DNS server authoritative for the DNS namespace used to resolve Active Directory domains results in an inability to locate the domain controllers for such domain. **See also** DNS Client.

Event Log—logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer. The Event Log service writes events sent by applications, services, and the operating system to log files. The events contain diagnostic information in addition to errors specific to the source application, service, or component. The logs can be viewed programmatically through the Event Log APIs or through the Event Viewer in a Microsoft Management Console (MMC) snap-in. If the event log is disabled, you will be unable to track events, which reduces your ability to quickly diagnose problems with your system. In addition, you won't be able to audit security events.

Fax Service—enables you to send and receive faxes. Disabling this service will render the computer unable to send or receive faxes.

File Replication—maintains file synchronization of file directory contents among multiple servers. File Replication is the automatic file replication service in Windows 2000. It is used to copy and maintain files on multiple servers simultaneously and to replicate the Windows 2000 system volume SYSVOL on all domain controllers. In addition, it can be configured to replicate files among alternate targets associated with the fault-tolerant Distributed File System (DFS). If this service is disabled, file replication will not occur, and server data will not be synchronized. In the case of a domain controller, stopping the File Replication service may seriously impair its ability to function.

File Server for Macintosh—enables Macintosh users to store and access files on this Windows server machine. If this service is turned off, Macintosh clients will not be able to view any NTFS shares. **See also** Print Server for Macintosh.

FTP Publishing Service—provides (file transfer protocol) FTP connectivity and administration through the Internet Information Service (IIS) snap-in. Features include bandwidth throttling, security accounts, and extensible logging.

Gateway Services for Netware—provides access to file and print resources on Netware networks.

IIS Admin Service—allows administration of Internet Information Services (IIS). If this service is not running, you will not be able to run Web, FTP, NNTP, or SMTP sites, or configure IIS. **See also** World Wide Web Publishing.

Indexing Service—indexes contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language. It also enables quick searching of documents on local and remote computers and a search index for content shared on the Web. The Indexing Service builds indexes of all textual information in files and documents. Once the initial index build is complete, the Indexing Service maintains its indexes whenever a file is created, modified, or deleted.

Initial indexing can be resource-intensive. By default, the Indexing Service will index only when the computer is idle. Using MMC, you can configure the Indexing Service to be more aggressive in its approach. MMC also allows configuration of resource allocation in the service to be optimized for query or indexing usage patterns. If this service is either stopped or disabled, all search functionality is provided by traversing the folder hierarchy and scanning each file for the requested string. With the service turned off, search response is typically much slower.

Internet Authentication Service (IAS)—performs centralized authentication, authorization, auditing, and accounting of users who are connecting to a network (LAN or Remote) using Virtual Private Network Equipment (VPNs), Remote Access Equipment (RAS), or 802.1x Wireless and Ethernet/Switch Access Points. Internet Authentication Service implements the IETF standard Remote Authentication Dial-In User Service (RADIUS) protocol, which enables use of heterogeneous network access equipment. If IAS is disabled or stopped authentication requests will fail over to a backup IAS server, if available. If none of the other backup IAS servers are available, users will not be able to connect.

Internet Connection Sharing (ICS)—provides network address translation (NAT)**,** addressing and name resolution services for all computers on your home or small-office network through a dial-up or broadband connection. When Internet Connection Sharing is enabled, your computer becomes an "Internet gateway" on the network, enabling other client computers to share one connection

to the Internet, share files, and use the same printers. This service is turned off by default. If this service is stopped or disabled services such as internet connection sharing, name resolution, and addressing will not be available to clients on the network. Therefore clients on the home or small office network may not be able to get to the Internet, and their IP addresses will expire, resulting in some clients using Automatic Private IP Addressing (APIPA) for peer-to-peer networking connectivity.

Intersite Messaging (ISM)—allows sending and receiving messages between Windows Server sites. This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport. SMTP support is provided by the SMTP service, which is a component of IIS. The set of transports used for communication between sites must be extensible; therefore, each transport is defined in a separate add-in dynamic link library (DLL). These add-in DLLs are loaded into the ISM service, which runs on all domain controllers that are candidates for performing communication between sites. The ISM service directs send requests and receive requests to the appropriate transport add-in DLLs, which then route the messages to the ISM service on the destination computer.

IPsec Policy Agent—manages IP security (IPsec) policy, starts the Internet Key Exchange (IKE) and coordinates IPsec policy settings with the IP security driver.

Kerberos Key Distribution Center—enables users to log on to the network using the Kerberos version 5 authentication protocol. If this service is stopped, users will be unable to log on to the domain and access services.

License Logging Service—tracks Client Access License usage for server products, such as IIS, Terminal Services, and File and Print services, as well as other products such as SQL Server and Microsoft Exchange Server. If disabled, licensing for these programs will work properly, but usage will no longer be tracked.

Logical Disk Manager—watches Plug and Play events for new drives to be detected and passes volume and/or disk information to the Logical Disk Manager Administrative Service to be configured. If disabled, the Disk Management snap-in display will not change when disks are added or removed. The Logical Disk Manager uses an administrator service and a watchdog service. The service should not be disabled if dynamic disks are in the system. **See also** Logical Disk Manager Administrative Service.

Logical Disk Manager Administrative Service—performs administrative service for disk management requests. This service is started only when you configure a drive or partition, or a new drive is detected. This service does not run by default, but it does get activated by whenever dynamic disk configuration changes occur or when the Disk Management MMC snap-in is open. Such changes include converting a basic disk to dynamic, recovery of fault tolerant volumes, volume formatting, or changing your page file. The service starts, completes the configuration operation, and then exits. **See also** Logical Disk Manager.

Message Queuing—a messaging infrastructure and development tool for creating distributed messaging applications for Windows. Such applications can communicate across heterogeneous networks and can send messages between computers that may be temporarily unable to connect to each other. Message

Queuing provides guaranteed message delivery, efficient routing, security, support for sending messages within transactions, and priority-based messaging. Message Queuing provides both Win32® and COM APIs for all programmatic functionality including administration and management. Disabling MSMQ affects a number of other services including COM+ Queued Component (QC) functionality, some parts of WMI, and the MSMQ Triggers service.

Messenger—sends and receives messages to or from users and computers, or those transmitted by administrators or by the Alerter service. If disabled, Messenger notifications cannot be sent to or received by the computer or by users currently logged on; NET SEND and NET NAME will no longer function.

Net Logon—supports pass-through authentication of account logon events for computers in a domain. This service is started automatically when the computer is a member of a domain. It is used to maintain a secure channel to a domain controller for use by the computer in the authentication of users and services running on the computer. In the case of a (domain controller) DC, It also handles the registration of the computer's DNS names specific to DC locator discoveries. In the case of a DC, it also allows pass-through authentication from other DCs running Net Logon that (pass-through authentication) is forwarded to the destination domain controller where the logon credentials are validated. If this service is turned off, the computer will not operate properly in a domain. Specifically, it may deny NTLM authentication requests and, in case of DC, it will not be discoverable by client machines.

NetMeeting Remote Desktop Sharing—allows authorized users to remotely access your Windows desktop from another PC over a corporate intranet by using Microsoft NetMeeting®. The service must be explicitly enabled by NetMeeting, and can be disabled in NetMeeting or shut down via a Windows tray icon. Disabling the service unloads the NetMeeting display driver used for application sharing.

Network Connections—manages objects in the Network and Dial-Up Connections folder, in which you can view both network and remote connections. This is the service that takes care of network configuration (client side) and displays status in the notification area on the desktop (the area on the taskbar to the right of the taskbar buttons). You may also access configuration parameters through this service.

Disabling this service results in a number of consequences including but not limited to the following:

- Because connections do not appear in the Connections folder, you will not be able to dial out or configure your local area network (LAN) settings.
- Other services that use it to check for Network Location aware Group Policies will start to have undefined behavior
- You will not receive events about media connect and disconnect.

- Internet connection sharing will not work.
- You will not be able to configure incoming connections, wireless settings, or your home network.
- You will not be able to create new connections.

Network DDE—provides network transport and security for dynamic data exchange (DDE) by applications running on the same computer or on different computers. You can create Network DDE "shares" programmatically or by using DDEshare.exe on your computer, and make them visible to other applications and computers. Traditionally, the user creating the share will create and run a server process to handle incoming requests from client processes and/or applications (running on the same computer or remotely); once connected, these processes can exchange any kind of data over a secure network transport.

This service is turned off by default, and it is only started when invoked by an application that uses NetDDE, such as Clipbrd.exe or DDEshare.exe. In addition, applications running on remote computers can send messages to other computers that will invoke the NetDDE service. If you disable or remove the service, any application that depends on NetDDE will time out when it tries to start the service. If an application on a remote computer is trying to start NetDDE on a different computer, it will appear as if that remote computer is not found on the network. **See also** Network DDE Distributed Share Database Manager (DSDM).

Network DDE DSDM—manages shared dynamic data exchange (DDE) and is used by Network DDE. This service is used only by Network DDE to manage shared DDE conversations. You can create and "trust" DDE shares by using DDEshare.exe to allow remote computers and applications to connect and share data. This service maintains a database of these DDE shares, including information on which ones are trusted. For each request for a connection from, or "conversation" with, an application, this service queries the database and validates your security settings to determine if the request should be granted. **See also** Network Dynamic Data Exchange (DDE).

Network News Transfer Protocol (NNTP)—makes the Windows 2000-based server a news server. You can use a news client such as Outlook® Express messaging client to retrieve newsgroups from the server and read headers or bodies of the articles in each newsgroup. You can then post back to the server. NNTP is an Internet standard. (Note that the version included in Windows 2000 doesn't support feeds, where two news servers replicate their contents between each other. However, the version included in Exchange 2000 does include this functionality.) If the service is off, client computers won’t be able to connect and read or retrieve posts.

NT LM Security Support Provider—enables users to log on to the network using the NTLM authentication protocol. If this service is stopped, users will be unable to log on to the domain and access services. NTLM is used mostly by Windows versions prior to Windows 2000.

Online Presentation Broadcast—links audio and/or video with your PowerPoint® presentation program slides as you deliver a presentation. This can occur either in real time (people on the other end), or asynchronously while at your desk preparing a presentation to be stored on a server and later viewed. There are no other dependencies on this service.

Performance Logs and Alerts— configures performance logs and alerts. This service is used to collect performance data automatically from local or remote computers that have been configured using the Performance Logs and Alerts snap-in. You can use the snap-in to define the performance data you want to collect, the conditions under which alerts should be sent to a user, the start and stop times for the collection, and additional parameters that you can save as a user-defined log collection setting. The Performance Logs and Alerts service then starts and stops performance data collections based on the information contained in the named log collection setting. This service only runs if there are collections scheduled. If the service is running and is then stopped by a user, currently running data collections will terminate and no future scheduled collections will take place.

Plug and Play—enables a computer to recognize and adapt to hardware changes with little or no user input. With Plug and Play, a user can add or remove devices, without any intricate knowledge of computer hardware, and without being forced to manually configure hardware or the operating system. For example, a user can plug in a USB keyboard and Plug and Play will detect the new device, find a driver for it and install it. Or, a user can dock a portable computer and use the docking station's Ethernet card to connect to the network without changing the configuration. Later, the user can undock that same computer and use a modem to connect to the network—again without making any manual configuration changes. Stopping or disabling this service will result in system instability.

Print Server for Macintosh—enables Macintosh clients to route printing to a print spooler located on a computer running Windows 2000 Server. If this service is stopped, printing will be unavailable to Macintosh clients. **See also** File Server for Macintosh.

Print Spooler—queues and manages print jobs locally and remotely. The print spooler is the heart of the Windows printing subsystem and controls all printing jobs. It manages the print queues on the system and communicates with printer drivers and input/output (I/O) components (such as the USB port, TCP/IP, and so on). If the spool service is disabled, you will not be able to print.

Process Control Service—a Datacenter Server tool that helps you organize and manage the processes on your system and the resources they use. The service monitors all processes starting and stopping on the system and applies the rules you have defined using the Process Control interface. Before stopping this service refer to the product documentation for Process Control.

Protected Storage—provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services processes or users. (Protected Storage) P-Store is a set of software libraries that allows applications to fetch and retrieve security and other information from a personal storage location, hiding the implementation and details of the storage itself.

The storage location provided by this service is secure and protected from modification. P-Store uses the Hash-Based Message Authentication Code (HMAC) and the SHA1 cryptographic hash function to encrypt the user's master key. This component requires no configuration. Disabling it will make information protected with this service (for example, private keys) inaccessible to you. P-Store is an earlier service that has been supplanted by the Data Protection API (DPAPI), which is currently the preferred service for protected storage. Unlike DPAPI, the interface to P-Store is not publicly exposed.

QoS Admission Control (RSVP)—provides network signaling and local, traffic-control, setup functionality for (Quality of Service) QoS-aware programs and control applets. **See also** QoS RSVP.

QoS RSVP—invoked when an application uses the (Generic Quality of Service) GQoS API requesting a specific quality of service on the end-to-end connection it uses. The services signals its peer and they agree (or not) on the parameters. The RSVP messages can also be intercepted by routers who can veto the resource request if it cannot guarantee it. Once a successful negotiation happens, the service then sets up appropriate flows with the Packet Scheduler which then ensures that a packet rate for that specific flow does not exceed the negotiated rate. If disabled or removed, QoS is not guaranteed to the application and must then decide whether to accept best-effort (the default) or refuse to run. **See also** QoS Admission Control RSVP.

Remote Access Auto Connection Manager—creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address. This service (sometimes called the autodial service) detects an attempt to resolve the name of a remote computer or share, or an unsuccessful attempt to send packets to a remote computer or share. The service is activated only when there is no network access. In that case, the service brings up a dialog which offers to make a dial-up or virtual private network (VPN) connection to the remote computer.

To assist users, the service maintains a local database of connections that were used in the past to reach named computers or shares. When the service detects an unsuccessful attempt to reach a remote computer or share, it will offer to dial the connection that was last used to reach this remote device.

Disabling the service has no effect on the rest of the operating system. You will have to set up connections to remote computers manually. **See also** Remote Access Connection Manager (RasMan).

Remote Access Connection Manager—creates a network connection. This service manages the actual work of connecting, maintaining, and disconnecting dial-up and VPN connections from your computer to the Internet or other remote networks. When you double-click a connection in the Network and Dial up Connections folder and select the Dial button, this generates a work request for this service that is queued with other requests for creating or destroying connections.

This service will unload itself when there are no requests pending. But in practice, the Connections folder calls on this service to enumerate the set of connections and to display the status of each one. So unless there are no connections in the Network Connections folder, the service will always be running. The service cannot be disabled without breaking other portions of the operating system, such as the Network Connections folder. **See also** Remote Access Auto Connection Manager.

Remote Procedure Call (RPC)—provides the endpoint mapper and other miscellaneous RPC services. This is the RPC endpoint mapper and the COM Service Control Manager (SCM). If this service is turned off, the computer will not boot. **See also** Remote Procedure Call (RPC) Locator.

Remote Procedure Call (RPC) Locator—provides the name services for RPC clients. This service supports the RpcNs family of APIs. It helps locate RPC servers that support a given interface within an enterprise (also known as an RPC named service).

This service is turned off by default. If stopped, depending on the role the particular server was playing in the discovery process, RPC clients that rely on RpcNs* APIs from the same computer may not be able to find RPC servers supporting a given interface, or if the service is turned off on a domain controller, RPC clients using the RpcNs* APIs and this domain controller may experience interruption of service while trying to locate clients. Note that no OS component uses the RpcNs* APIs so having this service turned on is only necessary if third part code requires it. **See also** Remote Procedure Call (RPC).

Remote Registry Service—allows remote registry manipulation. This service lets users connect to a remote registry and read and/or write keys to it—providing they have the required permissions. It is usually used by remote administrators and perf counters. If disabled, it doesn't affect registry operations on the system it runs; therefore, the local system will run in the same manner. Other computers or devices will no longer be able to connect to this computer's registry.

Remote Storage Engine—migrates infrequently used data to tape. It leaves a marker on disk allowing the data to be recalled automatically from tape if you attempt to access the file.

Remote Storage File—manages operations on remotely stored files.

Remote Storage Media—controls the media used to store date remotely.

Remote Storage Notification—allows Remote Storage to notify you when you have accessed an offline file. Because it takes longer to access a file that has been moved to tape, Remote Storage will notify you if you are attempting to read a file that has been migrated and also allow you to cancel the request. If the services is turned off, you won't receive any additional notification when you try to open offline files, nor will you be able to cancel an operation that involves an offline file.

Removable Storage—manages removable media drives and libraries. This service maintains a catalog of identifying information for removable media used by a system, including tapes, CDs, and so on. If the system also has automated devices for maintaining removable media (such as a tape autoloader or CD jukebox), Removable Storage also operates the robotics to mount, dismount, and eject media. It is used by applications such as Backup and Remote Storage to handle media cataloging and automation.

This service stops itself when there is no work to do. If there are no automated devices attached to the system, Removable Storage only runs while there are applications using it, so stopping it should never be necessary. If it is stopped on a system that has automated devices, then starting an application such as Backup or Remote Storage can take a very long time. When started in these circumstances, Removable Storage frequently needs to inventory the complete contents of attached autoloaders and jukeboxes, which includes mounting each media in a drive.

Routing and Remote Access—offers routing services in local area and wide area network environments. Routing and Remote Access service provides:

- Multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services
- Dial-up and VPN remote access services.

If this service is turned off, incoming remote access and VPN connections, dial-on-demand connections, and routing protocols will not be available. In a routing context, Routing and Remote Access service drives the TCP/IP stack forwarding engine. The forwarding code can be enabled outside the service for various reasons, most notably Internet connection sharing (ICS).

RunAs Service—allows you to run specific tools and programs with different permissions than your current logon provides.

It is good practice for administrators to use an account with restrictive permissions to perform routine, non-administrative tasks, and to use an account with broader permissions only when performing specific administrative tasks. To accomplish this without logging off and back on, log on with a regular user account and use the runas command to run the tools that require the broader permissions.

SAP Agent—advertises network services on an IPX network using the (Inter Packet eXchange) (Service Advertising Protocol) IPX SAP protocol. It also forwards advertisements on a multi-homed host. Some products such as Microsoft's

File and Print Services for Netware rely on the SAP Agent. If this service is turned off, these products may not function correctly.

Security Accounts Manager—startup of this service signals other services that the Security Accounts Manager subsystem is ready to accept requests. This service should not be disabled. Doing so will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to not start correctly.

Server—provides RPC support and file print and named pipe sharing over the network. The Server service allows the sharing of your local resources (such as disks and printers) so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC.

Disabling this service results in:

- An inability to share files and printers on your computer with other computers on the network.
- An inability of your computer to service RPC requests.
- An inability to communicate via named pipes between machines.

Simple Mail Transfer Protocol (SMTP)—transports e-mail across the network.

The SMTP service is used as an e-mail submission and relay agent. It can accept and queue e-mail for remote destinations and retry at specified intervals. Windows domain controllers use the SMTP service for intersite e-mail-based replication. The Collaboration Data Objects (CDO) for Windows 2000 COM component can use the SMTP Service to submit and queue outbound e-mail.

Other applications may use the SMTP Service as the basis for the SMTP support in their product, for example, Microsoft Exchange 2000 Server.

Simple TCP/IP Services—implements support for the following protocols:

- Echo (port 7, RFC 862)
- Discard (port 9, RFC 863)
- Character Generator (port 19, RFC 864)
- Daytime (port 13, RFC 867)
- Quote of the Day (port 17, RFC 865)

Once the service is enabled, all five protocols are enabled on all adapters. There is no provision for selectively enabling specific services or enabling this service on per-adapter basis. Disabling the service has no effect on the rest of the operating system.

Single Instance Storage (SIS) Groveler—an integral component of Remote Installation Services (RIS). In an effort to reduce the amount of disk space used by a RIS Server's installation folders, SIS will grovel through the partition containing the RIS installation directory, searching for redundant files, storing them centrally, and replacing them with symbolic links. Although the SIS Groveler is installed by default in Windows Server installations, it is set to disabled unless you either add the Remote Installation Services component from Add/Remove Windows Components, or select it when initially installing the operating system.

If the service is turned off, RIS installation images will consume their full image size, and no space savings can be realized. If the SIS Groveler is no longer needed on the system, you should use Add/Remove Windows components to remove the Remote Installation Services component, which will disable it.

Site Server ILS Service—as part of IIS, this service scans TCP/IP stacks and updates directories with the most current user information. Windows 2000 is the last version of the operating system to support the Site Server ILS service.

Smart Card—manages and controls access to a smart card inserted into a smart card reader attached to the computer. The smart card subsystem is based on personal computer/smart card (PC/SC) consortium standards and consists of the following components:

- The Resource Manager. This component manages access to readers and smart cards. To manage these resources, it performs the following functions:

  1. Identifies and tracks resources.
  2. Allocates readers and resources across multiple applications.
  3. Supports transaction primitives for accessing services available on a given card.

The resource manager also exposes a subset of the Win32 API to provide applications with access to these functions.

- A Card/Reader Selection UI. This component allows simple smart card aware applications to access a card and reader with minimum coding.

Disabling the smart card subsystem will result in a loss of smart card support in the system. **See also** Smart Card Helper.

Smart Card Helper—provides support for earlier smart card readers attached to the computer. This component is designed to provide enumeration services for the smart card subsystem so that earlier non Plug and Play smart card reader devices can be supported. Turning off this service will remove support for non-Plug and Play readers. **See also** Smart Card.

SNMP Service—allows incoming (Simple Network Management Protocol) SNMP requests to be serviced by the local computer. SNMP includes agents that

monitor activity in network devices and report to the network console workstation. If the service is turned off, the computer no longer responds to SNMP requests. If the computer is being monitored by network management tools, the tools won't be able to collect data from the computer or control its functionality via SNMP. **See also** SNMP Trap Service.

SNMP Trap Service—receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on the computer. If the service is turned off, SNMP applications won't receive SNMP traps that they are registered to receive. If this computer is being used to monitor network devices or server applications using SNMP traps significant system occurrences could be missed. **See also** SNMP Service.

Still Image Service—loads necessary drivers for imaging devices (scanners and digital still image cameras) and manages events for those devices and associated applications and maintains device state. The service is needed to capture events generated by imaging devices (button presses, connections). If the service is not running, events from imaging devices are not captured and processed. In addition, for device drivers, relying on state, access to respective devices will be disabled.

System Event Notification (SENS)—tracks system events such as Windows logon network and power events. Notifies COM+ Event System subscribers of these events. SENS is an AutoStarted service that depends on COM+ EventSystem service.

Disabling this service has the following effects:

- Win32 APIs IsNetworkAlive() and IsDestinationReachable() won't work well. These are mostly used by mobile applications and on portable computers.
- SENS interfaces don't work properly. In particular, SENS' Logon/Logoff notifications will not work.
- Internet Explorer 5.0 or later uses SENS on portable computers to trigger when to go offline or online (the "Work offline" prompt).
- SyncMgr (Mobsync.exe) will not work properly. It depends on connectivity information and Network Connect/Disconnect and Logon/Logoff notifications from SENS.
- COM+ EventSystem will try to notify SENS of some events, but will not be able to.

Task Scheduler—enables a program to run at a designated time. This service enables you to perform automated tasks on a chosen computer. The Task Scheduler monitors whatever criteria you choose and carries out the task when the criteria for it have been met. For example, you can have the computer run ScanDisk at 7:00 P.M. every Sunday.

Task Scheduler is automatically installed with Windows 2000 and is started each time the operating system is started. It can be run from Windows 2000 (by means of the Task Scheduler graphical user interface [GUI]) or through the Task Scheduler API. If Task Scheduler is disabled, jobs that are scheduled to run won't run at their designated time or interval. Scheduled Tasks using local accounts won't run without a password.

Any task that is using a local account (non-domain account) as the account under which the scheduled task is to run requires a password. If the local account doesn't have a password one needs to be created for that account, and then the task needs to be scheduled using that account name and password. You can create a password for an account by going to Control Panel, User Accounts, Create a Password. Any valid password is acceptable, but it cannot be a blank password.

`TCP/IP NetBIOS Helper Service`—enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution. This service is an extension of the kernel mode NetBT. It should be considered an integral part of NetBT, not a normal service. It does two things for NetBT, which cannot be done in kernel mode:

- It performs DNS name resolution.
- It pings a set of IP address and returns a list of reachable IP addresses.

If this service is disabled, NetBT's clients, including Redirector (RDR), SRV, Netlogon, and Messenger, could stop responding. As a result, you may not be able to share files, printers, and logon.

`TCP/IP Print Server`—enables TCP/IP-based printing using the Line Printer Daemon protocol. If this service is stopped, TCP/IP-based printing will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

`Telephony`—provides Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and through the LAN on servers that are also running the service. The telephony service enables applications to act as clients to telephony equipment such as PBXs, telephones, and modems. The service supports the TAPI under which different wire protocols that communicate with telephony equipment can be supported. These protocols are implemented in Telephony Service Providers (TSPs). The telephony service cannot be stopped if there is another dependent service, such as Remote Access service, currently active. If no other dependent service is running and you stop the telephony service, it will be restarted when any application makes an initialization call to the TAPI interface. If the service is disabled, no program that depends upon it, including modem support, will be able to run.

`Telnet`—allows a remote user to log on to the system and run console programs by using the command line. A computer running the Telnet service can support

connections from various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If the Telnet service is stopped, remote users won't be able to connect to the computer using telnet clients.

Terminal Services—provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server. Terminal Services allows multiple users to be connected interactively to a computer and to the display of desktops and applications to remote computers. **See also** Terminal Services Licensing.

Terminal Services Licensing—installs a license server and provides registered client licenses when connecting to a Terminal Server. The Terminal Services License Service is a low-impact service that stores the client licenses that have been issued for a Terminal server and tracks the licenses that have been issued to client computers or terminals. If this service is turned off, the server will be unavailable to issue Terminal Server licenses to clients when they are requested. If another License Server is discoverable on a DC in the forest, the requesting Terminal Server will attempt to use it. **See also** Terminal Services.

Trivial FTP Daemon— TFTP (trivial file transfer protocol) is an integral part of the Remote Installation Services, this implements support for the TFTP protocol defined in the following RFCs:

- RFC 1350 - TFTP
- RFC 2347 - Option extension
- RFC 2348 - Blocksize option
- RFC 2349 - Timeout interval, transfer size options

To disable this service, uninstall Remote Installation Services. Disabling the service directly will cause Remote Installation Services to malfunction.

Uninterruptible Power Supply—manages communications with a UPS connected to the computer by a serial port. If this service is turned off, communications with the UPS will be lost. In the event of power loss on the AC line, the UPS will be unable to direct the PC to shut down while the UPS battery discharges toward a critically low state. This could result in loss of data.

Utility Manager—starts and configures accessibility tools from one window. Utility Manager allows faster access to some accessibility tools and also displays the status of the tools or devices that it controls. This program saves users time because an administrator can designate that certain features start when Windows 2000 starts. Utility Manager includes three built-in accessibility tools: Magnifier, Narrator, and On-Screen Keyboard.

Volume Snapshot—manages volume snapshots used by backup applications. This service manages the volume snapshots. When a backup application attempts to start a backup utilizing the new snapshots infrastructure, the backup application

calls methods to determine the number of writers that are running on the service, then queries each writer to gather the required metadata. Following this, the backup application can collect the volumes that need to get a snapshot to ensure a successful backup session. The volumes are presented to the snapshot coordinator and a snapshot is created. The snapshot creates volumes that match the original volumes at the snapshot point of time. If turned off, no snap shot backups can be done.

`Windows Installer`—installs, repairs, or removes software according to instructions contained in .MSI files provided with the applications. If disabled, the installation, removal, repair, and modification of applications that make use of the Windows Installer will fail. Some applications make use of this service while running, and those applications might not run. **See also** Application Management.

`Windows Internet Name Service (WINS)`—enables NetBIOS name resolution. Presence of the WINS server(s) is crucial for locating the network resources identified using NetBIOS names. WINS servers are required unless all domains have been upgraded to Active Directory and all computers on the network are running Windows 2000.

Disabling or turning off WINS results in the following:

- Location of the Windows NT 4 domains fails.
- Location of Windows 2000 Active Directory domains by Windows NT 4 clients fails.

NetBIOS name resolution fails unless a device whose name should be resolved is on the same subnet as the device attempting name resolution and the latter is configured to attempt NetBIOS name resolution using broadcast.

`Windows Management Instrumentation (WMI)`—provides system management information. WMI is an infrastructure for building management applications and instrumentation shipped as an integral part of the current generation of Microsoft operating systems. Its primary purpose is to reduce cost of ownership for Microsoft operating systems and applications.

WMI makes applications and systems less expensive and easier to manage by providing comprehensive, easily accessible information about applications and services, including management events those applications and services may generate. WMI provides access to the management data through a number of interfaces, including COM API, scripts and command-line interfaces. WMI is compatible with previous management interfaces and protocols, such as Simple Network Management Protocol (SNMP)

WMI is a crucial part of Microsoft Operations Manager 2000 infrastructure, and the service is used by internal and external partners to access management information. If this service is turned off, this valuable information will be unavailable. **See also** Windows Management Instrumentation Driver Extensions.

Windows Management Instrumentation Driver Extensions—tracks of all of the drivers that have registered WMI information to publish. If the service is turned off, clients cannot access the WMI information published by drivers. However, if the APIs detect that the service is not running, it will attempt to restart it. **See also** Windows Management Instrumentation (WMI).

Windows Media Monitor Service—provides services to monitor client and server connections to the Windows Media™ services.

Windows Media Program Service—groups Windows Media streams into a sequential program for the Windows Media Station Service.

Windows Media Station Service—provides multicasting and distribution services for streaming Windows Media content.

Windows Media Unicast Service—provides Windows Media streaming content on-demand to networked clients.

Windows Time Service (W32Time)—sets the computer clock. W32Time maintains date and time synchronization on all computers running on a Microsoft Windows network. It uses the Network Time Protocol (NTP) to synchronize computer clocks so that an accurate clock value, or timestamp, can be assigned to network validation and resource access requests. The implementation of NTP and the integration of time providers makes W32Time a reliable and scalable time service for enterprise administrators. For computers not joined to a domain, W32Time can be configured to synchronize time with an external time source. If this service is turned off, the time setting for local computers will not be synchronized with any time service in the Windows domain, or an externally configured time service.

Workstation—provides network connections and communications. The workstation service is a user-mode wrapper for the Microsoft Networks redirector. It loads and performs configuration functions for the redirector, provides support for making network connections to remote servers, provides support for the WNet APIs and furnishes redirector statistics. If this service is turned off, no network connections can be made to remote computers using Microsoft Networks.

World Wide Web Publishing Service—provides HTTP services for applications on the Windows platform. The service depends on the IIS administration service and kernel TCP/IP support. If this service is turned off the operating system will no longer be able to serve act as a Web server. **See also** IIS Admin Service.

Vos remarques sur ce document / Technical publications remarks form

Titre / Title :	**Sécurité sur les systèmes DIANE**

N° Référence / Reference No. :	47 F2 02EL 00

Date / Dated :	Juillet 2003

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront attentivement examinées. Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.
Your comments will be promptly investigated by qualified personnel and action will be taken as required. If you require a written reply, furnish your complete mailing address below.

NOM / NAME : ---------- DATE : ----------

SOCIETE / COMPANY : ----------

ADRESSE / ADDRESS : ----------

Remettez cet imprimé à un responsable Bull S.A. ou envoyez-le directement à :
Please give this technical publications remarks form to your Bull S.A. representative or mail to:

Bull S.A.
CEDOC
Atelier de reprographie
357, Avenue Patton BP 20845
49008 ANGERS Cedex 01
FRANCE