Active Directory

Chapter 3 - Deploying Secure Domain Controllers

The Active Directory executables and database are stored on the domain controllers in your Active Directory infrastructure. The domain controllers are the servers in your network infrastructure that you must secure to protect Active Directory. If the security of any domain controller in your Active Directory infrastructure is compromised, the entire Active Directory security is at risk.

An essential part of deploying your domain controllers is ensuring that they are deployed securely. If you are in the process of deploying your domain controllers, the steps in this section include recommendations for deploying your domain controllers in a manner that enhances their security. If you have already deployed your domain controllers, consider whether to configure your existing domain controllers to reflect the security recommendations in this section.

To deploy secure domain controllers, perform the following tasks:

1. Establish secure domain controller build practices.
2. Ensure predictable, repeatable, and secure domain controller deployments.
3. Enable only essential services.
4. Secure domain controller files and executables.
5. Run virus scans on domain controllers.
6. Maintain physical security.

Establishing Secure Domain Controller Build Practices

One of the essential practices in deploying secure domain controllers is building the domain controllers in as secure an environment as possible. Building the domain controllers is the process of installing the Windows 2000 Server operating system and then promoting the server to a domain controller. The physical environment and the method that you use for building domain controllers influence the security of the domain controllers.

Secure domain controller build practices include the following:

- Securing the domain controller build environment
- Selecting secure domain controller build methods

Securing the Domain Controller Build Environment

The domain controller build environment is the network environment (routers, network segments, switches, and so forth) and physical room (datacenter, secured room, wiring closet, utility closet, and so forth) in which you build your domain controllers. Depending on your IT organizational infrastructure, you may have a centralized datacenter that is secure, both from a network perspective and physically. On the other hand, your IT organization infrastructure may have locations that are not secure from either perspective, such as branch offices.

Building Domain Controllers in Datacenter Environments

Whenever possible, build your domain controllers in a secure environment, such as a datacenter. Building your domain controllers in a secure datacenter environment reduces the security risks by restricting domain controller access to trusted personnel during the critical build process. This helps to prevent rogue applications, drivers, services, or configurations from being introduced by unauthorized personnel.

If possible, build domain controllers in the datacenter environment, and then ship them to the final location for deployment. This deployment approach is referred to as a *staged* domain controller deployment.

To help ensure that the domain controller stays secure until deployment, ship the domain controller to the final location using a trusted shipping method, for example, one that requires signatures for the domain controller at the origination and destination locations. Building and shipping the domain controller in this way enhances the integrity of the domain controller.

For more information about building (staging) domain controllers, see the "*Active Directory Branch Office Planning Guide*" on the Microsoft Web site at http://go.microsoft.com/fwlink/?LinkID=3459.

Building Domain Controllers in Branch Office Environments

If your organization supports branch offices, in some instances you may need to build a domain controller in this relatively insecure environment. For example, you may need to replace a failed domain controller on-site. Table 4 lists recommendations and the corresponding rationales for building domain controllers in branch offices.

Table 4 Recommendations for Building Domain Controllers in Branch Offices

Recommendation	Rationale
Limit physical access to domain controllers to trusted personnel only.	To avoid the theft of directory data or the possibility of an altered, less secure domain controller configuration through human intervention, domain controllers should not be left unattended.
Use an automated method for operating system installation and Active Directory promotion.	Domain controllers should be promoted using an automated script to reduce the possibility of human intervention, which could result in a vulnerable domain controller configuration.
Promote and operate new domain controllers in a restricted access area.	To prevent unauthorized users from compromising the domain controller's security, the domain controller should be physically located in a room with restricted access.

Selecting Secure Domain Controller Build Methods

Automating the build process for domain controllers minimizes the possible introduction of rogue programs, rogue services, and insecure configuration into the build process through manual intervention. Automating the installation of Windows 2000 Server helps to ensure a secure platform on which to run Active Directory. Automate the promotion of a server to a domain controller through the use of the Active Directory Installation Wizard (Dcpromo.exe) to ensure that Active Directory is configured in a secure and consistent manner.

Automating the Windows 2000 Installation Process

Automated installation processes for Windows 2000 Server can be categorized as *image-based* and *non-image-based*. Because non-image-based methods can affect the integrity and predictability of the installation process as a result of the need for manual intervention, we recommend using only image-based methods for installing Windows 2000 Server.

When using an image-based process to install Windows 2000 Server, perform the following tasks:

1. Create a clean installation of Windows 2000 Server.
2. Configure server security as specified in the following sections, which appear later in this guide:
   - "Ensuring Predictable, Repeatable, and Secure Domain Controller Deployments"
   - "Enabling Only Essential Services"
   - "Securing Domain Controller Files and Executables."
3. Configure the computer to run Dcpromo.exe when it starts for the first time. For more information, see "Automating the Promotion of Servers to Domain Controllers" later in this guide.
4. Create an image of that computer.
5. Deploy the image to the target computer using one of the methods listed below.
6. Configure computer-specific settings, such as the computer name and IP addresses, on the newly imaged computer.

You can use one of the following image-based methods for the automated installation of Windows 2000 Server:

- SYSPREP
- Remote Installation Services (RIS)
- Third-party tools

If you must use a non-image-based method, unattended setups generally present few security risks and provide consistent server configuration.

SYSPREP, RIS, and unattended setup are Windows 2000 features. Table 5 compares and contrasts SYSPREP, RIS, and unattended setup. Third-party tools have some combination of the features found in each of these technologies. For further information about third-party automated setup software that may be used by your organization, see the documentation that accompanies the software.

Table 5 Comparison of Windows 2000 Automated Installation Methods

Characteristics	SYSPREP	RIS	Unattended Setup
Provides image-based installations	●	●	
Allows a variety of hardware configurations from		●	●

a single automation script or image			
Requires high-bandwidth, well-connected network infrastructure		●	
Appropriate for datacenter deployments	●	●	
Appropriate for branch office deployments	●		●

For more information about SYSPREP, RIS, and unattended setup, see "Automating Server Installation and Upgrade" in the *Windows 2000 Server Deployment Planning Guide* of the Microsoft® Windows® 2000 Server Resource Kit at: http://go.microsoft.com/fwlink/?LinkId=18578

Automating the Promotion of Servers to Domain Controllers

The Active Directory Installation Wizard (Dcpromo.exe), which is used to promote domain controllers, can be automated through the use of an answer file. Automating the promotion process generally increases its predictability and consistency by eliminating the need for manual intervention. When running Dcpromo.exe, use the following command:

dcpromo.exe /answer:*answer_file_name*

You can automatically start Dcpromo.exe after you complete the installation of Windows 2000 Server by running this command the first time the server starts. Automatically starting Dcpromo.exe ensures that the promotion to a domain controller occurs immediately after the implementation of Windows 2000 Server. This reduces the potential for the introduction of unauthorized files or executables before the server is promoted. Configure the server to automatically start Dcpromo.exe just before making your image.

Automatically start Dcpromo.exe the first time the server starts, following the installation of Windows 2000, by using one of the following methods:

- For third-party tools or RIS-based deployments, add the following entry under the registry key **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**:

  Entry name: `dcpromo`
  Data type: `REG_SZ`
  Value: `dcpromo.exe`

  > **Caution** Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference in the *Microsoft Windows 2000 Server Resource Kit* at http://go.microsoft.com/fwlink/?LinkId=9372.

- For SYSPREP, modify the [GuiRunOnce] section of the Sysprep.inf answer file before running SYSPREP.

  The following is an example of a Sysprep.inf answer file that is modified to start Dcpromo.exe automatically the first time the server starts:

```
[GuiRunOnce]
Command0 = "dcpromo /answer:ansfile.txt"
```

If you are creating an image of a server that you plan to use for imaging multiple domain controllers, place the Dcpromo.exe answer file on a floppy disk so that one image can be used to deploy all domain controllers. Also, ensure that the Dcpromo.exe answer file path designates the floppy disk drive.

> **Important** Because the Dcpromo.exe answer file is stored on the floppy disk in plaintext, do not include an administrative account name or a password in this file. This information must be entered during the automated domain controller promotion process. The answer file automatically provides all other parameters.

For more information about automating the promotion of servers to domain controllers, see "Automating Server Installation and Upgrade" in the *Windows 2000 Server Deployment Planning Guide* of the *Windows 2000 Server Resource Kit* on the Microsoft Web site at http://go.microsoft.com/fwlink/?LinkId=18578.

Ensuring Predictable, Repeatable, and Secure Domain Controller Deployments

Throughout the domain controller deployment process, there are security configuration settings that you need to apply to all domain controllers. To ensure that these security settings are applied uniformly to all domain controllers, implement a predictable, repeatable domain controller deployment process by performing the following tasks:

1. Install Windows 2000 Server with the latest service packs and hotfixes.
2. Disable NTFS automatic 8.3 name generation.
3. Run virus-scanning software on the server.

4. Select secure domain controller promotion settings.
5. Prohibit the use of cached credentials when unlocking a domain controller console.
6. Create a reserve file to enable recovery from potential disk-space, denial-of-service attacks.

Installing Windows 2000 Server with Service Packs and Hotfixes

When you create the first master image of a secure Windows 2000 server to be used for installing and promoting multiple domain controllers, apply the configuration settings that are listed in Table 6 to enhance security.

In situations where your domain controllers already exist, check these recommendations and modify domain controller configurations accordingly.

Table 6 Configuration Settings for Windows 2000 Servers

Setting	Rationale
Format all partitions as NTFS.	NTFS provides a secure file system.
Install only TCP/IP as the transport protocol.	Limiting transport protocols reduces the attack surface on the domain controller.
Do not install Internet Information Services (IIS); remove its default selection during Windows 2000 Server setup.	IIS is not required for domain controller operations. Eliminating IIS on dedicated domain controllers reduces the attack surface.
Do not install Simple Mail Transfer Protocol (SMTP) during Windows 2000 Server setup unless you are using SMTP for Active Directory intersite replication.	SMTP is not required for normal domain controller operations unless it is used for intersite replication. This recommendation reduces the attack surface on the domain controller.
Do not install Indexing Service; remove its default selection during Windows 2000 Server setup.	Indexing Service is not required for domain controller operations. Inadvertently indexing files can make the location and content of the files available through Web query interfaces. This recommendation reduces the attack surface on the domain controller.
Install Domain Name System (DNS) by selecting it during Windows 2000 Server setup.	Installing DNS during Windows 2000 Server setup ensures that DNS is available in the master image.
Use a strong password for the computer local administrator account.	A strong password reduces the threat of spoofing this administrator account, which becomes the domain "Administrator" account after the server is promoted to a domain controller.

Creating a Strong Administrator Password

A strong password minimizes the threat of an attacker guessing (cracking) the password and acquiring the credentials of the administrator account (spoofing). A strong password includes all of the following characteristics:

- Contains at least nine characters.
- Does not contain an account name, real name, or company name.
- Does not contain a complete dictionary word.
- Is significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3 ...) are not strong.
- Contains at least one symbol in the first seven characters.
- Contains characters from each of the groups listed in Table 7.

Table 7 Groups of Characters to Include in Strong Passwords

Uppercase letters	A, B, C ...
Lowercase letters	a, b, c ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)	` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

Examples of strong passwords are Pa$sw0rD1 and J*p2leO4>F.

After you complete the installation of Windows 2000 Server, obtain any additional security protections that may have been implemented for Windows 2000 Server by applying the most recent service packs and security-related hotfixes from the Microsoft Web site at http://go.microsoft.com/fwlink/?LinkId=102.

Disabling NTFS Automatic 8.3 Name Generation

Many viruses and utilities that are used by attackers are 16-bit applications that expect 8.3-compatible file names. Secure domain controllers do not run 16-bit applications locally. Therefore, disable 8.3 automatic name generation to prevent these viruses and utilities from compromising your domain controller security.

Disable automatic 8.3 name generation by setting the following entry under the registry key **HKLM\SYSTEM\CurrentControlSet\Control\FileSystem**:

Entry name: `NtfsDisable8dot3NameCreation`
Data type: `REG_DWORD`
Value: `1`

> **Caution** Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference in the *Microsoft Windows 2000 Server Resource Kit* at http://go.microsoft.com/fwlink/?LinkId=9372.

You can create a script that disables automatic 8.3 name generation on all domain controllers in the domain automatically by performing the following tasks:

1. Create the ComputerSearch.vbs script, and copy it to a computer that is a member of the domain.

   For information about how to create this script, see "Identifying Computers to Receive New Registry Settings with ComputerSearch.vbs" in "Appendix B: Procedures" of the *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II*.

2. Create a list of domain controllers in the domain by typing the following command at a command prompt:

   ```
   Cscript computersearch.vbs /r:DC
   ```

   This command creates a list of domain controllers in the domain and saves this list as *ComputerSearch-date-time.csv*.

3. Create the ApplyReg.vbs script and copy it to a computer that is a member of the domain.

   For information about how to create this script, see "Applying Registry Settings to a List of Computers with ApplyReg.vbs" in "Appendix B: Procedures" of the *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II*.

4. Create a .reg file for the following path, registry entry, and value:

   ```
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem]
   ```

   ```
   "NtfsDisable8dot3NameCreation"=dword:00000001
   ```

   Save the file as *Registryfile*.reg. For information about how to create the .reg file, see "Creating a .reg File" in "Appendix: Procedures" of this guide:

5. Apply the registry entry to the domain controllers by typing the following command at the command prompt:

   ```
   Cscript ApplyReg.vbs /r:registryfile.reg /f:ComputerSearch-date-time.csv
   ```

   This task applies the registry changes that are expressed in the file *Registryfile*.reg to all computer that are listed in the file ComputerSearch-*date-time*.csv.

Running Virus-Scanning Software on the Server

After you install Windows 2000 Server, but before you promote the server to a domain controller, install and run antivirus software on the domain controller to ensure that no viruses have been introduced during the installation of Windows 2000 Server.

For image-based methods of automating the installation of Windows 2000 Server, make sure that you install the virus-scanning software as part of the image. For other methods, install and run the virus scanning software immediately after installing Windows 2000 Server.

> **Note** If you are automatically starting Dcpromo.exe by using one of the RunOnce methods discussed later in this section, modify your scripts to run the virus-scanning software first and then automatically start Dcpromo.exe.

Selecting Secure Domain Controller Promotion Settings

During domain controller promotion, a number of configuration settings should be applied to the server to enhance security. These settings are specified in the Dcpromo.exe answer file.

Note Many of the configuration settings that are required for domain controller promotion depend on whether you are installing the first domain controller or an additional domain controller in the forest or domain. If you are installing the first domain controller in the forest or domain, the configuration settings in the Dcpromo.exe answer file are different from the settings that are required for adding a domain controller to an existing domain.

Specifying Locations for the Active Directory Database, Logs, and SYSVOL

By default, Dcpromo.exe places the database, log files, and SYSVOL folder on the system volume. During the promotion of a server to a domain controller, the Dcpromo.exe answer file can specify an alternative location for the Active Directory database (Ntds.dit), log files, and SYSVOL folder. Table 8 provides recommended alternative locations for these Active Directory components for enhanced security and improved performance.

Table 8 Recommended Drive Locations for Active Directory Components

Recommendation	Security Rationale
Place the database and SYSVOL folder on the same dedicated physical drive that does not contain the system volume.	• The system volume is a common target of disk-space attacks, such as spooling large print jobs. Putting the database on a separate drive makes it immune to damage caused by attacks that target the system volume. • Placing the database and SYSVOL in a location other than the default location reduces the likelihood of disk-space attacks. • Attacks can be performed against IIS that allow unauthorized users to navigate the folder structure of its disk volume. Because Web sites are typically stored on the system volume, this increases the risk of information disclosure on this volume. Although dedicated domain controllers are recommended, this cannot always be adhered to in a branch office situation. • This recommendation improves the reliably of recovering Active Directory operations after a disk-space attack. For more information, see "Creating a Reserve File to Enable Recovery from Disk-Space Attacks" later in this guide.
Place the log files on a dedicated physical drive that does not contain the system volume.	• This recommendation has no security implications, but it will improve performance. The system volume typically includes the paging file, which has high disk utilization.

On existing domain controllers, move the Active Directory database, log files, and SYSVOL folder to a dedicated physical drive, for the reasons described in Table 8.

For information about:

- Moving the database and log files, see "Moving the Directory Database Files to a Local Drive" in the Active Directory Operations Guide at http://go.microsoft.com/fwlink/?LinkId=18545.
- Moving the SYSVOL folder, see "Moving SYSVOL Manually" in the Active Directory Operations Guide at http://go.microsoft.com/fwlink/?LinkId=18545.

Disabling Pre–Windows 2000 Compatibility

During the promotion of the first domain controller in a domain, one optional configuration setting that significantly affects Active Directory security is "Permissions compatible with pre–Windows 2000 servers." This setting enables Pre–Windows 2000 Compatibility for certain applications that need to query the directory using anonymous access.

Applications or services that may query the directory using anonymous access include those applications or services that run in the security context of Local System:

- On a server running Windows NT 4.0 within or outside the forest.
- On a server running Windows 2000 in a trusting domain outside the forest.

An example of such an application or service is the Routing and Remote Access Service (RRAS) running on Windows NT 4.0.

In Active Directory, the group Pre–Windows 2000 Compatible Access is assigned Read permissions on the domain root, as well as on all user, computer, and group objects. When you enable Pre–Windows 2000

Compatibility, the special group Everyone is added as a member of the Pre–Windows 2000 Compatible Access group. Because Everyone includes anonymous users, in addition to authenticated users, anyone with network access can read these objects.

When this setting is enabled, any user with network access, even one without an account in the forest, can query and discover information about Active Directory users, groups, and computers. If you do not have applications that require Active Directory access enabled for Pre–Windows 2000 Compatibility, you should not select this setting during domain controller promotion.

Note By default, the setting **Permissions compatible with pre–Windows 2000 servers** is selected in the Active Directory Installation Wizard.

Analyzing the Need for Pre–Windows 2000 Compatibility

Disable Pre–Windows 2000 Compatibility, unless your applications require anonymous access to Active Directory. Before deploying a production domain, you need to know whether it will be possible to disable Pre–Windows 2000 Compatibility. During the lab testing phase of your deployment, determine the applications that require anonymous access by performing the following tasks:

1. When deploying the first domain controller in your test domain, select **Permissions compatible with pre–Windows 2000 servers**.
2. Include at least one instance of each application running in your organization.
3. Enable security auditing on all domain controllers in the test domain to monitor anonymous access to the directory. Collect security logs for 30 days.

   For additional information about performing this task, see "Enabling Monitoring for Anonymous Access" in "Appendix: Procedures" later in this guide.
4. Analyze the security logs for computers that initiate anonymous access to the directory.

   For additional information about performing this task, see "Monitoring for Anonymous Access" in "Appendix: Procedures" later in this guide.
5. Identify the applications or services running on the computers from which anonymous access was initiated.

Note Access to resources between domains that are connected by an external trust requires Pre–Windows 2000 Compatibility. Because external trusts only support NTLM authentication, queries to a directory in a different forest are always handled as anonymous access.

After you have determined the applications that require anonymous access, determine if the applications can be upgraded to versions that do not require anonymous access. After upgrading the applications to newer versions, verify that the applications no longer require anonymous access in your lab environment.

Typically, a newer version of the software, for example, Routing and Remote Access in Windows 2000, does not require anonymous access. Whenever possible, upgrade to a newer version of the software running on Windows 2000 or later operating systems so that you can disable Pre–Windows 2000 Compatibility.

Prohibiting the Use of Cached Credentials When Unlocking a Domain Controller Console

When the console on a domain controller is locked, either by the action of a user or automatically by a screensaver time-out, the console must be unlocked to regain access to the domain controller. The domain controller maintains cached credentials for any users that have been authenticated locally. When the console is unlocked, by default the domain controller uses these cached credentials, if they exist, for the user who attempts to unlock the console.

When cached credentials are used to unlock the console, any changes to the account, such as user rights assignment, group membership changes, or disabling of the account, are not enforced. For example, if an administrator, who is logged on to a domain controller console, is terminated, he can still unlock the console, even if his account is disabled. To ensure that any changes to the account are enforced immediately, require domain controller authentication of the account to unlock the console, instead of cached credentials.

You can configure the domain controller to require domain controller authentication to unlock the domain controller console by adding or modifying the following entry under the registry key **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon**:

Entry name: `ForceUnlockLogon`
Data type: `REG_DWORD`
Value: `1`

Caution Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference in the *Microsoft Windows 2000 Server Resource Kit* at http://go.microsoft.com/fwlink/?LinkId=9372.

You can create a script that specifies automatically that domain controller authentication is required to unlock any domain controllers in the domain by performing the following tasks:

1. Create the ComputerSearch.vbs script, and copy it to a computer that is a member of the domain.

   For information about how to create this script, see "Identifying Computers to Receive New Registry Settings with ComputerSearch.vbs" in "Appendix B: Procedures" of the *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II*.

2. Create a list of domain controllers in the domain by typing the following command at a command prompt:

   ```
   Cscript computersearch.vbs /r:DC
   ```

   This command creates a list of domain controllers in the domain and saves this list as ComputerSearch-*date-time.*csv.

3. Create the ApplyReg.vbs script, and copy it to a computer that is a member of the domain.

   For information about how to create this script, see "Applying Registry Settings to a List of Computers with ApplyReg.vbs" in "Appendix B: Procedures" of the *Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II*.

4. Create a .reg file for the following path, registry entry, and value:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
   "ForceUnlockLogon"=reg_dword:00000001
   ```

   Save the file as *Registryfile*.reg. For information about how to create the .reg file, see "Creating a .reg File" in "Appendix: Procedures" of this guide.

5. Apply the registry entry to the domain controllers by typing the following command at the command prompt:

   ```
   Cscript ApplyReg.vbs /r:registryfile.reg /f:ComputerSearch-date-time.csv
   ```

   This set of tasks applies the registry changes that are expressed in the file *Registryfile*.reg to all computers that are listed in the file ComputerSearch-*date-time*.csv.

Creating a Reserve File to Enable Recovery from Disk-Space Attacks

Many security attacks attempt to consume the system resources of the targeted system. One of the commonly attacked system resources is available disk space. Available disk space can be exhausted by the addition of a large number of objects to the directory by a malicious user or administrator. Active Directory requires that deleted objects continue to exist in the directory as *tombstones* for an extended period of time to allow the deletion to replicate. Therefore, the disk space that is consumed by the deleted objects cannot be reclaimed until the tombstone lifetime has expired (by default, 60 days).

One way of mitigating the effects of this type of attack is by implementing preventive measures. You can provide for a fast recovery by creating a reserve file on the same disk volume as the Active Directory database (Ntds.dit file). A reserve file is simply a large file that takes up available disk space. In the event that an attacker exhausts all disk space by adding a large number of objects to the directory, you can delete the reserve file to quickly restore normal operation while the rogue objects inside Active Directory are identified and removed. For a procedure for performing this task, see "Creating a Reserve File" in "Appendix: Procedures" later in this guide.

Enabling Only Essential Services

Every service running on a domain controller provides a potential target for an attack that can compromise domain controller security. Therefore, it is prudent to enable only those services that are essential to normal domain controller function, so that you can reduce the surface area of attack. Table 9 lists the services that are installed during Windows 2000 Server installation if you follow the security recommendations provided in "Installing Windows 2000 Server with Service Packs and Hotfixes" earlier in this guide. Table 9 also provides the recommended startup type for each service to be configured.

Note For new domain controller deployments, configure these service startup types before creating the master image for image-based deployments, as discussed in "Automating the Windows 2000 Installation Process" earlier in this guide.

Table 9 Recommended Services to Install on Windows 2000 Server

Service Name	Default Startup Type	Recommended Startup Type	Comment
Alerter	Automatic	(No change)	Notifies selected users and computers of administrative alerts.

Application Management	Manual	(See comment)	Provides software installation services for applications that are deployed through Add/Remove Programs. On dedicated domain controllers, this service can be disabled to prevent unauthorized installation of software.
Automatic Updates	Automatic	(See comment)	Provides the download and installation of critical Windows updates, such as security patches or hotfixes. This service can be disabled when automatic updates are not performed on the domain controller. It is included when Service Pack 3 (SP3) is applied.
Background Intelligent Transfer Service	Manual	(See comment)	Provides a background file transfer mechanism and queue management, and it is used by Automatic Update to automatically download programs, such as security patches. This service can be disabled when automatic updates are not performed on the domain controller. It is included when SP3 is applied.
ClipBook	Manual	(See comment)	Enables the Clipbook Viewer to create and share "pages" of data to be reviewed by remote users. On dedicated domain controllers, this service can be disabled.
COM+ Event System	Manual	(No change)	Provides automatic distribution of events to COM components.
Computer Browser	Automatic	(See comment)	Maintains the list of computers on the network, and supplies the list to clients that request the list. If you do not have earlier versions of clients that use this feature, set to Manual.
DHCP Client	Automatic	(See comment)	Updates DNS records using Dynamic update. If your organization does not use dynamic IP addresses for domain controllers, set to Manual.
Distributed File System	Automatic	(No change)	Manages logical volumes that are distributed across a local area network (LAN) or wide area network (WAN), and it is required for the Active Directory SYSVOL share.
Distributed Link Tracking Client	Automatic	Disabled	Maintains links between NTFS v5 file system files on the domain controllers and other servers in the domain. Disable this service on dedicated domain controllers.
Distributed Link Tracking Server	Manual	Disabled	Tracks information about files that are moved between NTFS v5 volumes throughout a domain. Disable this service on dedicated domain controllers.
DNS Client	Automatic	(No change)	Allows resolution of DNS names.
DNS Server	Automatic	(No change)	Required for Active Directory–integrated DNS zones.

Event Log	Automatic	(No change)	Writes event log messages that are issued by Windows-based programs and components to the log files.
Fax Service	Manual	Disabled	Provides the ability to send and receive faxes through fax resources that are available on the domain controller and the network. On dedicated domain controllers, this service can be disabled, because sending and receiving faxes is not a normal function of a domain controller.
File Replication Service	Manual	(No change)	Enables files to be automatically copied and maintained simultaneously on multiple computers, and it is used to replicate SYSVOL among all domain controllers.
Indexing Service	Manual	(See comment)	Indexes content and properties of files on the domain controller to provide rapid access to the file through a flexible querying language. On dedicated domain controllers, disable this service to prevent users from searching files and file content if sensitive files and folders are inadvertently indexed.
Internet Connection Sharing	Manual	Disabled	Provides network address translation (NAT), addressing and name resolution, and intrusion detection when connected through a dial-up or broadband connection. On dedicated domain controllers, disable this service to prevent inadvertent enabling of NAT, which would prevent the domain controller from communicating with the remainder of the network.
Intersite Messaging	Disabled	(No change)	Required by SMTP replication in Active Directory, Distributed File System (DFS), and Netlogon.
IPSEC Policy Agent	Automatic	(See comment)	Provides management and coordination of Internet Protocol security (IPSec) policies with the IPSec driver. If your organization does not use IPSec, set the startup type to Manual.
Kerberos Key Distribution enter	Disabled	(No change)	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
License Logging Service	Automatic	(See comment)	Monitors and records client access licensing for portions of the operating system, such as IIS, Terminal Services, and file and print sharing, and for products that are not a part of the operating system, such as Microsoft® SQL Server or Microsoft® Exchange Server. On a dedicated domain controller, this service can be disabled.

Logical Disk Manager	Automatic	(No change)	Required to ensure that dynamic disk information is up to date.
Logical Disk Manager Administrative Service	Manual	(No change)	Required to perform disk administration.
Messenger	Automatic	(See comment)	Transmits net sends and Alerter service messages between clients and servers. If your organization does not use this feature, set the startup type to Manual.
Net Logon	Manual	(No change)	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and trusting domains.
NetMeeting Remote Desktop Sharing	Manual	Disabled	Eliminates a potential security threat by allowing domain controller remote administration through NetMeeting.
Network Connections	Manual	(No change)	Manages objects in the Network Connections folder.
Network DDE	Manual	(See comment)	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the domain controller. This service can be disabled when no DDE applications are running locally on the domain controller.
Network DDE DSDM	Manual	(See comment)	Used by Network DDE. This service can be disabled when Network DDE is disabled.
NTLM Security Support Provider	Manual	(No change)	Provides security to remote procedure call (RPC) programs that use transports other than named pipes, and enables users to log on using the NTLM authentication protocol.
Performance Logs and Alerts	Manual	(See comment)	Collects performance data for the domain controller, writes the data to a log, or generates alerts. This service can be set to automatic when you want to log performance data or generate alerts without an administrator being logged on.
Plug and Play	Automatic	(No change)	Automatically recognizes and adapts to changes in the domain controller hardware with little or no user input. If your organization does not change hardware on domain controllers, set the startup type to Manual.
Print Spooler	Automatic	(See comment)	Manages all local and network print queues, and controls all print jobs. Can be disabled on dedicated domain controllers where no printing is required.
Protected Storage	Automatic	(No change)	Protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. This service is used on domain controllers

			for smart card logon.
QoS RSVP	Manual	(See comment)	Provides support for Quality of Service (QoS) Resource Reservation Protocol (RSVP) routing information. This service can be disabled when QoS is not used to allocate network bandwidth in network infrastructure.
Remote Access Auto Connection Manager	Manual	(See comment)	Detects unsuccessful attempts to connect to a remote network or computer, and provides alternative methods for connection. This service can be disabled on dedicated domain controllers where no virtual private network (VPN) or dial-up connections are initiated.
Remote Access Connection Manager	Manual	(See comment)	Manages VPN and dial-up connection from the domain controller to the Internet or other remote networks. This service can be disabled on dedicated domain controllers where no VPN or dial-up connections are initiated.
Remote Procedure Call (RPC)	Manual	(No change)	Serves as the RPC endpoint mapper for all applications and services that use RPC communications.
Remote Procedure Call (RPC) Locator	Automatic	(No change)	Enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database.
Remote Registry Service	Automatic	(No change)	Enables remote users to modify registry settings on the domain controller, provided that the remote users have the required permissions. By default, only Administrators and Backup Operators can access the registry remotely.
Removable Storage	Automatic	(See comment)	Manages and catalogs removable media, and operates automated removable media devices, such as tape auto loaders or CD jukeboxes. This service can be disabled when removable media devices are not directly connected to the domain controller.
Routing and Remote Access	Disabled	(No change)	Enables LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services.
RunAs Service	Automatic	(No change)	Allows you to run specific tools and programs with different privileges than your current logon provides.
Security Accounts Manager	Automatic	(No change)	A protected subsystem that manages user and group account information.
Server	Automatic	(No change)	Provides RPC support, file print, and named pipe sharing over the network.
Smart Card	Manual	(No change)	Manages and controls access to a smart card that is inserted into a smart card reader that is attached to

			the domain controller.
Smart Card Helper	Manual	(No change)	Provides support for legacy, non-plug-and-play smart card readers.
System Event Notification	Automatic	(No change)	Monitors system events and notifies subscribers to the COM+ Event System of these events.
Task Scheduler	Automatic	(No change)	Provides the ability to schedule automated tasks on the domain controller.
TCP/IP NetBIOS Helper Service	Automatic	(No change)	Provides support for the NetBIOS over TCP/IP (NetBT) service and network basic input/output system (NetBIOS) name resolution for clients.
Telephony	Manual	(See comment)	Provides Telephony API (TAPI) support of client programs that control telephony devices and IP-based voice connections. This service can be disabled on dedicated domain controllers where TAPI is not used by applications.
Telnet	Manual	Disabled	Enables a remote user to log on and run applications from a command line on the domain controller. Enable Telnet only when it is used for remote administration for branch offices or remotely administered domain controllers. Terminal Services is the recommended method for remote administration.
Terminal Services	Disabled	(See comment)	Allows multiple remote users to be connected interactively to the domain controller, and provides display of desktops and run applications. To reduce the surface area of attack, disable Terminal Services unless it is used for remote administration for branch offices or remotely administered domain controllers.
Uninterruptible Power Supply	Automatic	(No change)	Manages an uninterruptible power supply (UPS) that is connected to the domain controller by a serial port.
Utility Manager	Manual	Disabled	Allows faster access to some accessibility tools, such as Magnifier, Narrator, and On-Screen Keyboard, and also displays the status of the tools or devices that it controls. Disable Utility Manager unless you require these special accessibility tools.
Windows Installer	Manual	(No change)	Adds, modifies, and removes applications that are provided as a Windows Installer (.msi) package.
Windows Management Instrumentation	Manual	(No change)	Provides a common interface and object model to access management information about the domain controller through the WMI interface.
Windows Management	Manual	(No change)	Monitors all drivers and event trace

Instrumentation Drivers			providers that are configured to publish WMI or event trace information.
Windows Time	Manual	(No change)	Sets the domain controller clock, and maintains date and time synchronization on all computers in the network.
Workstation	Automatic	(No change)	Creates and maintains client network connections to remote servers.

Note The antivirus software installed earlier in the process describe in this section may run as a service in Windows 2000 Server. Do not change the default configuration of your antivirus software.

Table 10 lists the changes to the service startup configuration when a server running Windows 2000 is promoted to a domain controller. This table is provided as a reference, and you can combine it with the list in Table 9 to arrive at the final list of services to have running on a domain controller.

Table 10 Recommended Changes to Service Startup Type After Promotion to Domain Controller

Service Name	Default Startup Type	Recommended Startup Type	Comment
Distributed Link Tracking Server	Automatic	Disabled	Tracks information about files that are moved between NTFS v5 volumes throughout a domain. Disable this service on dedicated domain controllers.
File Replication Service	Automatic	(No change)	Enables files to be automatically copied and maintained simultaneously on multiple computers. This service is used to replicate SYSVOL between all domain controllers.
Intersite Messaging	Automatic	(No changes)	Required by SMTP replication in Active Directory, DFS, and Netlogon.
Kerberos Key Distribution enter	Automatic	(No change)	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
Net Logon	Automatic	(No change)	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and in trusting domains.
Remote Procedure Call (RPC) Locator	Automatic	(No change)	Enables RPC clients using the RpcNs* family of APIs to locate RPC servers and manage the RPC name service database.
Windows Management Instrumentation	Automatic	(No change)	Provides a common interface and object model to access management information about the domain controller through the WMI interface.
Windows Time	Automatic	(No change)	Sets the domain controller clock, and maintains date and time synchronization on all computers in the network.

The recommended services as listed in Table 9 and Table 10 are just the services that are required to support a dedicated domain controller. Although it is recommended that you have only dedicated domain controllers, if your domain controller serves other roles, such as a file server or print server, you may need to enable other services for proper operation.

Securing Domain Controller Files and Executables

When Windows 2000 Server is installed with NTFS partitions, the files and executables on the server are assigned baseline NTFS permissions. After successfully promoting a server to a domain controller, Dcpromo.exe sets secure NTFS permissions on the system files and executables, as well as on Active Directory files and folders.

After promotion to domain controller, the default permissions on the root of each logical disk volume grant Full Control access to the special group Everyone. This causes the root of each disk volume, including the volume housing the Active Directory database files, to be susceptible to disk-space attacks.

To guard against this threat, secure each volume with the additional settings listed in Table 11.

Table 11 Additional Files and Folders to Be Secured After Promotion to Domain Controller

File or Folder	Permissions
Root of each logical disk volume	• Allow Read and Execute for Everyone • Allow Full Control for Administrators

Running Virus Scans on Domain Controllers

After domain controllers are promoted, continue to run virus scans and to obtain regular virus signature updates from your antivirus software vendor. Before you initiate regular antivirus scanning, be aware that some antivirus software can interfere with the proper operation of domain controllers by:

- Interfering with directory database and log file access by the Extensible Storage Engine (ESE).
- Interfering with File Replication service (FRS) database and log file access by ESE.
- Causing excessive replication by FRS.

Some versions of antivirus software modify the security descriptor of files during scans. Modifying security descriptors triggers FRS, which creates high volumes of replication traffic unnecessarily. These issues with running antivirus software on domain controllers are addressed by the recommendations in the following three sections.

For more information about using antivirus software on your domain controller, see article 284947, "Antivirus Problems May Modify Security Descriptors Causing Excessive Replication of FRS Data in Sysvol and DFS" in the Microsoft Knowledge Base at http://go.microsoft.com/fwlink/?LinkId=4441.

Preventing Interference Between Virus Scans and Active Directory Database and Log File Access

ESE, which underlies Active Directory, opens database and log files in exclusive mode. This means that if the antivirus software opens one of these files, ESE fails when it tries to open the same file. Alternatively, the antivirus software cannot open these files for scanning if they have already been opened by ESE.

Furthermore, these database and log files have internal checksums that, when altered through file changes by the antivirus software, can cause either an access error to occur or the database to fail on restart or restore. In all cases, this results in Active Directory failing on the domain controller.

To run antivirus software on your domain controllers, configure the antivirus software to exclude from scanning the Active Directory database and log files that are specified in Table 12.

Table 12 Files Not Scanned and Registry Entry Values Specifying Their Location

Exclude from Scan	In HKLM\System\Services\NTDS\Parameters
Ntds.dit	**DSADatabaseFile**
Edb*.log, Edb*.pat, Res.log, and Res2.log	**DatabaseLogFilesPath**
Temp.edb and Edb.chk	**DSAWorkingDirectory**
Ntds.pat	**DSADatabaseFile**

Note For Windows Server 2003 and later operating systems, the Ntds.pat file is no longer used. Therefore, it is not an issue when you run antivirus software on those operating systems.

Excluding the files in Table 12 from regular virus scanning does not increase a domain controller's vulnerability to a virus attack. Viruses tend to attach to files that are executed, such as binaries or scripts, rather than to data files. Dedicated domain controllers with no user-modifiable content are therefore less vulnerable to common virus attacks.

Preventing Interference Between Virus Scans and FRS Database and Log File Access

As previously explained for Active Directory database access, either the antivirus software can prevent ESE from opening the FRS database and log files or the other way around. Furthermore, a change in the internal checksums of these files can cause an access error to occur or the database to fail on restart or restore. In all cases, this results in Active Directory failing on the domain controller.

To run antivirus software on your domain controllers, configure the antivirus software to exclude from regular virus scanning the FRS database and log files that are specified in Table 13.

Table 13 Files and Folders Not Scanned and Registry Entry Values Specifying Their Location

Exclude Files from Scan	**In HKLM\System\CurrentControlSet\Services\NtFrs\Parameters**
Jet\sys\edb.chk, jet\ntfrs.jdb and jet\log*.log	**WorkingDirectoryFile**
Log*log	**DBLogFileDirectory**
Exclude Folders from Scan	**HKLM\ System\CurrentControlSet\Services\NtFrs\Parameters\ ReplicaSets\GUID**
replica_root	**ReplicaSetRoot**
staging_directory	**ReplicaSetStage**
preinstall_directory	*replica_root***DO_NOT_REMOVE_Ntfrs_Preinstall_Directory**

Preventing Virus Scans from Triggering Excessive FRS Replication

Domain controllers running Windows 2000 use FRS to replicate system policy and logon scripts that reside in the SYSVOL folder. Antivirus software can interfere with the normal functioning of FRS by modifying the security descriptor and the time stamp of files in the SYSVOL folder. This causes FRS to replicate the changes to other domain controllers, which create a high volume of file replication traffic.

Because some antivirus software scans every file and directory in an FRS replicated tree, this action is similar to requesting a full synchronization of all files and folders from every domain controller running the antivirus software. Administrators may see the following symptoms of this problem in their environments:

- Files in SYSVOL shares replicate excessively.
- Network traffic between replication partners consumes excessive bandwidth.
- The number of files in the staging directory constantly grows and then empties sometime after the antivirus scan completes or after FRS replication.

  Note The staging directory behavior changes for Windows Server 2003, Windows 2000 Server SP3 and later. These systems contain an updated FRS version that leaves staging files in place for one week before removing them.

For more information about running antivirus software on domain controllers, see article 815263, "Antivirus, Backup, and Disk Optimization Programs That Are Compatible with the File Replication Service" in the Microsoft Knowledge Base at http://go.microsoft.com/fwlink/?LinkId=4441.

You can prevent antivirus software from causing excessive replication, while continuing to maintain a high level of security on domain controllers, by performing the following tasks:

- Configure antivirus software to not scan files in the SYSVOL directory tree.
- Require script signing on domain controllers and administrative workstations.

Excluding Antivirus Scanning of SYSVOL

Antivirus software can interfere with the normal functioning of FRS by modifying the security descriptor and time stamp of files in the SYSVOL folder. This triggers FRS to replicate the changes in the SYSVOL folder to other domain controllers, creating a high volume of file replication traffic. The result is excessive FRS replication between domain controllers.

Note The following antivirus applications do not modify SYSVOL files in a way that triggers excessive replication:

- eTRUST Antivirus build 96 or later with the NTFS incremental scan feature disabled
- McAfee/NAI NetShield 4.50 with the NetShield Hot Fix Rollup
- Norton Antivirus 7.6 or later

To run antivirus software on domain controllers, configure the antivirus software to exclude from scanning the SYSVOL folder its subdirectories.

Requiring Script Signing on Domain Controllers and Administrative Workstations

In contrast to the situation for the directory database and log files, excluding the SYSVOL folder from virus scanning does increase the risk of a virus attack on a domain controller. Viruses tend to attach to files that are executed, such as binaries or scripts. If you exclude the SYSVOL folder from virus scans, you increase the risk of virus attacks on logon scripts and startup scripts in the SYSVOL folder on domain controllers. As a countermeasure, implement script signing to protect the integrity of scripts running on domain controllers and administrative workstations.

Windows 2000 supports the enforcement of script signing to validate the integrity of scripts and binaries before executing them. Establish a practice for your organization that requires all scripts in the SYSVOL folder to be signed. Windows Script Host (WSH) scripts (such as .vbs, .js, and .wmf scripts) can be signed or verified using the same tools that are ordinarily used to sign other executables. The script signer, one of the security tools provided by WinTrust, generates a digital signature of the contents of a script. That information is then formatted as a comment and added to the end of the script.

Note You can obtain the WinTrust tools for signing and verifying scripts (signcode.exe and chktrust.exe, respectively) in the Windows 2000 Platform Software Development Kit (SDK).

Sign scripts, and verify that the scripts are properly signed, by performing the following tasks on every domain controller and administrative workstation:

1. To require that only signed scripts be run on a computer, add the following entry under the registry key **HKEY_LOCAL_SYSTEM\Software\Microsoft\Windows Script Host**:

   ```
   Entry name: TrustPolicy
   Data type: REG_DWord
   Value: 2
   ```

   Caution Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the Registry Reference in the *Microsoft Windows 2000 Server Resource Kit* at http://go.microsoft.com/fwlink/?LinkId=9372.

2. Enroll to acquire a certificate from an internal certification authority (CA).

   Choose an internal CA so that confirmation of the current validity of the certificate does not require an Internet lookup. To ensure that the certificate has not been revoked, the code checks the CA's certificate revocation list (CRL).

3. Secure all scripts by signing.

   Two alternatives exist for creating signed scripts. If you are interested in developing your own script host, the Windows Product SDK contains a set of tools for signing scripts (signcode.exe and chktrust.exe). Alternatively, WSH version 5.6 ships with a signer object to sign or verify scripts.

4. Verify that all scripts are signed.

   For the code required to verify that the scripts have been signed, see "Securing Scripts with Script Signing" in "Appendix: Procedures" later in this guide.

   Note As a minimum, you should enforce script signing on domain controllers and administrative workstations. However, it is a best practice recommendation that script signing be enforced on all computers on the network running operating systems that support script signing. Operating systems that support script signing include the Windows 2000 family of operating systems, Windows XP, and the Windows Server 2003 family.

For more information about implementing script signing, see:

- "Digital Code Signing Step-by-Step Guide" on the Microsoft MSDN Web site at http://go.microsoft.com/fwlink/?LinkId=18548.
- "Windows Script Host: New Code-Signing Features Protect Against Malicious Scripts" on the Microsoft MSDN Web site at http://go.microsoft.com/fwlink/?LinkId=18550.

Note Batch files cannot be signed; therefore, they are inherently less secure. Convert all batch files to Microsoft® Visual Basic® scripts as soon as possible.

Maintaining Physical Security

All of the descriptions of domain controller security measures in the previous sections assume that the domain controller is *physically secure*. Physical security ensures that unauthorized users cannot turn the domain controller on or off, add or remove hardware, insert or remove removable media, log on by using the domain controller's keyboard and display, or remove backup media.

To maintain physical security for your domain controllers, perform the following tasks:

- Secure domain controllers against physical access.
- Prevent domain controllers from booting into alternate operating systems.
- Protect domain controllers on restart by using SYSKEY.
- Secure backup media against physical access.
- Enhance the security of the network infrastructure.
- Secure the remote restart of domain controllers.

Securing Domain Controllers Against Physical Access

The first line of defense in maintaining physical security is to secure domain controllers against any attacks that can be accomplished with physical access to the domain controller. Note that changes in the domain controller's environmental conditions, such as power failures, can also compromise the security of the domain controller.

Take the following common security precautions for restricting physical access to the domain controller:

- Use UPSs to prevent loss of power.
- Place domain controllers and UPSs in a locked room.
- Require cardkey locks or cipher-locks on the entrances to the locked room.
- Require locks on individual domain controllers or on doors to the racks housing the domain controllers.
- Require specific processes and procedures for any administration or repair of the domain controllers.

These security precautions are intended to prevent a potential attacker from gaining physical access to your domain controllers. However, in an environment where these recommendations cannot be strictly enforced, such as in branch offices, additional security measures may be required, as described in the following sections.

Preventing Domain Controllers from Booting into Alternate Operating Systems

A domain controller can be booted into an alternate operating system. For example, public domain drivers exist for MS-DOS that an attacker can use to boot the domain controller and directly access files that are stored on NTFS disk volumes, bypassing existing NTFS permissions. Similar utilities exist for Linux and UNIX operating systems. You can take steps to avoid this type of attack.

To minimize the possibility of domain controllers booting into an alternate operating system:

- Disable or remove the floppy disk drive, unless it is required by SYSKEY. For more information, see "Protecting Domain Controllers on Restart Using SYSKEY" later in this guide.
- Disable or remove the CD-ROM or DVD drive.
- Set the [timeout] parameter in the Boot.ini file to 0.
- Disable remote network boot and installation, for example, by RIS or Bootstrap Protocol (BOOTP).
- When you are unable to use SYSKEY with a password or floppy disk, require a basic input/output system (BIOS) password to boot the computer.

Protecting Domain Controllers on Restart by Using SYSKEY

In secure datacenter environments, generally, only authorized personnel can restart domain controllers. However, in an environment where these recommendations cannot be strictly enforced, such as in branch offices, there is increased potential for an unauthorized person to restart a domain controller.

An unplanned or unexpected restart of a domain controller can indicate that an attacker has booted the domain controller with an alternate operating system and compromised its security. On the other hand, the restart might simply be due to a loss of power or to scheduled maintenance on the domain controller.

Evaluating the Need for SYSKEY

The system key (SYSKEY) in Windows 2000 protects security information, including passwords in the Active Directory database and other Local Security Authority (LSA) secrets, against offline attacks by encrypting their storage on the domain controller. SYSKEY can either be derived from a secret password that you specify, or it can be stored on offline media, such as a floppy disk. On a domain controller reboot, either the password or the floppy disk containing SYSKEY must be supplied to successfully restart the computer.

Implementing SYSKEY provides two security advantages:

- Point-in-time control of the domain controller restart, which evaluates the reason for the domain controller restart and determines if security has been compromised
- Protection for passwords that are stored in the directory database against offline attacks if the domain controller or a disk are stolen

You can use the system key utility (Syskey.exe), which is installed on the domain controller during the Windows 2000 Server installation, to select one of these two configurations for the SYSKEY source.

There are certain logistic operational issues involved with the use of SYSKEY:

- Management of SYSKEY passwords or floppy disks can present challenges.

  Requiring a branch manager or local administrative staff to come to the office at 3 A.M. to enter the passwords or insert a floppy disk might be difficult.

  Alternatively, allowing centralized IT operations personnel to provide the SYSKEY password remotely requires additional hardware, such as Compaq Remote Insight Lights-out (RILO) or Dell Remote Access Card (DRAC III) boards. For more information about restarting domain controllers remotely, see "Securing the Remote Restart of Domain Controllers" later in this guide.
- Loss of the SYSKEY password or floppy disk leaves the domain controller in a state in which it cannot be restarted.

  There is no way to recover a domain controller if the SYSKEY password or floppy disk is lost. In this situation, it would be necessary to rebuild the domain controller.

Selecting a Method for Securing Domain Controller Restarts with SYSKEY

Each method noted in the previous section (specifically, manually entered SYSKEY or SYSKEY supplied on a floppy disk) has advantages and difficulties. If you choose to add SYSKEY protection to your domain controllers, you should first evaluate your security environment to determine which method will work best for you.

Providing SYSKEY Passwords to Secure Domain Controller Restarts

SYSKEY passwords do not require physical media that could be lost, as there are no floppy disks. Trusted personnel must enter a password in the event that the domain controller needs to be restarted. The password should be known to only a small group of trusted administrators, preferably only member of the Domain Admins group. The disadvantage of using passwords to secure SYSKEY is that trusted personnel are required to memorize another password and be on-site to enter the password.

To support branch offices, you may need to provide the SYSKEY password remotely through central IT trusted personnel. However, this requires additional hardware, such as Compaq RILO or Dell DRAC III boards. For more information about restarting domain controllers remotely, see "Securing the Remote Restart of Domain Controllers" later in this guide.

Because passwords can be compromised, you may be able to increase the security of passwords that are used for SYSKEY restarts by:

- Using strong passwords.
- Storing the passwords in a secure environment, such as a bank safety deposit box.
- Requiring the periodic changing of the SYSKEY passwords.

Providing SYSKEY Floppy Disks to Secure Domain Controller Restarts

Using SYSKEY with a password that is stored on a floppy disk does not require that a password be memorized by trusted personnel. However, implementing SYSKEY with a floppy disk does introduce the risk of lost or damaged physical media. Furthermore, trusted personnel are required to insert the floppy disk during domain controller restart. Again, only trusted personnel, preferably members of the Domain Admins group, should have access to the SYSKEY floppy disk.

To support branch offices, you may need to install third-party hardware devices, such as Compaq RILO or Dell DRAC III boards, so that images of floppy disks can be remotely transferred to the domain controller. Using these devices, central IT trusted personnel can transfer a copy of the SYSKEY disk image to a remote domain controller. After the domain controller is restarted, IT operations personnel can delete the remote image of the SYSKEY floppy disk.

Because the floppy disk contains the cryptographic key for SYSKEY, you should take measures to ensure that the floppy disk is not stolen, lost, destroyed, or copied by an unauthorized person. Some ways to mitigate these possibilities include:

- Copying the floppy disk and storing the copy off-site, such as in a bank safe deposit box.
- Storing the working copy of the floppy disk in a secure place on-site.

- Removing the floppy disk from the domain controller immediately after it restarts.

Securing Backup Media Against Physical Access

As part of your normal operational practices, you should regularly back up your domain controllers and secure the backup media to minimize the risk of data tampering or theft.

Because the backup contains all the information in the Active Directory database, theft of the backup media presents the same risks as theft of the domain controller or a disk drive from the domain controller. The attacker can restore the information elsewhere and illegally access Active Directory data.

Some methods for helping to prevent unauthorized users from gaining physical access to backup media include:

- Storing backup media for on-site use in a secure location where access is audited.
- Storing archival backup media securely off-site.
- Establishing processes and procedures that require the signatures of authorized administrators when any archival backup media is brought back on-site.
- Ensuring that backup media is only in the backup device during backup or recovery.

Enhancing the Security of the Network Infrastructure

The placement of domain controllers in your environment directly affects the security of your domain controllers. The primary focus in network security is to isolate the domain controllers from unauthorized users while providing high-speed, secure access to authorized users. To ensure that domain controllers are properly isolated, secure any cabling rooms, and place domain controllers on secured network segments in your network.

Securing Cabling Rooms

If an attacker can gain access to your cabling rooms, the attacker can potentially use a protocol analyzer to capture network traffic and compromise your network's security, including domain controller security. In intranet and perimeter network datacenters, the possibility of unauthorized personnel gaining access to these cabling rooms is negligible. However, in branch offices the cabling rooms may be shared with telephony wiring and other utilities.

Typically, your cabling rooms are where some of your routers and switches are located. The routers and switches contain a logical diagram of your network because they manage and maintain routing information. This routing information is used by Active Directory to determine IP subnets, and it determines the preferred domain controller for computers in the network.

Attackers can gain access to your switches and routers by using Telnet or Web interfaces that are provided by these devices. If attackers gain access to the configuration information of these devices, they can use this information to mount attacks on your domain controllers.

In most environments, all routers and switches use the same passwords for reading and configuring information. IT administrators may want to have a single password to simplify the management of a large number of switches, or the management software for routers and switches may only support the use of a single name.

Regardless of the environment, you can improve the security of your cabling rooms by:

- Requiring cardkey locks or cipher-locks on entrances to the cabling rooms.
- Requiring locks on the racks that house wiring panels, switches, or routers.
- Including UPSs to prevent loss of power.
- Requiring specific processes and procedures for any administration or repair of cabling, switches, or routers.
- Using strong passwords to secure the configuration of routers and switches.
- Using different passwords for reading and configuring routers and switches.

Placing Domain Controllers in Secured Network Segments

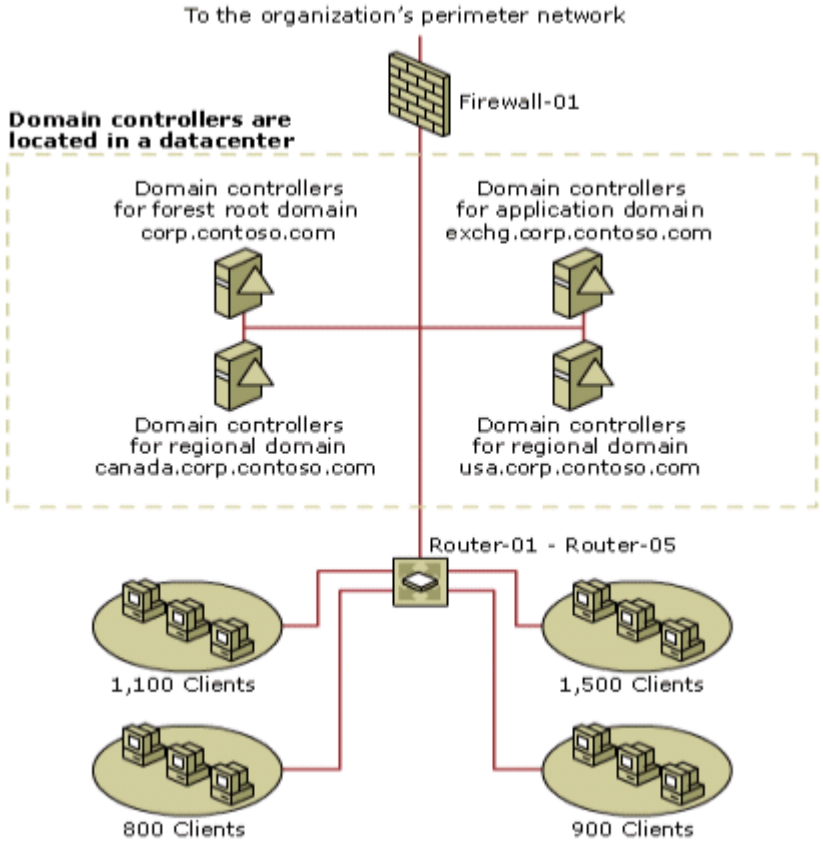
Placing domain controllers in secured segments of your network assists in isolating the domain controllers from unauthorized users. At the same time, ensure that users and computers have high-speed connectivity to their respective domain controllers.

Placing Domain Controllers in Datacenters

Place domain controllers physically within the datacenter so that only designated personnel have direct physical

contact with the domain controllers. Place your forest root, application, and regional domain controllers for use in your organization's private network in the datacenter. The placement of domain controllers for your perimeter network is discussed in a later section.

Placing domain controllers physically within the datacenter reduces the chance that anyone other than designated personnel will have direct physical contact with the domain controllers. Place domain controllers so that firewalls protect domain controllers from Internet users while routers, and possibly firewalls, protect domain controllers from users within the organization's private network. Figure 7 illustrates the placement of domain controllers in a datacenter.



If your browser does not support inline frames, click here to view on a separate page.

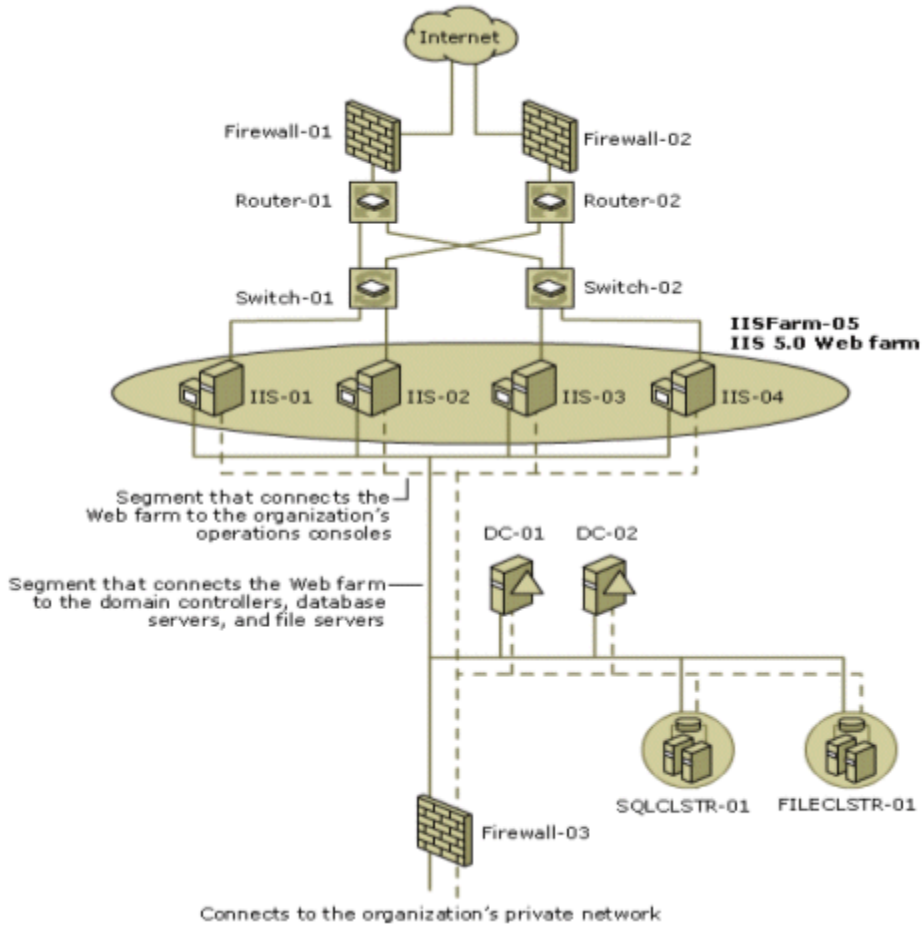
Figure 7 Domain Controllers in a Datacenter

Placing Domain Controllers in Perimeter Networks

Place domain controllers in your perimeter networks so that the domain controllers are not directly accessible by Internet users. Ensure that only Web servers, database servers, file servers, users in the private network, and computers in the private network have direct access to the domain controllers.

Placing the domain controller behind a standalone router helps prevent Internet users from directly accessing the domain controller. To help minimize security risks, place the domain controller on the same network segment as the client computers. You should also ensure that the router communicates exclusively with the organization's hub or central location by using VPN tunnels. Prevent any other requests that originate from the Internet from reaching the branch office's network segment and, subsequently, the domain controller.

Figure 8 illustrates the placement of domain controllers in a perimeter network.



If your browser does not support inline frames, click here to view on a separate page.

Figure 8 Domain Controllers in a Perimeter Network

Placing Domain Controllers in Branch Offices

In branch offices, domain controllers often provide other services, such as file or print services, to users in the branch office. These multifunction domain controllers communicate with the rest of the organization through a routed connection, possibly a dial-up modem that is managed by a stand-alone router. The stand-alone router provides the isolation and firewall functionality to protect the domain controller and the users in the branch office.

Place the domain controller behind the stand-alone router to prevent Internet users from directly accessing the domain controller. Place the domain controller on the same network segment as the client computers. Ensure that the router communicates exclusively with the organization's hub or central location by using VPN tunnels. Prevent any other requests that originate from the Internet from reaching the branch office's network segment and, subsequently, the domain controller.

Note Whenever possible, use dedicated domain controllers in branch offices to minimize the threats that can compromise the security of Active Directory.

Figure 9 illustrates the placement of domain controllers in a branch office.

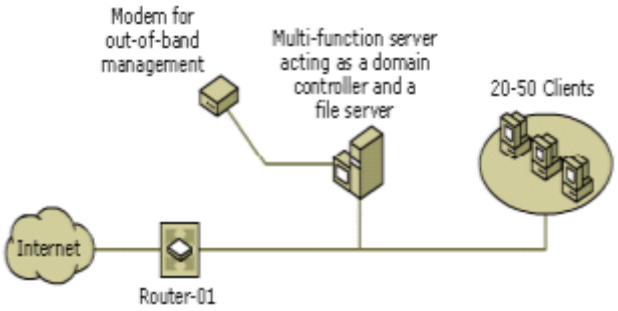


Figure 9 Domain Controllers in a Branch Office

Additionally, a modem can provide out-of-band management capability for a remote domain controller. The modem directly connects either to a COM port on the domain controller or to remote management hardware (such as the Compaq RILO board) or an intelligent UPS. This out-of-band management capability can provide the ability to perform BIOS configuration, monitor and select the boot process, and turn the domain controller on and off.

Ensure that the number to the modem is kept secret. Require the modem to call back to a predetermined list of numbers, and require user identification for callback.

Securing the Remote Restart of Domain Controllers

In some situations, your domain controllers may require *remotely administered* management, or they may be placed in branch offices outside your organization's datacenter. In these situations, the restart of a domain controller must be performed remotely.

Tasks that must be performed during the remote restart of a domain controller include:

- Selection of the Windows 2000 Server boot options
- Configuration of the BIOS on the domain controller

Terminal Services is unable to perform these tasks, because Windows 2000 Server must be running to support Terminal Services. These tasks require additional hardware to support remote restart functionality. Examples of this type of hardware include:

- Smart UPSs
- Remote access hardware that is integrated into the server, such as Compaq RILO or Dell DRAC III boards
- Video switches that connect to the keyboard, mouse, and display that provide services similar to Terminal Services

Most of these devices communicate by using RS-232 or Ethernet, and they have only rudimentary security, such as a password. In datacenters, the devices that communicate through RS-232 are connected to a terminal concentrator. The terminal concentrator multiplexes a number of RS-232 connections into a single RS-232 or Ethernet connection. Smart UPS and remote access hardware typically communicate through Telnet.

Secure the remote restart of domain controllers by doing the following:

- When the domain controller is in a datacenter, connect the remote restart device's RS-232 or Ethernet connection to a network segment that is dedicated to network management and that is isolated from clients.
- When the domain controller is in a branch office, connect the remote restart device to a dedicated modem, and require the modem to provide password identification and callback functionality.

Recommendations: Deploying Secure Domain Controllers

Following the security recommendations that are described earlier in this section will help minimize the security risks involved in deploying domain controllers. Of course, as previously mentioned, you should consider the recommendations described in other sections in considering how best to enhance your comprehensive Active Directory security.

In most instances, these recommendations are intended for intranet datacenter, extranet datacenter, and branch office scenarios. However, some of the recommendations depend on the particular scenario. When the recommendations are scenario specific, notes are included to direct you to the section where the recommendation is discussed.

Recommendations for Establishing Secure Domain Controller Build Practices

The following table provides a checklist of recommendations for establishing secure domain controller rollout

practices.

	Securing the Domain Controller Build Environment
☐	Whenever possible, build domain controllers in secured environments, such as datacenters.
☐	When building domain controllers in unsecured environments, ensure that only trusted personnel have physical access.
	Selecting Secure Domain Controller Build Methods
☐	Use imaged-based, automated deployment methods for installing Windows 2000 Server. **Note** This recommendation may vary or may not be feasible, based on your scenario. For more information, see "Selecting Secure Domain Controller Build Methods" earlier in this guide.
☐	Automate the promotion of servers to domain controllers.

Recommendations for Ensuring Predictable, Repeatable, and Secure Domain Controller Deployments

The following table provides a checklist of recommendations for ensuring that your domain controller deployments are predictable, repeatable, and secure.

	Installing Windows 2000 Server with Service Packs and Hotfixes
☐	Install Windows 2000 Server with the most recent service packs.
☐	Apply all current security-related hotfixes.
☐	Format all partitions as NTFS.
☐	Create a strong password for the Administrator account.
☐	Deselect IIS during installation.
☐	Select DNS during installation.
☐	Deselect SMTP unless Active Directory replication uses SMTP.
	Disabling NTFS Automatic 8.3 Name Generation
☐	Disable NTFS automatic 8.3 name generation.
	Running Virus-Scanning Software on the Server
☐	Run virus-scanning software before promoting any server to a domain controller.
☐	Ensure that virus-scanning software includes any updates to detect and remove the latest viruses.
	Selecting Secure Domain Controller Promotion Settings
☐	Place the Active Directory database (Ntds.dit) on a separate physical drive.
☐	Place the Active Directory logs on a separate physical drive.
☐	Place SYSVOL on the same physical drive as the Active Directory database.
☐	Disable Pre–Windows 2000 Compatibility, if possible.
	Prohibiting the Use of Cached Credentials when Unlocking a Domain Controller Console
☐	Prohibit cached credentials from unlocking a domain controller console.
	Creating a Reserve File to Enable Recovery from Disk-Space Attacks
☐	Create a reserve file on the same disk volume as Ntds.dit. Ensure that the reserve file is either 250 MB or 1 percent of the available disk space, whichever is larger.

Recommendations for Enabling Only Essential Services

The following table provides a checklist of recommendations for enabling only essential services and protocols on your domain controllers.

	Enabling Only Essential Services

☐	Enable only the services that are required for a computer running Windows 2000 Server in the role of a domain controller.

Recommendations for Securing Domain Controller Files and Executables

The following table provides a checklist of recommendations for securing the Active Directory files and executables on your domain controllers.

	Setting Appropriate NTFS File and Folder Permissions
☐	Change the default permissions assignment on the volume root from Everyone to Administrators.

Recommendations for Running Virus Scans on Domain Controllers

The following table provides a checklist of recommendations for running virus scans on domain controllers.

	Running Virus Scans on Domain Controllers
☐	After promoting servers to domain controllers, continue to run virus scans and to obtain regular virus signature updates from your antivirus software vendor.
	Preventing Interference Between Virus Scans and Active Directory Database and Log File Access
☐	Configure the antivirus software to exclude from scanning the Active Directory database and log files that are specified in Table 12.
	Preventing Interference Between Virus Scans and FRS Database and Log File Access
☐	Configure the antivirus software to exclude from scanning the FRS database and log files that are specified in Table 13.
	Preventing Virus Scans from Triggering Excessive FRS Replication
☐	Configure antivirus software to not scan files in SYSVOL.
☐	Require script signing on domain controllers and administrative workstations.

Recommendations for Maintaining Physical Security

The following table provides a checklist of recommendations for maintaining the physical security of your domain controllers.

	Securing Domain Controllers Against Physical Access
☐	Include UPSs.
☐	Place domain controllers and UPSs in locked rooms.
☐	Require cardkey locks or cipher-locks on the entrances to the locked rooms.
☐	Require locks on individual domain controllers or on doors to the racks housing domain controllers.
☐	Require specific processes and procedures for the administration or repair of domain controllers.
	Preventing Domain Controllers from Booting into Alternate Operating Systems
☐	Disable or remove the floppy disk drive, unless it is required for SYSKEY.
☐	Disable or remove the CD-ROM or DVD drive.
☐	Set the [timeout] parameter in the Boot.ini file to 0.
	Protecting Domain Controllers on Restart by Using SYSKEY
☐	Enable SYSKEY. **Note** This recommendation may vary or may not be feasible, based on your scenario. For more information, see "Protecting Domain Controllers on Restart by Using SYSKEY."
	Securing Backup Media Against Physical Access
☐	Store backup media used on-site in a locked cabinet or container.

☐	Store archival backup media in off-site storage.
☐	Establish processes and procedures that require signatures to bring any archival storage back on-site.
☐	Ensure that backup media is only installed during backup and that it is in secured storage otherwise.
	Enhancing the Security of the Network Infrastructure
☐	Require cardkey locks or cipher-locks on the entrances to cabling rooms.
☐	Require processes and procedures for any administration or repair of cabling, switches, or routers.
☐	Use strong passwords to secure the configuration of routers and switches.
☐	Use different passwords for reading and configuring your routers and switches.
	Securing the Remote Restart of Domain Controllers
☐	When the domain controller is in a datacenter, connect the remote restart devices to the secured management network.
☐	When the domain controller is in a branch office, connect the remote restart device to a dedicated modem, and require the modem to provide password identification and callback functionality.
