Security

Chapter 4 - Hardening Domain Controllers

Overview

The domain controller server role is one of the most important roles to secure in any environment with computers running Microsoft® Windows Server™ 2003 that use Microsoft Active Directory® directory service. Any loss or compromise of a domain controller in the environment could prove devastating to clients, servers, and applications that rely on domain controllers for authentication, Group Policy, and a central lightweight directory access protocol (LDAP) directory.

Due to their importance, domain controllers should always be stored in physically secure locations that are accessible only to qualified administrative staff. When domain controllers must be stored in unsecured locations, branch offices for example, several security settings can be adjusted to limit the potential damage from physical threats.

Domain Controller Baseline Policy

Unlike the other server role policies detailed later in this guide, the Group Policy for the Domain Controllers server role is a baseline policy, putting it in the same class as the Member Server Baseline Policy (MSBP) defined in Chapter 3, "Creating a Member Server Baseline." The Domain Controllers Baseline Policy (DCBP) is linked to the Domain Controllers organizational unit (OU) and takes precedence over the Default Domain Controllers Policy. The settings included in the DCBP will strengthen the overall security across the domain controllers in any given environment.

Most of the DCBP is a direct copy of the MSBP. Since the DCBP is based on the MSBP, Chapter 3, "Creating a Member Server Baseline," should be closely reviewed in order to fully understand the many settings that are also included in the DCBP. Only the DCBP settings that differ from those in the MSBP are documented in this chapter.

Domain controller templates are uniquely designed to address the security needs of the three environments defined in this guide. The following table shows the relationship between the domain controller .inf files included with this guide, and these environments. For example, the Enterprise Client – Domain Controller.inf file is the security template for the Enterprise Client environment.

Table 4.1 Domain Controller Baseline Security Templates

Legacy Client	Enterprise Client	High Security
Legacy Client – Domain Controller.inf	Enterprise Client – Domain Controller.inf	High Security – Domain Controller.inf

Note Linking an incorrectly configured group policy object (GPO) to the Domain Controllers OU could severely hinder the proper operation of a domain. Exercise extreme care when importing these security templates, and verify all settings imported are correct before linking a GPO the Domain Controllers OU.

Audit Policy Settings

The Audit Policy settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 3, "Creating a Member Server Baseline." The baseline policy settings in the DCBP ensure that all the relevant security audit information is logged on the domain controllers.

User Rights Assignments

The DCBP specifies a number of user rights assignments for the domain controllers. In addition to the default settings, seven other user rights were modified to strengthen the security for the domain controllers in the three environments defined in this guide.

This section provides details on the prescribed user rights settings for the DCBP which differ from those in the MSBP. For a summary of the prescribed settings in this section, refer to the Windows Server 2003 Security Guide Settings Excel workbook included with this guide.

Access this computer from the network

Table 4.2 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS, Everyone, Pre-Windows 2000 Compatible Access.	Not Defined.	Not Defined	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS

The **Access this computer from the network** user right determines which users and groups are allowed

to connect to the computer over the network. This user right is required by a number of network protocols including server message block (SMB) – based protocols, network basic input/output system (NetBIOS), Common Internet File System (CIFS), Hypertext Transfer Protocol (HTTP).and Component Object Model Plus (COM+).

Although permissions granted to the **Everyone** security group no longer grant access to anonymous users in Windows Server 2003, guest groups and accounts can still be granted access through the **Everyone** security group. For this reason, this guide recommends removing the **Everyone** security group from the **Access this computer from the network** user right in the High Security environment to further guard from attacks targeting guest access to the domain.

Add workstations to domain

Table 4.3 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Authenticated Users	Administrators	Administrators	Administrators

The **Add workstations to domain** user right allows the user to add a computer to a specific domain. For this right to take effect, it must be assigned to the user as part of the Default Domain Controllers Policy for the domain. A user who has been granted this right can add up to 10 workstations to the domain. Users who have been granted the **Create Computer Objects** permission for an OU or the Computers container in Active Directory can also join a computer to a domain. Users who have been granted this permission can add an unlimited number of computers to the domain regardless of whether they have been assigned the **Add workstations to a domain** user right or not.

By default, all users in the **Authenticated Users** group have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container.

In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. Some organizations want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage them.

Allowing users to add workstations to the domain can hamper this effort. It also provides avenues for users to perform activities that are more difficult to trace because they can create additional unauthorized domain computers.

For these reasons, the **Add workstations to domain** user right is granted only to the **Administrators** group in the three environments defined in this guide.

Allow log on locally

Table 4.4 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Account Operators, Backup Operators, Print Operators, and Server Operators	Administrators	Administrators	Administrators

The **Allow log on locally** user right allows a user to start an interactive session on the computer. Users who do not have this right are still able to start a remote interactive session on the computer if they have the **Allow logon through Terminal Services** right.

Limiting which accounts can be used to log on to domain controller consoles in an environment will help prevent unauthorized access to domain controller file systems and system services. A user who is able to log on to the console of a domain controller could maliciously exploit the system, and possibly compromise the security of an entire domain or forest.

By default, the **Account Operators**, **Backup Operators**, **Print Operators**, and **Server Operators** groups are granted the right to log on locally to domain controllers. Users in these groups should not need to log on to a domain controller to perform their management tasks. Users in these groups can normally perform their duties from other workstations. Only users in the **Administrators** group should perform maintenance tasks on domain controllers.

Granting this right only to the **Administrators** group limits physical and interactive access to domain controllers to only highly trusted users, therefore enhancing security. For this reason, the **Allow log on locally** user right is granted only to the **Administrators** group in the three environments defined in this guide.

Allow log on through Terminal Services

Table 4.5 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Not Defined	Administrators	Administrators	Administrators

The **Allow log on through Terminal Services** user right allows a user to log on to the computer by using a Remote Desktop connection.

Limiting which accounts can be used to log on to domain controller consoles via Terminal Services will help prevent unauthorized access to domain controller file systems and system services. A user who is able to log onto the console of a domain controller via Terminal Services can exploit that system, and possibly compromise the security of an entire domain or forest.

Granting this right only to the **Administrators** group limits interactive access to domain controllers only to highly trusted users, therefore enhancing security. For this reason, the **Allow log on locally** user right is granted only to the **Administrators** group in the three environments defined in this guide. Although logging on to a domain controller via Terminal Services requires administrative access by default, configuring this user right helps protect against inadvertent or malicious actions that might compromise this restriction.

As a further security measure, the DCBP denies the default **Administrator** account the right to log on to a domain controller via Terminal Services. This setting also prevents malicious users from attempting to remotely break into a domain controller using the default **Administrator** account. For more details on this setting, see Chapter 3, "Creating a Member Server Baseline."

Change the system time

Table 4.6 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Server Operators	Administrators	Administrators	Administrators

The **Change the system time** user right allows the user to adjust the time on the computer's internal clock. This right is not required to change the time zone or other display characteristics of the system time.

Synchronized system time is critical to the operation of Active Directory. Proper Active Directory replication and authentication ticket generation process used by the Kerberos version 5 authentication protocol both rely on time being synchronized across any environment.

A domain controller configured with a system time that is out of sync with the system time on other domain controllers in the environment could interfere with the operation of domain services. Allowing only administrators to modify system time minimizes the possibility of a domain controller being configured with an incorrect system time.

By default, the **Server Operators** group is granted the right to modify system time on domain controllers. Because of the possible repercussions that may result from members of this group incorrectly modifying system time on a domain controller, this user right is configured in the DCBP so that only the **Administrators** group can change the system time in any of the three environments defined in this guide.

For more information on the Microsoft Windows® Time Service, refer to Knowledge Base articles 224799, "Basic Operation of the Windows Time Service," located at: http://support.microsoft.com/default.aspx?scid=kb;en-us;224799&sd=tech and 216734, "How to Configure an Authoritative Time Server in Windows 2000," located at: http://support.microsoft.com/default.aspx?scid=kb;en-us;216734&sd=tech.

Enable computer and user accounts to be trusted for delegation

Table 4.7 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators	Not Defined	Not Defined	Administrators

The **Enable computer and user accounts to be trusted for delegation** user right allows the user to change the Trusted for Delegation setting on a user or computer object in Active Directory. Delegation of authentication is a capability that is used by multi – tier client/server applications. It allows a front – end service to use the credentials of a client in authenticating to a back – end service. For this to be possible, both client and server must be running under accounts that are trusted for delegation.

Misuse of this right could lead to unauthorized users impersonating other users on the network. An attacker could exploit this right to gain access to network resources while appearing to be a different user, which could make determining what has happened after a security incident more difficult to decipher.

This guide recommends assigning the **Enable computer and user accounts to be trusted for delegation** right to the **Administrators** group on domain controllers.

> **Note** Although the Default Domain Controllers Policy assigns the Administrators group this right, the DCBP enforces this right in the High Security environment only because it was originally based on

the MSBP. The MSBP assigns this right a NULL value.

Load and unload device drivers

Table 4.8 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Print Operators	Administrators	Administrators	Administrators

The **Load and unload device drivers** user right determines which users can load and unload device drivers. This user right is necessary for loading and unloading Plug and Play devices.

Maliciously loading or unloading a device driver on a domain controller can have an adverse impact on its operation. Limiting the accounts that are capable of loading and unloading device drivers to only the most trusted users minimizes the opportunity of device drivers being used to compromise domain controllers in your environment.

By default, the **Print Operators** group is granted this right. As mentioned earlier, it is not recommended to create printer shares on domain controllers. This removes the need for **Print Operators** to require the right to load and unload device drivers. Therefore, this user right is granted only to the **Administrators** group in the three environments defined in this guide.

Restore files and directories

Table 4.9 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Backup Operators, Server Operators	Administrators	Administrators	Administrators

The **Restore files and directories** user right allows a user to circumvent file and directory permissions when restoring backed – up files and directories, and to set any valid security principal as the owner of an object.

Enabling a user account to restore files and directories to the file system of a domain controller gives the account owner the power to easily modify service executables. Malicious users can exploit the access this right provides to not only render a domain controller useless, but compromise the security of a domain or an entire forest.

By default, the **Server Operators** and **Backup Operators** groups are granted this right. Removing this user right from these groups and granting it only to the **Administrators** group reduces the likelihood of a domain controller being compromised by improper modifications to the file system. Therefore, this user right is granted only to the **Administrators** group in the three environments defined in this guide.

Shutdown the system

Table 4.10 Settings

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Administrators, Server Operators, Print Operators, Backup Operators	Administrators	Administrators	Administrators

The **Shutdown the system** user right allows a user to shut down the local computer.

Malicious users with the ability to shutdown domain controllers can easily initiate a denial of service (DoS) attack that could severely impact an entire domain or forest. Furthermore, this user right can be exploited to launch an elevation of privilege attack on a domain controller's system account when it is restarting services. A successful elevation of privilege attack on a domain controller compromises the security of a domain or an entire forest.

By default the **Administrators**, **Server Operators**, **Print Operators**, and **Backup Operators** groups are granted this right to shutdown domain controllers. In secure environments, none of these groups, except for **Administrators**, require this right to perform administrative tasks. For this reason, this user right is granted to the **Administrators** group only in the three environments defined in this guide.

Security Options

Most of the Security Options settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 3, "Creating a Member Server Baseline." Differences between the MSBP and the DCBP are described in the following section.

Network security: Do not store LAN Manager hash value on next password

change

Table 4.11 Settings

Member Server Default	Legacy Client	Enterprise Client	High Security
Disabled	Disabled	Enabled	Enabled

The **Network security: Do not store LAN Manager hash value on next password change** security option setting determines if the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT® hash. For this reason, this MSBP enables this setting in the three security environments defined in this guide.

The DCBP enables this setting on domain controllers in the Enterprise Client and High Security environments, and disables it on domain controllers in the Legacy Client environment. If this setting were enabled on domain controllers in the Legacy Client environment, Windows 98 clients would be unable to login after changing their passwords.

> **Note** Legacy operating systems and some third – party applications may fail when this setting is enabled. Furthermore, enabling this setting will require all accounts to change their password.

Event Log Settings

The Event Log settings for domain controllers are the same as those specified in the MSBP. For more information, see Chapter 3, "Creating a Member Server Baseline." The baseline Group Policy settings in the DCBP ensure that all the relevant security audit information is logged on the domain controllers, including Directory Services Access.

System Services

The following system services must be enabled on all Windows Server 2003 domain controllers. The baseline policy settings in the DCBP ensure that all the required system services are configured uniformly across domain controllers.

This section provides details on the prescribed system services settings for the DCBP which differ from those in the MSBP. For a summary of the prescribed settings in this section, refer to the Windows Server 2003 Security Guide Settings Excel workbook included with this guide.

> **Note** If you run the DCDiag.exe utility from the Windows Server 2003 Support Tools, it will check for all services that can run on the domain controllers in your environment. The DCDiag.exe will report errors because some services are disabled in the Domain Controller Baseline Policy — including IISADMIN, SMTPSVC, and TrkSvr. This information does not indicate a problem with your configuration.

Distributed File System

Table 4.12 Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	Dfs	Automatic	Automatic	Automatic

The **Distributed File System (DFS)** service distributes and integrates disparate file shares into a single logical namespace. The service manages logical volumes distributed across a local or wide area network (WAN), and is required for the Active Directory System Volume (SYSVOL) share. SYSVOL replication relies on the proper operation of DFS.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

DNS Server

Table 4.13 Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	Dns	Automatic	Automatic	Automatic

The **DNS Server** service resolves Domain Name System (DNS) queries and update requests for DNS names. **DNS Server** is a crucial service for locating devices identified using DNS names and domain controllers in Active Directory.

The reliability and availability of Active Directory relies heavily on the proper operation of the **DNS Server** service. Without DNS, domain controllers cannot locate each other to replicate directory information, and clients cannot contact domain controllers for authentication.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

File Replication

Table 4.14 Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	NtFrs	Automatic	Automatic	Automatic

The **File Replication** service allows files to be automatically copied and maintained simultaneously on multiple servers. File Replication Service (FRS) is the automatic file replication service in Windows 2000 and the Windows Server™ family. The service replicates the SYSVOL on all domain controllers, and can be configured to replicate files on other targets associated with the fault tolerant DFS. SYSVOL replication also relies on the proper operation of the **File Replication** service.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Intersite Messaging

Table 4.15 Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	IsmServ	Automatic	Automatic	Automatic

The **Intersite Messaging** (ISM) service enables messages to be exchanged between computers running Windows Server sites. This service is used for mail – based replication between sites. Active Directory includes support replication between sites using Simple Mail Transfer Protocol (SMTP) over Internet Protocol (IP) transport. SMTP support is provided by the SMTP service, which is a component of Microsoft Internet Information Services (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 may perform intersite communication. The ISM service directs send and receive message requests to the appropriate transport add – in DLLs, and then routes the messages to the ISM service on the destination computer. Active Directory replication relies on the **Intersite Messaging** service running properly.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Kerberos Key Distribution Center

Table 4.16 Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	Kdc	Automatic	Automatic	Automatic

The **Kerberos Key Distribution Center** (KDC) service enables users to log on to the network using the Kerberos v5 authentication protocol.

The KDC service is required for users to log on to the network. Disabling this service blocks users from logging on to the network.

Using a group policy to secure and set the startup mode of a service grants access only to server

administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Remote Procedure Call (RPC) Locator

Table 4.17 Settings

Domain Controller Default	Service Name	Legacy Client	Enterprise Client	High Security
Automatic	RpcLocator	Automatic	Automatic	Automatic

The **Remote Procedure Call (RPC) Locator** service enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database.

Stopping or disabling this service may prevent RPC clients using RpcNs* APIs from locating servers or fail to start. Also, RPC clients that rely on RpcNs* APIs from the same computer may not find RPC servers supporting a given interface. Stopping or disabling this service on your domain controller may cause RPC clients using the RpcNs* APIs and the domain controller to experience service interruption while trying to locate clients.

Using a group policy to secure and set the startup mode of a service grants access only to server administrators, therefore preventing the service from being configured or operated by unauthorized or malicious users. The group policy will also prevent administrators from inadvertently disabling the service. For these reasons, the service is configured to start automatically in the DCBP in the three environments defined in this guide.

Additional Security Settings

This section describes manual modifications that must be made to the DCBP, as well as additional settings and countermeasures that cannot be implemented via Group Policy.

Manually Adding Unique Security Groups to User Rights Assignments

Most User Rights Assignments applied via the DCBP have been properly specified in the security templates that accompany this guide. However, there are a few accounts and security groups that cannot be included in the templates because their security identifiers (SIDs) are specific to individual Windows 2003 domains. User rights assignments that must be configured manually are specified below.

> **Warning** The following table contains values for the built – in Administrator account. This account is not to be confused with the built – in Administrators security group. If the Administrators security group is added to any of the deny access user rights below you will need to log on locally in order to correct the mistake.
>
> In addition, the built – in Administrator account may have been renamed based on some of the recommendations described in Chapter 3, "Creating a Member Server Baseline." When adding the Administrator account, ensure the renamed account is specified.

Table 4.18 Manually Added User Rights Assignments

Domain Controller Default	Legacy Client	Enterprise Client	High Security
Deny access to this computer from the network	Built – in Administrator; Support_388945a0; Guest; all NON – Operating System service accounts	Built – in Administrator; Support_388945a0; Guest; all NON – Operating System service accounts	Built – in Administrator; Support_388945a0; Guest; all NON – Operating System service accounts
Deny log on as a batch job	Support_388945a0 and Guest	Support_388945a0 and Guest	Support_388945a0 and Guest
Deny log on through Terminal Services	Built – in Administrator; all NON-operating system service accounts	Built – in Administrator; all NON-operating system service accounts	Built – in Administrator; all NON-operating system service accounts

> **Important** All non – operating system service accounts include service accounts used for specific applications across an enterprise. This does NOT include LOCAL SYSTEM, LOCAL SERVICE or the NETWORK SERVICE accounts which are built – in accounts the operating system uses.

Directory Services

Domain controllers running Windows Server 2003 store directory data and manage user and domain interactions, including user logon processes, authentication, and directory searches.

Relocating Data – Active Directory Database and Log Files

Safeguarding the Active Directory database and log files is crucial to maintaining directory integrity and reliability.

Moving the ntds.dit, edb.log, and temp.edb files from their default location will help to conceal them from an attacker if a domain controller is compromised. Furthermore, moving the files off the system volume to a separate physical disk will also improve domain controller performance.

For these reasons, this guide recommends moving the Active Directory database and log files for the domain controllers in the three environments defined in this guide from their default location on the system volume to a non – system striped or striped/mirrored disk volume.

Resizing Active Directory Log Files

Ensuring an adequate amount of information is logged and maintained for domain controllers across an environment is crucial to effectively monitor and maintain the integrity, reliability, and availability of Active Directory.

Increasing the maximum size of the log files to support this effort will assist administrators in maintaining an adequate amount of information needed to perform meaningful audits in the event of hacker attacks.

For these reasons, this guide recommends increasing the maximum size of the Directory Service and File Replication Service log files from the 512 KB default to 16 MB on the domain controllers in the three environments defined in this guide.

Using Syskey

On domain controllers, password information is stored in directory services. It is not unusual for password – cracking software to target the Security Accounts Manager (SAM) database or directory services to access passwords for user accounts.

The System Key utility (Syskey) provides an extra line of defense against offline password – cracking software. Syskey uses strong encryption techniques to secure account password information that is stored in directory services.

Table 4.19 Syskey Modes

System Key Option	Security Level	Description
Mode 1: System Generated Password, Store Startup Key Locally	Secure	Uses a computer – generated random key as the system key and stores an encrypted version of the key on the local computer. This option provides strong encryption of password information in the registry, and enables the user to restart the computer without the need for an administrator to enter a password or insert a disk.
Mode 2: Administrator generated password, Password Startup	More secure	Uses a computer – generated random key as the system key and stores an encrypted version of the key on the local computer. The key is also protected by an administrator – chosen password. Users are prompted for the system key password when the computer is in the initial startup sequence. The system key password is not stored anywhere on the computer.
Mode 3: System Generated Password, Store Startup Key on Floppy Disk	Most secure	Uses a computer-generated random key and stores the key on a floppy disk. The floppy disk that contains the system key is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.

Syskey is enabled on all Windows Server 2003 servers in Mode 1 (obfuscated key). There are many reasons to recommend using Syskey in Mode 2 (console password) or Mode 3 (floppy storage of Syskey password) for any domain controller that is exposed to physical security threats.

From a security standpoint, this appears sensible at first, as the domain controller would be vulnerable to being restarted by an attacker with physical access to it. Syskey in Mode 1 allows an attacker to read and alter the contents of the directory.

However, the operational requirements for ensuring that domain controllers can be made available through restarts tend to make Syskey Mode 2 or Mode 3 difficult to support. To take advantage of the added protection provided by these Syskey modes, the proper operational processes must be implemented in

your environment to meet specific availability requirements for the domain controllers.

The logistics of Syskey password or floppy disk management can be quite complex, especially in branch offices. For example, requiring one of your branch managers or local administrative staff to come to the office at 3 A.M. to enter the passwords, or insert a floppy to enable other users to access the system is expensive and makes it very challenging to achieve high availability service level agreements (SLAs).

Alternatively, allowing your centralized IT operations personnel to provide the Syskey password remotely requires additional hardware — some hardware vendors have add – on solutions available to remotely access server consoles.

Finally, the loss of the Syskey password or floppy disk leaves your domain controller in a state where it cannot be restarted. There is no method for you to recover a domain controller if the Syskey password or floppy disk is lost. If this happens, the domain controller must be rebuilt.

Nevertheless, with the proper operational procedures in place, Syskey can provide an increased level of security that can greatly protect the sensitive directory information found on domain controllers.

For these reasons, Syskey Mode 2 or Mode 3 is recommended for domain controllers in locations without strong physical storage security. This recommendation also applies to domain controllers in any of the three environments described in this guide.

To create or update a system key:

1. Click **Start**, click **Run**, type **syskey**, and then click **OK**.
2. Click **Encryption Enabled**, and then click **Update**.
3. Click the desired option, and then click **OK**.

Active Directory Integrated DNS

Microsoft recommends using Active Directory integrated DNS in the three environments defined in this guide, in part because integrating the zones into Active Directory simplifies the process of securing the DNS infrastructure.

Protecting DNS Servers

Safeguarding DNS servers is essential to any environment with Active Directory. The following sections provide several recommendations and explanations for doing this.

When a DNS server is attacked, one possible goal of the attacker is to control the DNS information being returned in response to DNS client queries. In this way, clients can be inadvertently misdirected to unauthorized computers. IP spoofing and cache poisoning are examples of this type of attack.

In IP spoofing, a transmission is given the IP address of an authorized user to obtain access to a computer or network. Cache poisoning is an attack in which an unauthorized host transmits false information regarding another host into the cache of a DNS server. The attack results in redirecting clients to unauthorized computers.

Once clients start inadvertently communicating with unauthorized computers, those computers may attempt to gain access to information stored on the client computers.

Not all attacks focus on spoofing DNS servers. Some DoS attacks could alter DNS records in legitimate DNS servers to provide invalid addresses in response to client queries. By causing the server to respond with invalid addresses, clients and servers cannot locate the resources they need to function, such as domain controllers, Web servers, or file shares.

For these reasons, this guide recommends configuring the routers used in the three environments to drop spoofed IP packets to ensure that the IP addresses of the DNS servers cannot be spoofed by other computers.

Configuring Secure Dynamic Updates

The Windows Server 2003 DNS client service supports Dynamic DNS updates, which allow client systems to add DNS records directly into the database. Dynamic DNS servers can receive malicious or unauthorized updates from an attacker using a client that supports the DDNS protocol if the server is configured to accept unsecured updates.

At a minimum, an attacker can add bogus entries to the DNS database; at worst, the attacker can overwrite or delete legitimate entries in the DNS database. Such an attack may result in any of the following conditions:

- Directing clients to unauthorized domain controllers: When a client submits a DNS query looking for the address of a domain controller, a compromised DNS server can be instructed to return the address of an unauthorized server. Then, with the use of other non – DNS related attacks, the client might be tricked into passing on secure information to the bogus server.
- Responding to DNS queries with invalid addresses: This makes clients and servers unable to locate one another. If clients cannot locate servers, they cannot access the directory. When domain controllers cannot locate other domain controllers, directory replication stops, creating a DoS condition that could affect users throughout a forest.

- Creating a DoS condition in which a server's disk space may be exhausted by a huge zone file filled with dummy records, or large numbers of entries that slow down replication.

Using secure DDNS updates guarantees that registration requests are only processed if they are sent from valid clients in an Active Directory forest. This greatly limits the opportunity for an attacker to compromise the integrity of a DNS server.

For these reasons, this guide recommends configuring Active Directory DNS servers in the three environments defined in this guide to accept only Secure Dynamic Updates.

Limiting Zone Transfers to Authorized Systems

Because of the important role that zones play in DNS, they should be available from more than one DNS server on the network to provide adequate availability and fault tolerance when resolving name queries. Otherwise, name queries sent to just one server that does not respond in the zone can fail to resolve. For additional servers to host a zone, zone transfers are required to replicate and synchronize all copies of the zone used at each server configured to host the zone.

Furthermore, a DNS server that is not configured to limit who can request zone transfers is vulnerable to transferring the entire DNS zone to anyone who requests it. This can be easily accomplished using tools such as nslookup.exe. Such tools can expose the entire domain's DNS dataset, including such things as which hosts are serving as domain controllers, directory – integrated Web servers, or Microsoft SQL Server™ 2000 databases.

For these reasons, this guide recommends configuring Active Directory Integrated DNS servers in the three environments defined in this guide to allow zone transfers, but to limit which systems can make transfer requests.

Resizing the Event Log and DNS Service Log

Ensuring an adequate amount of information is logged and maintained for domain controllers across an environment is crucial to effectively monitor the DNS Service.

Increasing the maximum size of the DNS Service log file will assist administrators in maintaining an adequate amount of information to perform meaningful audits in the event of an attack.

For this reason, this guide recommends configuring the maximum size for the DNS Service log file on the domain controllers in the three environments defined in this guide to at least 16 MB, and ensure that the **Overwrite events as needed** option in the DNS Service is selected to maximize the amount of log entries preserved.

Securing Well Known Accounts

Windows Server 2003 has a number of built – in user accounts that can not be deleted but can be renamed. Two of the most well known built – in accounts in Windows 2003 are **Guest** and **Administrator**.

By default, the **Guest** account is disabled on member servers and domain controllers. This setting should not be changed. The built – in **Administrator** account should be renamed and the description altered to help prevent attackers from compromising a remote server using a well known account.

Many variations of malicious code use the built – in administrator account in an initial attempt to compromise a server. The value of this configuration change has diminished over the past few years since the release of attack tools that attempt to break into the server by specifying the SID of the built – in Administrator account to determine its true name. A SID is the value that uniquely identifies each user, group, computer account, and logon session on a network. It is not possible to change the SID of this built – in account. Renaming the local administrator account to a unique name can make it easy for your operations groups to monitor attempted attacks against this account.

Complete the following steps to secure well known accounts on domains and servers:

1. Rename the **Administrator** and **Guest** accounts, and change their passwords to a long and complex value on every domain and server.
2. Use different names and passwords on each server. If the same account names and passwords are used on all domains and servers, an attacker who gains access to one member server will be able to gain access to all others with the same account name and password.
3. Change the account descriptions to something other than the defaults to help prevent easy identification of the accounts.
4. Record these changes in a secure location.

   Note The built – in administrator account can be renamed via Group Policy. This setting was not configured in the DCBP because you should choose a unique name for your environment. The Accounts: Rename administrator account can be configured to rename administrator accounts in the three environments defined in this guide. This setting is a part of the Security Options settings of a GPO.

Securing Service Accounts

Never configure a service to run under the security context of a domain account unless absolutely necessary. If a server is physically compromised, domain account passwords can be easily obtained by dumping Local Security Authority (LSA) secrets.

Terminal Services Settings

Table 4.20 Settings

Default	Legacy Client	Enterprise Client	High Security
Set client connection encryption level	High	High	High

The **Set client connection encryption level** setting determines the level of encryption for Terminal Services client connections in your environment. The **High Level** setting option that uses 128 – bit encryption prevents an attacker from eavesdropping on Terminal Services sessions using a packet analyzer. Some older versions of the Terminal Services client do not support this high level of encryption. If your network contains such clients, set the encryption level of the connection to send and receive data at the highest encryption level supported by the client. For these reasons, this guide recommends configuring the **Set client connection encryption level** setting to **Enabled**, and the option for **High Level** encryption is selected in the DCBP in the three security environments defined in this guide.

This path for configuring this setting in the Group Policy Object Editor is:

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security.

There are three levels of encryption available:

Table 4.21 Terminal Services Encryption Levels

Encryption Level	Description
High level	This level encrypts data sent from client to server and from server to client by using strong 128 – bit encryption. Use this level when the terminal server is running in an environment containing 128 – bit clients only (such as Remote Desktop Connection clients). Clients that do not support this level of encryption will not be able to connect.
Client Compatible	This level encrypts data sent between the client and the server at the maximum key strength supported by the client. Use this level when the terminal server is running in an environment containing mixed or legacy clients.
Low level	This level encrypts data sent from the client to the server using 56 – bit encryption. **Important** Data sent from the server to the client is not encrypted.

Error Reporting

Table 4.22 Settings

Default	Legacy Client	Enterprise Client	High Security
Report Errors	Disabled	Disabled	Disabled

The **Error Reporting** service helps Microsoft track and address errors. You can configure this service to generate reports for operating system errors, Windows component errors, or program errors. Enabling the **Report Errors** service causes such errors to be reported to Microsoft via the Internet or to an internal corporate file share.

This setting is only available on Microsoft Windows® XP Professional and Windows Server 2003. The path for configuring this setting in the Group Policy Object Editor is:

Computer Configuration\Administrative Templates\System\Error Reporting

Error reports can potentially contain sensitive or even confidential corporate data. The Microsoft privacy policy regarding error reporting ensures that Microsoft will not use such data improperly, but the data is transmitted in cleartext Hypertext Transfer Protocol (HTTP), which could be intercepted on the Internet and viewed by third – parties. For these reasons, this guide recommends configuring the **Error Reporting** setting to **Disabled** in the DCBP in all three security environments defined in this guide.

Blocking Ports with IPSec Filters

Internet Protocol Security (IPSec) filters can provide an effective means for enhancing the level of security required for servers. This guide recommends this optional guidance for the High Security environment defined in this guide to further reduce the attack surface of the server.

For more information on the use of IPSec filters, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP.*

The following table lists all of the IPSec filters that can be created on domain controllers in the High Security environment defined in this guide.

The following table lists all of the IPSec filters that should be created on domain controllers in the High Security environment defined in this guide.

Table 4.23 Domain Controller IPSec Filter Network Traffic Map

Service	Protocol	Source Port	Destination Port	Source Address	Destination Address	Action	Mirror
CIFS/SMB Server	TCP	ANY	445	ANY	ME	ALLOW	YES
	UDP	ANY	445	ANY	ME	ALLOW	YES
RPC Server	TCP	ANY	135	ANY	ME	ALLOW	YES
	UDP	ANY	135	ANY	ME	ALLOW	YES
NetBIOS Server	TCP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	137	ANY	ME	ALLOW	YES
	UDP	ANY	138	ANY	ME	ALLOW	YES
	TCP	ANY	139	ANY	ME	ALLOW	YES
Monitoring Client	ANY	ANY	ANY	ME	MOM Server	ALLOW	YES
Terminal Services Server	TCP	ANY	3389	ANY	ME	ALLOW	YES
Global Catalog Server	TCP	ANY	3268	ANY	ME	ALLOW	YES
	TCP	ANY	3269	ANY	ME	ALLOW	YES
DNS Server	TCP	ANY	53	ANY	ME	ALLOW	YES
	UDP	ANY	53	ANY	ME	ALLOW	YES
Kerberos Server	TCP	ANY	88	ANY	ME	ALLOW	YES
	UDP	ANY	88	ANY	ME	ALLOW	YES
LDAP Server	TCP	ANY	389	ANY	ME	ALLOW	YES
	UDP	ANY	389	ANY	ME	ALLOW	YES
	TCP	ANY	636	ANY	ME	ALLOW	YES
	UDP	ANY	636	ANY	ME	ALLOW	YES
NTP Server	TCP	ANY	123	ANY	ME	ALLOW	YES
	UDP	ANY	123	ANY	ME	ALLOW	YES
Static AD Replication Server	TCP	ANY	57952	ANY	ME	ALLOW	YES
DC Comms	ANY	ANY	ANY	ME	Domain Controller	ALLOW	YES

DC Comms	ANY	ANY	ANY	ME	Domain Controller 2	ALLOW	YES
ICMP	ICMP	ANY	ANY	ME	ANY	ALLOW	YES
All Inbound Traffic	ANY	ANY	ANY	ANY	ME	BLOCK	YES

All of the rules listed in the table above should be mirrored when they are implemented. This ensures that any network traffic coming into the server will also be allowed to return to the originating server.

The table above represents the base ports that should be opened for the server to perform its role – specific functions. These ports are sufficient if the server has a static IP address. Additional ports may need to be opened to provide for additional functionality. Opening additional ports will make the domain controllers in your environment easier to administer, however, they may greatly reduce the security of these servers.

Recommendations from Knowledge Base article 224196, "Restricting Active Directory Replication Traffic to a Specific Port," located at http://support.microsoft.com/default.aspx?scid=kb;en-us;224196&sd=tech, need to be implemented on domain controllers. This ensures that domain replication occurs over a specific port. Once again, a random port over 50,000 should be used for this purpose. In the example above, the port 57952 was chosen. A different port should be used in your environment, but this change should be made on all domain controllers where this guidance will be implemented. After the steps from the Knowledge Base article are implemented, the servers must be restarted for the changes to take effect.

As seen above, if Microsoft Operations Manager (MOM) is implemented in the environment, all network traffic must be allowed to travel between the server where the IPSec filters are implemented and the MOM server. This is necessary because of the large amount of interaction between the MOM server and the OnePoint client — the client application that reports to the MOM console. Other management packages may have similar requirements. The filter action for the OnePoint client can be configured to negotiate IPSec with the MOM server if an even greater level of security is desired.

This IPSec policy will effectively block traffic through random high ports, therefore disallowing remote procedure call (RPC) traffic. This can make management of the server difficult. Because so many ports have been effectively closed, Terminal Services has been enabled. This will allow administrators to perform remote administration.

The network traffic map above assumes that the environment contains Active Directory enabled DNS servers. If stand – alone DNS servers are used, additional rules may be required.

The implementation of IPSec policies should not have a noticeable impact on the performance of the server. However, testing should be performed before implementing these filters to verify that the necessary functionality and performance of the server is maintained. Additional rules may also need to be added to support other applications.

> **Note** Domain controllers are extremely dynamic, and implementing IPSec filters on them should be carefully evaluated, and then thoroughly tested in a lab environment. Because of the large amount of interaction between domain controllers, IPSec filters need to be added to allow all traffic between domain controllers that replicate information with each other. In complex environments with many domain controllers, this will require the creation of dozens of additional filters so the filters can effectively protect the domain controllers. This could make it very difficult to implement and manage IPSec policies. Nevertheless, environments with few domain controllers can efficiently leverage the advantages gained by implementing IPSec filters.

Included with this guide is a .cmd file that simplifies the creation of the IPSec filters prescribed for a domain controller. The PacketFilters-DC.cmd file uses the NETSH command to create the appropriate filters. This .cmd file must be modified to include the IP addresses of the other domain controllers in the environment. The script contains place holders for two domain controllers to be added. Additional domain controllers can be added if desired. This list of IP addresses for the domain controllers must be kept up to date.

If MOM is present in the environment, the IP address of the appropriate MOM server must also be specified in the script. This script does not create persistent filters. Therefore, the server will be unprotected until the IPSec Policy Agent starts. For more information on building persistent filters or creating more advanced IPSec filter scripts, see Chapter 11, "Additional Member Server Hardening Procedures" in the companion guide, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP. Finally, this script is configured to not assign the IPSec policy it creates. The IP Security Policy Management snap-in can be used to examine the IPSec filters created, and to assign the IPSec policy in order for it to take effect.

Summary

This chapter explained the server hardening settings required to secure domain controllers in each of the three environments defined in this guide. Most of the settings discussed were configured and applied using Group Policy. A Group Policy object (GPO) designed to compliment the Default Domain Controller Policy was linked to the Domain Controllers Organizational Unit (OU). The settings included in the Domain Controllers Baseline Policy (DCBP) will enhance overall security across the domain controllers in any given

environment. Using two GPOs to secure domain controllers allows for the default environment to be preserved and simplifies troubleshooting.

Several of the server hardening settings cannot be applied through Group Policy. In these cases, details on configuring these settings manually have been provided.

Now that the domain controllers are secured, the following chapters of this guide will focus on securing several other specific server roles.

More Information

The following information sources were the latest available on topics closely related to securing domain controllers in an environment with computers running Windows Server 2003 at the time this product was released to the public.

For information about the Microsoft Systems Architecture: Enterprise Data Center prescriptive architecture guides, see:

http://www.microsoft.com/technet/itsolutions/edc/default.asp.

For information about enabling anonymous access to Active Directory, see Knowledge Base article 257988, "Description of Dcpromo Permissions Choices," see:

http://support.microsoft.com/default.aspx?scid=kb;en-us;257988&sd=tech.

For information about Windows 2000 DNS, see the "Windows 2000 DNS White Paper" at: http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/w2kdns.asp.

For more information about Windows 2000 DNS, see Chapter 6 of the online version of "TCP/IP Core Networking Guide" at: http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp.

For information about Windows 2003 DNS, see the "Changes to DNS in Windows Server 2003 at:

http://www.microsoft.com/windows2000/technologies/communications/dns/dns2003.asp

For more information on IPSec filtering, see "How To: Use IPSec IP Filter Lists in Windows 2000," at: http://support.microsoft.com/default.aspx?scid=313190.

For more information on restricting Active Directory, see "Restricting Active Directory Replication Traffic to a Specific Port," at:

http://support.microsoft.com/default.aspx?scid=224196.

For more information on restricting FRS replication traffic, see "How to Restrict FRS Replication Traffic to a Specific Static Port," at:

http://support.microsoft.com/default.aspx?scid=319553.

For more information on the Windows Time Service, see "Basic Operation of the Windows Time Service," at: http://support.microsoft.com/default.aspx?scid=224799.

For more information on configuring the Windows Time Service, see "How to Configure an Authoritative Time Server in Windows 2000," at:

http://support.microsoft.com/default.aspx?scid=216734.

For more information on IP spoofing, see the article in the SANS Info Sec Reading Room, at: http://www.sans.org/rr/threats/intro_spoofing.php.
