Global Information Assurance Certification Paper

Windows 2000 Domain Controller Operating in a Mixed Network Environment

Security Configuration Guidance

Andrew J. Broadaway
Prepared for SANS GIAC NT Practical
Securing Windows Track, SANS New Orleans, Feb 2001

1.0 INTRODUCTION

1.1 Purpose and Scope

This document is written as a guide for configuring security options and implementing security countermeasures on Windows 2000 Domain Controllers in a mixed mode Windows NT and Windows 2000 heterogeneous environment. Setting up a Windows 2000 Domain Controller to interoperate with Windows NT Clients requires slightly more permissive settings in some areas of security policy. Many network administrators will not have the option of going directly to a native Windows 2000 network, so it is important to maintain the interoperability and backwards compatibility that Windows 2000 allows. The settings recommended in this document are based in part on current DOD computer security policies, NIST's CSPP-OS-COTS Security Protection Profile-Operating System, or are industry best practices. This document is meant to assist system administrators and managers in the configuration of systems to be used as Windows 2000 Domain Controllers.

The following essential assumptions have been made to limit the scope of this document:

- All Microsoft Windows 2000 domain controllers are clean-installs (i.e., not upgraded).
- The latest Windows 2000 service pack (currently Service Pack 1) and hotfixes have been installed according to the instructions herein.
- All network machines are Intel-based architecture.
- Users of this guide have a working knowledge of Windows 2000 installation and basic system administration skills.

2.0 WINDOWS 2000 SERVER OVERVIEW

Windows 2000 provides security that is flexible and scalable. Features that exceed the capabilities of Windows NT 4.0 include such things as native support for Smart Cards, an Encrypting File System (EFS), and Certificate Services. Notable enhancements have been made to several pre-existing features such as user authentication and access controls. Also, to ensure that administrators can manage these features easily and efficiently, Windows 2000 makes use of Active Directory. Active Directory extends the features of previous Windows directory services and adds entirely new features, many of which have security implications.

In Windows 2000, the basic components of a network architecture are known as objects, which can be users, computers, groups, Organizational Units, etc. A more complete description of Windows 2000 objects and the behavior of objects can be found in any number of Windows 2000 networking and implementation guides. An object's security-relevant behavior is defined by its security settings.

Security settings (or security configuration) include such things as security policies, access control, event log, group membership, Internet Protocol Security (IPSec) policies and public key policies. When applying security settings to objects in the Active Directory by the use of group policy, administrators must determine the functional and organizational character of each site, domain or organizational unit (OU) to be included. Different objects will require different levels of security, depending upon their usage.

To accomplish this, Windows 2000 includes a set of security templates, to be used based on the role of a computer. Templates are provided for security ranging from low-level security domains to highly secure Domain Controllers. These templates can be used in the default configuration, modified, or used as a basis to create custom security templates. Administrators can apply security templates by using the Security Templates snap-in. Security can be configured and analyzed locally by using the Security Configuration and Analysis snap-in, or can be configured centrally in Active Directory by using the Group Policy snap-in.

3.0 INSTALLATION

This section discusses aspects of the Windows 2000 Server installation process that relate directly to security matters. Before beginning the installation process of Windows 2000 Server, you must prepare for the installation by gathering information and making decisions about how you want to install and implement Windows 2000 in your organization. This installation guide assumes that required information relating to design and implementation issues have been gathered, and that the Windows 2000 installation and implementation process has been thoroughly planned.

- Unless operationally necessary, Windows 2000 Server should be a clean install, not an upgrade.

3.1 Set Power-On Password

Set the power-on password in the computer's BIOS setup. This can still be disabled by changing hardware switches so unauthorized access to internal components should be protected with a locking case or securing the entire computer.

3.2 File System

When installing Windows 2000 Server onto un-partitioned disk space, you are prompted to select the file system that should be used to format the partition. While Windows 2000 Server supports the NTFS, File Allocation Table (FAT) 16 and FAT 32 file systems, for security reasons, and also to allow the use of Active Directory, you must choose to install on an NTFS file system. If you are upgrading to Windows 2000 from a pre-existing install on a FAT file system, you must be sure that you convert the file system to NTFS using the provided conversion tools. However, once you use the convert utility, the ACLs for the

converted drive will be set to Everyone: Full Control. Access controls must then be set to the appropriate level.

3.3 Windows 2000 Server Components

When installing Windows 2000, you must ensure that only necessary software components and services are installed during a new installation or upgrade. By default, there are many services and software components enabled or optionally available, which are not necessary for the functionality of a Domain Controller. You must determine specific operational requirements and then decide which additional components to enable. Unless there is an overriding operational necessity requiring the use of a particular component, it should be disabled.

3.4 Hardware Issues

Windows 2000 Setup automatically checks your hardware and software and reports any potential conflicts. But to ensure a successful, secure installation, you should make sure that your server hardware is compatible with Windows 2000 Server before starting the setup process. To do this, verify that your hardware is on the Hardware Compatibility List (HCL). The HCL is included on your Windows 2000 Server installation CD-ROM in the Support folder in Hcl.txt. The HCL lists each hardware model that has passed the Hardware Compatibility Tests determined by Microsoft. The list also indicates which devices Windows 2000 Server supports. Installing Windows 2000 Server on a computer that does not have hardware listed in the HCL might not be successful or security may be compromised.

Microsoft releases an updated HCL on a regular basis. Review the most up-to-date list of supported hardware at the Microsoft HQL Web Site, at http://www.microsoft.com/hcl.

3.4.1 Disabling Unused Hardware

For security reasons, it is prudent to remove or disable all hardware and hardware components that are not currently being used in the normal operation of any Windows 2000 Server. Disabling these devices decreases the likelihood of their unauthorized or malicious usage. Unused devices that may be disabled include, but are not limited to: Floppy Disks, COM Ports, LPT Ports, Modems, CD ROM drives, and extra unused hard disks.

3.4.2 Enable Hardware Boot Protection

Windows 2000 Servers' BIOS should be configured to allow booting from the hard disk only. The specifics of setting the BIOS vary based on the type of hardware. The BIOS can be accessed during the boot, often by pressing DEL, F1, F2, or CTRL-S. At various times, it may be necessary to boot from something other than the primary hard drive. In those cases, you can enter the

BIOS (after entering the BIOS password) and temporarily enable different boot devices.

3.4.3 External Drives

External drive devices should have locking capabilities. Each removable media device should be capable of being locked to prevent unauthorized access to data. A single locked door covering the drives is sufficient. The locking mechanism must render the device useless, whether locking is done electronically or mechanically

3.4.4 Computer Cases

Computer case and switches should have locking capabilities to prevent unauthorized internal access. An OEM-specific method can be implemented, either electronically or mechanically. When available controls and remote alerts should be implemented for chassis-open intrusion.

3.5 Alternative Or Multiple Operating Systems

No other operating system should be installed on the same system where a Windows 2000 Domain Controller resides and only one copy of the operating system should be installed.

4.0 Post Installation

After the installation of Windows 2000 Server, the first thing that should be done is running the dcpromo.exe command from the command line. That opens the Active Directory Installation Wizard and promotes the server to a Domain Controller. This installs Active Directory on the server, as well as setting default access controls on critical files and initializing the security subsystem on the Domain Controller. Additionally, if a Windows 2000 DNS server does not yet exist on the network, the Wizard suggests that you install and configure a DNS server. It is best to do that now, and later follow the configuration information below.

5.0 Security Configuration Toolset

The process of configuring security in the Windows 2000 environment is complex and detailed because of the large number of system components involved, their relationship to each other, and the level of change that may be required. Windows 2000 also provides a number of security enhancements over Windows NT 4. In order to facilitate the use and management of the security components, Windows 2000 provides the Security Configuration Tool Set. The Tool Set was specifically designed to facilitate the use of these security enhancements and manage the highly complex security attributes of Windows 2000. The Tool Set functions primarily within the Microsoft Management Console (MMC), first introduced in the last Service Pack for Windows NT 4.

With the Security Configuration Tool Set, configuration tasks can be grouped and automated. From the MMC, security can be configured using Group Policy, Security Templates, and Security Configuration and Analysis snap-ins. The MMC integrates all these separate tools in order to configure and analyze security on one or more Windows 2000 or Windows NT-based machines in your network. In Windows 2000, these features also provide support for Internet-aware enterprise networks and the new distributed services included in the operating system.

The Security Configuration Tool Set answers the need for a central security configuration tool, and provides the framework for enterprise-level analysis functionality. It also reduces the cost of security-related administration by defining a single point where the entire system's security can be viewed, analyzed, and adjusted.

The Tool Set consists of the following components:

- **Security Configuration Service.** This service is the core engine of the Security Configuration Tool Set. It runs on every Windows 2000 system and is responsible for all security configuration and analysis functionality provided by the tool set. This service is central to the entire infrastructure.

- **Setup Security.** This tool, using predefined configurations that ship with the system, performs the initial security configuration during setup. This creates an initial security database, the Local Computer Policy database, on every computer with a clean installation of Windows 2000. It is important to note that this is not the case when a Windows NT 4 or earlier machine is upgraded, because a client may have customized the security configuration, which must not be overwritten. In this case, the client can use the Configure option of the tool set to apply a configuration.

- **Security Template snap-in.** The Security Template snap-in provides a single location where system security can be viewed, changed, applied to a local computer, or exported to a Group Policy Object. The Security Configuration Tool Set includes standard and recommended configurations to be used in typical Windows 2000 configurations, including those installations that have Internet and intranet components. The editing capabilities of this stand-alone snap-in tool allow you to define security templates with prescribed security settings for attributes in each security area (including account policies, local policies, restricted groups, the registry, etc.), or create new ones by customizing them for your particular environment. These files can then be imported to the security database on computers throughout the system. The configurations can also be imported into Group Policy objects and be propagated automatically to the local computer policy database.

- **Security Configuration and Analysis snap-in.** The Security Configuration and Analysis (SCA) snap-in is the key tool for analyzing and reviewing the analysis of the system's security. It also provides recommendations to resolve discrepancies found by the analysis.

- **Security settings extension to the Group Policy Editor.** This snap-in tool extends the capabilities of the Group Policy Editor. It allows you to define security configuration as part of a group policy object. Group Policy objects can then be assigned to a specific Computer Object or at the Domain or Organizational Unit scope in Active Directory so that the Group Policy objects are applied to all the computers in that specific scope. Security configurations from various group policy objects (Local, Domain, and Organizational Units) are propagated to the computer and imported into the local computer policy database. The composite configuration from this database is applied to the computer periodically to ensure that the system adheres to corporate policy. This is referred to as the computer's security policy.

- **Command-line tool-Secedit.exe.** This is the command-line interface to some of the features of the tool set.

Using the above tools it is possible to define and save security configurations, which can be transferred from one location to another. This can help to reduce the management cost for security issues and help to ensure a uniform security configuration system-wide. Since configurations are saved as text-based .inf files, you can use any text editor to read the sample configuration provided with the tool and modify its content.

When one or more configurations are imported to a specific computer, a security configuration and analysis database is created. Likewise, there will be an initial database created when a computer has a clean installation of Windows 2000. This security configuration and analysis database is the starting point for all configurations and analyses done on a system. The local computer policy database is the security database on the system; it defines the existing security policy. Security configuration attributes that are not enforced by policy may take any value, whether by default or defined by another tool. Nevertheless, any custom configurations using other tools that conflict with the policy are overridden by the definitions in the policy.

6.0 Security Policy Settings

****As shown above, there are many ways to modify security policy settings throughout a Windows 2000 Domain and on specific local Windows 2000 Servers and Workstations. Additionally, there is more than one "correct" way to implement the following suggestion settings, and this recommended way may or may not be the most effective for any particular organization.

In order to set Security Policy settings on a Domain Controller, you are going to need to rely mainly upon two pre-defined toolsets that appear in the

Administrative Tools menu in the **Start** menu. These tools (or more appropriately, MMC Snap-ins) are called **Domain Security Policy** and **Domain Controller Security Policy**. These tools are actually the security subset of the Default Domain Group Policy Object and the Default Domain Controller Group Policy Object, respectively. This is important to keep in mind, because any changes that you make to the security policy using these two tools is reflected in the Default Group Policy Objects. If the Default Group Policy Object is disabled or in any other way rendered ineffective on the domain objects, any changes made using the above two tools will not take effect. Also, precedence of Group Policy Settings takes effect, so if any conflicting settings are implemented on an OU or Domain above the order of inheritance of the Default Group Policy Objects, they will take precedence over the Default Settings. For the purposes of this document, it will be assumed that both the Default Domain Group Policy Object and the Default Domain Controller Group Policy Object are enabled.

Opening both of these tools, you will see that they look very similar. See figures 1 and 2 below for a comparison.

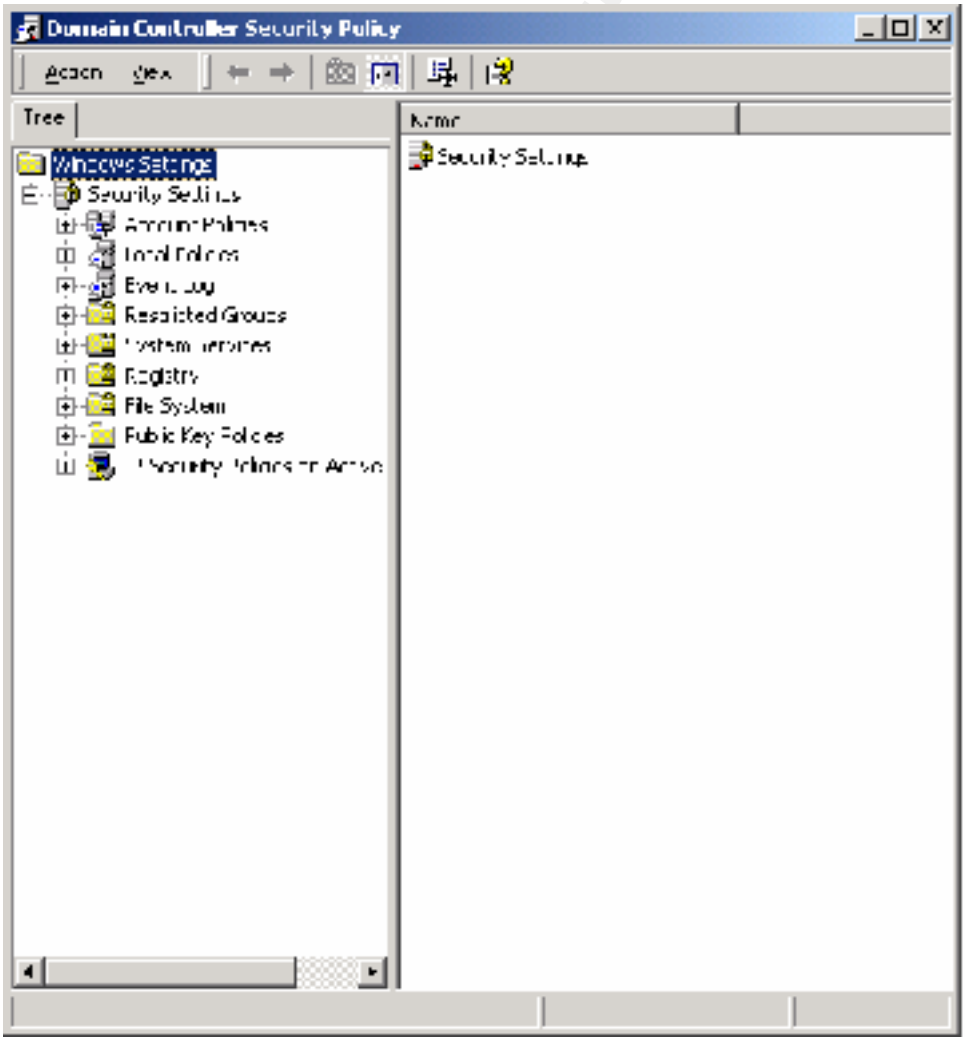


Figure 1

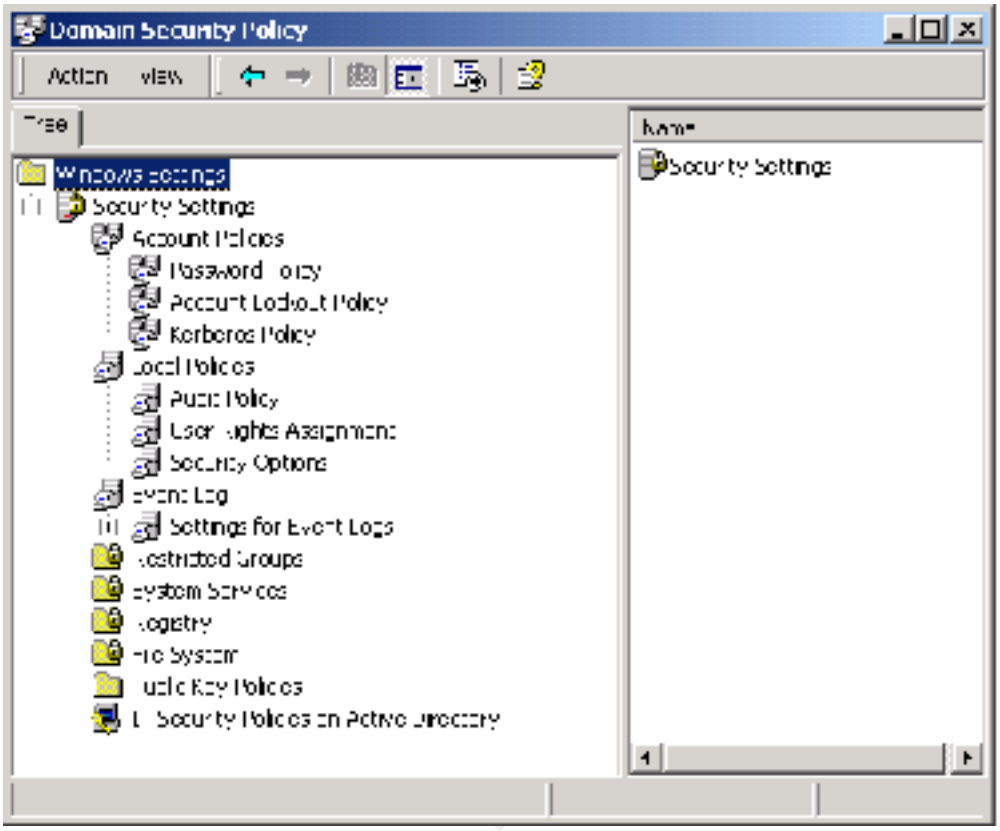


Figure 2

The following series of tables instructs you on certain settings that will be made using either one of the tools. Note that only policies that will effect the entire domain are made in the **Domain Security Policy** tool while settings meant to affect only the Domain Controller are made in the **Domain Controller Security Policy** tool.

6.1 Account Policies

A key component of controlling the security in a Windows 2000 domain is the proper setting of account policies. Depending on the type of system (e.g. domain controller, workstation, member server), account policy configuration will impact the network differently. In Windows 2000 domains, account policy is set and enforced in the domain's Group Policy. Attempts to configure domain account policies in other Group Policy Objects (GPOs) are ignored. Configuring account policies directly on workstations and member servers only impacts the local password or lockout policy on the machine. To ensure a consistent password and lockout policy throughout the entire domain for both local and domain logons, the same policy must be set on the domain controllers (via the domain GPO), member servers and workstations.

6.1.1 Password Policies

Passwords should be changed frequently and should not be reused. Avoid using passwords that can be guessed easily and words that appear in the dictionary. Passwords should contain a combination of letters, symbols and numbers.

Before making modifications to the **Account Policy** dialog box, review your organization's written password security policy. The settings made in the **Account Policy** dialog box should comply with the written password policy. Users should read and sign statements acknowledging compliance with the organizational computer policy.

Table 1 lists the recommended password policy settings.

Password Policy Options	Domain Security Policy	Domain Controller Security Policy
Enforce password uniqueness by remembering last x passwords Prevents users from toggling among their favorite passwords and reduces the chance that a hacker/password cracker will discover passwords. If this option is set to 0, users can revert immediately back to a password that they previously used. Allowable values range from 0 (do not keep password history) to 24.	15 Passwords	Not Defined
Maximum Password Age The period of time that a user is allowed to have a password before being required to change it. Allowable values include Forever (password never expires) or between 1 and 999 days.	90 Days	Not Defined
Minimum Password Age The minimum password age setting specifies how long a user must wait after changing a password before changing it again. By default, users can change their passwords at any time. Therefore, a user could change their password, then immediately change it back to what it was before. Allowable values are 0 (allow changes immediately) or between 1 and 42 days.	5 Days	Not Defined
Minimum Password Length Blank passwords and shorter-length passwords are easily guessed by password cracking tools. To lessen the chances of a password being cracked, passwords should be longer in length. Allowable values for this option are 0 or between 1 and 14 characters.	7 Characters	Not Defined
Password must meet complexity requirements of installed password filter Enforces strong password requirements for all users by use of a dynamic link library called `passfilt.dll`. Stronger passwords provide some measure of defense against password guessing and dictionary attacks launched by outside intruders. Passwords must contain characters from 3 of 4 classes: upper case letters, lower case letters, numbers, and special characters (e.g., punctuation marks). Also, passwords cannot be the same as the user's logon name. Complexity requirements will take effect the next time a user changes his password. Already-existing passwords will not be affected.	Enabled	Not Defined
Store Passwords Using Reversible Encryption Stores User's passwords using reversible encryption on the Domain Controller.	Disabled	Not Defined

Table 1

6.1.2 Account Lockout Policy

An organization should enforce that users be locked out after a specified number of failed logon attempts. To preclude password guessing, an intruder lock out feature should suspend accounts after five invalid attempts to log on. In a 24/7 facility that supports system administration service, system administrator intervention should be required to clear a locked account. Where a 24/7 facility that supports system administration service is not available, accounts should remain locked out for at least ten minutes.

Account lockout is recommended after three invalid logon attempts. This setting will slow down a dictionary attack in which thousands of well-known passwords are tried. If the account is locked out after each invalid attempt to logon, the hacker must wait until the account is enabled again. If an account is locked out, the administrator can reset it using **Active Directory Users and Computers** for domain accounts or **Computer Management** for local accounts instead of waiting the allotted lockout duration.

Table 2 lists the recommended account lockout policy settings.

Account Lockout Policy Options	Domain Security Policy	Domain Controller Security Policy
Account lockout duration Sets the number of minutes an account will be locked out. Allowable values are Forever (until admin unlocks) or between 1 and 99999 minutes.	30 Minutes	Not Defined
Account lockout threshold Prevents brute-force password cracking/guessing attacks on the system. This option specifies the number of invalid logon attempts that can be made before an account is locked out. Allowable values range from 0 (no account lockout) to 999 attempts.	5 Attempts	Not Defined
Reset account lockout count after Sets the number of minutes until the invalid logon count is reset. Allowable values range from 1 to 99999 minutes.	10 Minutes	Not Defined

Table 2

6.1.3 Kerberos Policy Options

Kerberos is the default authentication method used in Windows 2000 Active Directory.

Table 3 lists the Kerberos Policy options.

Kerberos Policy Options	Domain Security Policy	Domain Controller Security Policy
Enforce user logon restrictions Forces the Key Distribution Center (KDC) to check if a user requesting a service ticket has either the "Log on locally" (for local machine service access) or "Access this computer from the network" user right on the machine running the requested service. If the user does not have the appropriate user right, a service ticket will not be issued. Enabling this option provides increased security, but may slow network access to servers.	Enabled	Not Defined
Maximum lifetime for service ticket Determines the number of minutes a Kerberos service ticket is valid. Values must be between 10 minutes and the setting for "Maximum lifetime for user ticket." This value is set to 600 minutes in the default domain GPO.	300 Minutes	Not Defined
Maximum lifetime for user ticket Determines the number of hours a Kerberos ticket-granting ticket (TGT) is valid. Upon expiration of the TGT, a new one must be obtained or the old one renewed. This value is set to 10 hours in the default domain GPO.	5 Hours	Not Defined
Maximum lifetime for user ticket renewal Sets the maximum number of days that a user's TGT can be renewed. This value is set to 7 days in the default domain GPO	5 Days	Not Defined
Maximum tolerance for computer clock synchronization Sets the maximum number of minutes by which the KDC and client machine's clocks can differ. Kerberos makes use of time stamps to determine authenticity of requests and aid in preventing replay attacks. Therefore, it is important that KDC and client clocks remain synchronized as closely as possible. This value is set to 5 minutes in the default domain GPO.	5 Minutes	Not Defined

Table 3

6.2 Local Policies

Local policies are used to configure local audit policy, user rights assignment, and various security options such as control of floppy disk, CD-ROM, etc.

6.2.1 Audit Policy

Auditing is critical to maintaining the security of the Domain Controller. On Windows 2000 servers (and workstations), complete auditing is not enabled by default. Each Windows 2000 system includes auditing capabilities that collect information about individual system usage. The logs collect information on applications, system, and security events.

Auditing can consume a large amount of processor time and disk space. It is highly recommended that administrators check, save, and clear audit logs daily/weekly to reduce the chances of system degradation or save audit logs to a separate machine. It is also recommended that logs be kept on a separate partition.

Table 4 lists recommended Audit Policy Settings.

Audit Policy Options	Domain Security Policy	Domain Controller Security Policy
Audit Account Logon Events Tracks user logon events on other computers in which the local computer was used to authenticate the account.	Not Defined	Success, Failure
Audit Account Management Tracks changes to the Security Account database (i.e., when accounts are created, changed, or deleted).	Not Defined	Success, Failure
Audit Directory Service Access Audits users' access to Active Directory objects that have their system access control list (SACL) defined. This option is similar to Audit Object Access except that it only applies to Active Directory objects and not files and registry objects. Since this option only applies to Active Directory, it has no meaning on workstations and member servers.	Not Defined	Success, Failure
Audit Logon Events Tracks users who have logged on or off, or made a network connection. Also records the type of logon requested (interactive, network, or service). This option differs from "Audit Account Logon Events" in that it records where the logon occurred versus where the logged-on account lives. Track failures to record possible unauthorized attempts to break into the system.	Not Defined	Success, Failure
Audit Object Access Tracks unsuccessful attempts to access objects (e.g., directories, files, printers). Individual object auditing is not automatic and must be enabled in the object's properties.	Not Defined	Failure

Audit Policy Change Tracks changes in security policy, such as assignment of privileges or changes in the audit policy.	Not Defined	Success, Failure
Audit Privilege Use Tracks unsuccessful attempts to use privileges. Privileges indicate rights assigned to Administrators or other power users.	Not Defined	Failure
Audit Process Tracking Detailed tracking information for events such as program activation and exits. This option is useful to record specific events in detail if your system is believed to be under attack.	Not Defined	No Auditing
Audit System Events Tracks events that affect the entire system or the Audit log. Records events such as restart or shutdown.	Not Defined	Success, Failure

Table 4

6.2.2 User Rights Assignment

User rights are allowable actions that can be assigned to users or groups to supplement built-in abilities. Careful allocation of user rights can significantly strengthen the security of a Windows 2000 system. Advanced user rights are assigned to Administrators or other trusted users who are allowed to run administrative utilities, install service packs, create printers, and install device drivers. If resources are available it is recommended assigning these duties to several trusted users. Administrators are not explicitly listed for rights they implicitly have.

Table 5 Lists Recommend User Rights Assignment Settings.

Standard/Advanced User Rights	Domain Security Policy	Domain Controller Security Policy

Standard/Advanced User Rights	Domain Security Policy	Domain Controller Security Policy
Access this computer from network Allows a user to connect over the network to the computer.	Not Defined	Administrators Authenticated Users
Act as part of the operating system Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	Not Defined	(No one)
Add workstations to the domain Allows a user to add workstations to a particular domain. This right is meaningful only on domain controllers. The Administrators and Account Operators groups have the ability to add workstations to a domain and do not have to be explicitly given this right.	Not Defined	(No one)
Back up files and directories Allows a user to back up files and directories. This right supersedes file and directory permissions.	Not Defined	Administrators Backup Operators
Bypass traverse checking Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories.	Not Defined	Authenticated Users
Change the system time Allows a user to set the time for the internal clock of the computer.	Not Defined	Administrators
Create a pagefile Allows a user to create new pagefiles for virtual memory swapping and change the size of a pagefile.	Not Defined	Administrators
Create a token object Allows a process to create access tokens that can be used to access local resources. Only the Local Security Authority should be allowed to create this object.	Not Defined	(No one)
Create permanent shared object Allows a user to create special permanent directory objects, such as \\Device, that are used within the Windows 2000 object manager.	Not Defined	(No one)
Debug programs Allows a user to debug various low-level objects such as threads.	Not Defined	(No one)
Deny access to this computer from the network Prevents specific users and/or groups from accessing the computer via the network. This setting supercedes the "Access this computer from the network" setting if an account is subject to both policies.	Not Defined	(No one)
Deny logon as a batch job Prevents specific users and/or groups from logging on as a batch job. This setting supercedes the "Logon as a batch job" setting if an account is subject to both policies.	Not Defined	(No one)
Deny logon as a service Prevents specific service accounts from registering a process as a service. This setting supercedes the "Log on as a service" setting if an account is subject to both policies.	Not Defined	(No one)

Standard/Advanced User Rights	Domain Security Policy	Domain Controller Security Policy
Deny logon locally Prevents specific users and/or groups from logging on directly at the computer. This setting supercedes the "Log on locally" setting if an account is subject to both policies.	Not Defined	(No one)
Enable computer and user accounts to be trusted for delegation Allows a user to set the "Trusted for Delegation" setting on a user or computer object. The user granted this right must have write access to the account control flags on the computer or user object.	Not Defined	Administrators
Force shutdown from a remote system Allows a user to shutdown a Windows 2000 system remotely over a network.	Not Defined	Administrators
Generate security audits Allows a process to generate security audit log entries.	Not Defined	(No one)
Increase quotas Allows a user to increase the processor quota assigned to a process.	Not Defined	Administrators
Increase scheduling priority Allows a user to boost the execution priority of a process.	Not Defined	Administrators
Load and unload device drivers Allows a user to install and remove device drivers. This right is necessary for Plug and Play device driver installation.	Not Defined	Administrators
Lock pages in memory Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys. This right is obsolete in this version of Windows 2000.	Not Defined	(No one)
Log on as a batch job Allows a user to log on by means of a batch-queue facility. In Windows 2000, the Task Scheduler automatically grants this right as necessary.	Not Defined	(No one)
Log on as a service Allows a process to register with the system as a service. Some applications such as Microsoft Exchange require a service account, which should have this right.	Not Defined	As needed
Log on locally Allows a user to log on at a system's console. To allow a user to log on locally at a domain controller, this right must be enabled in the Domain Controller group policy object.	Not Defined	Administrators Backup Operators
Manage auditing and security log Allows a user to view and clear the security log and specify what types of object access (such as file access) are to be audited. Users with this right can enable auditing for a specific object by editing the auditing options in the security tab of the object's Properties dialog box. This right does not allow a user to enable file and object access auditing in general. Setting the "Audit object access" item under Audit Policies enables object auditing. Members of the Administrators group always have the ability to view and clear the security log.	Not Defined	Administrators

Standard/Advanced User Rights	Domain Security Policy	Domain Controller Security Policy
Modify firmware environment variables Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.	Not Defined	Administrators
Profile single process Allows a user to perform profiling (performance sampling) on a process.	Not Defined	Administrators
Profile system performance Allows a user to perform profiling (performance sampling) on the system.	Not Defined	Administrators
Remove computer from docking station Allows a user to undock a laptop from a docking station.	Not Defined	(No one)
Replace a process-level token Allows a user to modify a process's security access token. This is a powerful right used only by the system.	Not Defined	(No one)
Restore files and directories Allows a user to restore backed-up files and directories. This right supercedes file and directory permissions.	Not Defined	Administrators Backup Operators
Shut down the system Allows a user to shut down Windows 2000.	Not Defined	Administrators
Synchronize directory service data This right has no effect in the initial release of Windows 2000.	Not Defined	(No one)
Take ownership of files or other objects Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Not Defined	Administrators

Table 5

6.2.3 Security Options

The Security Options section in the Local Settings menu contains many extra security features that can be set using the security editing tools. Changing these settings affects a change in the registry, and I tried to include all of the registry setting changes in the description of the options below. Please note that changes made utilizing the Security Policy tool do not then have to be made by hand using a registry editor. All of these settings are to be applied only to the **Domain Controller Security Policy** tool and not to the **Domain Security Policy** tool. All entries in this section in the latter tool should be set to "Not Defined".

Table 6 Lists Recommend Security Options Settings.

Security Option	Domain Controller Security Policy Setting
Additional restrictions for anonymous access Places restrictions on anonymous users. The options are: *None. Rely on default permissions.* Default permissions allow anonymous users to enumerate the names of domain accounts and network shares and have the same amount of access to resources as the "Everyone" group. The registry value for this option is 0. *Do not allow enumeration of SAM accounts and shares.* Replaces the "Everyone" group with "Authenticated Users" in resource security permissions. The registry value for this option is 1. *No access without explicit anonymous permissions.* Requires that "Anonymous" be given explicit permissions to access resources by removing the "Everyone" and "Network" groups from the anonymous user token. The registry value for this option is 2. Setting the Restrict Anonymous key value = 2 could result in undesired effects when setting up trust relationships, authenticating in a mixed environment, or running certain services or applications. Please see http://support.microsoft.com/support/kb/articles/Q246/2/61.asp for further information on setting this key. If setting the key = 2 is not feasible, it is recommended that the value be set to "Do not allow enumeration of SAM accounts and shares" (value = 1). **HKLM\System\CurrentControlSet\Control\Lsa\ RestrictAnonymous = 1**	Do Not allow enumeration of SAM accounts and Shares.

Security Option	Domain Controller Security Policy Setting
Allow Server Operators to schedule tasks (Domain Controllers Only) Allows Server Operators to use Schedule Service (AT Command) or schedule task to automatically run. By default, Administrators are able to schedule tasks. Options are: *Disabled* Only allow Administrators to schedule tasks *Enabled* Allow Administrators and Server Operators to schedule tasks **HKLM\System\CurrentControlSet\Services\Schedule = 0**	Disable
Allow system to be shut down without having to log on On Windows 2000, a **Shutdown** button is available in the **Logon** dialog box. When this option is disabled, users must be able to log on to the system and have the **Shut down the system** user right in order to shutdown the computer. By default, this option is disabled on servers. **HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon\ShutdownWithoutLogon = 0**	Disabled
Allowed to eject removable NTFS media By default, only Administrators are allowed to eject removable NTFS media. This setting allows for the following options: *Administrators* *Administrators and Power Users* *Administrators and Interactive Users* **HKLM\Software\Microsoft\Windows NT\ CurrentVersion\winlogon\AllocateDASD = 0**	Administrators
Amount of idle time required before disconnecting a session Sets the amount of continuous idle time in a Server Message Block (SMB) session before a session is disconnected. If client activity resumes after a disconnect, the session is automatically reestablished. Allowable values are between 0 (disconnect idle session immediately) and 0xFFFFFFFF (disabled). **HKLM\System\CCS\Services\LanManServer\ Parameters\AutoDisconnect = 30**	30 minutes

Security Option	Domain Controller Security Policy Setting
Audit the access of global system objects When enabled, this option will assign a default SACL to system objects such as mutexes, events, semaphores, and DOS devices. In order for these system objects to be audited, **Audit Object Access** must be enabled under auditing. **HKLM\System\CurrentControlSet\Control\Lsa\ AuditBaseObjects = 1**	Enabled
Audit use of all user rights including Backup and Restore Enables auditing of all user rights in conjunction with **Audit Privilege Use** auditing being enabled. If this option is disabled, the **Backup** and **Restore** rights will not be audited even if **Audit Privilege Use** is enabled. Since there could be many Backup and Restore events generated during the course of system backups, this option may be disabled if there are concerns about the growth of the security log. **HKLM\System\CurrentControlSet\Control\Lsa\ FullPrivilegeAuditing =1**	Enabled
Automatically log off users when logon time expires Causes client SMB sessions to be forcibly disconnected when a user's logon hours expire. This setting affects all machines in a domain.	Enabled
Automatically log off users when logon time expires (local) Causes client SMB sessions to be forcibly disconnected when a user's logon hours expire. This policy affects the local machine on which it is applied. **HKLM\System\CurrentControlSet\Services\ LanManServer\Parameters\EnableForcedLogoff = 1**	Enabled
Clear virtual memory pagefile when system shuts down Wipes the system pagefile clean when Windows 2000 shuts down, ensuring that sensitive information that may be in the pagefile is not available to malicious users. When this option is enabled, it also causes the hibernation file (`hiberfil.sys`) to be cleared when hibernation is disabled on a laptop system. **HKLM\CurrentControlSet\Control\Session Manager\MemoryManagement\ ClearPageFileAtShutdown = 1**	Enabled

Security Option	Domain Controller Security Policy Setting
Digitally sign client-side communication (always) Forces an SMB client to always digitally sign SMB communications. Digital signatures provide mutual authentication during SMB exchanges, preventing "man-in-the-middle" and active message attacks. To use SMB digital signing, this option must be enabled on both the SMB client and server. **HKLM\System\CurrentControlSet\Services\ LanmanWorkstation\Parameters\ RequireSecuritySignature = 0**	Disabled
Digitally sign client-side communication (when possible) Enables an SMB client to perform digital packet signing when communicating with an SMB server that also supports packet signing. Digital signatures provide mutual authentication during SMB exchanges, preventing "man-in-the-middle" and active message attacks. **HKLM\System\CurrentControlSet\Services\ LanmanWorkstation\Parameters\ EnableSecuritySignature = 1**	Enabled
Digitally sign server-side communication (always) Forces an SMB server to always digitally sign SMB communications. Digital signatures provide mutual authentication during SMB exchanges, preventing "man-in-the-middle" and active message attacks. To use SMB digital signing, this option must be enabled on both the SMB client and server. **HKLM\System\CurrentControlSet\Services\ LanmanServer\Parameters\RequireSecuritySignatur e = 0**	Disabled
Digitally sign server-side communication (when possible) Enables an SMB server to perform digital packet signing when communicating with an SMB client that also supports packet signing. Digital signatures provide mutual authentication during SMB exchanges, preventing "man-in-the-middle" and active message attacks. **HKLM\System\CurrentControlSet\Services\ LanmanServer\Parameters\EnableSecuritySignature = 1**	Enabled

Security Option	Domain Controller Security Policy Setting
Disable CTRL+ALT+DEL requirement for logon If this option is enabled, a user is not required to press CTRL+ALT+DEL to log on. CTRL+ALT+DEL establishes a trusted path to the operating system when entering a username/password pair; therefore, disabling it poses a security risk to the users' logon credentials. By default, this option is disabled on systems in a domain and enabled on stand-alone workstations. **HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System\DisableCAD = 0**	Disabled
Do not display last username in logon screen By default, Windows 2000 displays the name of the last user to log on the computer in the **Logon** dialog box. To prevent malicious users from gaining information about user names on the system, disallow display of the last logon. This is especially important if a generally accessible computer is being used for system administration. **HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Winlogon\DontDisplayLastUserName = 1**	Enabled

Security Option	Domain Controller Security Policy Setting
LAN Manager authentication level This parameter specifies the type of challenge/response authentication to be used for network logons with non-Windows 2000 Windows clients. LanManager authentication (LM) is the most insecure method, allowing encrypted passwords to be easily sniffed off the network and cracked. NT LanManager (NTLM) is somewhat more secure. NTLMv2 is a more robust version of NTLM and is available with Windows NT 4.0 Service Pack 4 and higher as well as Windows 95/98 with Directory Services Client. The following options are available: *Send LM & NTLM responses* Registry value = 0. *Send LM & NTLM – use NTLMv2 session security if negotiated* Registry value = 1. *Send NTLM response only* Registry value = 2. *Send NTLMv2 response only* Registry value = 3. *Send NTLMv2 response only\refuse LM* Registry value = 4. *Send NTLMv2 response only\refuse LM and NTLM* Registry value = 5. Setting this value higher than 2 on a Windows 2000 system could prevent some connectivity to systems that support only LM authentication (Windows 95®/98® and Windows for Workgroups®) or only NTLM (Windows NT 4.0 prior to Service Pack 4). If adding a Windows 2000 machine to a Windows NT 4.0 domain, this value may need to be set to 4 "Send NTLMv2 response only\refuse LM" on the Windows NT 4.0 domain controller. **HKLM\System\CurrentControlSet\Control\Lsa\ LMCompatibilityLevel = 3**	Send NTLMv2 response only

Security Option	Domain Controller Security Policy Setting
Message text for users attempting to log on It is recommended that systems display a warning message before logon, indicating the private nature of the system. Many organizations use this message box to display a warning message that notifies potential users that their use can be monitored and they can be held legally liable if they attempt to use the computer without proper authorization. The absence of such a notice could be construed as an invitation, without restriction, to enter and browse the system. **HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ LegalNoticeText = "Text you want displayed"**	According to Organizational Policy
Message title for users attempting to log on In conjunction with the Logon Text, it is recommended that systems display a warning message title before logon, indicating the private nature of the system. **HKLM\Software\Microsoft\WindowsNT\CurrentVersion** **Winlogon\ LegalNoticeCaption = "Text you want displayed on title bar"**	According to Organizational Policy
Number of previous logons to cache (in case domain controller is not available) The default Windows 2000 configuration caches the last 10 logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons such as the user's machine being disconnected from the network or domain controllers not being available. By setting this value to 0, users will NOT be able to log on to the domain unless connected to the network. **HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Winlogon\CachedLogonsCount = 0**	0 logons
Prevent system maintenance of computer account password By default, computer account passwords are changed every seven days. Enabling this option prevents machines from requesting a weekly password change. **HKLM\System\CurrentControlSet\Services\Netlogon** **Parameters\DisablePasswordChange = 0**	Disabled

Security Option	Domain Controller Security Policy Setting
Prevent users from installing printer drivers Prevents members of the users group from adding printer drivers on the local machine. Users can still connect to Network Print shares on which they have permissions. After enabling this option, users will not be able to add printers that have not been previously installed. **HKLM\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrintDrivers = 1**	Enabled
Prompt user to change password before expiration Sets how far in advance users are warned that their passwords will expire. **HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\PasswordExpiryWarning = 14**	14 days
Recovery Console: Allow automatic administrative logon If this option is enabled, the Recovery Console will not prompt for an administrator password and will automatically log on to the system. **HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Setup\RecoveryConsole\SecurityLevel = 0**	Disabled
Recovery Console: Allow floppy copy and access to all drives and folders Enables the Recovery Console SET command, which allows setting of console environment variables such as AllowWildCards, AllowAllPaths, AllowRemovableMedia, and NoCopyPrompt. **HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Setup\RecoveryConsole\SetCommand = 0**	Disabled

Security Option	Domain Controller Security Policy Setting
Rename Administrator account name The **Administrator** account is created by default when installing Windows 2000. Associating the Administrator SID with a different name may thwart a potential hacker who is targeting the built-in Administrator account.	According to Organizational Policy. It is recommended to rename the Administrator account.
Rename Guest Account The **Guest** account is created by default when installing Windows 2000, but is disabled. Associating the Guest SID with a different name may thwart a potential hacker who is targeting the built-in Guest account.	According to Organizational Policy. It is recommended to rename the Guest account.
Restrict CDROM access to locally logged on user only By default, Windows 2000 allows any program to access files on CD-ROM drives. In a highly secure, multi-user environment, it only allows interactive users to access these devices. When operating in this mode, the CD-ROM(s) are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off. There exists a known bug when installing Office 2000 from a CD and having this option enabled. For more information, refer to http://support.microsoft.com/support/kb/articles/Q230/8/95.asp. **HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Winlogon\ AllocateCDRoms = 1**	Enabled

Security Option	Domain Controller Security Policy Setting
Restrict Floppy access to locally logged on user only By default, Windows 2000 allows any program to access files on floppy drives. In a highly secure, multi-user environment, it only allows interactive users to access these devices. When operating in this mode, the floppy disks are allocated to a user as part of the interactive logon process. These devices are automatically deallocated when the user logs off. **HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Winlogon\ AllocateFloppies = 1**	Enabled
Secure Channel: Digitally encrypt or sign secure channel data (always) Forces a computer to always digitally encrypt or sign secure channel data. A secure channel is created between a system and its domain controller when the system boots. By default, communications sent via the secure channel are authenticated and sensitive information, such as passwords, is encrypted, but the channel is not integrity checked and not all information is encrypted. This option will encrypt or sign all data passing through the secure channel. All domain controllers in all trusted domains must support digital encryption and signing if this option is enabled. **HKLM\System\CurrentControlSet\Services\Netlogon \ Parameters\RequireSignorSeal = 0**	Disabled
Secure Channel: Digitally encrypt secure channel data (when possible) Enables a computer to digitally encrypt secure channel data. See the explanation of secure channel communication in the previous option. If this option is enabled, all outgoing secure channel traffic should be encrypted. **HKLM\System\CurrentControlSet\Services\Netlogon \ Parameters\SealSecureChannel = 1**	Enabled
Secure Channel: Digitally sign secure channel data (when possible) Enables a computer to digitally sign secure channel data. See the explanation of secure channel communication in the previous option. If this option is enabled, all outgoing secure channel traffic should be signed. If Digitally encrypt secure channel data (when possible) is enabled, it will override any setting for this option and automatically enable it. **HKLM\System\CurrentControlSet\Services\Netlogon \ Parameters\SignSecureChannel = 1**	Enabled

Security Option	Domain Controller Security Policy Setting
Secure channel: Require strong (Windows 2000 or later) session key Requires strong encryption keys for all outgoing secure channel communications. This option should be enabled only if all domain controllers in all trusted domains also support strong session keys. **HKLM\System\CurrentControlSet\Services\Netlogon\ Parameters\RequireStrongKey = 0**	Disabled
Secure System partition (for RISC platforms only) Restricts access of the RISC system partition (which is FAT) to administrators only when the operating system is running.	Not defined
Send unencrypted password in order to connect to 3rd Party SMB server Some non-Microsoft SMB servers only support unencrypted (plain text) password exchanges during authentication. Check with the vendor of the SMB server product to see if there is a way to support encrypted password authentication, or if there is a newer version of the product that adds this support. Enabling this will allow unencrypted (plain text) passwords to be sent across the network when authenticating to an SMB server that requests this option. This reduces the overall security of an environment and should only be done after careful consideration of the consequences of plain text passwords in your specific environment. **HKLM\System\CurrentControlSet\Services\Rdr\ Parameters\EnablePlainTextPassword = 0**	Disabled
Shutdown system immediately if unable to log security audits If events cannot be written to the security log, the system is halted immediately. If the system halts as a result of a full log, an administrator must log onto the system and clear the log. Before clearing the security log, save the data to disk. Even though a possible Denial of Service condition exists, it is more important on a Domain Controller to have current audit logs than to have the DC available. This is a judgement call on the part of the administrator. **HKLM\System\CurrentControlSet\Control\Lsa\ CrashOnAuditFail = 1**	Enabled

Security Option	Domain Controller Security Policy Setting
Smart card removal behavior Determines the action taken when a smart card for a logged-on user is removed from the smart card reader. Options are: *No action* *Lock Workstation* Users can remove their smart card, leave the area, then return to their same session at a later time. *Force Logoff* Users are automatically logged off when the card is removed.	Lock Workstation
Strengthen default permissions of global system objects (e.g., symbolic links) Strengthens the DACLs on the global list of shared system resources (such as DOS device names, mutexes, and semaphores) so that non-administrative users can read, but not modify shared objects they did not create. **HKLM\Software\CurrentControlSet\Session Manager\ ProtectionMode = 1**	Enabled
Unsigned driver installation behavior Determines the action taken when a device driver that has not been certified for Windows 2000 attempts to load. Options are: *Silently succeed* *Warn but allow installation* *Do not allow installation* **HKLM\Software\Microsoft\Driver Signing\Policy = 1**	Warn but allow installation
Unsigned non-driver installation behavior Determines the action taken when non-device driver software that has not been certified for Windows 2000 attempts to load. Options are: *Silently succeed* *Warn but allow installation* *Do not allow installation* **HKLM\Software\Microsoft\Non-driver Signing\Policy = 1**	Warn but allow installation

Table 6

6.3 Event Log

This menu allows setting local event log parameters, such as size, retention, etc.

6.3.1 Settings for Event Log

Event log settings that can be configured with the security editor include maximum size, guest access, how long logs will be retained, and how the operating system handles logs at the maximum size. Again, these settings are local, and should be set using the **Domain Controller Security Policy** tool.

Table 7 lists recommended Event Log settings for the Application, Security, and System logs.

Event Log Settings	Recommended Settings
Maximum Log Size for Application Log **Maximum Log Size for Security Log** **Maximum Log Size for System Log** If the event logs are too small, logs will fill up often and administrators must save and clear the event logs more frequently than required. Allowable values range from 64 KB to 4194240 KB. This setting will allow the log file to equal the size of the available space on the hard disk or up to 4GB, whichever is smaller. This is to ensure that the system will not halt if the event log exceeds specified log space while there is additional space available on the hard drive.	4194240 KBytes
Restrict Guest access to Application Log **Restrict Guest access to Security Log** **Restrict Guest access to System Log** Default configuration allows guests and null logons the ability to view event logs (system and application logs). While the security log is protected from guest access by default, it is viewable by users who have the Manage Audit Logs user right. This option disallows guests and null logons from viewing any of the event logs.	Enabled
Retain Application Log for Application Log **Retain Security Log for Security Log** **Retain System Log for System Log** These options control how long the event logs will be retained before they are overwritten. Since it is not recommended that any event logs be overwritten when they become full, this option should not be configured.	According To organizational security policy
Retention method for Application Log **Retention method for Security Log** **Retention method for System Log** How the operating system handles event logs that have reached their maximum size. The event logs can be overwritten after a certain number of days, overwritten when they become full, or have to be cleared manually. To ensure that no important data is lost, especially in the event of a security breach of the system, the event logs should not be overwritten.	According To organizational security policy

Event Log Settings	Recommended Settings
Shutdown system when security audit log becomes full If events cannot be written to the security log, the system should be halted immediately. If the system halts as a result of a full log, an administrator must restart the system and clear the log.	Disable

Table 7

6.4 Restricted Groups

The restricted group area of the **Domain Controller Security Policy** and **Domain Security Policy** tools allows you to manage the members of built-in groups that have certain predefined capabilities. Restricted Groups policies contain a list of members of specific groups whose membership is defined centrally as part of the security policy. Enforcement of Restricted Groups automatically sets any computer local group membership to match the membership list settings defined in the policy. Changes to group membership by the local computer administrator are overwritten by the restricted Groups policy defined in Active Directory. A system administrator can add groups that can be considered sensitive or privileged to the Restricted Groups list, along with their membership information. They can do this to the Restricted Group List once they have determined specific user groups. This enforces the membership of these groups by policy and does not allow local variations on each computer.

Also, this area tracks and controls reverse membership of each restricted group in the Members Of column of the tool. This column shows other groups to which the restricted group can belong. You can use this field to control exactly which groups your restricted group members can join. You can also use this feature to limit a group of users to one group and prevent them from joining any others. Applying the configuration ensures that group memberships are set as specified in the configuration file. Groups and users that are not specified are removed from the restricted group. In addition, the Reverse Membership Configuration option ensures that each restricted group is a member of only those groups specified in the Member Of column.

Since the settings in the Restricted Groups option should be environment-specific, no recommendations are given for restricted group settings. However, a site may need to restrict the membership of sensitive groups within the domain.

6.5 System Services

The System Services option allows for configuration of Startup Modes and Access Control Lists for all system services. Configuration options include startup settings (Automatic**,** Manual**,** or Disabled) for services such as network, file, and print services. Security settings can also be established that control which users and/or groups can read and execute, write to, delete, start, pause, or stop a service.

Because of the broad nature of this area, system service configuration is environment-specific. Services not listed in this option can be added. However, a new DLL attachment will need to be created and attached. For more information on creating service attachments, refer to the "Security Configuration Tool Set" white paper available at: http://www.microsoft.com/windows2000/library/howitworks/security/sctoolset.asp.

The following are the only services that are absolutely necessary to be running unless there is an operational reason to have another. This list of services may not apply to all Domain Controllers, but should be seen as a suggested list of services to start with.

- DNS Client
- DNS Server
- Event Log
- File Replication Service
- IPSec Policy Agent
- Kerberos Key Distribution Center
- Logical Disk Manager
- Net logon
- Network Connections Manager
- NTLM Service Provider
- Plug & Play
- Protected Storage
- Remote Procedure Call
- Remote Procedure Call Locater
- Remote Registry Service
- RunAs Service
- Security Accounts Manager
- Server
- Windows Time
- Workstation

6.6 Registry and File System Settings

The Registry and File Setting options on the **Domain Controller Security Policy** tool can be handled with the same action. Instead of setting each registry and file system DACL by hand, it is much easier, and just as effective, to apply a pre-defined security template in this case. The default template called "DC Security" is a template that only has settings defined for the Registry and File System options. The settings contained in this template serve to tighten the access lists on very important system files and imperative registry areas. Instead of giving an exhaustive list of permissions that the template implements, following are

instructions on how to apply the security template “DC Security”. It is important to ensure that you apply the template to the **Domain Controller Security Policy** only, as it only should be applied to the local machine (the Domain Controller).

From the **Domain Controller Security Policy** tool set, right click on the **Security Settings Menu**. See Figure 3.

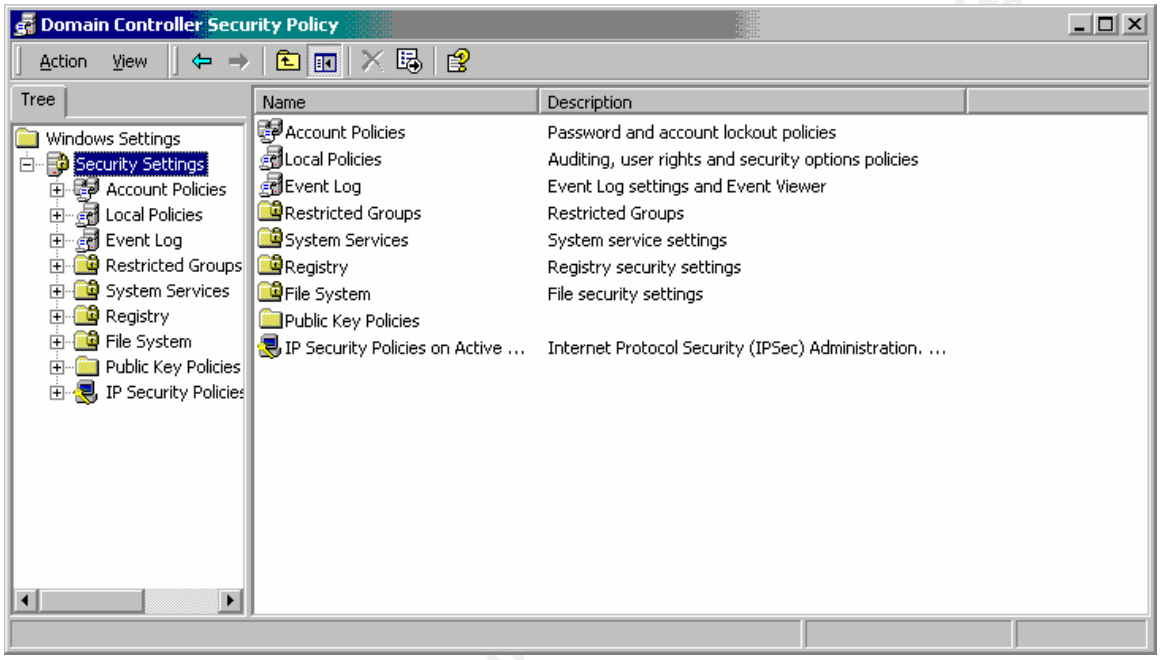
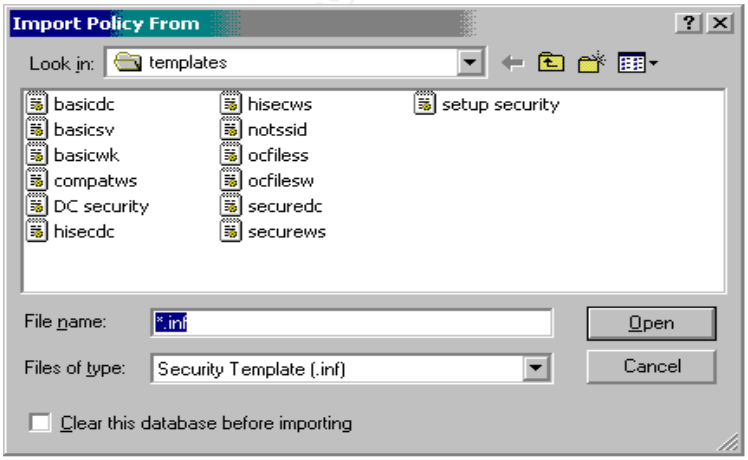


Figure 3

Choose “Import Policy” from the drop-down menu. The following dialog box will open:



Choose “DC Security” and hit Open.

After this is completed, you can open the Registry and the File System options in the **Domain Controller Security Template**, and the following changes should have been applied. See figures 4 and 5.

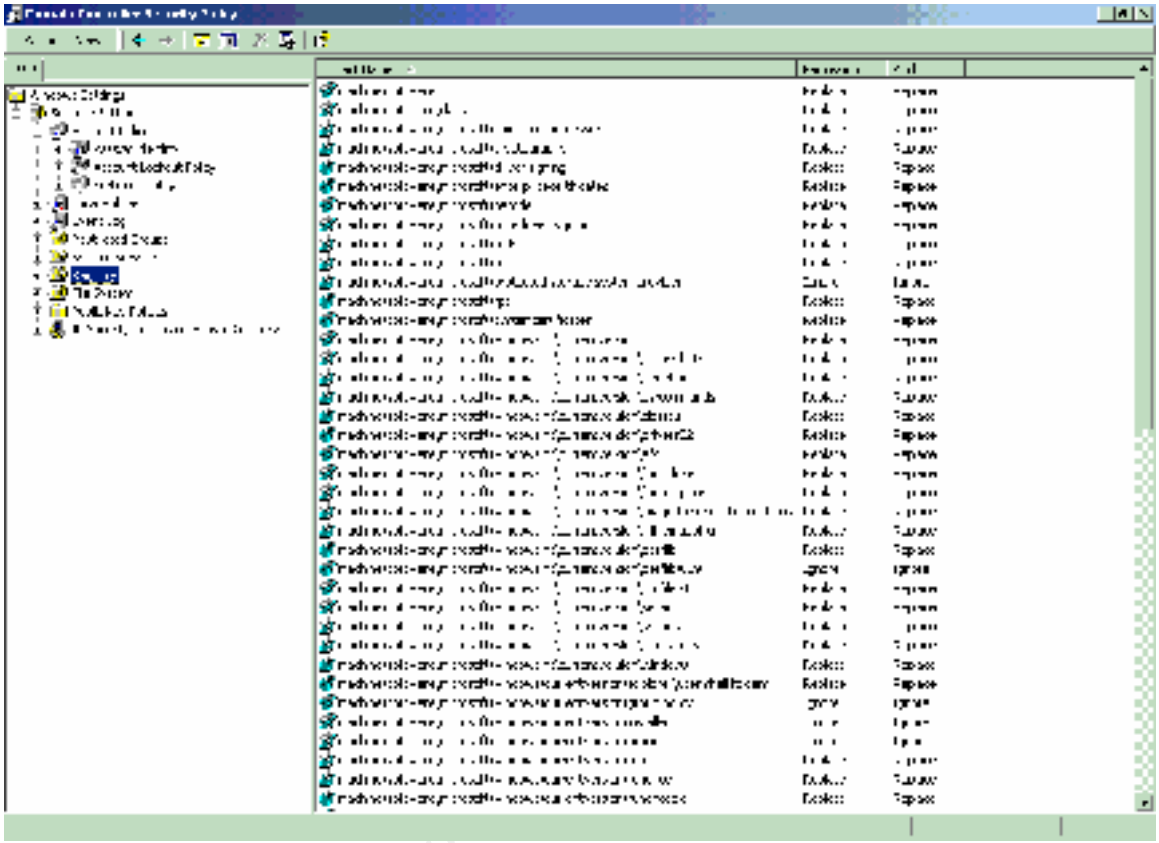


Figure 4

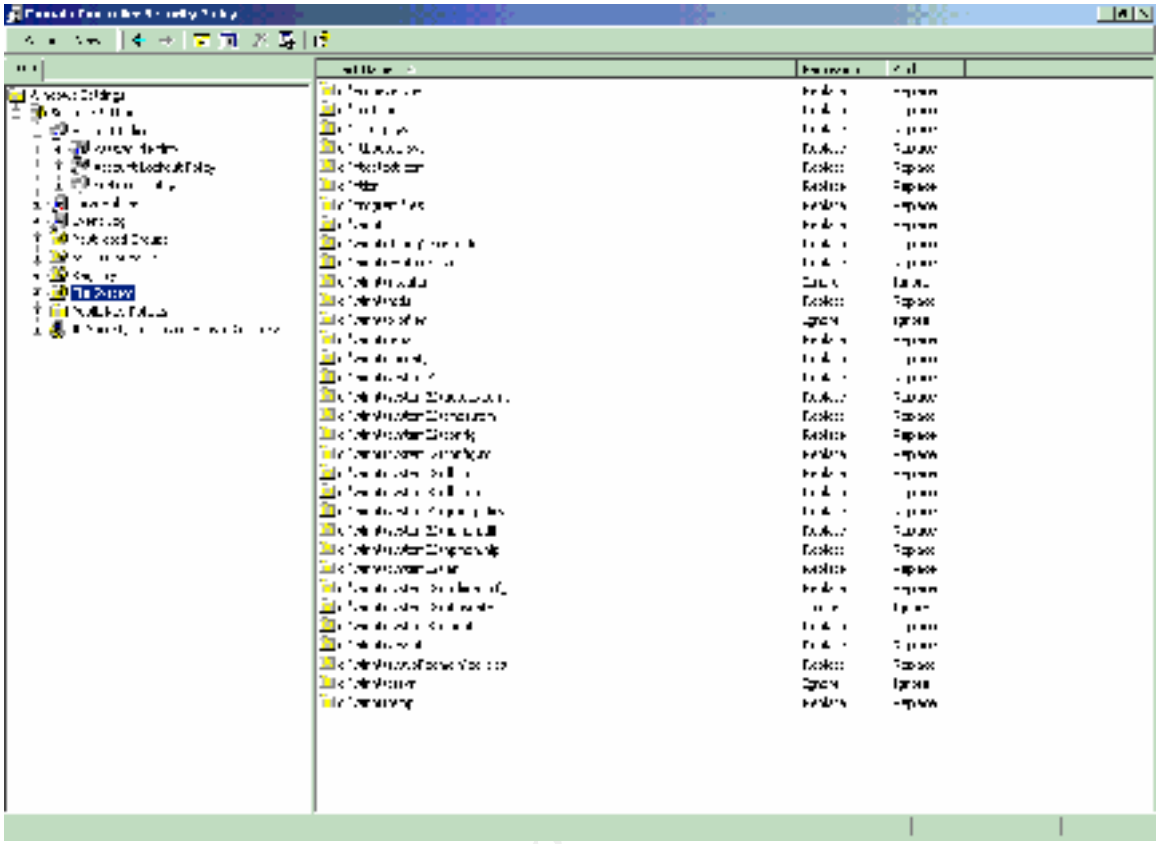


Figure 5

***Note that after all of these changes are made (especially DACL and Registry Changes), the Domain Controller must be restarted **twice** for the settings to take effect. This is contrary to Microsoft documentation and should be a practice that is utilized when making all configuration changes to Windows 2000 Servers. The registry settings do not actually take effect after the first restart because the Security Policy is applied for the first time after the restart. Changes that are made in registry and DACLs that come from the Security Policy then take effect after the **next** restart. Just to be sure, make sure to restart your servers twice before putting them into a production environment.

7.0 Service Packs and Hot fixes

To maintain the most up-to-date security, install service packs and hot fixes as appropriate. The most recent of these can be found at the Microsoft Windows 2000 Service Pack Web site located at http://www.microsoft.com/technet/security/current.asp. To date Microsoft has released one service pack and 24 additional patches not included in the Service Pack. Service Pack 1 (SP1), the High-Encryption Pack and the remaining patches must be installed to secure the server to the highest degree possible. SP1 goes beyond merely fixing security issues. It also covers operating system

reliability, application compatibility, and setup. Most importantly, the service pack includes fully regression-tested versions of the patches for all security vulnerabilities that had been discovered in Windows 2000 up to the closing date of Service Pack development. The security fixes that are addressed by SP1 are described in the Microsoft Security Bulletin links in Appendix 1.

7.1 Patches/Hot Fixes

The following patches listed in Appendix 2 have been identified as significant to resolve security issues in Windows 2000, but to date these patches have not been included in a service pack and will have to be installed individually. The exact direction for installation of each of the patches is contained at the link listed in Appendix 2.

The following is a list of the vulnerabilities for which there are fixes, but which are not included in SP1:

- **Directory Service Restore Mode Password Vulnerability**. This vulnerability could allow a malicious user with physical access to a DC to install malicious software on it.

- **Simple Network Management Protocol (SNMP) Parameters Vulnerability**. The default permissions could allow a malicious user to monitor or reconfigure certain devices on a network.

- **Phone Book Service Buffer Overflow Vulnerability**. This vulnerability could allow a malicious user to execute hostile code on a remote server that is running the service.

- **Domain Account Lockout Vulnerability**. This vulnerability could allow a malicious user to make repeated attempts to guess an account password, even if the domain administrator has set an account lockout policy.

- **ActiveX Parameter Validation Vulnerability**. This vulnerability could allow a malicious user to potentially run code on another user's machine.

- **Netmon Protocol Parsing Vulnerability**. This vulnerability could allow a malicious user to gain control of an affected server.

- **New Variant of Virtual Machine (VM) File Reading Vulnerability**. Like the original vulnerability, this new variant could enable a malicious web site operator to read files from the computer of a person who visited his site, or read web content from inside an intranet if the malicious site was visited by a computer from within that intranet.

- **HyperTerminal Buffer Overflow Vulnerability**. This vulnerability could, under certain circumstances, allow a malicious user to execute arbitrary code on another user's system.

- **Microsoft VM ActiveX Component Vulnerability**. This vulnerability could allow a malicious web site operator to take any desired action on a visitor's machine, once he was able to coax a user into visiting his site.

- **Multiple LPC and LPC Ports Vulnerabilities**. These vulnerabilities could allow a range of effects, from Denial of Service (DoS) attacks to, in some cases, privilege elevation.

- **Windows 2000 Telnet Client NTLM Authentication Vulnerability**. This vulnerability could, under certain circumstances, allow a malicious user to obtain cryptographically protected logon credentials from another user.

- **Malformed RPC Packet Vulnerability**. This vulnerability could allow a malicious user to cause a DoS on a Windows 2000 computer.

- **Still Image Service Privilege Escalation Vulnerability**. This vulnerability could allow a user logged onto a Windows 2000 machine from the keyboard to become an administrator on the machine.

7.2 Post Installation

Make sure that all services and applications are running correctly after the installation. Also recognize that some patches may need to be reinstalled if new applications or services are installed after the patch installation date.

8.0 Networking Security

After installing the Windows 2000 Server, you should minimize the security risk to your domain's network. This section discusses the security implications of different networking components and protocols.

8.1 Networking Components

Networking components are programs or protocols that provide specific services to network clients. In order to have a fully functioning network environment, certain network components and services must be installed. Like many other facets of network design and technology implementation, Windows 2000 Networking Components must be thoroughly planned and appropriately configured to provide an acceptable level of security. Although the exact components that must be installed are environment specific, you should remove all networking components that are not operationally necessary.

8.2 Networking Protocols

Microsoft provides native support for three protocols to perform local or wide area networking (LAN or WAN) services. These protocols are NetBIOS Extended User Interface (NetBEUI), NWLink/IPX, and TCP/IP.

NetBEUI is Microsoft's proprietary network protocol that was designed for usage in small networks. NetBEUI is non-routable, broadcast-based, and is sometimes implemented for legacy protocol support for networking between old NT LAN Manager, LAN Server, and Windows for Workgroups. NetBEUI is also occasionally used to support Windows 9x workgroups.

NWLink/IPX is Microsoft's implementation of Novell's IPX/SPX protocol. It is used to provide support for operation between Microsoft networking components and Novell NetWare Servers and Clients. NWLink/IPX is fully routable and provides for data transfer over both WANs and LANs. This protocol should not be installed on the an organization's Windows 2000 network.

TCP/IP is the standard and primary protocol of both the Internet and Windows 2000. Unlike Windows NT, Windows 2000's central features are built around TCP/IP and are its primary networking protocol. It is fully routable and supports communication between multiple operating systems including UNIX, Windows NT, Windows 9x and Windows 2000. TCP/IP is a directed protocol that eliminates most of the broadcast traffic associated with the NetBEUI and NWLink/IPX protocols.

TCP/IP should be installed on Windows 2000 Servers and only that protocol should be active on a Windows 2000 network. If it is absolutely necessary to have compatibility with legacy systems operating Novell NetWare, it is possible to install NWLink/IPX on those machines that must have the communication capability. After configuring the Windows 2000 Server, it is best to go into Networking Properties and uninstall (or disable) all networking protocols except for TCP/IP.

8.3 Firewall Issues

A discussion of firewall setup, implementation and usage is beyond the scope of this document. It is important to note that a well-implemented firewall solution is integral to maintaining a good network security posture and is an important tool to limit certain network-based attacks that originate from outside of the network segment that is protected by the firewall. For some background information on applying IP egress and ingress filtering rules see RFC 2267 (ftp://ftp.isi.edu/in-notes/rfc2267.txt).

8.4 Remote Access Service

RAS provides a means for a remote Windows NT or Windows 2000 system to connect to a LAN via a dial-up connection. RAS allows a Windows 2000 network to be extended beyond the physical boundaries of the actual office or site. All

traffic to and from the remote system passes through the host server, and all application processing takes place on the remote system.

Due to security concerns, RAS connections should not be allowed to the Domain Controller. If you need to expand the network beyond the boundaries of the physical site, it is recommended that you implement an IPSec or L2TP VPN using Windows 2000 native VPN support.

9.0 Windows 2000 DNS

This chapter is meant to inform a system administrator about the available security settings for the Windows 2000 Domain Name System (DNS) Server Service, how to design a secure implementation of the Windows 2000 DNS, and how to properly implement that design. It is typical to set up Windows 2000 DNS on a Domain Controller in many network design environment, although it is not necessarily required. Windows 2000 will work with non-Windows 2000 DNS servers, but the information will not be Active Directory integrated, and some of the built-in security features relating to DNS will not be available. Windows 2000 relies very heavily on DNS to provide it's services and to resolve names, much more so than Windows NT 4.0. Because exact DNS implementations will vary, this section is designed to provide system administrators and network managers the ability to choose appropriate security settings for their environment. This is by no means a complete guide to DNS configuration, but is instead meant as an overview to certain DNS security issues.

9.1 Server Configuration Choices

There are several deployment methods for DNS in a Windows 2000 environment. These methods are defined by the operational requirements of the network where DNS is to be implemented. It is recommended that the following three configurations are the only ones implemented (depending upon operational requirements) in organization's networks.

9.1.1 DNS in an Enclosed Environment

This type of DNS scheme only requires securing the DNS servers and operating systems, because there is not an active connection to the Internet, and the DNS will only service request relating to the internal network. It is recommended that the External Router and Firewall block all DNS traffic (UDP and TCP port 53). Since this guide assumes that the servers will be configured for a Windows 2000 domain, it is recommended to make the DNS zones Active Directory Integrated and only allow zone transfers to servers listed in the **Name Servers** tab as discussed below.

9.1.2 DNS with an Internet Presence

Most environments require a connection to the Internet. To function correctly, a DNS server is required to provide addresses for clients. It is recommended to separate the External DNS server from the DNS servers that are being utilized for the internal Windows 2000 domain.

Further security recommendations for this configuration include:

- Use Active Directory Integrated DNS servers internally.
- Perform zone transfers on internal DNS servers to servers listed in the **Name Servers** tab as discussed below.
- Secure the zone transfer on the external servers to a specific list of servers, or no servers, as described in the section below, Controlling Zone Transfers. If several servers are used within one DNS domain then controlling the zone transfers by using the **Name Servers** tab, as discussed below, is recommended.
- Disable all unnecessary services on the external DNS server.

9.1.3 DNS with an Internet Presence with Reverse Lookup Requirements

In many secured corporate and government networked systems, it is necessary to verify that someone is coming from another trusted system. This verification is commonly accomplished using reverse lookup zones. These zones take an IP address and convert it to a name which can then be checked for the appropriate trusted domain suffix. There are two ways to provide this functionality:

1) Add a reverse lookup zone to the external DNS server that contains a list of all the internal network IP addresses. Match each IP address with a fictitious client name with the appropriate extension. This setup will allow the IP address to be verified. It is recommended to use this option because it will limit an attackers ability to correctly map the Protected Network.

2) Add a reverse lookup zone to the external DNS server as a secondary zone to the internal network. Add the external server to the list of valid DNS servers to allow zone transfers to on one internal DNS server. Properly configure the router and firewall settings to allow communication between one External DNS server and one, modified, Internal DNS server. Furthermore, it is recommended to not run any other services on the internal DNS server.

As noted at the end of each option, the solutions are labeled with a degree of projected vulnerability. No matter how it occurs, there will always be a higher risk that an attacker has access to your DNS records if DNS zones are transferred over the Internet.

9.2 Zone Security

It is recommended to secure the location of the zone information a DNS server uses. This information is stored in the Windows 2000 Active Directory (if DNS is installed on a Windows 2000 domain controller) or in files stored on the hard drive.

9.2.1 Converting to an Active Directory Integrated Server

It is recommended to convert a DNS zone to an Active Directory Integrated Zone. This action requires the DNS server to be on a Windows 2000 Domain Controller. If the DNS server is not located on a domain controller this option will be grayed out as shown in **Figure 6.**

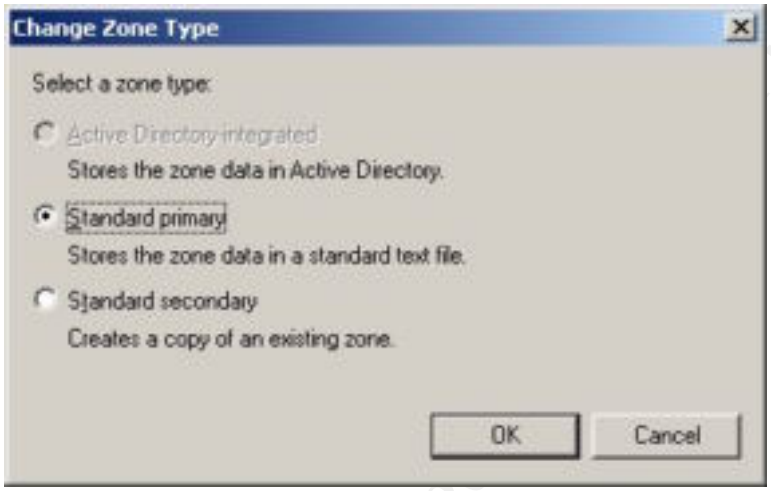


Figure 6

If the DNS server is on a Windows 2000 Domain Controller, the zone types include the Active Directory integrated zone. These options are shown in **Figure 7.** This zone type offers many advantages to the DNS server and is recommended. Some of these options include the zone information being stored, replicated, and secured in the Active Directory.

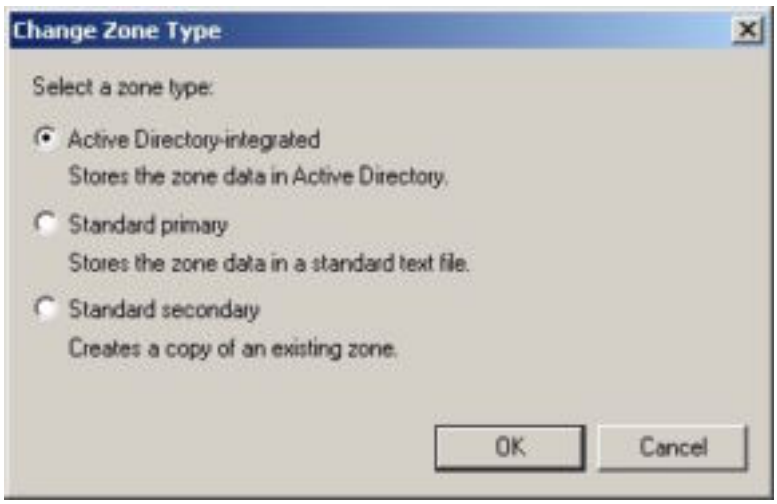


Figure 7

9.3 Controlling Zone Transfers

The ability to control zone transfers is extremely important when securing DNS servers. In Windows 2000 modifying the access lists available for each individual zone controls zone transfers. Since zone transfers move all the records for a particular zone from one server to another it is extremely important to not transfer the forward lookup zone on a DNS server that contains Windows 2000 domain information to any server outside the Windows 2000 domain. **Figure 8** shows the four available options for zone transfers. This figure is a screenshot from the forward lookup zone properties of the test.gov DNS zone.

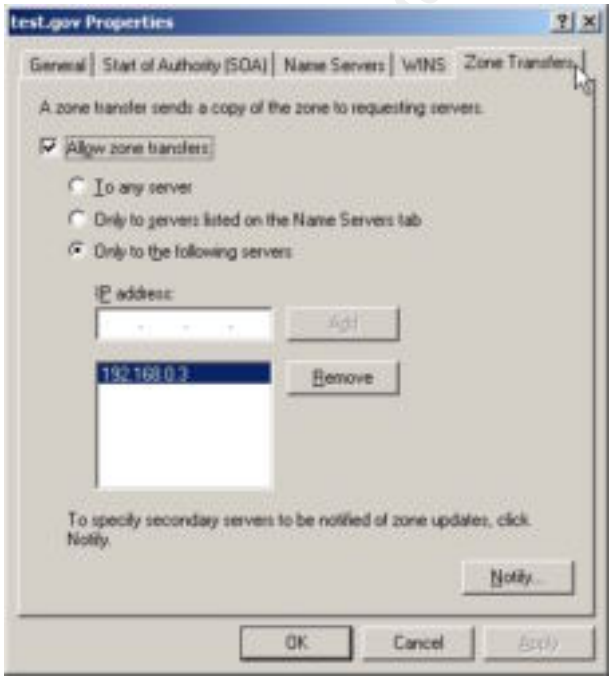


Figure 8

The four options for zone transfers are:

1. Do not allow zone transfers:
   This option stops a complete zone transfer from occurring. However, this server will still be capable of receiving zone transfers from other DNS servers. Clients will be able to receive DNS query responses from this server. This option is recommended for any DNS server that does not specifically need to allow zone transfers.
2. Allow zone transfers to any server:
   This option will allow any server or proper command sequence to transfer the DNS zone from the computer. Although this is the default configuration, it is not recommended to use this option on any DNS server.
3. Allow zone transfers to all servers listed in the **Name Servers** property tab:
   This option uses the **Name Servers** list as represented in **Figure 9.** Since this list contains all domain servers within the DNS domain, this configuration is recommended when zone transfers will only be done within one domain. For example, when the DNS zone is hosting a Windows 2000 Domain this option would allow the DNS servers within the domain to share their zone information.

Figure 9

4. Allow zone transfers to a specific list of IP addresses:
   This option controls zone transfers through a list of IP addresses as shown in **Figure 9.** This option allows information to be shared with specific servers outside the DNS domain. This configuration is recommended when communicating between protected DNS servers and

a DNS server that can be accessed from the Internet. It is recommended to never transfer the forward lookup zone containing active directory records to any server that can be accessed via the Internet.

9.4 Securing Dynamic DNS

Because of the importance of DNS and its data to a Windows 2000 network, the ability to perform dynamic updates presents a security issue. If unauthorized systems are permitted to modify DNS records, the efficacy of the name service could be compromised. For this reason, the Windows 2000 DNS server also supports the use of secured dynamic updates. Secured dynamic updates work just like standard dynamic updates, except that only authorized users are permitted to submit changes to the DNS records.

To perform secure dynamic updates, DNS clients and servers establish a security context by exchanging tokens that negotiate the use of a particular protocol and exchange key. Once the security context has been established, the messages exchanged between the two systems contain a transaction signature that verifies their authenticity. The tokens and transaction signatures are packaged as two special resource records called TKEY and TSIG, respectively.

Only DNS zones that are integrated into Active Directory support secured dynamic updates. Standard primary zones support dynamic updates, but not secured updates. This is because the ACLs of the *dnsZone* and *dnsNode* objects specify which users and groups are permitted to modify the resource records contained in those objects. You can modify the permissions for these objects by using either the DNS or Active Directory Users and Groups console, just as you would modify the permissions for any other type of object.

9.4.1 Changing DNS Server Security Defaults

By default, all Active Directory-integrated zones are configured to accept only secured dynamic updates. If you create a standard primary zone and then decide to convert it to an Active Directory-integrated zone, you must manually configure the zone to accept secured dynamic updates. To do this, open the Properties dialog box for the zone you want to configure in the DNS console by right-clicking it and selecting the Properties item from the menu. Using the Allow Dynamic Updates field on the General page, you can enable or disable the dynamic update feature for the zone, or configure it to accept only secured dynamic updates.

In this same dialog box, you can also click the Security tab to display the standard Windows 2000 permissions controls, which enable you to specify which users and groups should be able to modify the properties of the *dnsZone* object. By default, the Authenticated Users group is granted the Create All Child Objects permission, enabling its members to use dynamic updates to create *dnsZone* objects in the zone. The user who creates the new object also becomes the

objects owner, and is granted full control over the object. You can also modify the permissions for a specific resource record by clicking Security on the record's Properties dialog box.

APPENDIX 1 – PATCHES ADDRESSED IN SERVICE PACK 1

The following patches are included in Windows 2000 Service Pack 1 and do not need to be separately applied if Service Pack 1 has been installed. Cosmetology

- MS00-006 – Patch Available for "Malformed Hit-Highlighting Argument" Vulnerability
- MS00-011 – Patch Available for "VM File Reading" Vulnerability
- MS00-019 – Patch Available for "Virtualized UNC Share" Vulnerability
- MS00-020 – Patch Available for "Desktop Separation" Vulnerability
- MS00-021 – Patch Available for "Malformed TCP/IP Print Request" Vulnerability
- MS00-023 – Patch Available for "Myriad Escaped Characters" Vulnerability
- MS00-026 – Patch Available for "Mixed Object Access" Vulnerability
- MS00-027 – Patch Available for "Malformed Environment Variable" Vulnerability
- MS00-029 – Patch Available for "IP Fragment Reassembly" Vulnerability
- MS00-030 – Patch Available for "Malformed Extension Data in URL" Vulnerability
- MS00-031 – Patch Available for "Undelimited .HTR Request" and "File Fragment Reading via .HTR" Vulnerabilities
- MS00-032 – Patch Available for "Protected Store Key Length" Vulnerability
- MS00-037 – Patch Available for "HTML Help File Code Execution" Vulnerability
- MS00-039 – Patch Available for "SSL Certificate Validation" Vulnerability
- MS00-043 – Patch Available for "Malformed E-mail Header" Vulnerability
- MS00-045 – Patch Available for "Persistent Mail-Browser Link" Vulnerability
- MS00-046 – Patch Available for "Cache Bypass" Vulnerability

- MS00-062 – Patch Available for "Local Security Policy Corruption" Vulnerability

APPENDIX 2 – PATCHES THAT NEED TO BE INSTALLED

The following bulletins describe patches have not been included in any service pack but need to be installed to secure Windows 2000 Professional. There may be additional patches if you choose to run additional services or components on your Windows 2000 Professional Client. Check http://www.microsoft.com/technet/security/current.asp for the most recent security bulletins.

- MS01-013: Windows 2000 Event Viewer Contains Unchecked Buffer
- MS01-011: Malformed Request to Domain Controller can Cause CPU Exhaustion
- MS01-007: Network DDE Agent Requests can Enable Code to run in System Context
- MS01-005: Packaging Anomaly Could Cause Hotfixes to be Removed
- MS01-001: Web Client Will Perform NTLM Authentication Regardless of Security Settings
- MS00-099: Patch Available for "Directory Service Restore Mode Password" Vulnerability
- MS00-098: Patch Available for "Indexing Service File Enumeration" Vulnerability
- MS00-096: Tool Available for "SNMP Parameters" Vulnerability
- MS00-094: Patch Available for "Phone Book Service Buffer Overflow" Vulnerability
- MS00-089: Patch Available for "Domain Account Lockout" Vulnerability
- MS00-085: Patch Available for "ActiveX Parameter Validation" Vulnerability
- MS00-083: Patch Available for "Netmon Protocol Parsing" Vulnerability
- MS00-081 - Patch Available for New Variant of "VM File Reading" Vulnerability
- MS00-079: Patch Available for "HyperTerminal Buffer Overflow" Vulnerability
- MS00-075: Patch Available for "Microsoft VM ActiveX Component" Vulnerability
- MS00-070: Patch Available for "Multiple LPC and LPC Ports" Vulnerabilities
- MS00-066: Patch Available for "Malformed RPC Packet" Vulnerability
- MS00-065: Patch Available for "Still Image Service Privilege Escalation" Vulnerability
- MS00-053: Patch Available for "Service Control Manager Named Pipe Impersonation" Vulnerability
- MS00-052: Patch Available for "Relative Shell Path" Vulnerability
- MS00-047: Patch Available for "NetBIOS Name Server Protocol Spoofing" Vulnerability
- MS00-036: Patch Available for "ResetBrowser Frame" and "HostAnnouncement Flooding" Vulnerabilities

APPENDIX 3 – REFERENCES

Ackerman, Pilar, et. al., *Microsoft Windows 2000 Professional Resource Kit*, Redmond, WA

Haney, Julie M., *Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set*, National Security Agency, August 2000

McLean, Ian, *Windows 2000 Security Little Black Book*, Scottsdale, Arizona: Coriolis Group, 2000

Microsoft Corporation, *Configuring Windows 2000 Active Directory for Exchange 2000 Server*, White Paper. Microsoft Corporation, Redmond, WA, 2001

Microsoft Corporation, *Default Access Control Settings in Windows 2000*, White Paper. Microsoft Corporation, Redmond, WA, 2000

Microsoft Corporation, *Deploying the Active Directory Connector,* White Paper. Microsoft Corporation, Redmond, WA, 2001.

Microsoft Corporation, *Microsoft Windows 2000 Server: An Introduction to the Windows 2000 Public-Key Infrastructure,* White Paper. Microsoft Corporation, Redmond, WA, 1999

Microsoft Corporation, *Microsoft Windows 2000 Server: Microsoft Windows 2000 Public Key Infrastructure*, White Paper. Microsoft Corporation, Redmond, WA, 1999

Microsoft Corporation, *Microsoft Windows 2000 Server: Secure Networking Using Windows 2000 Distributed Security Services,* White Paper. Microsoft Corporation, Redmond, WA, 1999

Microsoft Corporation, *Microsoft Windows 2000 Server: Security Configuration Tool Set, White Paper*. Microsoft Corporation, Redmond, WA, 1999

Microsoft Technet, http://www.microsoft.com/technet.

Microsoft's Web Page

Russel, Charlie and Sharon Crawford, *Microsoft Windows 2000 Server Administrator's Companion*, Redmond, Washington: Microsoft Press, 2000.