

Five Key Lessons to Securing Your Active Directory

Roberta Bragg
MCSE, CISSP, Author, Columnist,
Speaker, Consultant

Chapters

1. Perform a Self-Audit
2. Know and Use Security Tools and Techniques
3. Monitor Active Directory Operations
4. Leverage People and Processes
5. Active Directory Security Maintenance

Sponsored by:



© Copyright Quest Software, Inc. 2004. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

Warranty

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

Trademarks

All trademarks and registered trademarks used in this guide are property of their respective owners.

Last revised December 22, 2004

World Headquarters
8001 Irvine Center Drive
Irvine, CA 92618
www.quest.com

email: info@quest.com

US and
Canada: 949.754.8000

CONTENTS

CHAPTER 5: ACTIVE DIRECTORY SECURITY MAINTENANCE	5
SECURITY CONTINUITY	6
PATCHES AND UPDATES	7
OBTAINING AND ROLLING OUT THE CHANGE.....	7
<i>Know What's Out There</i>	8
CHANGE TESTING.....	9
CHANGE AUDITING.....	10
MANAGE AND MONITOR ACCESS	12
CONFIGURE AUDIT POLICIES.....	12
CONFIGURE OBJECT AUDITING.....	14
CONFIGURE EVENT LOG SETTINGS.....	16
EVENT LOG MONITORING	18
MANAGE ANTI-VIRUS CONTROL FOR DCS	20
AUDIT KEY SECURITY CONTROLS	22
AUDIT SECURITY SETTINGS WITH SECEDIT.....	22
AUDIT GROUP POLICY APPLICATION USING RSOP.....	24
MONITOR AD FUNCTION	27
DISASTER RECOVERY	28
FOREST-WIDE RECOVERY PREPARATION.....	28
<i>Backup Process</i>	28
<i>Backup Schedule</i>	29
<i>Backing Up DCs</i>	30
<i>Forest Recovery Steps</i>	30
<i>Storage Backup</i>	32
<i>AD Restoration</i>	33
REVIEW POLICY AND PROCESS	35
ABOUT QUEST WINDOWS MANAGEMENT	36
ABOUT QUEST SOFTWARE	36

CHAPTER 5: ACTIVE DIRECTORY SECURITY MAINTENANCE

It should come as no surprise that securing Active Directory (AD) is not a one-and-done process. Keeping Active Directory secure requires:

- Providing security continuity
- Applying patches and updates
- Establishing an auditing policy
- Monitoring event logs
- Managing anti-virus controls
- Auditing key security controls
- Monitoring AD function
- Implementing a disaster recovery plan
- Reviewing policy and processes

SECURITY CONTINUITY

The security of Active Directory is dependent on both the establishment of secure policies, procedures, standards, and processes and the continuation of these processes. It is not enough to determine what is necessary to do and to do it. You must continue to follow these practices while considering new security information. This is the reason for many of the monitoring and auditing steps detailed in other sections of this e-book, but it is also the result of the enforcement of established policies.

Within this requirement is the need to ensure the security of Active Directory by enforcing all information security practices. A network is only as secure as its weakest component, and lack of security on desktops and at remote locations can impact the security of domain controllers (DCs) and Active Directory.

In Chapter 1, a complete audit review of AD security was detailed. Many of the functions necessary for its completion have been expanded upon in successive chapters, including this one. The audit checklist from Chapter 1 should be periodically reviewed. At this time, a quick review of the categories in Chapter 1 will provide a list of items that should remain in place.

PATCHES AND UPDATES

The saying, “If it isn’t broken, don’t fix it” was once the cornerstone of network and server administration. Even if the operating system (OS) vendor provided updates and patches, the wisdom of experienced administrators cautioned against applying them, unless the patch fixed something already causing problems. The corollary of this rule was to inspect the update or patch documentation to ensure it had nothing to offer in the way of a performance boost or other benefit. However, this inspection was often not done, as it was easier to let a functioning network continue to function. Updates were also not applied because this often meant taking a server offline, something never welcome in busy enterprises.

This policy of ignoring updates and patches is no longer a best practice. Today, IT must pay attention to vendor-supplied changes as they often signal critical security updates. Without these updates, even a hardened server or network is more likely to be compromised. A policy for managing all changes to the network should be a part of the overall security plan. In addition, procedures should be developed to handle emergency patches or security configuration changes. Many changes are not AD-specific but may be server OS-specific and need to be applied to DCs as well as member servers. There are four parts to the process:

- Knowledge of a necessary change
- Obtaining the change
- Testing the change
- Applying the change

Obtaining and Rolling Out the Change

Two parts of the update process can and should be automated: obtaining the change and applying the change. Microsoft’s Software Update Services (SUS) and System Management Server (SMS) can be configured to automatically download patches and service packs as they are released. Once tested and approved, changes can be automatically rolled out. SUS does not currently provide an opportunity to add changes other than those provided by Microsoft, while SMS does. SUS, however, is a free product. Visit the SUS site, www.microsoft.com/windows/serversystem/sus/default.mspx for information and to download SUS.

SUS has been available for a few years now. The next version of the product, Windows Update Server (WUS), adds new features, including:

- Patch deployment support for Microsoft Office, SQL Server, Exchange, and critical hardware drivers
- An expansion of update classification to include connectors, guidance (scripts, code samples, and technical guidance) and tools (utilities and new features)
- The ability to use SQL Server to hold update information
- Improved reporting on update status and compliance across multiple computers
- Maximized bandwidth efficiency, if Background Intelligent Transfer Services (BITS) Version 2.0 is also installed
- Targeted updating (update only selected computers)
- Filtering options (filter updates by product and update classification)

In addition, third-party products also can manage the update process. They may also be able to manage changes for other OSs and applications.

Changes not available as automatic downloads, such as application or configuration changes, also may be required. A separate process for their rollout, via methods such as Group Policy and scripting, should be developed, tested, and implemented.

Know What's Out There

Even in an enterprise with sound procedures in place, it is not always possible to immediately start the testing and implementation process, so it is critical to know of changes as soon as possible. Several sources should be used to determine if a change is available and what it fixes.

- The current Microsoft policy is to release patches and hot fixes one day per month, generally the second Tuesday. Microsoft sometimes deems it necessary, however, to release critical updates at other times.
- Subscribe to the Security Notification Service, which provides e-mail notification of security update announcements. This is important since Microsoft occasionally announces interim security updates at times other than its monthly release day. To sign up, go to www.microsoft.com/technet/security/bulletin/notify.msp.

- In November 2004, Microsoft announced a new policy of releasing information on planned monthly security bulletins at least three days before the normal release date. The notifications can be viewed on the TechNet site at www.microsoft.com/technet/security/bulletin/advance.mspx, along with the projected date for the next announcement. It should now be possible to sign up to receive e-mail notification of these announcements.
- Security bulletins provide information on patches and reference additional documentation. Review all information to help determine which, if any, Windows systems need updating, and how important the patch is.
- A monthly webcast, typically the day after the patch release, briefly outlines the nature of the patches and provides an opportunity to ask questions. Check the TechNet notification pages for more information on upcoming webcasts.
- It is a good idea to implement a backup notification system. While patch releases now follow a regular monthly schedule, severe issues may require an interim release. If you are on the notification list, you should learn of these patches, but it is still better to receive two notifications than none. Several newsgroups and letters also forward this notification. NTBugtraq (subscribe at www.ntbugtraq.com/) is one of the more well known.

Change Testing

Any proposed change should be tested before being implemented in a production environment, especially patches and service packs. Changes should be tested on representative computers; for every configuration present in the production network, a computer or virtual machine in the test network should be similarly configured, including hardware and software.

In addition to testing changes, monitor newsgroups and lists dedicated to Windows products. Problems with patches will often be reported to them, and the information can be very valuable. If a change is causing problems, wait for a workaround or re-release of the patch. You may also discover that a reported problem affects a narrow subset of users or servers and determine that you are safe.

Change Auditing

Change auditing determines whether or not changes have been applied. A number of factors can keep changes from being applied, including misconfigurations or faulty processes.

The Microsoft Baseline Security Analyzer (MBSA) is a free tool that can report major security vulnerabilities and determine a system's patch status. MBSA can scan local machines or multiple machines and provide HTML-based reports. A command-line version records missing patch information in a text file. Import the text file into a database and use queries to report patching status on multiple machines. Figure 1 displays an MBSA HTML patch status report. Note that information on a new version is provided and a summary form provides links. When the **Result details** link is clicked, the listing of missing patches is provided, as shown in figure 2.

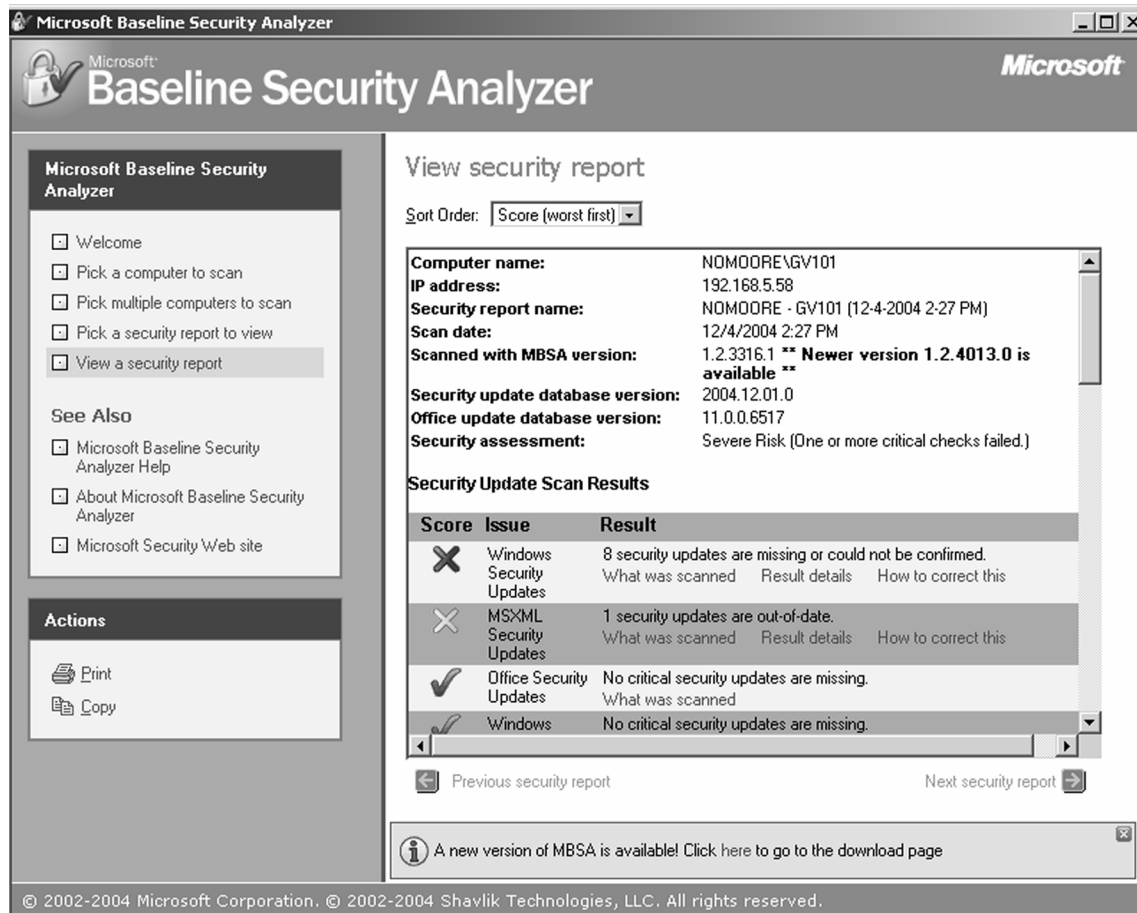


Figure 1. An MBSA scan summarizes several security issues on a computer, including missing patches.

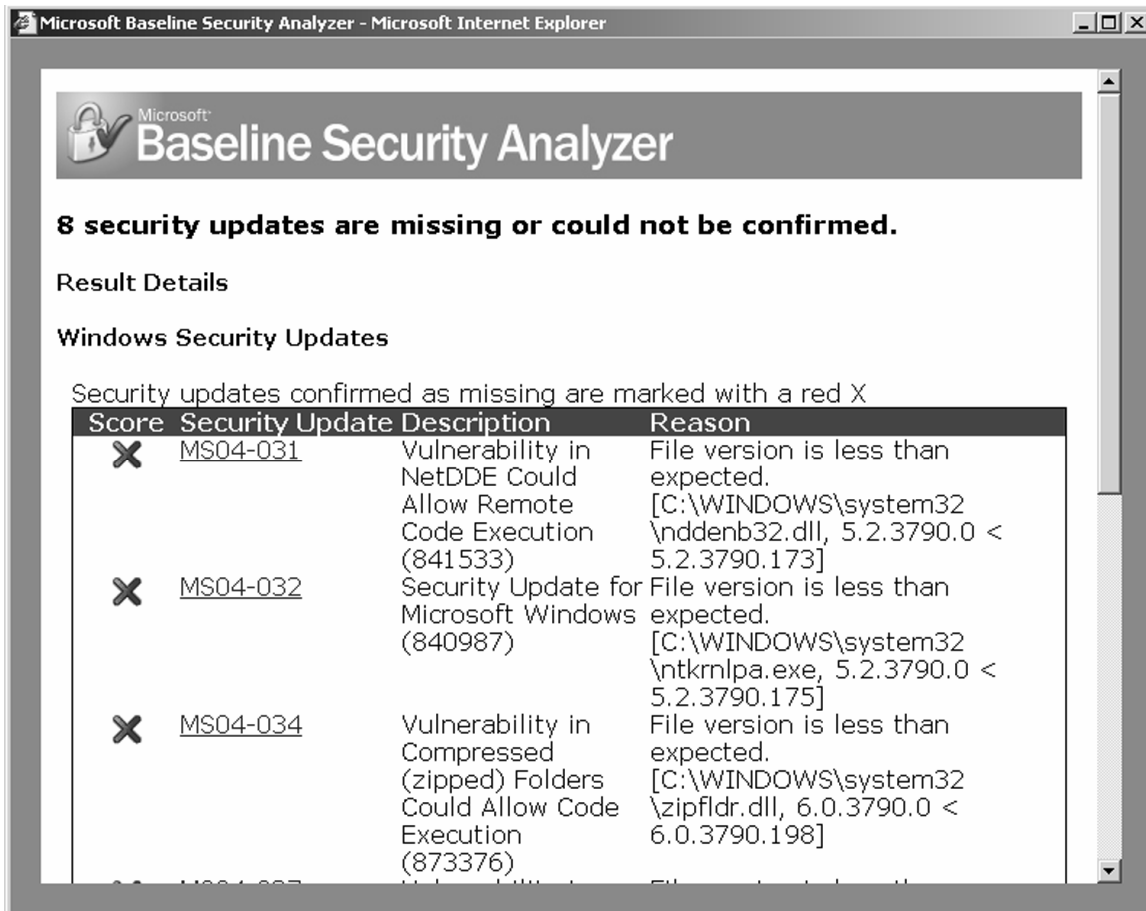


Figure 2. The details section explains the patches and provides a link where they can be downloaded.

MBSA information and a download link are available at www.microsoft.com/technet/security/tools/mbsahome.mspx. My article at <http://mcpmag.com/columns/article.asp?EditorialsID=531> provides information on using the results to produce a centralized report.

MANAGE AND MONITOR ACCESS

Ensuring that only authorized users can access and modify domain resources can go a long way in securing Active Directory. But strengthening the password policy and assigning user rights and resource access based on least privilege is only half the battle. You must also monitor that access. The first step is to configure the audit and event log policies and set appropriate object System Access Control Lists (SACLs). (Using the log entries is detailed in the section titled “Event Log Monitoring.”)

Configure Audit Policies

When audit policies are enabled, security events are written to a computer’s Security event log. Since some events that can impact AD security (such as logon) include activity on multiple computers, it is important to enable auditing on all computers. In an AD forest, configure audit policies at different levels:

- To require all DCs to record audit events, configure the Default DCs policy
- To apply the same auditing policy to all other servers and workstations, configure auditing in a Group Policy Object (GPO) linked to the domain.
- If auditing policy should be different for different computers, create different policies in GPOs linked to specific organizational units (OUs).

Audit policies are configured in the Windows Settings\Security Settings\Local Policies section of the GPO.

Audit Policy	Purpose	Default Setting	Recommended Setting
Audit account logon events	Records logon events that occur at the DC, including Kerberos events.	Success	Success, Failure
Audit account management	Records changes to accounts such as user, group, and computer creation and deletion; password changes; group membership changes.	Success	Success, Failure

Audit Policy	Purpose	Default Setting	Recommended Setting
Audit directory service access	Enables logging of access to AD objects. To record specific object activity, configure settings on specific objects in Active Directory (some settings are on by default but not recorded until this audit policy is set). To record those events in the Security log, you must turn on object auditing for this policy.	Success	Success, Failure
Audit logon events	Records logon events at the console where logon occurs such as logon and logoff. When IPSec negotiate policies are used, Internet Key Exchange events are recorded. Security Identifier (SID) filtering events are also logged.	Success	Success, Failure
Audit object access	Enables recording of access to files, folders, Registry keys, and printers. Auditing also must be configured on the specific objects.	Success	Success, Failure
Audit policy change	Records changes to user rights and trust relationships, changes to the audit policy, changes to the IPSec agent, and changes to Kerberos policy.	Success	Success, Failure
Audit privilege use	Records privileges added to a user's access token, and the use of privileges. Setting this policy can generate multiple events per use of privilege and clog the event logs with information. This is why I recommend not using this option.	No Auditing	No auditing or Not configured
Audit process tracking	Records process creation and exit, access to objects, backup and recovery of data protection master key, installation of services, and creation of scheduled jobs. This policy should probably not be configured except in development environments or in environments where software evaluation is undertaken.	No Auditing	No auditing or Not configured
Audit system events	Records startup and shutdown events, loading of authentication packages, clearing of the audit log and change to the system time.	Success	Success, Failure

Table 1. Audit Policy Recommendations

Configure Object Auditing

Once auditing is configured, events will be recorded to the event logs. However, the policy settings *Audit object access* and *Audit directory service access* depend on settings made to SACLs on the objects themselves. Setting SACLs on objects will generate object access events and can potentially bloat the Security event log. Some SACLs are already set on directory objects. No SACLs are set by default on files, folders, or printers, so enabling object access for them won't add to the event log.

SACLs on AD objects can be viewed or configured from the Auditing page of the Advanced Security Settings object property page. Figure 3 displays the settings on the DCs OU. The default SACLs on AD objects provide insight into Microsoft's view of important events to monitor.

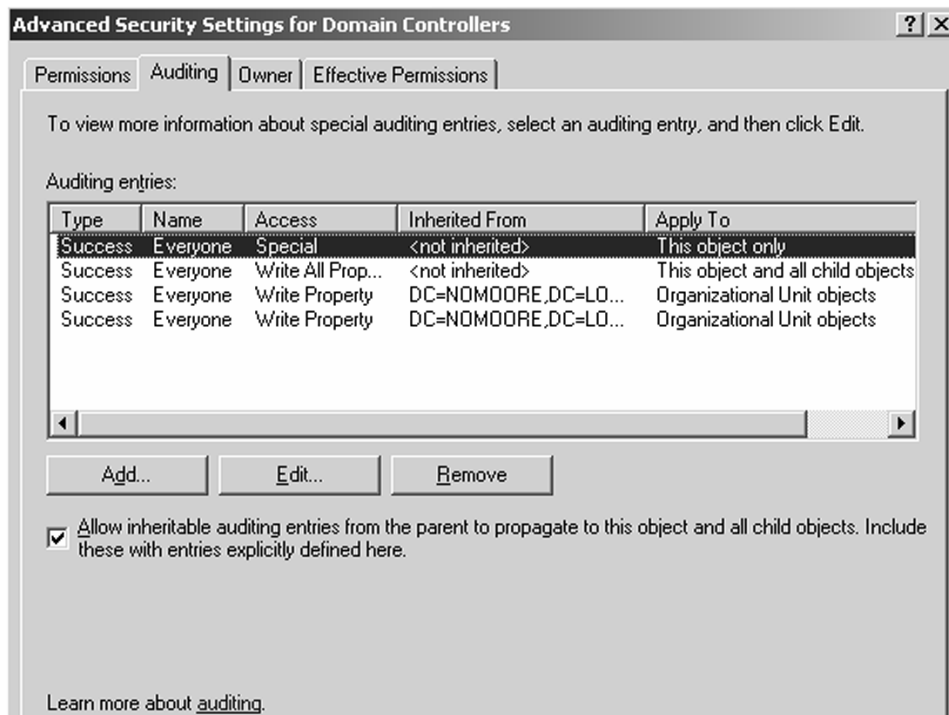


Figure 3. SACLs are preconfigured on some AD objects.

For example, note that the group audited is Everyone and that no special groups are singled out. Instead of making the assumption that only administrators will be given permissions to create a new DC, for example, the SACL uses the Everyone group, so the creation of a DC by any user will be recorded. To view exactly what activities are audited, select one of the settings in Figure 3 and click the **Edit** button to view detail.

Figure 4 displays the permissions audited on the OU. Note that while most possible object permissions are checked, some are not. Items checked include permission modification, child object creation and deletion, GPO creation and change, and so on. Note too, that they are audited for successful behavior. A record of these types of successful changes is important. While a failed attempt might be useful in troubleshooting, and might indicate an attack, including Failed access attempts here might record too many events. You can, of course, add Failed events to the SACL. Just remember that for any of this knowledge to be useful, you must regularly review the collected events.

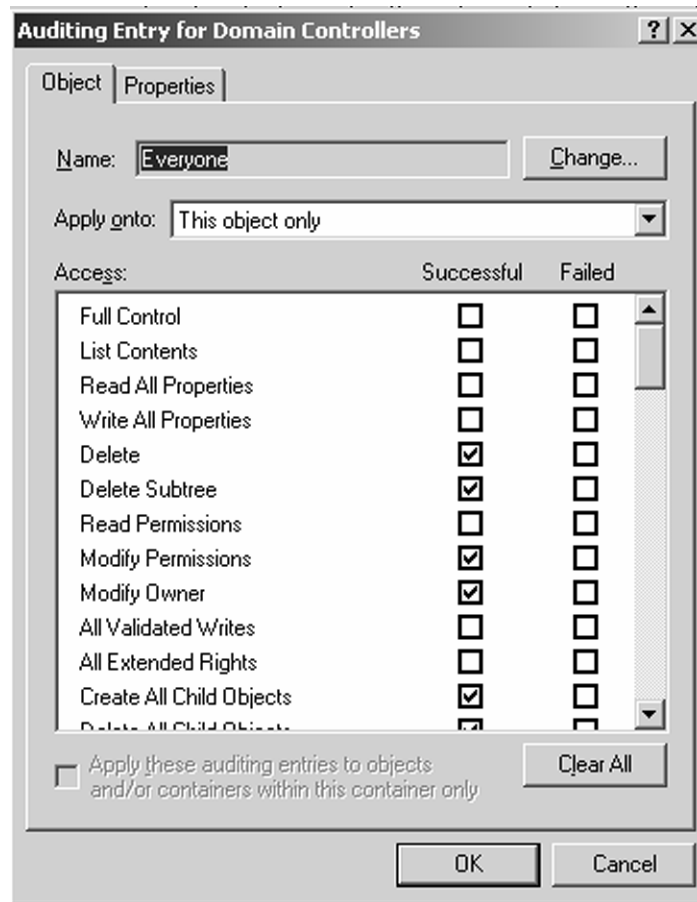


Figure 4. A listing of audited events for an object.

SACL qualifiers such as **This object only** and **This object and all child objects** limit event collection. A large number of properties are audited on the OU, while only the **Write All Properties** property is audited on the objects within the container. Examining a specific DC's properties will confirm this.

Configuring auditing for objects in the AD is a complex task because there are so many objects, and just as each object has its own set of object permissions, there are a large number of actions that can be audited. Start by observing the preconfigured settings and the usefulness of the information they produce. When applying auditing to other AD objects, start with this range of settings. You may then determine that additional settings are necessary or that the defaults are producing more information than you can manage.

In addition to configuring auditing for directory objects, audit access to key directory-related files. To determine what is important to audit, consider object permissions, including changes to permission and ownership of key files. For example, only the System and Administrators groups have access to Ntds.dit, the AD database file; both have Full Control. Permissions on objects within the database control access to the objects themselves. Ordinary users do not need access to the Ntds.dit file. Consider auditing the group Everyone for Change Permissions and Take Ownership.

Configure Event Log Settings

When auditing is configured, security events are logged in the Security event log, but events in other logs also are important to security. All logs should be carefully configured and protected from unwarranted access. Event log settings for the security, application, and system logs are configured in the Windows Settings\Security Settings\Event Log section of a GPO. Event log settings for event logs on a specific computer, including Directory Service, Domain Name System (DNS) server, and File Replication Service logs can be set in the Microsoft Management Console (MMC) Event Viewer local to that computer. Table 2 lists and recommends settings for event logs.

Setting	Description	Recommendation
Maximum log size	Specifies how much disk space can be used for events.	The default properties of event logs for Windows Server 2003 are set to a reasonable size for a newly initialized server. However, you will need to adjust this size to accommodate the activity your systems generate as well as to meet the needs of your audit policy. Log size will need to be monitored and coordinated with log archival periods. Larger logs mean less frequent archival, while smaller logs may have to be archived more frequently.

Setting	Description	Recommendation
Retention method (In individual log properties, listed as “When maximum log size is reached”)	Overwrite events as needed; overwrite events older than n days (also know as “Retain” n days); do not overwrite events (clear log manually).	Set to “overwrite events as needed”. In this case, if the event log is large enough and is archived frequently, no events will be lost. However, in times of heavy event logging or slow administrator response, only the older events will be lost.
Prevent local guests group from accessing application log	The guests group cannot access the log. By default, only Administrators and the operating system itself can access the Windows Server 2003 event logs.	Enable
Prevent local guests group from accessing security log	Same as above.	Enable
Prevent local guests group from accessing system log	Same as above.	Enable

Table 2: Group Policy Event Log Settings

In addition to the log retention policies defined in the Event Log Group Policy section, the Security selection **Audit: Shut down system immediately if unable to log security audits** is an option. When enabled in conjunction with the retention method **Do not overwrite events (clear log manually)**, most activity on the system is halted until the log is cleared and the option is reset. This setting is not recommended unless the system is extremely sensitive and your organization can withstand the down time.

Warning

Do not configure **Shut down system immediately if unable to log security audits** without considering the consequences. If this option is used and the security log fills up, user access to the computer will not be possible. This can bring critical activity to a standstill. Administrators, of course, can logon, archive and clear the log, and reset the system for normal operation.

EVENT LOG MONITORING

Unless your forest is small, you will need to centralize the collection and monitoring of events in order to manage them. While Group Policy can be used to ensure that security events are added to the security log on all required computers, there is no built-in way to centralize collection or review of event log data. There are many third-party products that can be used, and other inexpensive options, including:

- Freeware products such as ntsyslog, <http://ntsyslog.sourceforge.net/>, a free implementation of the popular Unix syslog service adapted for Windows.
- Creating text archives of event logs and importing them into an Access or SQL database.

Once the logs are consolidated, you still must review them. This is where third-party products and Microsoft Operations Manager (MOM) excel. These products have built-in queries that can analyze log data. If you build your own solution, create database queries to ferret out the information. The Microsoft article “Windows Server 2003 Security Events” (www.microsoft.com/technet/security/guidance/secmod128.mspx) details the events created by setting various aspects of the audit policy. This article is a good place to determine the events to monitor. While all events are worth monitoring, some events should be examined more frequently. Table 3 describes many of these events.

Event ID	Description	Use
675	Pre-authentication failed.	Identify when a user enters an incorrect domain account password. Bad password entry for local accounts will never trigger this event.
643	A domain policy was modified.	Be advised of changes to policy.
644	A user account was automatically locked	If account lockout is correctly set, this event may indicate a password cracking attack.
529	Logon failure. Unknown user name or bad password.	Depending on the number and frequency of these events, they may indicate password-cracking attacks.
530	Logon failure. Outside allotted time.	Possible attack on Kerberos credentials, or simply a workstation whose clock is not synchronized with the forest.

Event ID	Description	Use
531	Logon failure. Disabled account.	Possible attack, or a new account was not enabled before being assigned to a new employee.
532	Logon failure. Expired account.	Possible attack, or a temporary employee's account was not renewed when it should have been.
533	Logon failure. Account cannot logon at this computer.	If policy has been communicated correctly (letting users know which computers they can use to log on), this could be an attack or violation of security policy.
534	Logon failure. Password type not allowed.	This may be an attack, misconfigured application, or violation of security policy. "Password type" refers to the user rights concerning logon such as "access this computer from the network," "logon locally," and so on.
535	Logon failure. Expired password.	May indicate simple user error or an attack on a rarely used account.
539	Logon failure. Account lockout.	A large number of these events indicate the continuation of a cracking attack.
564	Object deleted.	Compare this event to authorized maintenance that may have required the deletion of a sensitive file.

Table 3: Suggested Events to Monitor

Until you have centralized logging in place, or when you simply want a quick view of current event logs, the free Microsoft utility Eventcomb can be used to view specific events on multiple computers in the network. The utility does not create a centralized database; instead, it filters existing logs on selected computers for events you identify, and then produces a report.

MANAGE ANTI-VIRUS CONTROL FOR DCS

A forest-wide or organization-wide virus control program should stipulate the operation of antivirus products at gateways and on servers and desktops. Running anti-virus products on DCs is a good idea, but you will have to take precautions to prevent performance issues. Anti-virus operations are typically triggered by file access and change. Since AD operation generates lots of file activity, this can cause a significant performance hit. Microsoft recommends the following precautions when using anti-virus products on DCs (see Knowledge Base article 822158, “Virus scanning recommendations on a Windows 2000 or on a Windows Server 2003 DC”).

- Obtain and use anti-virus products built to run specifically on DCs.
- Exclude files not at risk of infection (listed in Table 4).
- Do not use DCs as file servers or workstations.

File Type	File Names	Location
AD database	Ntds.dit, Ntds.pat	HKLM\SYSTEM\Services\NTDS\Parameters\DSA Default location is %windir%\ntds
AD transaction log files	EDB*.log (notice the wildcard; there can be several), RES1.log, RES2.log, Ntds.pat	HKLM\ SYSTEM \Services\NTDS\Parameters\Database Default location is %windir%\ntds
NTDS working files	TEMP.edb, EDB.chk	Folder specified at HKLM\ SYSTEM \ CurrentControlSet \Services\NTDS\Parameters\DSA WorkingDirectory
FRS working directory	FRS Working Dir\jet\sys\edb.chk FRS, Working Dir\jet\ntfrs.jdb, FRS Working Dir\jet\log*.log	FRS Working Directory specified in HKLM\ SYSTEM \CurrentControlSet\Services\NtFrs\Parameters\Working Directory
FRS database files	FRS Working Dir\jet\log*.log (if Registry key is not set), DB Log File Directory\log*.log (if Registry key is set)	HKEY_LOCAL_MACHINE\ SYSTEM \ CurrentControlSet \Services\NtFrs\Parameters\DB Log File Directory Default location is %windir%\ntds
FRS replica root files	Various files that are being replicated	HKEY_LOCAL_MACHINE\ SYSTEM \CurrentControlSet\Services\NtFrs\Parameters\Replica Sets\GUID\Replica Set Root Default: Windows\SYVOL\domain

File Type	File Names	Location
Staging directory	Various files that are being replicated	HKEY_LOCAL_MACHINE\ SYSTEM \ CurrentControlSet \NtFrs\Parameters\Replica Sets\GUID\Replica Set Stage Default: Windows\SYSDVOL\staging\domain
FRS preinstall directory		:<Replica_root>\DO_NOT_REMOVE_NtFrs_PreInstall_Directory

Table 4: Files to Exclude from Anti-Virus Scans

AUDIT KEY SECURITY CONTROLS

Security settings are not static. Changes often are required to meet a new security policy or as the result of increased understanding of threats and possible countermeasures. Changes also can be made in an effort to troubleshoot some operational difficulty. These types of changes often are forgotten and rarely reset to the standard for your organization's security policy. To ensure the consistent application of these controls, document GPOs and required computer settings. Then use two tools, Secedit.exe and Resultant Set of Policy (RSoP), to ensure that settings remain.

When documenting security settings, make sure there are procedures in place to approve and document changes. Use Secedit.exe to audit the security settings on a specific computer and RSoP, to determine if the application of Group Policy achieved the results required by the organization's security policy.

Audit Security Settings with Secedit

Secedit was introduced in Chapter 2 as a way to set security policy on stand-alone computers. It also can be used to audit security policy. Before Secedit can be used to audit security policy, you must create a security template that matches your approved security configuration. In many organizations, a security template is developed for use in applying security settings by importing the template into a GPO. If this is the case in your environment, this original template can be used. If security templates were not used, you can still audit security settings by creating a template that matches your policy.

Always review the security template before using it to make sure it reflects your current security policy. If you intend to use the template more than once, ensure that it is stored in a secure place where it cannot be tampered with. To use Secedit to audit security settings:

- 1) Open an MMC console. (Click **Start | Run**, type "mmc" and click **OK**.)
- 2) From the File menu, select **Add/Remove Snap-in**.
- 3) Click the **Add** button.
- 4) Select **Security Configuration and Analysis**, click **Add** and then **Close**.

- 5) Click **OK**.
- 6) Expand the **Security Configuration and Analysis** node.
- 7) Right-click the **Security Configuration and Analysis** node and select **Open database**.
- 8) Enter a name for the database and click **Open**.
- 9) Browse to and then select the security template file, and then click **Open**.
- 10) Right-click the **Security Configuration and Analysis** node and select **Analyze computer now**.
- 11) Browse to a location to record an error log, or select the default, and then click **OK**. By default the log is saved to the My Documents\Security\Log\name_of_database.log file.
- 12) Click **OK**.
- 13) When the analysis has completed, expand the **Security Configuration and Analysis** node and view the detail pane. If there are differences between the database setting (your security policy as entered into the security template selected in Step 9) and the computer setting, a white “x” in a red circle will identify it, as shown in figure 5.

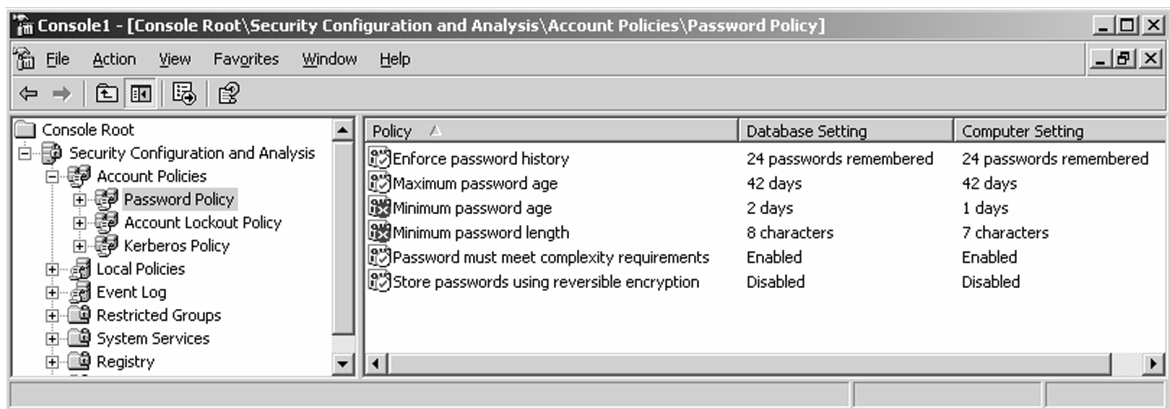


Figure 5: After a Secedit analysis of security settings, differences are identified with a white “x” in a red circle.

By expanding and viewing all areas of the graphical report, you can see the exact differences. The text file error log, as shown in Figure 6, records successful analysis (no differences) and reports where items differ but does not record exactly how they differ.

```
auditdb.log - Notepad
File Edit Format View Help

Attachment engines analysis completed successfully.
----Reading Configuration Info...
----Analyze Security Policy...
Mismatch - MinimumPasswordLength.
Mismatch - MinimumPasswordAge.
Not Configured - RequireLogonToChangePassword.
Analyze password information.
Mismatch - LockoutBadCount.
Analyze account lockout information.
Mismatch - ForceLogOffWhenHourExpire.
Analyze account force logoff information.
Not Configured - NewAdministratorName.
Not Configured - NewGuestName.
Mismatch - LSAAnonymousNameLookup.
Analyze LSA anonymous lookup setting.
Not Configured - EnableAdminAccount.
Analyze other policy settings.
Not Configured - ResetLockoutCount.
Not Configured - LockoutDuration.

System Access analysis completed successfully.
```

Figure 6. A text file error log notes differences in security policy.

Audit Group Policy Application Using RSoP

Security Configuration and Analysis can tell you if the security settings on the local machine match a specific security policy. It cannot, however, report on items configured in the Administrative templates section of Group Policy. RSoP can provide a report that includes these settings, but you will have to compare the applied settings manually to your security policy.

RSoP in logging mode, however, provides a way to audit what is actually being applied to a computer vs. what you might think based on GPO configuration. It's a good tool to use when a new GPO is applied, when changes are made to existing GPOs and as part of an annual security audit. If properly configured, you can sit at a single console, select representative member computers, and collect reports on their configuration. Representative member computers represent each computer role on your network. A computer role identifies a task a computer does, such as file server, desktop computer, DNS server, and so forth.

Use the RSoP wizard or the Group Policy Management Console (GPMC) to create RSoP queries, which you can save and access again. This type of query can be created with the RSoP snap-in to the GPMC.

In addition, RSoP planning and logging can be generated from an MMC to which the RSoP snap-in is added. To enable RSoP logging:

- 1) Add the snap-in to an MMC console.
- 2) Select **Generate RSoP** from the Action menu and click **Next**.
- 3) From the Mode Selection page, choose **Logging** mode, as shown in Figure 7 and click **Next**.

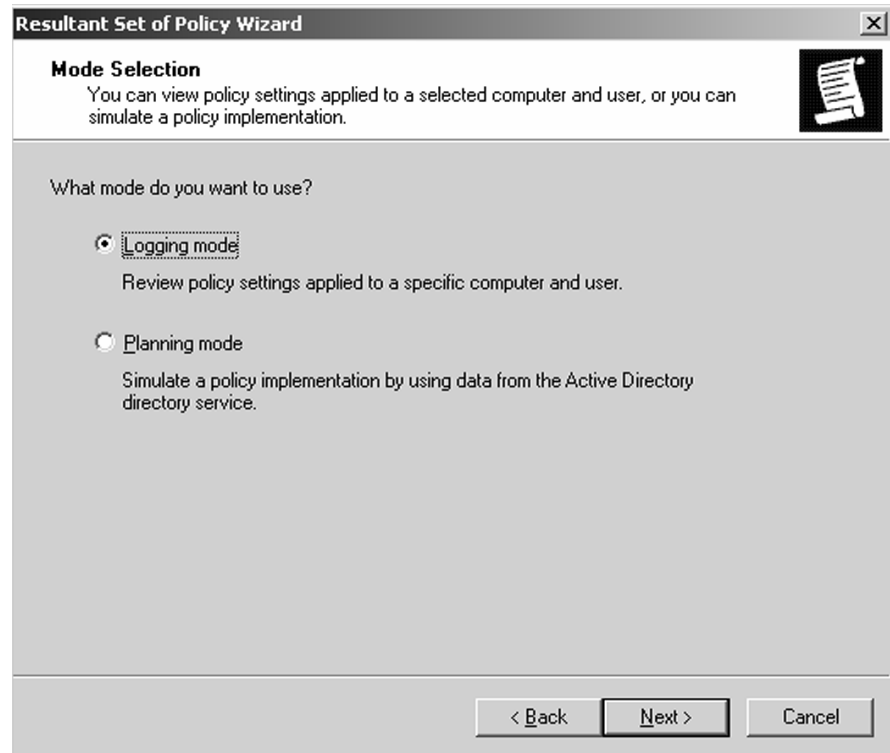


Figure 7. The RSoP snap-in can be used to generate RSoP planning or logging data.

- 4) Select the computer to generate data for. The computer must be accessible on the network.
- 5) Select whether to display computer and user settings or just user settings, then click **Next**.
- 6) Select the user to display, as shown in Figure 8, or select not to display user results (display computer only) and click **Next**.

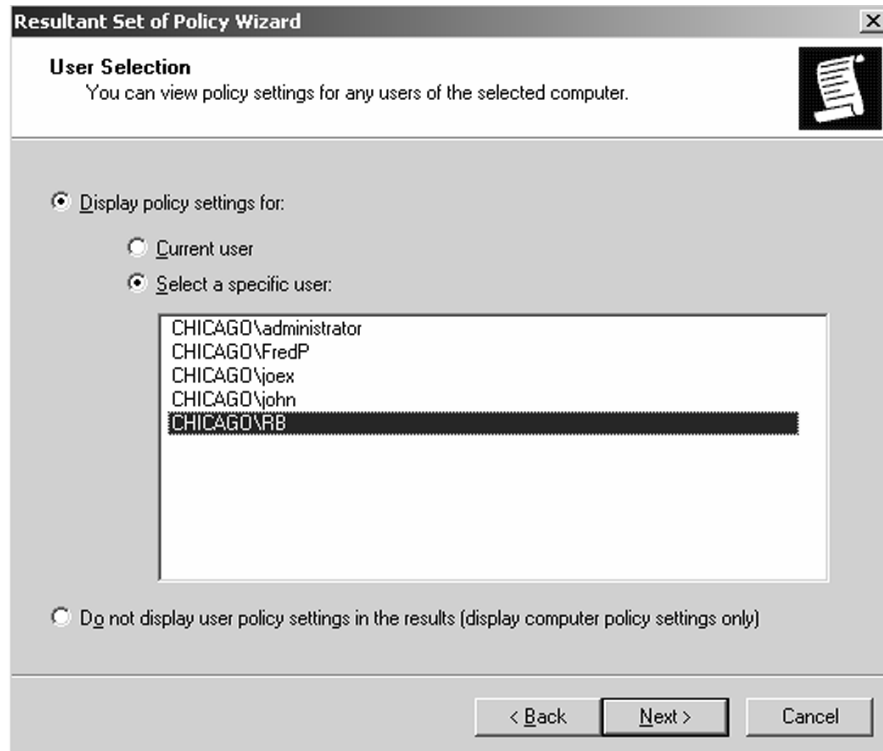


Figure 8. Select the user for which to display policy.

- 7) Review your selection and click **Next**. Click **Finish** when complete.
- 8) Expand the report.
- 9) Select an area to review. Note in Figure 9 that only enabled items are reported on. Double-click the policy in the detail pane to determine if the policy matches the required security policy for the user on this machine.

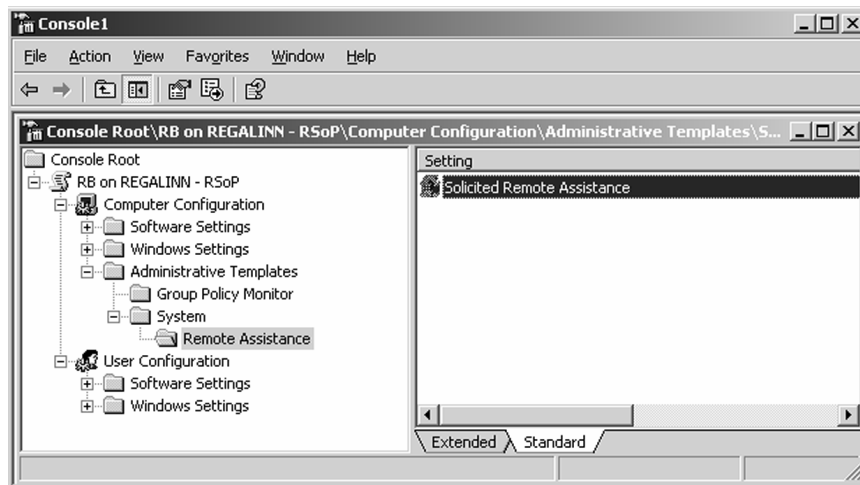


Figure 9. Examine RSoP results in the detail pane.

MONITOR AD FUNCTION

Many of the settings and options that help keep Active Directory secure are applied and enforced by Active Directory itself. Therefore, AD security is in jeopardy if Active Directory is not running correctly. That makes it an important part of ongoing security maintenance to keep Active Directory running smoothly. Chapter 3 provided instructions for monitoring DNS, AD replication, and the File Replication Service (FRS). Here are some other necessary tasks:

- Monitor disk space use and object growth. If the system disk or the disk on which the AD database is stored fills up, Active Directory cannot function.
- Set quotas in Active Directory. Quotas limit the number of objects a specific user can own. Since the creator is usually the owner of an object, limiting object creation can prevent a Denial-of-Service (DoS) attack by preventing excess object creation.
- Monitor for excessive Lightweight Directory Access Protocol (LDAP) and DNS traffic. If this traffic increases, it may signal an attack in process.
- Monitor the creation of new DCs. Are they authorized? If an intruder can create a new DC, he will have access to all domains and much forest information and can destroy the forest.
- Monitor the creation of new administrators. Are they authorized? A common attack pattern is to gain access via a compromised account and then create a new administrative account to use at a later date. If the compromised account becomes unavailable, the attacker still has a way back into the network.
- Refer to the “AD Product Operations Guide” (www.microsoft.com/downloads/details.aspx?familyid=84dfe61e-fb7b-4673-89b8-55bcc801b431&displaylang=en). The more you know about and take steps to properly run Active Directory, the more you improve your chances of securing it.

DISASTER RECOVERY

Information security should ensure the confidentiality, integrity, and availability of data. The proper configuration and management of Active Directory will assist you with the first two, disaster recovery and business continuity plans address the third. A disaster recovery plan details how IT operations can resume essential functions if a disaster should occur. Business recovery planning seeks to ensure that a business not only continues to operate in the short term, but also can continue in the long term. Your AD security design should incorporate elements of both.

To ensure that AD can be recovered, proper backups, backup storage, and recovery methods should be practiced. To start, ask what you would need in order to recover your entire forest infrastructure. A restoration of this scope should be your last resort, but if you are ready for this, you probably are prepared for recovery of a single machine or accidentally deleted directory object. Your forest-wide plan should include instructions for each type of restoration for any type of failure, and should include practicing all of these types of restoration.

Forest-Wide Recovery Preparation

Strictly speaking, recovery of an entire forest would include the recovery of all servers and desktop systems. You should have this type of plan in place. That's beyond the scope of this book, which is limited to AD infrastructure restoration. The first step is to plan and execute regular backups.

Backup Process

When a System State backup is made using NTBackup, the built-in Windows Server 2003 backup program, the AD database and all related files are backed up. Do not attempt to back up Active Directory simply by making copies or using a backup product to select and back up files. Many interrelated system files are required to successfully restore Active Directory. Use NTBackup or a third-party product specifically designed to back up Active Directory.

Backing up the entire hard drive will also back up System State information; however, since you cannot do differential or interim System State backups, you should also do normal System State backups. NTBackup can be used to perform an immediate or

scheduled System State backup, restore from backup, or perform automated system recovery. A System State backup backs up:

- Registry
- COM+ Class Registration database
- Boot files
- System files with Windows File Protection
- Certificate service database (if the server is a Certificate Authority)
- IIS metadirectory (if the server is an IIS server)
- AD database (if the server is a DC)
- SYSVOL directory (if the server is a DC)
- Cluster service information (if the server is part of a cluster)

To make a backup:

- 1) Select **Start | All Programs | Accessories | System Tools | Backup**.
- 2) Click **Advanced Mode**.
- 3) Select **Backup Wizard (Advanced)** and click **Next**.
- 4) Select **Only Backup the System State Data** and click **Next**.
- 5) Select a backup destination, provide a name for the backup, and click **Next**.
- 6) To make an immediate backup of the System State, click **Finish**. Click the **Advanced** button to create a schedule.

Backup Schedule

The key to recovery is to make frequent backups. While the frequency of backup will vary depending on things such as the volatility of System State data, AD backups should follow a few rules or they may become useless.

The first rule is that backups should never be older than the *tombstone lifetime*. A tombstone is created when an object is deleted from Active Directory. The tombstone is replicated throughout the forest so that copies of the object on the other DCs will also be deleted. Each tombstone replica will be deleted, without further intervention, according to the tombstone lifetime. The default tombstone lifetime is 60 days. If a backup is older than the tombstone lifetime, it cannot be used to restore Active Directory.

Backing Up DCs

A complete AD forest recovery requires:

- A list of all domains in the forest and all DCs in each domain. (After the forest root domain is restored, you can confirm all sites and domains using the **AD Domains and Trusts** and **AD Sites and Services** consoles.)
- A list of an Administrator account and a password for each domain.
- Backups for at least the DC for each domain in the forest. It is best to have a backup of every DC in every domain in the forest. Then, if a backup is corrupt or missing, you will have many alternatives. Also, many DCs have multiple roles, such as certificate authorities and so on. Their specific data would not be part of every DC backup.
- A backup of DNS data, or the original DNS server if DNS is not installed on the DCs.

Forest Recovery Steps

An entire forest can be restored if adequate backups exist by following these steps:

- 1) Identify all domains in the forest and all DCs in each domain. Identify which DCs have backups.
- 2) Identify Administrator accounts and passwords for each domain.
- 3) Identify the forest root domain.
- 4) For each domain in the forest, identify a DC for which there is a validated and trusted backup of AD.
- 5) Shut down any DCs that are still operational but corrupted. You do not want any corrupt or incorrect data to be replicated to the restored DCs. In a large enterprise it may be difficult to ensure that all these DCs are shut down, but it is important to follow the steps listed here carefully, as many of them are designed to prevent accidental replication with other DCs in the forest.
- 6) Recover the first DC in the forest root domain.
- 7) Mark the Sysvol primary. This is a standard best practice for the first DC in a domain.

- 8) Reboot the DC and verify that the AD and all other server data is intact and undamaged. (If there are any problems, use another backup and do a restore.)
- 9) If DNS is AD-integrated, ensure that the local DNS server is installed and running on this DC. Configure the server with its IP address as its preferred DNS server.
- 10) If the restored DC is also a Global Catalog (GC) server, remove the GC flag. It is best to enable a new GC to ensure that old data does not interfere with the process.
- 11) Raise the value of the current RID pool by 100,000. The RID pool is used when assigning SIDs to new objects. Raising the pool number should ensure that duplicate numbers will not be assigned. (New objects might have been created in the domain after the backup was taken.)
- 12) Seize all forest and domain operations master roles. (It is okay if seizure fails; it can be attempted later. Problems will occur if the DC is not a GC.)
- 13) Clean up metadata from other DCs in the forest root domain if you will restore them from backup. Cleaning metadata can prevent duplication of NTDS-settings objects (such as connections and site links) when DCs are created in another site, interference with the issuance of new RIDs, and so on.
- 14) Delete server and computer objects for all other DCs in the forest root domain. (New objects will be created when installing AD on other DCs.)
- 15) Reset the computer account password of this restored DC twice.
- 16) Reset the built-in Kerberos service account (krbtgt) password twice. By resetting account passwords twice, you remove the pre-failure password from password history.
- 17) Reset trust passwords twice (the Trusted Domain object password) for all trusts. This includes the implicit trusts between DCs in the same domain. Resetting these passwords will keep the new DC from replicating with any existing DCs not removed in Step 5.
- 18) Configure the DNS server with delegation resource records (name server (NS) and host (A) resource records) for each child DNS zone.
- 19) Physically isolate computers that will become the first DCs in each domain and restore them. As stated earlier, Sysvol should be marked primary for each of these DCs.
- 20) After rebooting, ensure that the data on these DCs is not corrupt. If it is, use a different backup.

- 21) If DNS is AD-integrated, install the DNS service on each of these DCs. Configure DCs with the IP address of the first server in the root forest of the domain, since it is the preferred DNS server.
- 22) Follow instructions 10–17 for each server that will become a DC.
- 23) When the first DC for each domain is operational and you have completed these steps, join these DCs to the network where the root forest domain exists.
- 24) Enable the DC in the root forest domain as a GC.
- 25) Begin recovering other DCs in the forest by installing Active Directory using Dcpromo.exe.
- 26) Make any DNS changes required. This can include deleting DC records for DCs that were not recovered and deleting WINS records for DCs that have not been recovered.
- 27) Distribute operations master roles to other DCs in the domain or forest and enable more GCs.
- 28) Restore or reinstall any server applications run on DCs.

Complete instructions for all these steps can be found in the Microsoft document “Best Practice Recommendation for Recovering your AD Forest.” (Referred to as “Best Practices: Active Directory Recovery” and downloadable at

www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3EDA5A79-C99B-4DF9-823C-933FEBA08CFE)

Storage Backup

Making backups is just half the process. You must be able to use them in a restore, realize the danger uncontrolled backups can pose, and appropriately secure backup media. Backups contain sensitive data. A backup could be restored and provide an attacker all the information needed to further compromise your network. Follow these best practices when dealing with backup media:

- Schedule backups and require backups to be documented.
- Label media and store in a safe place.
- A copy of the most recent backup should be kept onsite in a locked location, while a copy of the backup should be kept offsite. Keep in mind that recovery must be ensured even if the original site is not available.

- Split backup and restore privileges. An authoritative restore of an old DC can replace data with that from an old, no longer valid backup. This can damage your current operations. By splitting duties, you can better control backup media. Only those authorized to back up DCs should be able to handle backup media unless an approved restore is required.
- Log and track all media used for backups and restores. Require signatures for checking media in and out.
- Train personnel to question the return of backup media stored offsite. Since it should be returned only if a restore is necessary, you may prevent an accidental or malicious restore.

AD Restoration

Active Directory cannot be restored simply by copying its database and associated files back to their default location. The files must be restored in a very specific order. There are also different types of AD restore. The type used will depend on the status of the DC or objects to restore. Four types of restore exist:

- *Primary* - Necessary when restoring the first DC in a domain, or when restoring the only working server or a replicated data set (do this when all DCs in the domain are lost).
- *Normal (nonauthoritative)* - Done to restore a replica of the directory, which does not need to propagate any differences at the time of restore to the other DCs. Once restored, it will be updated with the changes that have occurred since the backup during normal replication with other DCs in the domain.
- *Authoritative restore of a deleted object* - This is done when an object is accidentally deleted. A replica of Active Directory from before the object was deleted is restored, and the object from the restored replica is replicated to the other DCs. Only the accidentally deleted object is restored.
- *Authoritative restore of an earlier version of Active Directory* - A replica of an earlier version is restored from backup and its contents are replicated to other DCs in the domain.

A normal restore is completed by doing a restore of the System State backup, following these steps:

- 1) Open the backup program.
- 2) Click **Advanced Mode**.
- 3) Click the **Restore Wizard (Advanced)** button and then click **Next**.
- 4) Select **Items to restore** and click **Next**.
- 5) Use the defaults or select a destination for the restoration. You may choose the original or alternative location.
- 6) Click **Finish** to start the restore.
- 7) Click the **Report** button to view a restore report.

After a normal restore, objects that have changed since the restore are replicated from other DCs in the forest to the newly restored DC.

To do an authoritative restore, you must adjust the update sequence number of the object to a number higher than any other update sequence number for the object on other DCs. Update sequence numbers are used to ensure that the latest change to an object is replicated. Each object has an update sequence number, with the higher numbers being assigned to newer or changed objects. During replication, the numbers are reviewed, and if two versions of an object exist, the object with the higher update sequence number will replace the lower-numbered version. In an authoritative restore, NTDSutil increases the update sequence number of the object to restore to a number higher than any other update sequence number in the AD replication system. Normal replication can then be used to restore the object.

An authoritative restore can have unintended consequences on computer accounts and trusts because earlier objects may not have the same computer or trust passwords. You may need to take this into consideration during your restoration planning. Complete instructions for authoritative restore are at <http://support.microsoft.com/default.aspx?scid=kb;en-us;816042>.

REVIEW POLICY AND PROCESS

Products change, as does our understanding of them. Once you have established sound practices for protecting and securing Active Directory, you should not assume they will remain best practices. As updates and new utilities are produced, review your practices and procedures and revise them as necessary. As your understanding of Active Directory increases, and newer findings are published, you may discover new techniques and processes that will enhance AD security. Do not be afraid to challenge your own status quo—but also do not assume that newer is better.

A Worthwhile Undertaking

This completes this chapter on AD maintenance and audit, as well as this e-book on AD security. While Active Directory is complex and securing it can be a challenge, it is a worthwhile undertaking. The security of your entire IT infrastructure depends on your ability to do so.

ABOUT QUEST WINDOWS MANAGEMENT

Quest Software, Microsoft's 2004 Global Independent Software Vendor Partner of the Year, provides solutions that simplify, automate and secure Active Directory, Exchange and Windows environments. The Quest Windows Management group delivers comprehensive capabilities for secure Windows management and migration. For more information on Quest Software's Windows Management group, please visit www.quest.com/microsoft.

ABOUT QUEST SOFTWARE

Quest Software, Inc. provides software to simplify IT management for 18,000 customers worldwide, including 75 percent of the Fortune 500. Quest products for application, database and Windows management help customers develop, deploy, manage, and maintain the IT enterprise without expensive downtime or business interruption. Headquartered in Irvine, Calif., Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

E-mail: info@quest.com

Mail: Quest Software, Inc.
World Headquarters
8001 Irvine Center Drive
Irvine, CA 92618
USA

Web site: www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink www.quest.com/support

E-mail: support@quest.com

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches

NOTES