Microsoft®
Training &
Certification

Microsoft® Official
Curriculum

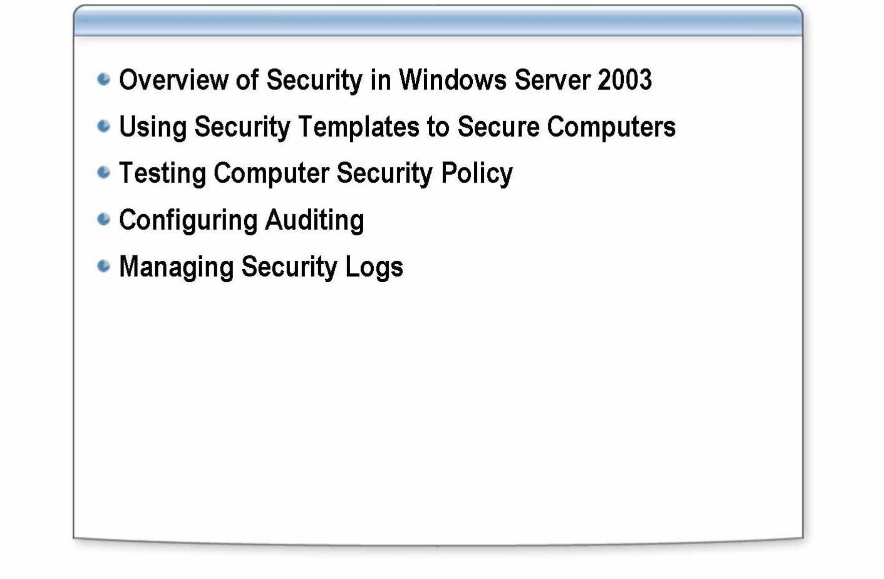
Module 10: Implementing Administrative Templates and Audit Policy

Contents

Microsoft®

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Overview



- Overview of Security in Windows Server 2003
- Using Security Templates to Secure Computers
- Testing Computer Security Policy
- Configuring Auditing
- Managing Security Logs

Introduction

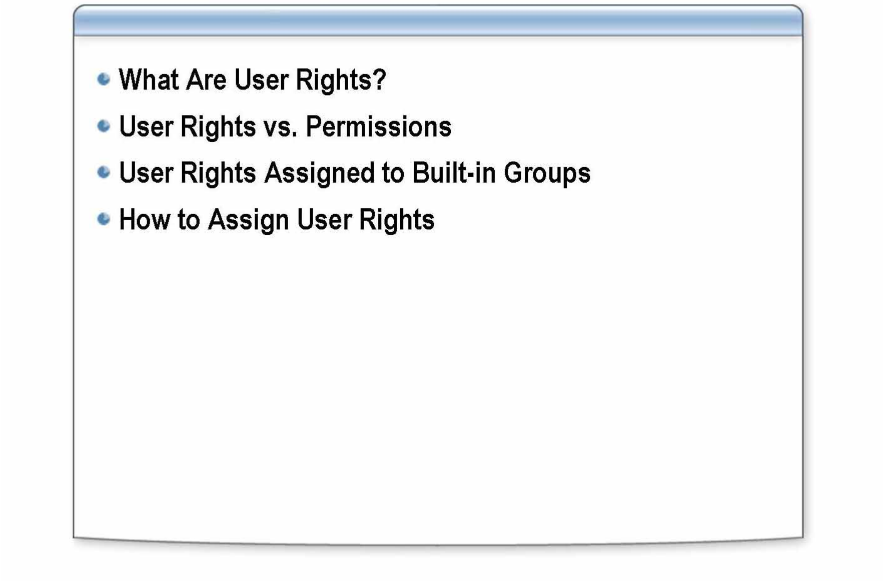
This module will provide a broad overview of security in Microsoft® Windows® Server 2003. You will learn how to use security templates and test computer security policy. You will also learn how to configure auditing and manage security logs.

Objectives

After completing this module, you will be able to:

- Describe administrative templates and audit policy in Windows Server 2003.
- Use security templates to secure computers.
- Test computer security policy.
- Configure auditing.
- Manage security logs.

Lesson: Overview of Security in Windows Server 2003



- What Are User Rights?
- User Rights vs. Permissions
- User Rights Assigned to Built-in Groups
- How to Assign User Rights

Introduction

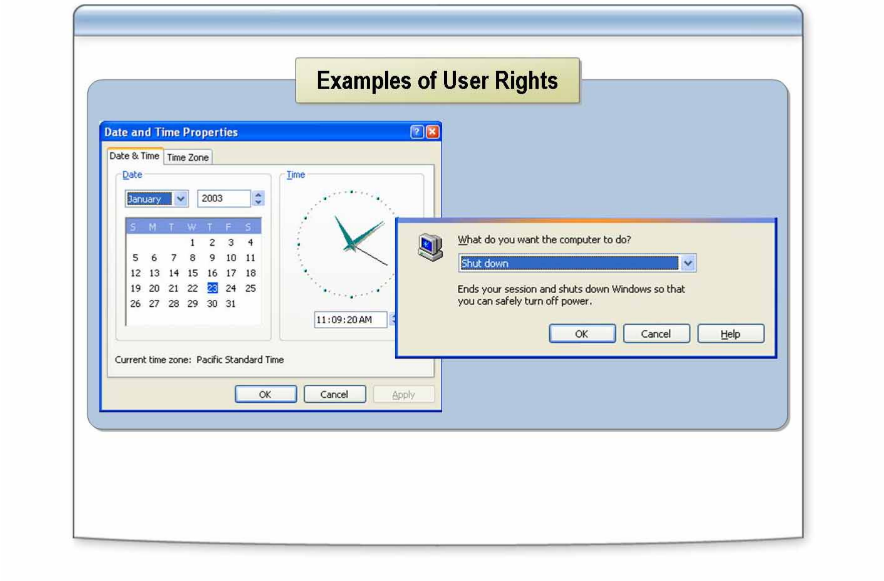
In this lesson, you will learn about user rights, permissions, and user rights assigned to built-in groups. You will also learn how to assign user rights.

Lesson objectives

After completing this lesson, you will be able to:

- Describe user rights.
- Distinguish between rights and permissions.
- Describe the user rights assigned to built-in groups.
- Assign user rights.

What Are User Rights?



Examples of User Rights

Date and Time Properties

Date & Time | Time Zone

Date: January 2003

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Time: 11:09:20 AM

Current time zone: Pacific Standard Time

What do you want the computer to do?

Shut down

Ends your session and shuts down Windows so that you can safely turn off power.

Definition

When a user logs on, the user receives an access token that includes user rights. A user right authorizes a user who is logged on to a computer or a network to perform certain actions on the system. If a user does not have the appropriate rights to perform an action, attempts to perform the action are blocked.

Who do rights apply to?

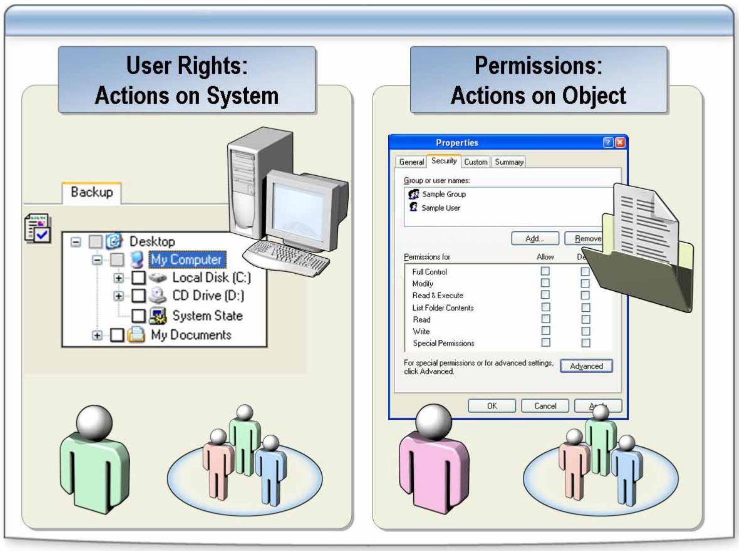
User rights can apply both to individual users and to groups. However, user rights are best administered when they are assigned to groups. This ensures that a user who logs on as a member of a group automatically receives the rights associated with that group. Windows Server 2003 enables an administrator to assign rights to users and groups.

Common user rights

Common user rights include the following:

- *Log on locally*. Enables a user to log on to the local computer or to the domain from a local computer.
- *Change the system time*. Enables a user to set the time of the internal clock of a computer.
- *Shut down the system*. Enables a user to shut down a local computer.
- *Access this computer from a network*. Enables a user to access a computer running Windows Server 2003 from any other computer on the network.

User Rights vs. Permissions



Introduction

Administrators can assign specific user rights to group accounts or to individual user accounts. These rights authorize users to perform specific actions, such as log on to a system interactively or back up files and directories. User rights are different from permissions, because user rights are attached to user accounts, and permissions are attached to objects.

What are user rights?

User rights determine which users can perform a specific task on a computer or in a domain. Although you can assign user rights to individual user accounts, user rights are best administered if they are assigned to group accounts. A user logging on as a member of a group automatically inherits the rights assigned to that group. By assigning user rights to groups rather than individual users, you simplify the task of administering user accounts. When users in a group all require the same user rights, you can assign the set of user rights once to the group, rather than repeatedly assigning the same set of user rights to each individual user account.

User rights that are assigned to a group are applied to all members of the group while they are members. If a user is a member of multiple groups, the user's rights are cumulative, which means that the user has more than one set of rights. The only time that rights assigned to one group might conflict with those assigned to another is in the case of certain logon rights. In general, user rights assigned to one group do not conflict with the rights assigned to another group. To remove rights from a user, the administrator simply removes the user from the group. The user no longer has the rights assigned to that group.

Rights apply to the entire system, rather than to a specific resource, and affect the overall operation of the computer or domain. All users accessing network resources must have certain common rights on the computers they use, such as the right to log on to the computer or change the system time of the computer. Administrators can assign specific common user rights to groups or to individual users. Additionally, Windows Server 2003 assigns certain rights to built-in groups by default.

What are permissions?

Permissions define the type of access granted to a user or group for an object or object property. For example, you can grant the Read and Write permissions to the Finance group for a file named Payroll.dat.

You can grant permissions for any secured objects such as files, objects in the Active Directory® directory service, or registry objects. You can grant permissions to any user, group, or computer. It is a good practice to grant permissions to groups.

You can grant permissions for objects to:

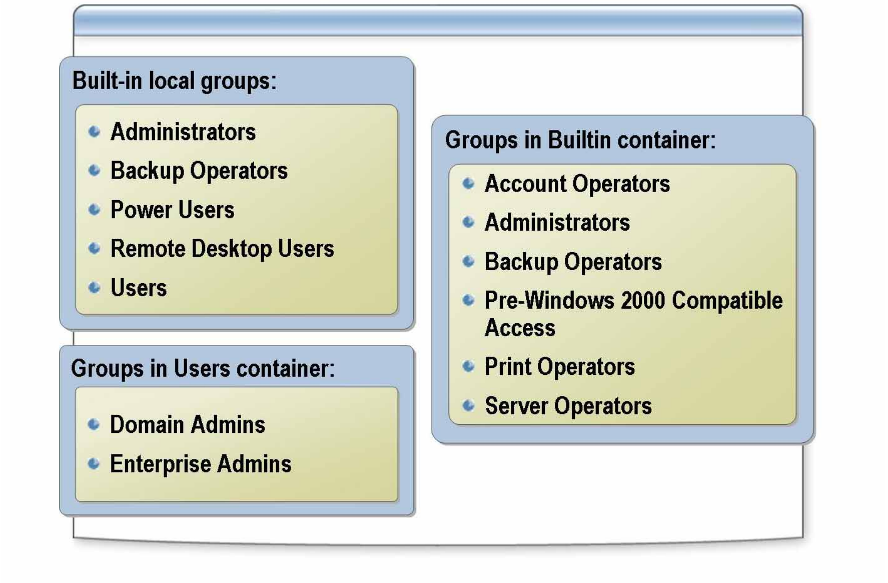
- Groups, users, and special identities in the domain.
- Groups and users in that domain and any trusted domains.
- Local groups and users on the computer where the object resides.

When you provide access to file resources on a computer running Windows Server 2003, you can control who has access to resources and the nature of their access by granting the appropriate permissions. Permissions define the type of access assigned to a user or group for any resource.

For example, users in the Human Resources department of an organization might need to modify the organization's document describing Human Resources policies. To facilitate this, the administrator must grant the appropriate permission to the members of the Human Resources department.

To grant permissions for individual files and folders, Windows Server 2003 uses the NTFS file system. You can also control the permissions for accessing shared folder resources and network printers.

User Rights Assigned to Built-in Groups



Built-in local groups:

- Administrators
- Backup Operators
- Power Users
- Remote Desktop Users
- Users

Groups in Users container:

- Domain Admins
- Enterprise Admins

Groups in Builtin container:

- Account Operators
- Administrators
- Backup Operators
- Pre-Windows 2000 Compatible Access
- Print Operators
- Server Operators

Introduction

By default, Windows Server 2003 assigns certain rights to built-in groups. The built-in groups include local groups, groups in the Builtin container, and groups in the Users container.

User rights assigned to local groups

The following user rights are assigned to local groups:

- Administrators

  Access this computer from the network; Adjust memory quotas for a process; Allow log on locally; Allow log on through Terminal Services; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Force shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Manage auditing and security log; Modify firmware environment variables; Perform volume maintenance tasks; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects

- Backup Operators

  Access this computer from the network; Allow log on locally; Back up files and directories; Bypass traverse checking; Restore files and directories; Shut down the system

- Power Users

  Access this computer from the network; Allow log on locally; Bypass traverse checking; Change the system time; Profile single process; Remove computer from docking station; Shut down the system

Caution Members of the Power Users group can elevate their privileges to administrator.

- Remote Desktop Users

  Allow log on through Terminal Services

- Users

  Access this computer from the network; Allow log on locally; Bypass traverse checking

User rights assigned to the Builtin container

The following user rights are assigned to groups in the Builtin container:

- Account Operators

  Allow log on locally; Shut down the system

- Administrators

  Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects

- Backup Operators

  Back up files and directories; Allow log on locally; Restore files and directories; Shut down the system

- Pre-Windows 2000 Compatible Access

  Access this computer from the network; Bypass traverse checking

- Print Operators

  Allow log on locally; Shut down the system

- Server Operators

  Back up files and directories; Change the system time; Force shutdown from a remote system; Allow log on locally; Restore files and directories; Shut down the system

User rights assigned to the Users container

The following user rights are assigned to groups in the Users container:

- Domain Admins

  Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force a shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects

- Enterprise Admins (only appears in the forest root domain)

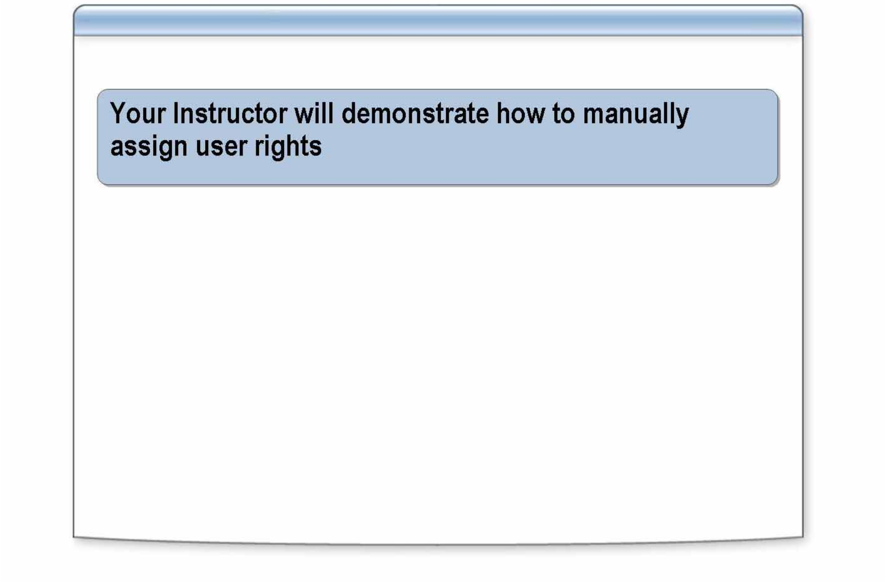
  Access this computer from the network; Adjust memory quotas for a process; Back up files and directories; Bypass traverse checking; Change the system time; Create a pagefile; Debug programs; Enable computer and user accounts to be trusted for delegation; Force shutdown from a remote system; Increase scheduling priority; Load and unload device drivers; Allow log on locally; Manage auditing and security log; Modify firmware environment values; Profile single process; Profile system performance; Remove computer from docking station; Restore files and directories; Shut down the system; Take ownership of files or other objects

Additional reading

For more information about user rights and upgrading operating systems, see article 323042, “Required User Rights for the Upgrade from Windows 2000 to Windows Server 2003” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=323042.

For more information about user rights and service accounts, see article 325349, “HOW TO: Grant Users Rights to Manage Services in Windows Server 2003” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=325349.

How to Assign User Rights



Your Instructor will demonstrate how to manually assign user rights

Introduction

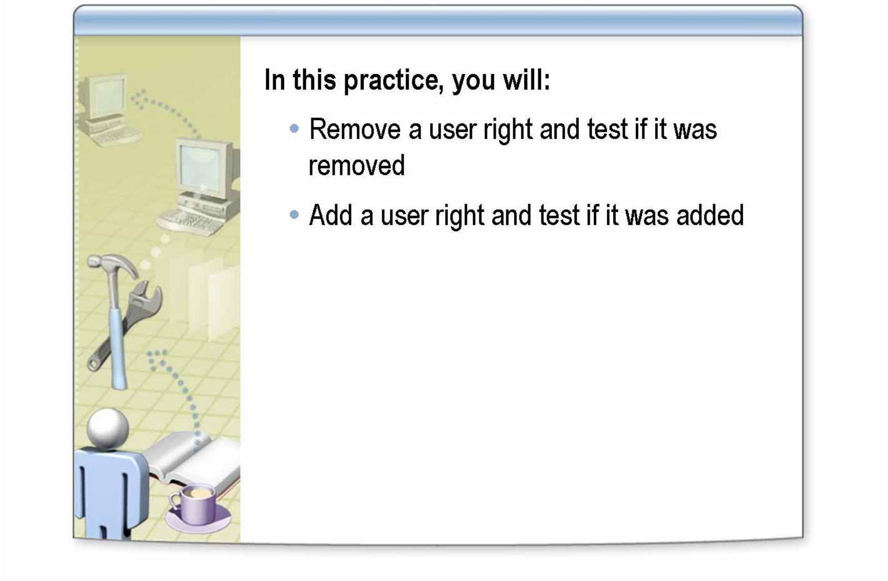
Typically, administrators add users or groups to built-in groups that already have rights. In some circumstances, a built-in group might give too much or too little rights to a user, so you must assign rights manually.

Procedure

To assign user rights:

1. Click **Start**, click **Run**, type **mmc** and then press ENTER.
2. Click **Console**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, double-click **Group Policy Object Editor**.
6. Click **Finish** to close the Welcome to Group Policy Wizard.
7. Click **Close** to close the **Add Standalone Snap-in** dialog box.
8. Click **OK** to close the **Add/Remove Snap-in** dialog box.
9. Expand **Local Computer Policy**, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, and then expand **Local Policies**.
10. Click **User Rights Assignment**.
11. Add or remove a group to a user right as needed.

Practice: Assigning User Rights



In this practice, you will:

- Remove a user right and test if it was removed
- Add a user right and test if it was added

Objective

In this practice, you will:

- Remove the right to log on locally from the Users group and test if the user right is removed.
- Assign the Users group the right to log on locally and test if the user right is assigned.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*Admin account.
- Open CustomMMC

Note This practice focuses on the concepts in this lesson and as a result may not comply with Microsoft security recommendations. For example, this practice does not comply with the recommendation that users log on with domain user account and use the **Run as** command when performing administrative tasks.

- Review the procedures in this lesson that describe how to perform this task.

Scenario

The systems engineers want to test user rights by preventing users from logging on locally to your computer. After the test is successful, you will assign users the right to log on locally.

Practice

► **Remove the right to log on locally from the Users group**

1. Remove the group Users from the following local computer policy:

   Computer Configuration/Windows Settings/Security Settings/
   Local Policies/User Rights Assignment/Allow log on locally

2. Close all programs and log off.

► **Test if the right was removed**

- Log on as *ComputerName*User.

  You should *not* be able to log on.

► **Assign the right to log on locally to the Users group**

1. Log on as *ComputerName*Admin.
2. Add the group Users to the following local computer policy:

   Computer Configuration/Windows Settings/Security Settings/
   Local Policies/User Rights Assignment/Allow log on locally

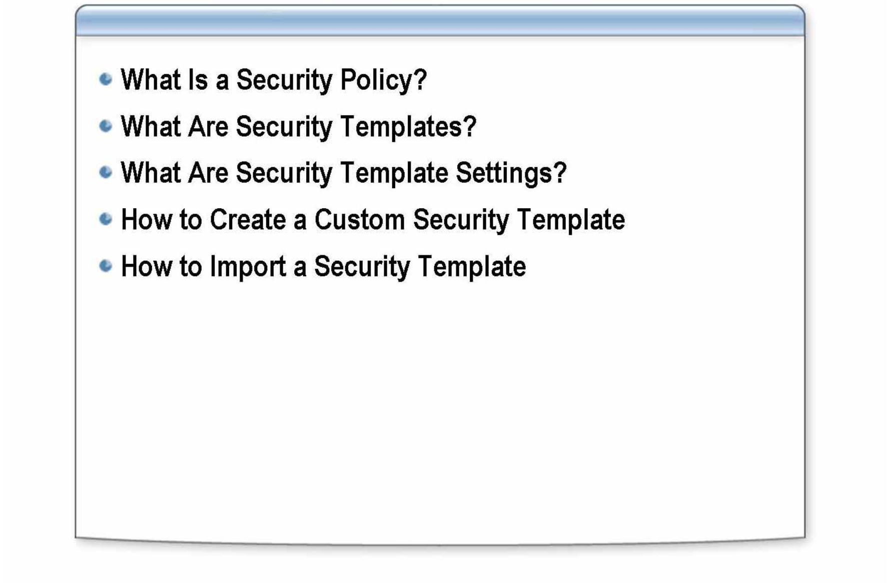
3. Close all programs and log off.

► **Test if the right was assigned**

- Log on as *ComputerName*User.

  You should be able to log on.

Lesson: Using Security Templates to Secure Computers



- What Is a Security Policy?
- What Are Security Templates?
- What Are Security Template Settings?
- How to Create a Custom Security Template
- How to Import a Security Template

Introduction

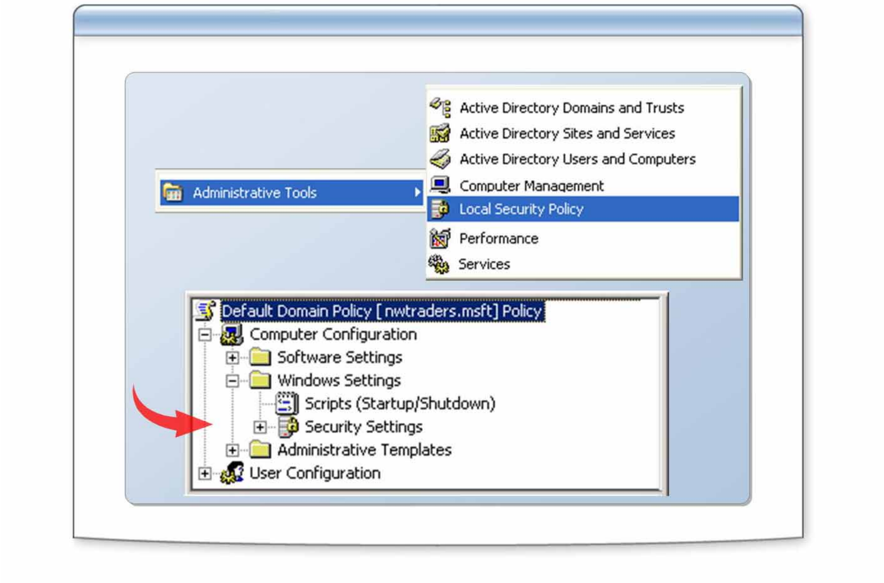
You can create security templates to create a security policy and alter a security policy to meet the security needs of your company. You can implement security policies in several different ways. The method you use depends on your organization's size and security needs. Smaller organizations, or those not using Active Directory, can configure security manually on an individual basis. If your organization is large or requires a high level of security, consider using Group Policy objects (GPOs) to deploy security policy.

Lesson objectives

After completing this lesson, you will be able to:

- Describe a security policy.
- Describe security templates.
- Describe security template settings.
- Create a custom security template.
- Import a security template.

What Is a Security Policy?



Introduction

A security policy is a combination of security settings that affect the security on a computer. You can use security policy to establish account policies and local policies on your local computer and in Active Directory.

Security policy on a local computer

You can use the security policy on a local computer to directly modify account and local policies, public key policies, and Internet Protocol security (IPSec) policies for your local computer.

With local security policy, you can control:

- Who accesses your computer.
- What resources users are authorized to use on your computer.
- Whether a user or group's actions are recorded in the event log.

If your network does not use Active Directory, you can configure security policy by using Local Security Policy, which is found on the **Administrative Tools** menu on computers running Windows Server 2003.

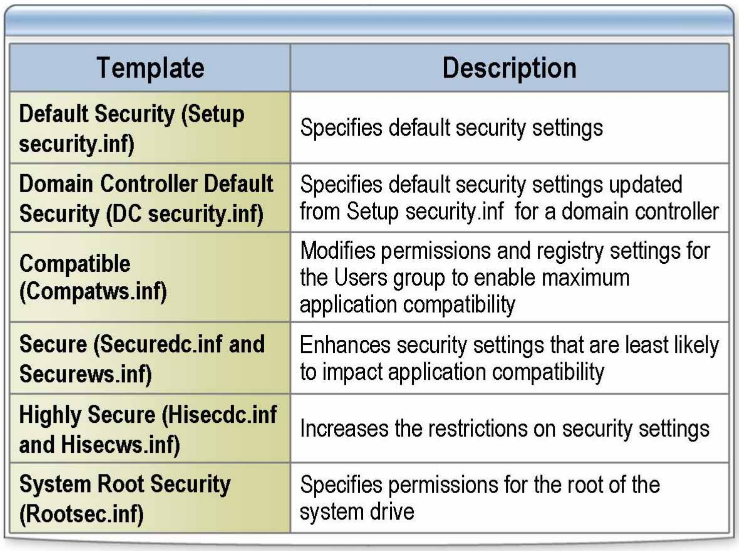
Security policies in Active Directory

Security policies in Active Directory have the same security settings as a security policy on local computers. However, administrators of Active Directory–based networks can save considerable administrative time by using Group Policy to deploy the security policy. You can edit or import security settings in a GPO for any site, domain, or organizational unit, and the security settings are automatically deployed to the computers when the computers start. When editing a GPO, expand **Computer Configuration** or **User Configuration** and then expand **Windows Settings** to find security policy settings.

Additional reading

For more information about default domain user rights, see article 324800, "HOW TO: Reset User Rights in the Default Domain Group Policy in Windows Server 2003" in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=324800.

What Are Security Templates?



Template	Description
Default Security (Setup security.inf)	Specifies default security settings
Domain Controller Default Security (DC security.inf)	Specifies default security settings updated from Setup security.inf for a domain controller
Compatible (Compatws.inf)	Modifies permissions and registry settings for the Users group to enable maximum application compatibility
Secure (Securedc.inf and Securews.inf)	Enhances security settings that are least likely to impact application compatibility
Highly Secure (Hisecdc.inf and Hisecws.inf)	Increases the restrictions on security settings
System Root Security (Rootsec.inf)	Specifies permissions for the root of the system drive

Definition

A security template is a collection of configured security settings. Windows Server 2003 provides predefined security templates that contain the recommended security settings for different situations.

You can use predefined security templates to create security policies that are customized to meet different organizational requirements. You customize the templates with the Security Templates snap-in. After you customize the predefined security templates, you can use them to configure security on an individual computer or thousands of computers.

How security templates are applied

You can configure individual computers with the Security Configuration and Analysis snap-in or the **secedit** command-line tool or by importing the template into Local Security Policy. You can configure multiple computers by importing a template into Security Settings, which is an extension of Group Policy.

You can also use a security template as a baseline for analyzing a system for potential security holes or policy violations by using the Security Configuration and Analysis snap-in. By default, the predefined security templates are stored in *systemroot*/Security/Templates.

Predefined templates

Windows Server 2003 provides the following predefined templates:

- Default security (Setup security.inf)

  The Setup security.inf template is created during installation of the operating system for each computer and represents default security settings that are applied during installation, including the file permissions for the root of the system drive. It can vary from computer to computer, based on whether the installation was a clean installation or an upgrade. You can use this template on servers and client computers, but not on domain controllers. You can apply portions of this template for disaster recovery.

  Default security settings are applied only to clean installations of Windows Server 2003 on an NTFS partition. When computers are upgraded from Microsoft Windows NT® version 4.0, security is not modified. Also, when you install Windows Server 2003 on a FAT (file allocation table) file system, security is not applied to the file system.

- Domain controller default security (DC security.inf)

  The DC security.inf template is created when a server is promoted to a domain controller. It reflects default security settings on files, registry keys, and system services. Reapplying it resets these settings to the default values, but it may overwrite permissions on new files, registry keys, and system services created by other applications. You can apply it by using the Security Configuration and Analysis snap-in or the **secedit** command-line tool.

- Compatible (Compatws.inf)

  Default permissions for workstations and servers are primarily granted to three local groups: Administrators, Power Users, and Users. Administrators have the most privileges, and Users have the least.

  Members of the Users group can successfully run applications that take part in the Windows Logo Program for Software. However, they may not be able to run applications that do not meet the requirements of the program. If other applications are to be supported, the Compatws.inf template changes the default file and registry permissions that are granted to the Users group. The new permissions are consistent with the requirements of most applications that do not belong to the Windows Logo Program for Software.

- Secure (Secure*.inf)

  The Secure templates define enhanced security settings that are least likely to affect application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings.

- Highly Secure (hisec*.inf)

  The Highly Secure templates are supersets of the Secure templates. They impose further restrictions on the levels of encryption and signing that are required for authentication and for the data that flows over secure channels and between server message block (SMB) clients and servers.

- System root security (Rootsec.inf)

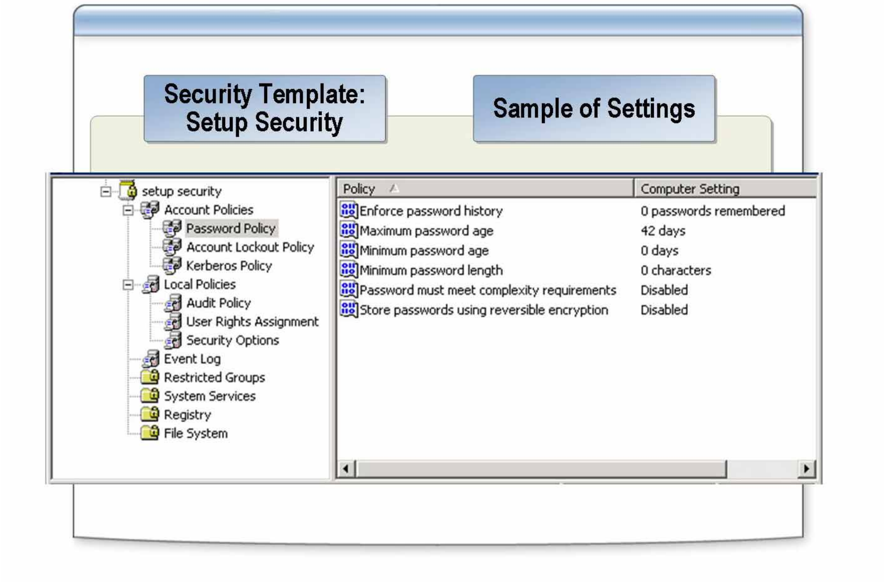
  By default, Rootsec.inf defines the permissions for the root of the system drive. You can use this template to reapply the root directory permissions if they are inadvertently changed, or you can modify the template to apply the same root permissions to other volumes. As specified, the template does not overwrite explicit permissions that are defined on child objects. It propagates only the permissions that are inherited by child objects.

Additional reading

For more information about applying security policies, see article 325351, “HOW TO: Apply Local Policies to All Users Except Administrators on Windows Server 2003 in a Workgroup Setting” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=325351.

For more information on **secedit**, see “Secedit” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/secedit_cmds.asp?frame=true.

What Are Security Template Settings?



Security Template: Setup Security

Sample of Settings

Policy	Computer Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Introduction

Security templates contain security settings for all security areas. You can apply templates to individual computers or deploy them to groups of computers by using Group Policy. When you apply a template to existing security settings, the settings in the template are merged into the computer's security settings.

You can configure and analyze security settings for computers by using the Security Settings Group Policy extension or Security Configuration and Analysis.

Types of security template settings

The following list describes each of the security template settings:

- Account Policies

  You can use account policy settings to configure password policies, account lockout policies, and Kerberos version 5 (V5) protocol policies for the domain. A domain's account policy defines the password history, the lifetime of the Kerberos V5 tickets, account lockouts, and more.

- Local Policies

  Local policy settings, by definition, are local to computers. Local policies include audit policies, the assignment of user rights and permissions, and various security options that can be configured locally.

  It is important not to confuse local policy settings with setting policies locally. As with all of these security settings, you can configure these settings by using Local Security Policy and Group Policy.

- Event Log

  You use event log settings to configure the size, access, and retention parameters for application logs, system logs, and security logs.

- Restricted Group

  You use restricted group settings to manage the membership of built-in groups that have certain predefined capabilities, such as Administrators and Power Users, in addition to domain groups, such as Domain Admins. You can add other groups to the restricted group, along with their membership information. This enables you to track and manage these groups as part of security policy.

  You can also use restricted group settings to track and control the reverse membership of each restricted group. Reverse membership is listed in the **Members Of** column, which displays other groups to which the restricted group must belong.

- System Services

  You use system services settings to configure security and startup settings for services running on a computer. System services settings include critical functionality, such as network services, file and print services, telephony and fax services, and Internet or intranet services. The general settings include the service startup mode (automatic, manual, or disabled) and security on the service.

- Registry

  You use registry settings to configure security on registry keys.

- File System

  You use file system settings to configure security on specific file paths.

- Public Key Policies

  You use public key policy settings to configure encrypted data recovery agents, domain roots, trusted certificate authorities, and so on.

  Note Public Key Policies are the only settings available under User Configuration.

- IP Security Policies on Active Directory

  You use IP security policy settings to configure IPSec.

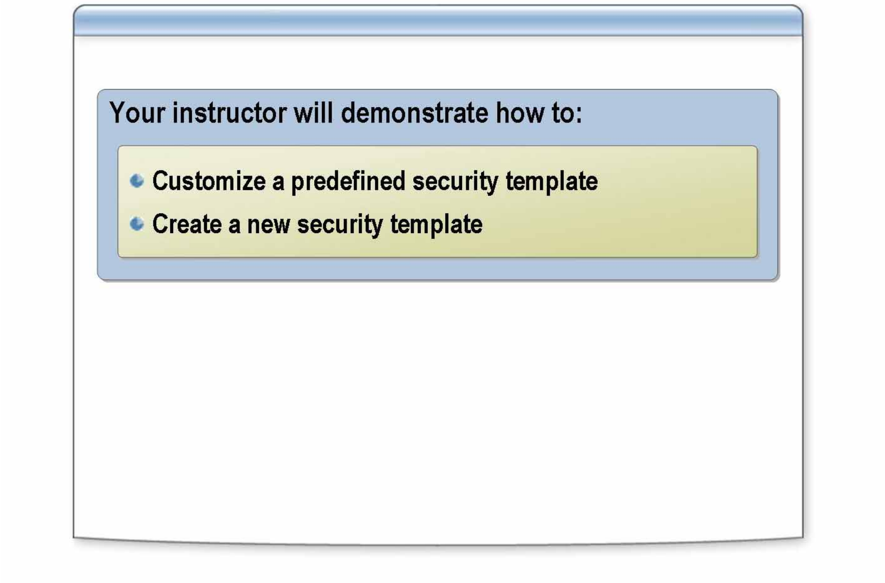
Important Only the Account Policies, Local Policies, Public Key Policies, and IP Security Policies on Active Directory areas are available when you use Local Security Policy.

Also, you can assign password settings, account lockout settings, and Kerberos settings at the domain or organizational unit level. However, if you configure the policy at the organizational unit level, the settings affect only the local Security Accounts Manager (SAM) databases of computer objects in the organizational unit, not the domain password policies. Windows Server 2003 does not process any changes that you make to these three settings in a GPO at the site level.

Additional reading

For more information about security template best practices, see the TechNet article “Best practices for Security Templates” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/sag_SCEbp.asp.

How to Create a Custom Security Template



Your instructor will demonstrate how to:

- Customize a predefined security template
- Create a new security template

Introduction

If the predefined templates are insufficient for your security needs, you must create custom templates.

Procedure for customizing a predefined template

To customize a predefined security template:

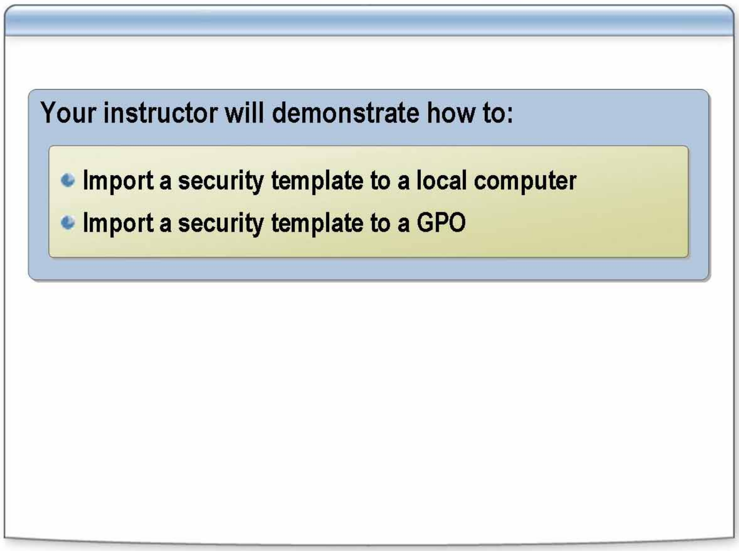
1. In a Microsoft Management Console (MMC), add the Security Templates snap-in.
2. In the console tree, expand **Security Templates**, and then double-click the default path folder (*systemroot*/Security/Templates).
3. In the details pane, right-click the predefined template you want to modify, and then click **Save As**.
4. In the **Save As** dialog box, type a new file name for the security template, and then click **Save**.
5. In the console tree, double-click the new security template to display the security policies, and navigate until the security attribute you want to modify appears in the details pane.
6. In the details pane, right-click the security attribute, and then click **Properties**.
7. In the **Properties** dialog box, select the **Define this policy setting in the template** check box, make your changes, and then click **OK**.
8. In the console tree, right-click the new security template, and then click **Save**.

Procedure for creating a new security template

To create a new security template:

1. In an MMC console, add the Security Templates snap-in.
2. In the console tree, expand **Security Templates**, right-click the default path folder (*systemroot*/Security/Templates), and then click **New Template**.
3. In the *systemroot*/**security/templates** dialog box, in the **Template Name** box, type the template name and description and then click **OK**.
4. In the console tree, double-click the new security template to display the security policies, and navigate until the security attribute you want to modify appears in the details pane.
5. In the details pane, right-click the security attribute, and then click **Properties**.
6. In the **Properties** dialog box, select the **Define this policy setting in the template** check box, make your changes, and then click **OK**.
7. In the console tree, right-click the new security template, and then click **Save**.

How to Import a Security Template



Your instructor will demonstrate how to:

- Import a security template to a local computer
- Import a security template to a GPO

Introduction

When you import a security template to a local computer, you can apply the template settings to the local computer. When you import a security template into a GPO, the settings in the template are applied to computers in the containers to which the GPO is linked.

Procedure for importing a template to a local computer

To import a security template to a local computer:

1. Open Security Configuration and Analysis.
2. In the console tree, right-click **Security Configuration and Analysis**, and then click **Import Template**.
3. (Optional) To clear the database of any template, select the **Clear this database before importing** check box.
4. In the **Import Template** dialog box, click a template file, and then click **Open**.
5. Repeat these steps for each template that you want to merge into the database.

Procedure for importing a template to a GPO without GPMC installed

To import a security template into a GPO when Group Policy Management is not installed:

1. Open Active Directory Users and Computers or Active Directory Sites and Services from the **Administrative Tools** menu.
2. Edit the appropriate GPO.
3. Expand **Computer Configuration**, and then expand **Windows Settings**.
4. Right-click **Security Settings**, and then click **Import Policy**.
5. Click a template, and then click **Open**.

   The template settings are applied to the GPO and will be applied the next time the computer is started.

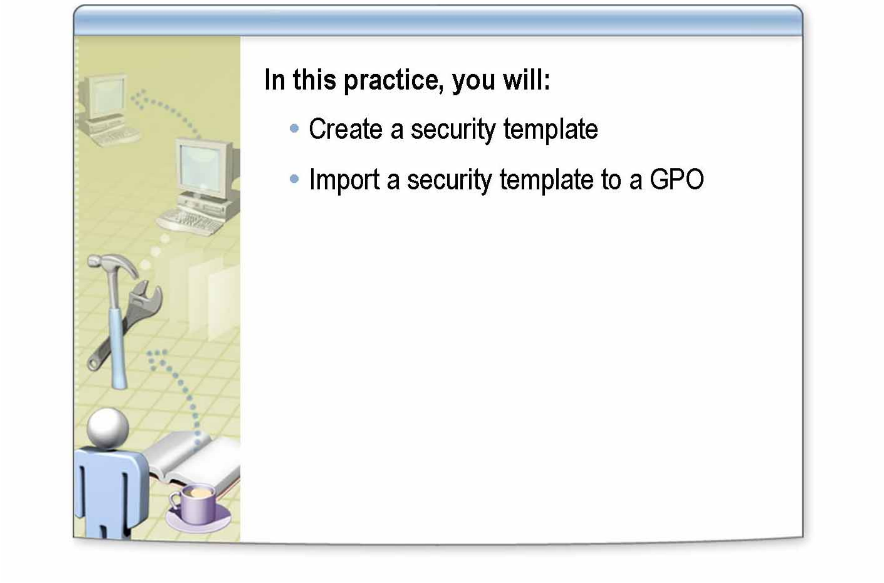
Procedure for importing a template to a GPO with GPMC

To import a security template into a GPO when Group Policy Management is installed:

1. In Group Policy Management, edit the appropriate GPO.
2. Expand **Computer Configuration**, and then expand **Windows Settings**.
3. Right-click **Security Settings**, and then click **Import Policy**.
4. Click a template, and then click **Open**.

   The template settings are applied to the GPO and will be applied the next time the computer is started.

Practice: Using Security Templates to Secure Computers



In this practice, you will:

- Create a security template
- Import a security template to a GPO

Objective

In this practice, you will:

- Create a security template.
- Import a security template to a GPO.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Open a command prompt with the Run as command.

  From the **Start** menu click **Run**, and then type **runas /user:nwtraders\***ComputerName***Admin cmd** and click **OK**. When prompted for a password, type **P@ssw0rd** and press **ENTER**.
- Review the procedures in this lesson that describe how to perform this task.

Practice: Creating a custom template on a local computer

► **Check the local group membership of the Power Users local group**

1. To verify that NWTraders\G IT Admins is not a member of the Power Users group from a command prompt type **net localgroup “power users”**
2. There should be no members listed under Members.
3. With a default installation of the operating system, the Power Users group should not contain any members.
4. Leave the command prompt open.

► Create a new security template called *ComputerName*

1. In CustomMMC, add the Security Templates snap-in.
2. In Security Templates, in the console tree, right-click **C:\WINDOWS\cecurity\templates**, and then click **New Template**.
3. In the **C:\WINDOWS\security\templates** dialog box, in the **Template Name** box, type *ComputerName* and then click **OK**.

► Edit the *ComputerName* custom security template

1. In Security Templates, in the console tree, expand *ComputerName*, and then click **Restricted Groups**.
2. Right-click **Restricted Groups**, and then click **Add Group**.
3. In the **Add Group** dialog box, type **Power Users** and then click **OK**.
4. In the **Power Users Properties** dialog box, under **Members of this group**, click **Add Members**.
5. In the **Add Member** dialog box, type **NWTRADERS\G IT Admins** and then click **OK**.
6. In the **Power Users Properties** dialog box, click **OK**.
7. In the console tree, right-click *ComputerName*, and then click **Save**.

► Import and apply the *ComputerName* custom security template

1. In CustomMMC, add the Security Configuration and Analysis snap-in.
2. Right-click **Security Configuration and Analysis**, and then click **Open Database**.
3. In the **Open database** box, type *ComputerName* and then click **Open**.
4. In the **Import Template** dialog box, click *ComputerName***.inf**, and then click **Open**.
5. Right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**.
6. In the message box, click **OK**.
7. Right-click **Security Configuration and Analysis**, and then click **View Log File**.
8. In the details pane for **Security Configuration and Analysis**, verify that the NWTRADERS\G IT Admins group was added to the Power Users group by looking for the following log file entry:

   ```
   ----Configure Group Membership...
   Configure Power Users.
   add NWTRADERS\G IT Admins.
   ```

► Check the local group membership of the Power Users local group

1. To verify that NWTraders\G IT Admins is a member of the Power Users group, from a command prompt type **net localgroup "Power Users"**
2. NWTraders\G IT Admins should be listed under Members.
3. Leave the command prompt open.

► Remove the imported custom security template

1. From a Command prompt type **net localgroup "power users" /delete "g it admins"**
2. Leave the command prompt open.

► Check the local group membership of the Power Users local group

1. To verify that NWTraders\G IT Admins is not a member of the Power Users group from a command prompt type **net localgroup "power users"**
2. There should be no members listed under Members.
3. Leave the command prompt open.

Practice: Importing a custom template to a GPO

► Import a security template to a GPO

1. In Group Policy Management, create a GPO called *ComputerName* **Restricted Users**.
2. Link the *ComputerName* Restricted Users GPO to the Locations/*ComputerName*/Computers organizational unit.
3. Edit the *ComputerName* Restricted Users GPO.
4. Import the custom security policy named *ComputerName*.inf.

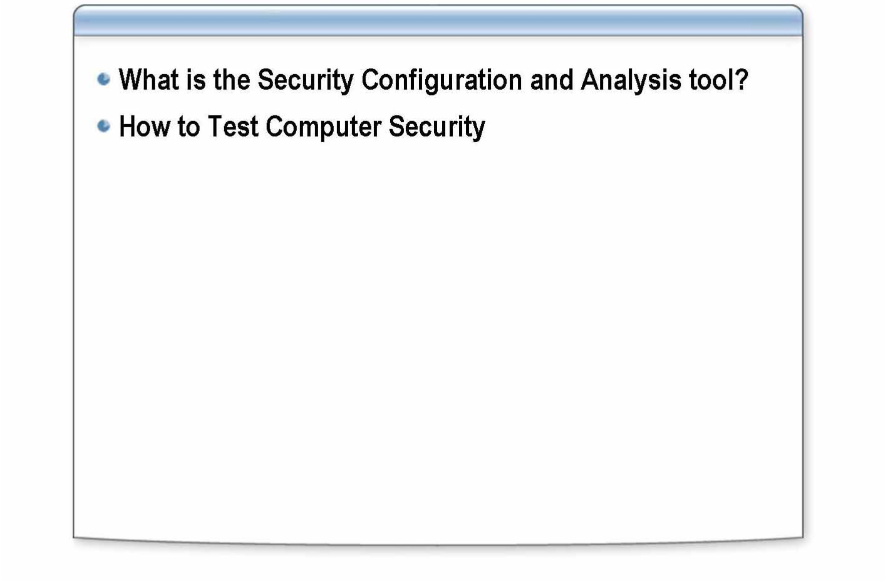
► Move your *ComputerName* computer account

1. Search for your *ComputerName* computer account in the nwtraders.msft domain.
2. Move your *ComputerName* computer account to the Locations/*ComputerName*/Computers organizational unit.
3. From a command prompt, type **gpupdate /force**
4. If prompted to logoff, type **N** and then press **ENTER**.

► Check the local group membership of the Power Users local group

1. To verify that NWTraders\G IT Admins is a member of the Power Users group, from a command prompt type **net localgroup "power users"**
2. NWTraders\G IT Admins should be listed under Members.
3. Close the command prompt

Lesson: Testing Computer Security Policy



- What is the Security Configuration and Analysis tool?
- How to Test Computer Security

Introduction

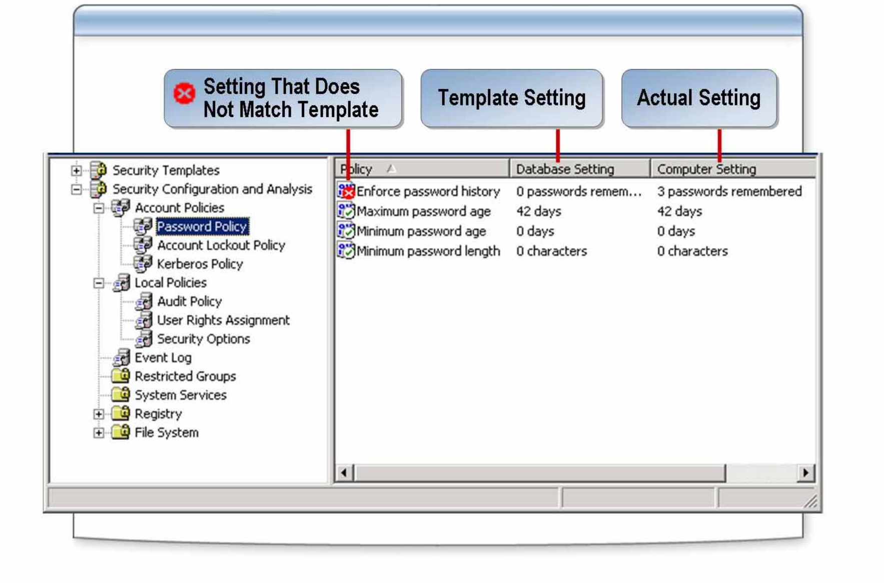
Before deploying a security template to large groups of computers, it is important to analyze the results of applying a configuration to ensure there are no adverse effects on applications, connectivity, or security. A thorough analysis also helps you identify security holes and deviations from standard configurations. You can use the Security Configuration and Analysis snap-in to create and review possible scenarios and adjust a configuration.

Lesson objectives

After completing this lesson, you will be able to:

- What is the Security Configuration and Analysis tool?
- Test computer security with the Security Configuration and Analysis tool.

What is the Security Configuration and Analysis tool?



Policy	Database Setting	Computer Setting
Enforce password history	0 passwords remem...	3 passwords remembered
Maximum password age	42 days	42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters

Introduction

The most common tool that is used to analyze computer security is the Security Configuration and Analysis tool.

Security Configuration and Analysis tool

The Security Configuration and Analysis tool compares the security configuration of the local computer to an alternate configuration that is imported from a template (an .inf file) and stored in a separate database (an .sdb file). When analysis is complete, you can browse the security settings in the console tree to see the results. Discrepancies are marked with a red flag. Consistencies are marked with a green check mark. Settings that are not marked with either a red flag or a green check mark are not configured in the database.

Why use Security Configuration and Analysis tool?

After analyzing the results by using the Security Configuration and Analysis tool, you can perform various tasks, including:

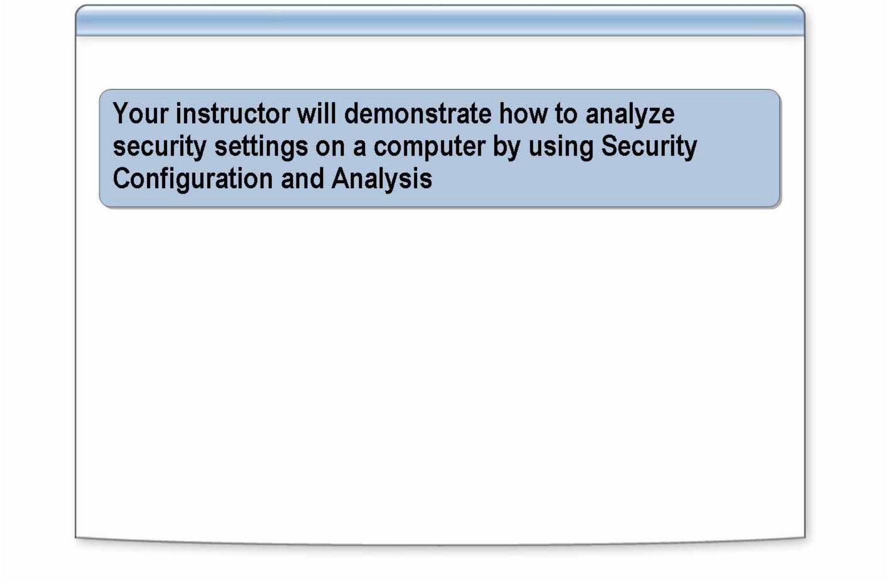
- Eliminate discrepancies by configuring the settings in the database to match the current computer settings. To configure database settings, double-click the setting in the details pane.
- Import another template file, merging its settings and overwriting settings where there is a conflict. To import another template file, right-click **Security Configuration and Analysis**, and then click **Import Template**.
- Export the current database settings to a template file. To export another template file, right-click **Security Configuration and Analysis**, and then click **Export Template**.

Additional reading

For more information about the security tools, see:

- “Security Configuration Manager” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/SEconcepts_SCM.asp.
- “Best Practices for Security Configuration and Analysis” at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SCMbp.asp.

How to Test Computer Security



Your instructor will demonstrate how to analyze security settings on a computer by using Security Configuration and Analysis

Introduction

Sometimes you must analyze a computer to see what security settings on a server are different from the settings in a base security template. To do this, you run the Security Configuration and Analysis tool.

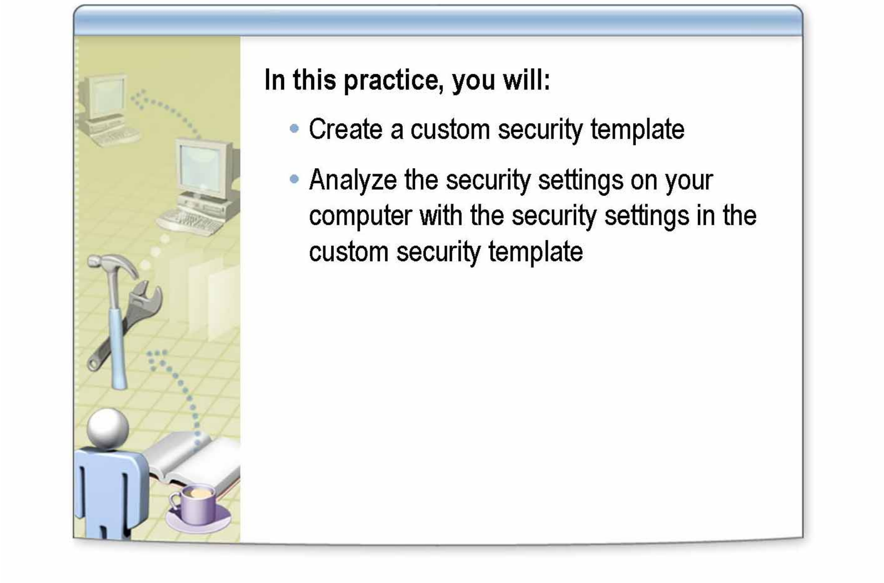
Procedure

To analyze security by using Security Configuration and Analysis:

1. Add the Security Configuration and Analysis snap-in to an MMC console.
2. Right-click **Security Configuration and Analysis**, and then click **Open database**.
3. In the **Open database** dialog box, select an existing database file or type a unique name to create a new database, and then click **Open**.

   Existing databases already contain imported settings. If you are creating a new database, the **Import Template** dialog box appears. Select a database, and then click **Open**.
4. Right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
5. In the **Perform Analysis** dialog box, choose a location for the analysis log file, and then click **OK**.
6. In the console tree, expand **Security Configuration and Analysis**.
7. Navigate through the security settings in the console tree, and compare the **Database Setting** and the **Computer Setting** columns in the details pane.

Practice: Testing Computer Security



In this practice, you will:

- Create a custom security template
- Analyze the security settings on your computer with the security settings in the custom security template

Objective

In this practice, you will:

- Create a custom security template.
- Compare the security settings on your computer to the settings in the custom security template.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Review the procedures in this lesson that describe how to perform this task.

Scenario

You are a systems administrator for Northwind Traders. You must implement the following security settings on your member servers:

- Passwords must be at least 10 characters.
- A dialog box must be displayed during the logon process, informing users that unauthorized access is not allowed.
- The alerter service, which is set to start manually, must be disabled.

Practice: Creating security templates

► **Create a custom security template**

1. In the Security Template snap-in, change the following policies in the securews template:
   - Set **Account Policies/Password Policy/Minimum password length** to 10 characters.
   - Set **Local Policies/Security Options/Interactive Logon/Message text for users attempting to log on** to **Authorized Access Only**.
   - Set **Local Policies/Security Options/Interactive Logon/Message title for users attempting to log on** to *ComputerName*.
   - Set **System Services/Alerter** to **Disabled**.
2. Save the custom security template as *ComputerName***Secure**.

Scenario

Now that you have configured the template and the appropriate policy settings, you want to perform a security analysis to create a baseline for future security analysis and to verify the current configuration.

Practice: Testing computer security

► **Import and clear the current security configuration and analysis baseline database**

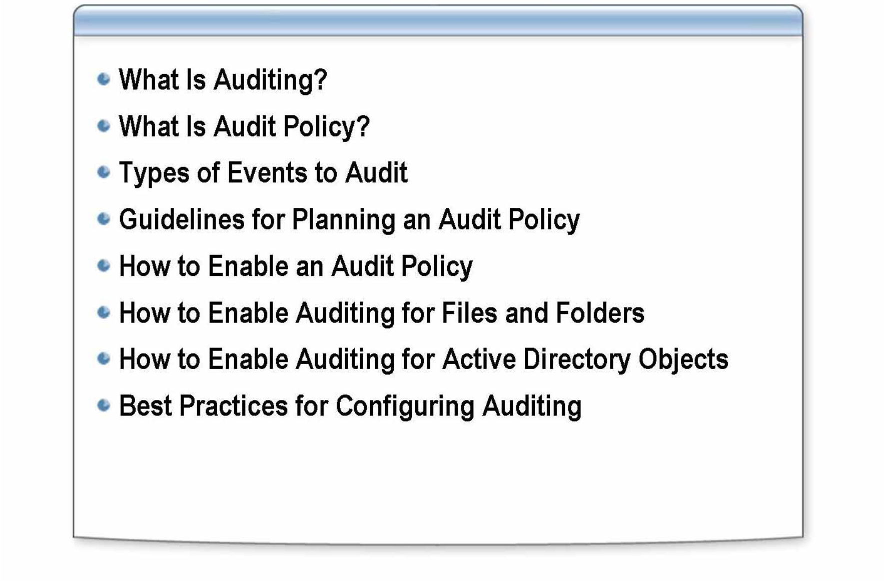
- In Security Configuration and Analysis, import the *ComputerName*Secure template and clear the database.

► **Perform the security analysis**

1. Right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
2. From **Perform Analysis** dialog box, click **OK**.
3. In Security Configuration and Analysis, expand **Local Policies**, and then click **Security Options**.
4. Notice the **Interactive logon: Message text for users attempting to log on and the Interactive logon: Message title for users attempting to log on** policies.
5. In the details pane, notice the system settings that have a red flag.

   A red flag indicates that the security template is different than the current computer settings.

Lesson: Configuring Auditing



- What Is Auditing?
- What Is Audit Policy?
- Types of Events to Audit
- Guidelines for Planning an Audit Policy
- How to Enable an Audit Policy
- How to Enable Auditing for Files and Folders
- How to Enable Auditing for Active Directory Objects
- Best Practices for Configuring Auditing

Introduction

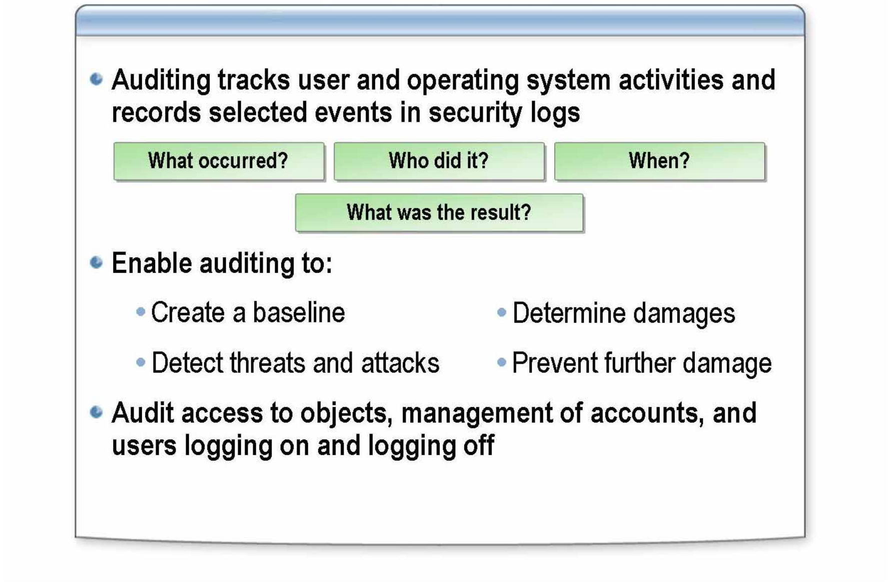
No security strategy is complete without a comprehensive auditing strategy. More often than not, organizations learn this only after they experience a security incident. Without an audit trail of actions, it is almost impossible to successfully investigate a security incident. You must determine as part of your overall security strategy what events you need to audit, the level of auditing appropriate for your environment, how the audited events and collected, and how they are reviewed.

Lesson objectives

After completing this lesson, you will be able to:

- Describe auditing.
- Describe what an audit policy is.
- Describe types of events to audit.
- Identify the guidelines for planning an audit policy.
- Enable an audit policy.
- Enable auditing for files and folders.
- Enable auditing for an organizational unit.
- Apply best practices while configuring auditing.

What Is Auditing?



- Auditing tracks user and operating system activities and records selected events in security logs

What occurred? Who did it? When?

What was the result?

- Enable auditing to:
  - Create a baseline
  - Determine damages
  - Detect threats and attacks
  - Prevent further damage
- Audit access to objects, management of accounts, and users logging on and logging off

Definition

Auditing is the process that tracks user and operating system activities by recording selected types of events in the security log of a server or a workstation. Security logs contain various audit entries, which contain the following information:

- The action that was performed
- The user who performed the action
- The success or failure of the event and when the event occurred
- Additional information, such as the computer where the event occurred

Why perform auditing?

Enable auditing and monitor audit logs to:

- Create a baseline of normal network and computer operations.
- Detect attempts to penetrate the network or computer.
- Determine what systems and data have been compromised during or after a security incident.
- Prevent further damage to networks or computers after an attacker has penetrated the network.

The security needs of an organization help determine the amount of auditing used. For example, a minimum-security network may choose to audit failed logon attempts to monitor against potential brute force attacks. A high-security network may choose to audit both successful and failed logon attempts to track any unauthorized users who successfully gain access to the network.

Although auditing may provide valuable information, excessive auditing fills the audit log with unnecessary information. This can potentially affect the performance of your system and make it extremely difficult to find relevant information.

Types of events to audit

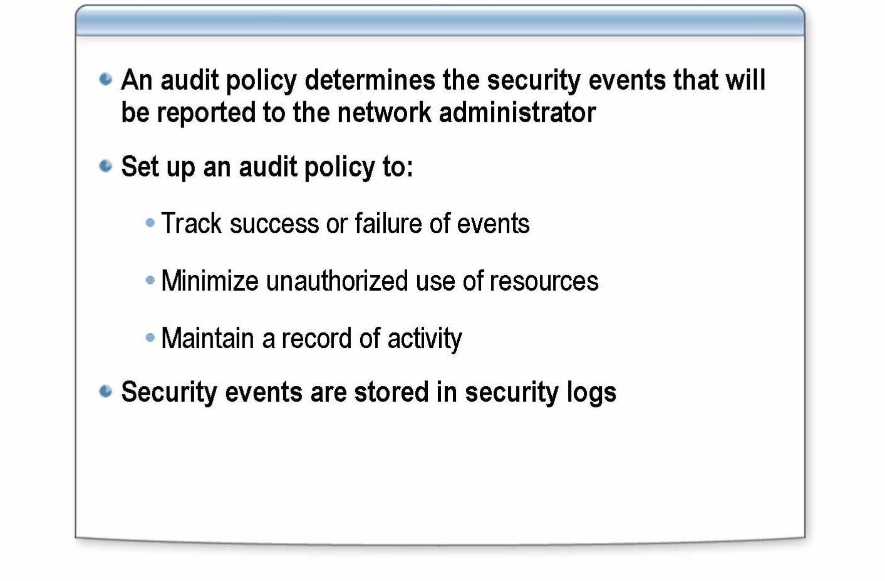
The most common types of events to audit are when:

- Objects, such as files and folders, are accessed
- Managing user accounts and group accounts
- Users log on to and log off from the system

Additional reading

For more information about auditing, see the TechNet article "Auditing overview" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SEconceptsAudit.asp.

What Is Audit Policy?



- **An audit policy determines the security events that will be reported to the network administrator**
- **Set up an audit policy to:**
  - Track success or failure of events
  - Minimize unauthorized use of resources
  - Maintain a record of activity
- **Security events are stored in security logs**

Introduction

Establishing an audit policy is an important part of security. Monitoring the creation or modification of objects gives you a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach.

Definition

An audit policy defines the types of security events that Windows Server 2003 records in the security log on each computer. Windows Server 2003 writes events to the security log on the specific computer where the event occurs.

Why set up an audit policy?

Set up an audit policy for a computer to:

- Track the success and failure of events, such as attempts to log on, attempts by a particular user to read a specific file, changes to a user account or group membership, and changes to security settings.
- Minimize the risk of unauthorized use of resources.
- Maintain a record of user and administrator activity.

Use Event Viewer to view events that Windows Server 2003 records in the security log. You can also archive log files to track trends over time. This is useful to determine trends in the use of printers, access to files, and attempts at unauthorized use of resources.

How can you implement an audit policy?

You can set up an audit policy on any single computer, either directly by using the Local Policy snap-in or indirectly by using Group Policy, which is more commonly used in large organizations. After an audit policy is designed and implemented, information begins to appear in the security logs. Each computer in the organization has a separate security log that records local events.

When you implement an audit policy:

- Specify the categories of events that you want to audit. Examples of event categories are user logon, user logoff, and account management. The event categories that you specify constitute your audit policy. There is no default audit policy.
- Set the size and behavior of the security log. You can view the security log with Event Viewer.
- Determine which objects you want to monitor access of and what type of access you want to monitor, if you want to audit directory service access or object access. For example, if you want to audit attempts by users to open a particular file, you can configure audit policy settings in the object access event category so that successful and failed attempts to read a file are recorded.

Default audit policies

The default auditing settings for servers are configured by administrative templates. The following security templates configure default auditing settings:

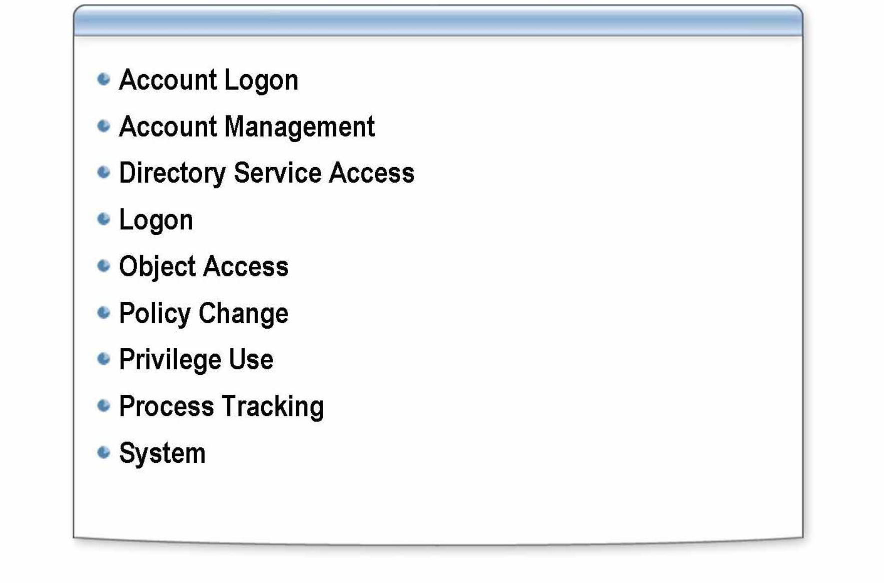
- Setup security.inf
- Hisecdc.inf
- Hisecws.inf
- Secuerdc.inf
- Securews.inf

To view the policy settings that each security template configures, in the Security Templates snap-in, navigate to Local Policies\Audit Policy for each administrative template.

Additional reading

For more information about audit policies, see the TechNet article "Auditing policy" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/APtopnode.asp.

Types of Events to Audit



- Account Logon
- Account Management
- Directory Service Access
- Logon
- Object Access
- Policy Change
- Privilege Use
- Process Tracking
- System

Introduction

The first step in creating a strategy for auditing the operating system is to determine what type of actions or operations that you need to record.

Determining what events to audit

What operating system events should you audit? You do not want to audit every event, because auditing all operating system events requires enormous system resources and may negatively affect system performance. You should work with other security specialists to determine what operating system events to audit. Only audit events that you believe will be useful for later reference.

An effective way to begin determining what events to audit is to gather the relevant group of people and discuss:

- What actions or operations you want to track.
- On what systems you want to track these events.

For example, you may decide to track:

- All domain and local logon events on all computers.
- The use of all files in the Payroll folder on the HR server.

The success and failure events

In Windows Server 2003, audit events can be split into two categories:

- Success events

  A success event indicates that the operating system has successfully completed the action or operation. Success events are indicated by a key icon.

- Failure events

  A failure event indicates that an action or operation was attempted, but did not succeed. Failure events are indicated by a padlock icon.

Failure events are very useful for tracking attempted attacks on your environment, but success events are much more difficult to interpret. The vast majority of success events are indications of normal activity, and an attacker who accesses a system also generates a success event.

Often, a pattern of events is as important as the events themselves. For example, a series of failures followed by a success may indicate an attempted attack that was eventually successful.

Similarly, the deviation from a pattern may also indicate suspicious activity. For example, suppose the security logs show that a user at your organization logs on every workday between 8 A.M. and 10 A.M., but suddenly the user is logging on to the network at 3 A.M. Although this behavior may be innocent, it should be investigated.

Events that Windows Server 2003 can audit

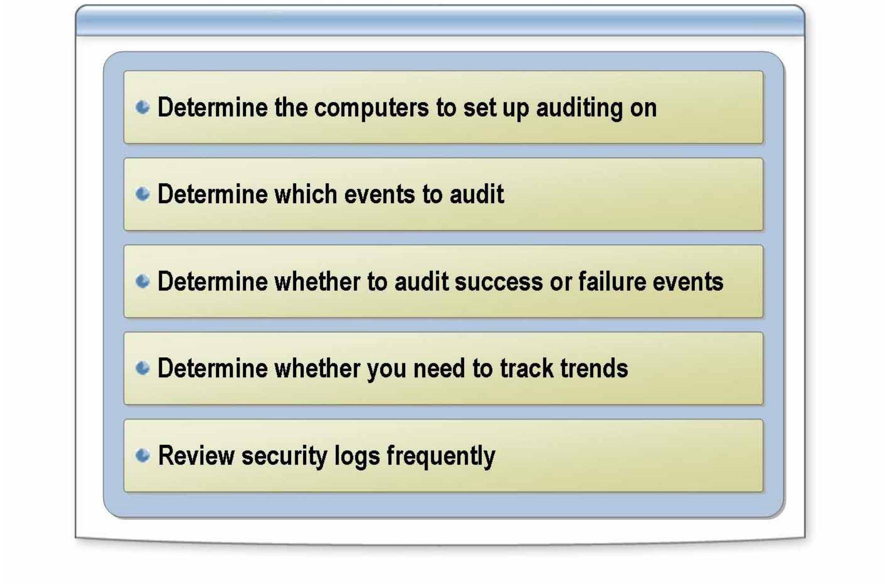
The first step in implementing an audit policy is to select the types of events that you want Windows Server 2003 to audit. The following table describes the events that Windows Server 2003 can audit.

Event	Example
Account Logon	An account is authenticated by a security database. When a user logs on to the local computer, the computer records the AccountLogon event. When a user logs on to a domain, the authenticating domain controller records the Account Logon event.
Account Management	An administrator creates, changes, or deletes a user account or group; a user account is renamed, disabled, or enabled; or a password is set or changed.
Directory Service Access	A user accesses an Active Directory object. To log this type of access, you must configure specific Active Directory objects for auditing.
Logon	A user logs on to or off of a local computer, or a user makes or cancels a network connection to the computer. The event is recorded on the computer that the user accesses, regardless of whether a local account or a domain account is used.
Object Access	A user accesses a file, folder, or printer. The administrator must configure specific files, folders, or printers for auditing.
Policy Change	A change is made to the user security options (for example, password options or account logon settings), user rights, or audit policies.
Privilege Use	A user exercises a user right, such as changing the system time (this does not include rights that are related to logging on and logging off) or taking ownership of a file.
Process Tracking	An application performs an action. This information is generally only useful for programmers who want to track details about application execution.
System	A user restarts or shuts down the computer, or an event occurs that affects Windows Server 2003 security or the security log.

Events edited by default

The Setup security.inf template includes default settings that enable auditing of successful account logon events and successful logon events. No other events are audited by default.

Guidelines for Planning an Audit Policy



- Determine the computers to set up auditing on
- Determine which events to audit
- Determine whether to audit success or failure events
- Determine whether you need to track trends
- Review security logs frequently

Introduction

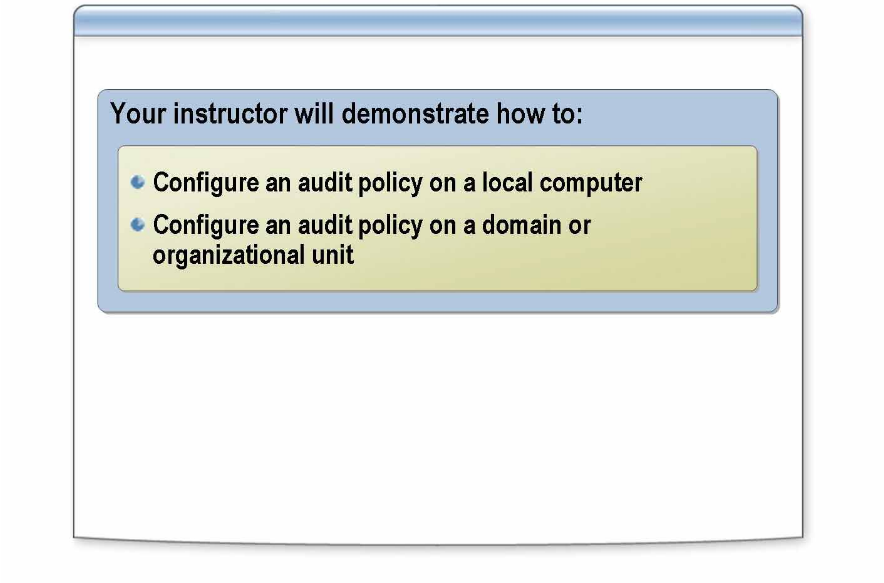
Auditing too many types of events may create excess overhead, which may result in diminished system performance.

Guidelines

Use the following guidelines when planning an audit policy:

- Determine the computers to set up auditing on. Plan what to audit for each computer, because Windows Server 2003 audits events on each computer separately. For example, you may frequently audit computers used to store sensitive or critical data, but you may infrequently audit client computers that are used solely for running productivity applications.
- Determine the types of events to audit, such as the following:
  - Access to files and folders
  - Users logging on and off
  - Shutting down and restarting a computer running Windows Server 2003
  - Changes to user accounts and groups
- Determine whether to audit success or failure events, or both. Tracking success events can tell you how often Windows Server 2003 or users access specific files or printers. You can use this information for resource planning. Tracking failure events can alert you to possible security breaches.
- Determine whether you need to track trends of system usage. If so, plan to archive event logs. Some organizations are required to maintain a record of resource and data access.
- Review security logs frequently and regularly according to a schedule. Configuring auditing alone does not alert you to security breaches.

How to Enable an Audit Policy



Your instructor will demonstrate how to:

- Configure an audit policy on a local computer
- Configure an audit policy on a domain or organizational unit

Introduction

There are two procedures for enabling an audit policy, depending on whether the computer is in a workgroup or a domain.

Procedure for an audit policy on a local computer

To enable an audit policy on a local computer:

1. From the **Administrative tools** menu, click **Local Security Policy**.
2. In the console tree, expand **Local Policies**, and then double-click **Audit Policy**.
3. In the details pane, double-click the policy that you want to enable or disable.
4. Do one or both of the following, and then click **OK**:
   - To audit success events, select the **Success** check box.
   - To audit failure events, select the **Failure** check box.

   For example, suppose you select the **Success** and **Fail** check boxes for logon and logoff events. If a user successfully logs on to the system, it is logged as a success audit event. If a user tries to access a network drive and fails, the attempt is logged as a failure audit event.

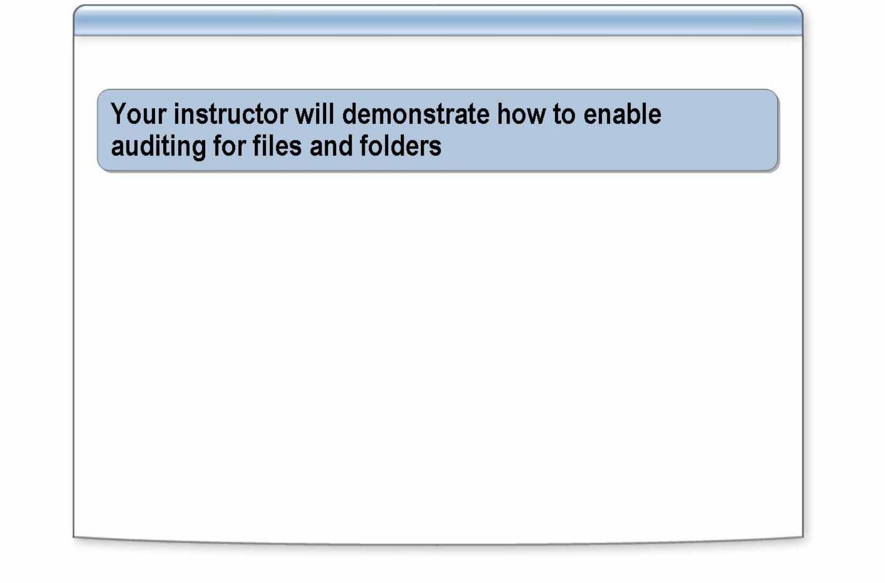
Note If you are a member of a domain, and a domain-level policy is defined, domain-level settings override the local policy settings.

Procedure for an audit policy on a domain or organizational unit

To enable an audit policy on a domain or an organizational unit:

1. In Group Policy Management, create or browse to a GPO linked to an organizational unit, and then edit it.
2. In the console tree, navigate to Computer Configuration/Windows Settings/Security Settings/Local Policies/Audit Policy.
3. In the details pane, double-click the policy that you want to enable or disable.
4. Do one or both of the following, and then click **OK**:
   - To audit success events, select the **Success** check box.
   - To audit failure events, select the **Failure** check box.

How to Enable Auditing for Files and Folders



Your instructor will demonstrate how to enable auditing for files and folders

Introduction

You enable auditing to detect and record security-related events, such as when a user attempts to access a confidential file or folder. When you audit an object, an entry is written to the security log whenever the object is accessed in a certain way.

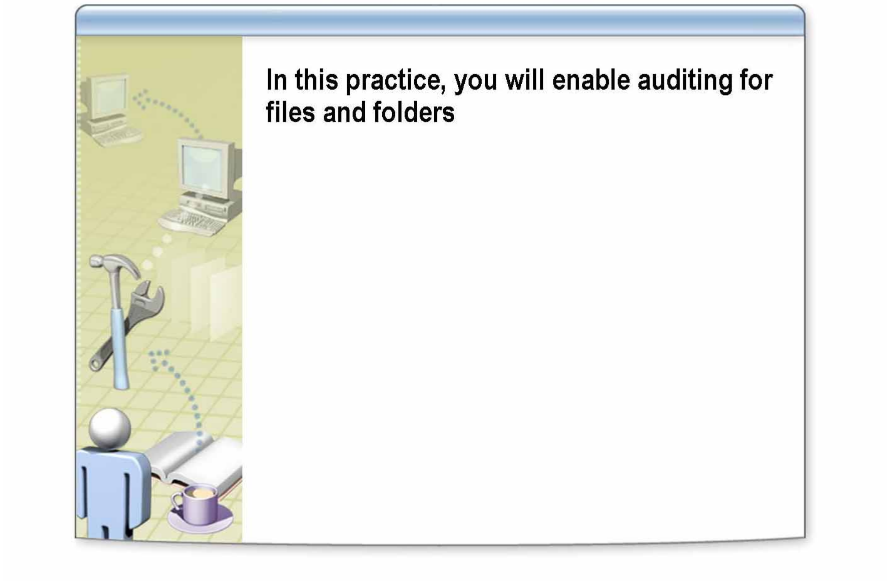
After you enable auditing, you can keep track of users who access certain objects and analyze security breaches. The audit trail shows who performed the actions and who tried to perform actions that are not permitted.

Procedure

To enable auditing for files and folders:

1. In Windows Explorer, locate the file or folder that you want to audit.
2. Right-click the file or folder, and then click **Properties**.
3. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.
4. In the **Advanced Security Settings** dialog box, on the **Auditing** tab, do one of the following:
   - To enable auditing for a new user or group, click **Add**. In the **Enter the object name to select** box, type the name of the user or group, and then click **OK**.
   - To view or change auditing for an existing group or user, click the name, and then click **Edit**.
   - To disable auditing for an existing group or user, click the name, and then click **Remove**.
5. Under **Access**, click **Successful**, **Failed**, or both **Successful** and **Failed**, depending on the type of access that you want to audit.
6. If you want to prevent child objects from inheriting these audit entries, select the **Apply these auditing entries to objects and/or containers within this container only** check box.

Practice: Enabling Auditing for Files and Folders



In this practice, you will enable auditing for files and folders

Objective

In this practice, you will enable auditing for files and folders.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Ensure that the D:\HR Reports folder is created and shared from a previous practice or lab.
- Review the procedures in this lesson that describe how to perform this task.

Scenario

You get a call from the Human Resources manager, who tells you that files are being deleted. The Sales manager wants to know which user is deleting files. You must enable auditing on your server for the HR-Reports folder.

Practice

► **Create a GPO that enables an audit policy**

- Tool: Group Policy Management
- GPO name: *ComputerName* **Audit Policy**
- GPO link to the following location: Locations/*ComputerName*/Computers
- Enable auditing of the success and failure of the following security policy: Computer Configuration/Windows Settings/Security Settings/ Local Policies/Audit Policy/Audit object access

► Verify the location of the computer account

1. Ensure your computer is in the Locations/*ComputerName*/Computers organizational unit.

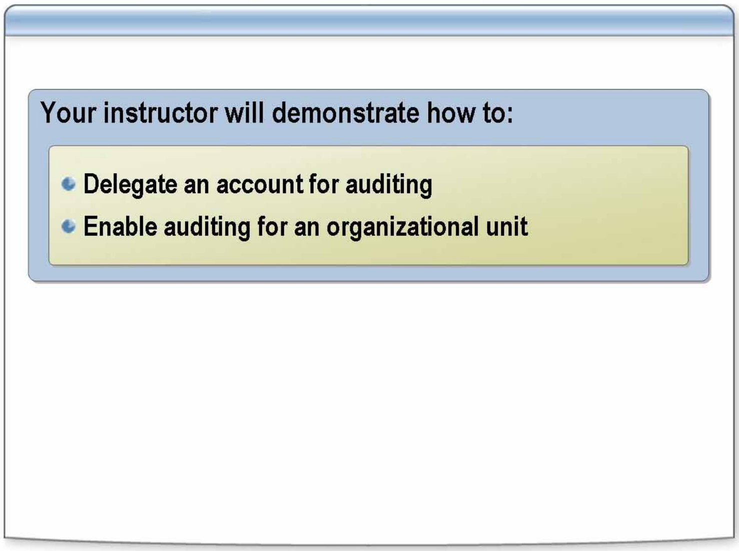
   If your computer is not in this organizational unit, search for it and move it.

2. From a command prompt, type **gpupdate /force**
3. If prompted to logoff, type **N** and press **ENTER**.

► Audit the HR-Reports folder

- Enable auditing for the folder D:\HR Reports by using the following criteria:
  - Audit the group G NWTraders HR Personnel.
  - Audit **Successful - Delete of Subfolders and Files**.
  - Audit **This folder, subfolders and files**.
  - Prevent child objects from inheriting these audit entries.

How to Enable Auditing for Active Directory Objects



Your instructor will demonstrate how to:

- Delegate an account for auditing
- Enable auditing for an organizational unit

Introduction

When you enable auditing for an organizational unit, you audit the event generated when a user accesses an Active Directory object that has permissions. By default, auditing is set to Success in the Default Domain Controller GPO, and it remains undefined for workstations and servers where it does not apply.

Note By default, only members of the Administrators group have privileges to configure auditing. You can delegate the task of configuring auditing for server events to another user account by assigning the Manage auditing and security log user right in Group Policy.

Procedure for delegating an account to enable auditing

To enable nonadministrators to manage and view audit logs on a member server, you must first delegate the authority to a user or group. To do this:

1. In Group Policy Object Editor, in the console tree, navigate to the following:

   Computer Configuration/Windows Settings/Security Settings/
   Local Polices/User Rights Assignment

2. Click **Manage auditing and security log**.
3. On the **Action** menu, click **Properties**.
4. In the **Manage auditing and security log** dialog box, select the check box, **Define these policy settings**, and then click **Add User or Group**.
5. Type the name of the appropriate user or user group from the list, and then click **OK**.
6. Click **OK**.

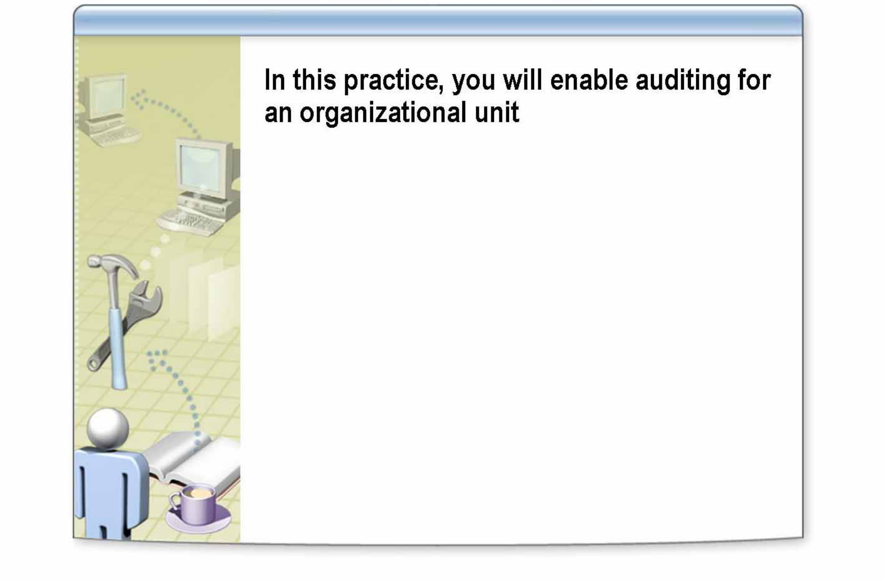
Procedure for enabling auditing for an organizational unit

To enable auditing for an organizational unit:

1. In Active Directory Users and Computers, right-click the organizational unit that you want to audit, and then click **Properties**.
2. In the **Properties** dialog box, on the **Security** tab, click **Advanced**.

   To view the security properties, you must click **Advanced Features** on the **View** menu of Active Directory Users and Computers.
3. In the **Advanced Security Settings** dialog box, on the **Auditing** tab, do one of the following:
   - To enable auditing for a new user or group, click **Add**. In the **Enter the object name to select** box, type the name of the user or group, and then click **OK**.
   - To remove auditing for an existing group or user, click the group or user name, click **Remove**, and click **OK**. Skip the rest of this procedure.
   - To view or change auditing for an existing group or user, click the group or user name, and then click **Edit**.
4. In the **Apply onto** box, click the location where you want auditing to take place.
5. Under **Access**, indicate what actions you want to audit by selecting the appropriate check boxes:
   - To audit success events, select the **Successful** check box.
   - To stop auditing success events, clear the **Successful** check box.
   - To audit failure events, select the **Failed** check box.
   - To stop auditing failure events, clear the **Failed** check box.
   - To stop auditing all events, click **Clear All**.
6. If you want to prevent child objects from inheriting these audit entries, select the **Apply these auditing entries to objects and/or containers within this container only** check box.

Practice: Enabling Auditing for an Organizational Unit



In this practice, you will enable auditing for an organizational unit

Objectives

After completing this practice, you will be able to configure an audit policy that audits the creation and deletion of objects in an organizational unit.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command using Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Review the procedures in this lesson that describe how to perform this task.

Scenario

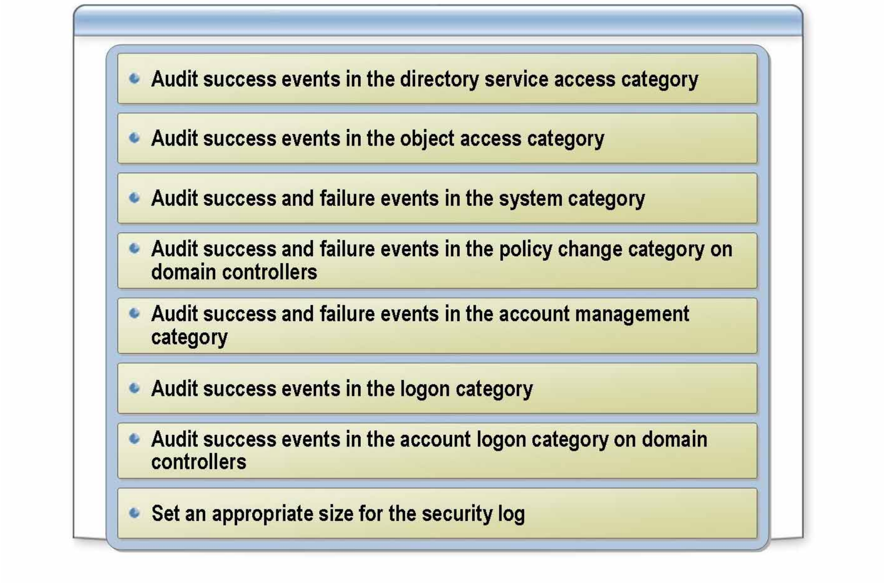
You are concerned that someone is adding and removing user, computer, and group objects in your *ComputerName* organizational unit. You want to configure an audit policy that audits the successful and unsuccessful creation and deletion of those objects in your *ComputerName* organizational unit.

Practice

► **Enable auditing for the organizational unit *ComputerName***

- Enable auditing by using the following criteria:
  - Audit the Everyone group.
  - Audit the *ComputerName* organizational unit and all child objects.
  - Audit the following access properties for success and failure events:
    - Create Account Objects
    - Delete Account Objects
    - Create Computer Objects
    - Delete Computer Objects
    - Create Group Objects
    - Delete Group Objects

Best Practices for Configuring Auditing



- Audit success events in the directory service access category
- Audit success events in the object access category
- Audit success and failure events in the system category
- Audit success and failure events in the policy change category on domain controllers
- Audit success and failure events in the account management category
- Audit success events in the logon category
- Audit success events in the account logon category on domain controllers
- Set an appropriate size for the security log

Best practices

Apply the following best practices while performing auditing:

- Audit success events in the directory service access category.

  By auditing success events in the directory service access category, you can find out who accessed an object in Active Directory and what operations were performed.

- Audit success events in the object access category.

  By auditing success events in the object access category, you can ensure that users are not misusing their access to secured objects.

- Audit success and failure events in the system category.

  By auditing success and failure events in the system category, you can detect unusual activity that indicates that an attacker is attempting to gain access to your computer or network.

- Audit success and failure events in the policy change category on domain controllers.

  If an event is logged in the policy change category, someone has changed the Local Security Authority (LSA) security policy configuration. If you use Group Policy to edit your audit policy settings, you do not need to audit events in the policy change category on member servers.

- Audit success and failure events in the account management category.

  By auditing success events in the account management category, you can verify changes that are made to account properties and group properties. By auditing failure events in the account management category, you can see if unauthorized users or attackers are trying to change account properties or group properties.

- Audit success events in the logon category.

  By auditing success events in the logon category, you have a record of when each user logs on to or logs off from a computer. If an unauthorized person steals a user's password and logs on, you can find out when the security breach occurred.

- Audit success events in the account logon category on domain controllers.

  By auditing success events in the account logon category, you can see when users log on to or log off from the domain. You do not need to audit events in the account logon category on member servers.

- Set an appropriate size for the security log.

  It is important to configure the size of the security log appropriately, based on the number of events that your audit policy settings generate.

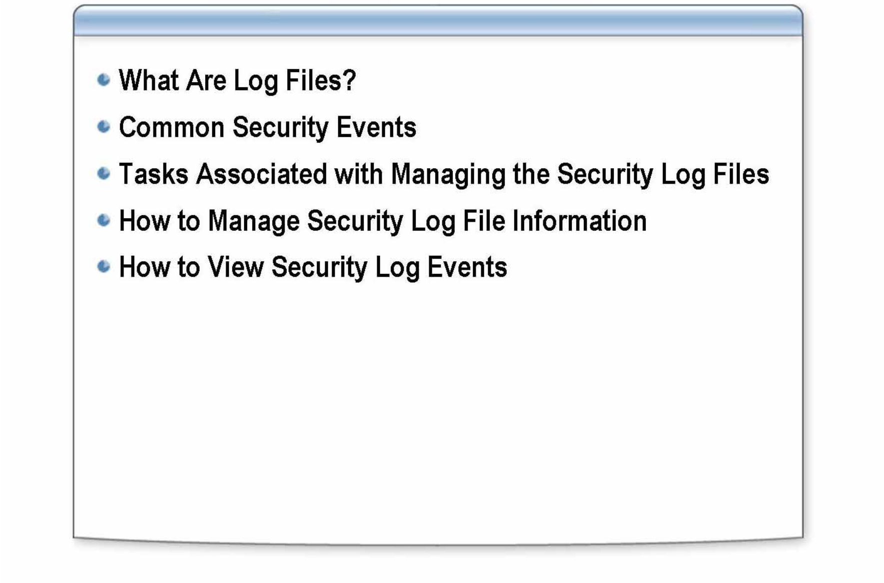
Additional reading

For more information about audit policy best practices, see the TechNet article "Best practices" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SEconceptsImpAudBP.asp.

For more information about managing audit logs see:

- TechNet article "Microsoft Operations Manager 2000" at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/mom/evaluate/mom2k.asp.
- Article 325898, "HOW TO: Set Up and Manage Operation-Based Auditing for Windows Server 2003, Enterprise Edition" in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=325898.

Lesson: Managing Security Logs



- What Are Log Files?
- Common Security Events
- Tasks Associated with Managing the Security Log Files
- How to Manage Security Log File Information
- How to View Security Log Events

Introduction

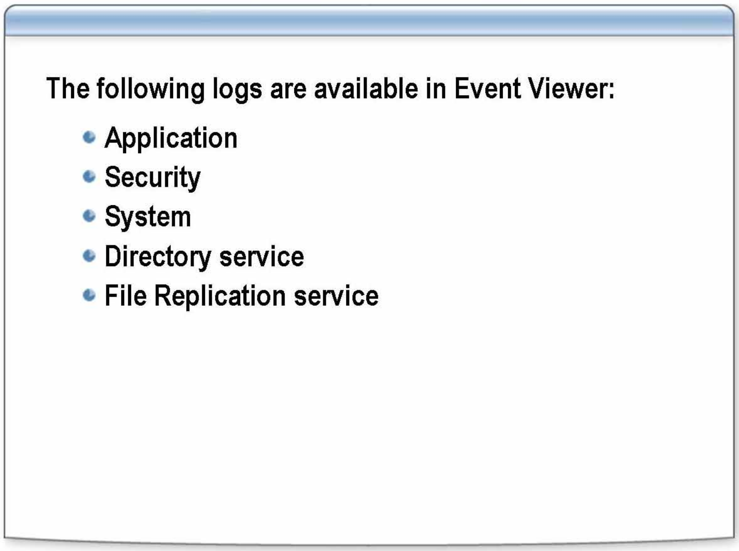
You can configure the security logs to record information about Active Directory and server events. These events are recorded in the Windows security log. The security log can record security events, such as valid and invalid logon attempts, as well as events that are related to resource use, such as creating, opening, or deleting files. You must log on as an administrator to control what events are audited and displayed in the security log.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the types of security log files and the information contained in each log file.
- Identify common security events.
- Describe tasks associated with managing the security log files.
- Manage security log file information.
- View security log events.

What Are Log Files?



The following logs are available in Event Viewer:

- Application
- Security
- System
- Directory service
- File Replication service

Introduction

The security log records events, such as valid and invalid logon attempts, and events related to resource use, such as creating, opening, or deleting files or other objects. For example, if logon auditing is enabled, attempts to log on to the system are recorded in the security log. After an audit policy is designed and implemented, information begins to appear in the security log.

Each computer in the organization has a separate security log that records local events. Domain controllers hold the security log information about Active Directory.

Logs available in Event Viewer

You can view the following logs in Event Viewer, depending on the type of computer that you are using and the services that are installed on that computer:

- Application

  Contains events generated by applications installed on the computer, including server applications, such as Microsoft Exchange Server or Microsoft SQL Server™, and desktop applications, such as Microsoft Office.

- Security

  Contains events generated by auditing. These events include logons and logoffs, access to resources, and changes in policy.

- System

  Contains events generated by components and services in Windows Server 2003.

- Directory service

  Appears only on domain controllers. The directory service event log contains, for example, Active Directory replication.

- File Replication service

  Appears only on domain controllers. The file replication service event log contains, for example, events that are related to the replication of Group Policy.

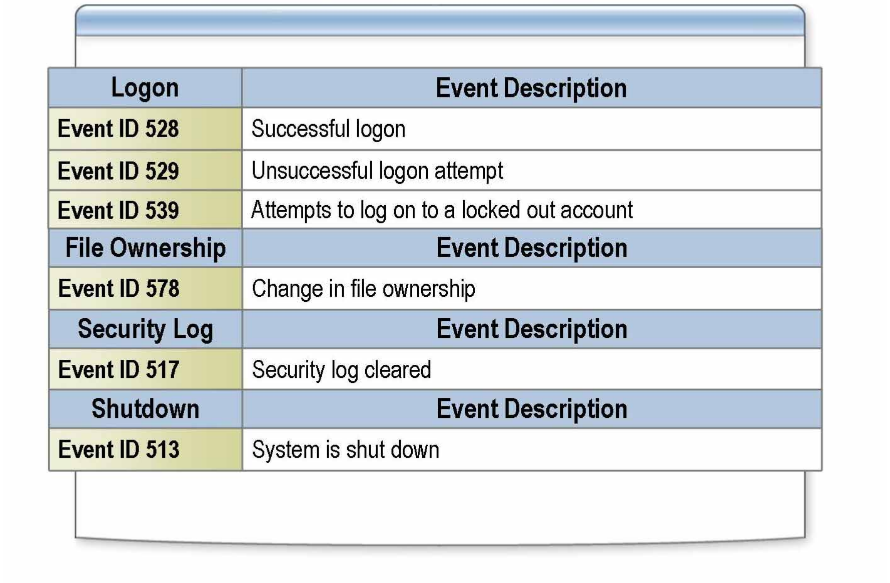
Tip If you decide to use auditing extensively, increase the size of the security log in the Event Log section of the security policy for the Default Domain Controllers GPO.

Security log files format

Security log files are also stored in the *systemroot*/system32/config directory. Security logs can be exported and archived in the following file formats:

- Event log files (.evt) (Default)
- Comma delimited (.csv)
- Text file (.txt)

Common Security Events



Logon	Event Description
Event ID 528	Successful logon
Event ID 529	Unsuccessful logon attempt
Event ID 539	Attempts to log on to a locked out account
File Ownership	**Event Description**
Event ID 578	Change in file ownership
Security Log	**Event Description**
Event ID 517	Security log cleared
Shutdown	**Event Description**
Event ID 513	System is shut down

Introduction

Many events appear in the security log. The following are some common scenarios that may be cause for concern and suggestions for diagnosing problems by using the event log.

Invalid logon attempts and account lockout

A successful logon generates an Event ID 528. When a user attempts to guess another user's password, they will likely make several incorrect guesses. Each incorrect guess generates an Event ID 529, which is also generated by a misspelled user name. If an account becomes locked out, subsequent attempts generate an Event ID 539.

Notice that one or two of these events might occur when a user types incorrectly, does not realize that the CAPS LOCK key is on, or forgets a password.

Change of file ownership

The owner of a file in the NTFS file system can modify the file's permissions to read and modify the file. A user who has the user right to take ownership can access any file by first taking ownership of that file. This change of ownership constitutes the use of a user right and generates an Event ID 578.

Clearing the security log

An unscrupulous administrator with the user right to clear the security log from Event Viewer can clear the log to hide his or her security-sensitive activities.

The security log must always be cleared according to a well-planned schedule and only immediately after a full copy of the log is archived. If the log is cleared under any other circumstances, the administrator must justify his or her actions. Clearing the security log generates an Event ID 517, which is the first event generated in the new log.

System shutdown

Ordinarily, mission-critical servers must be shut down only by administrators. You can prevent others from shutting down a server by assigning or denying the Shut down the system user right in the local security policy or by using Group Policy.

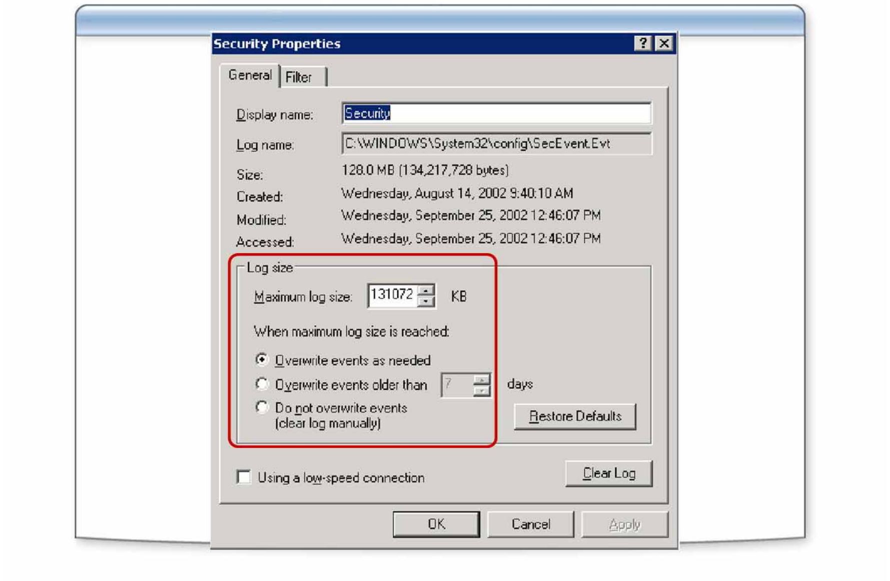
To identify if the **Shut down the system** right was mistakenly assigned, audit the system Event ID 513, which indicates who shut down the computer.

Additional reading

For more information about security events, see:

- Article 299475, “Windows 2000 Security Event Description (Part 1 of 2)” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=299475.
- Article 301677, “Windows 2000 Security Event Description (Part 2 of 2)” in the Microsoft Knowledge Base at http://support.microsoft.com/?kbid=301677.
- The TechNet article “Security Operations Guide for Windows 2000 Server” at http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp.

Tasks Associated with Managing the Security Log Files



Security Properties

General | Filter

Display name: Security

Log name: C:\WINDOWS\System32\config\SecEvent.Evt

Size: 128.0 MB (134,217,728 bytes)

Created: Wednesday, August 14, 2002 9:40:10 AM

Modified: Wednesday, September 25, 2002 12:46:07 PM

Accessed: Wednesday, September 25, 2002 12:46:07 PM

Log size

Maximum log size: 131072 KB

When maximum log size is reached:

● Overwrite events as needed

○ Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

Introduction

All events related to operating system security in Windows NT, Windows Server 2003, and Microsoft Windows XP are recorded in the security log in Event Viewer. Security-related events may also be recorded in the application and system logs.

Evaluate the configuration of the log file

Before you enable audit policies, you must evaluate whether the default configuration of the log files in Event Viewer is appropriate for your organization.

To view the log files settings in Event Viewer:

1. From the **Administrative Tools** menu, open Event Viewer.
2. Right-click the security event log, and then click **Properties**.

Log file location

By default, the security log is stored in the *systemroot*/System32/config directory in a file named SecEvent.evt. In Windows Server 2003, you can change the log file location in the security log properties. In Windows NT 4.0 and Windows Server 2000, you must edit the registry to change the location of each log file.

By default, only the System account and the Administrators group have access to the security log. This ensures that nonadministrators cannot read, write, or delete security events. If you move the log to a new location, ensure that the new file has the correct NTFS permissions. Because the Event Viewer service cannot be stopped, changes to this setting are not applied until the server is restarted.

Maximum log file size

By default, the maximum size that the security log can grow to before the overwrite behavior is initiated is 512 KB. Because hard disk space is much more readily available now than it was in the past, you will likely want to increase this setting. The amount by which you increase this setting depends on the overwrite behavior configured for the log file, but a good general guideline is to set the maximum size to at least 50 MB. You can change the maximum size of the log file on individual computers in the security log properties or on many computers by using security templates or editing the registry.

The maximum size that you should set for the combined total size of all event logs is 300 MB. Each security event is 350 to 500 bytes, so a 10-MB event log contains approximately 20,000 to 25,000 security events.

Log file overwrite behavior

When you configure the security log settings, you must define the overwrite behavior when the maximum log file size is reached. The following list describes the overwrite event options.

- **Overwrite events as needed**

  New events continue to be written when the log is full. Each new event replaces the oldest event in the log.

- **Overwrite events older than** [*x*] **days**

  Events are retained in the log for the number of days you specify before they are overwritten. The default is seven days.

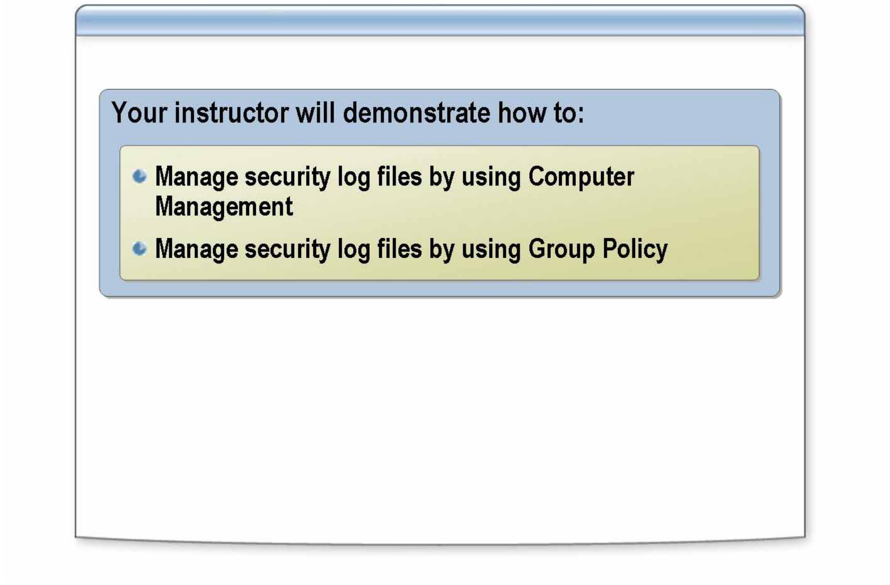
- **Do not overwrite events**

  New events are not recorded, and the event log must be cleared manually.

Delegate the right to manage the file

To delegate the rights to manage the security log file, configure the Group Policy setting **Manage auditing and security log**. This is found in Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment.

How to Manage Security Log File Information



Your instructor will demonstrate how to:

- Manage security log files by using Computer Management
- Manage security log files by using Group Policy

Introduction

The more security information you capture, the bigger the security log file you need. You want a log file to track what security events have occurred since the last archival of the events.

Procedure for using Computer Management

To manage security log file information through Computer Management:

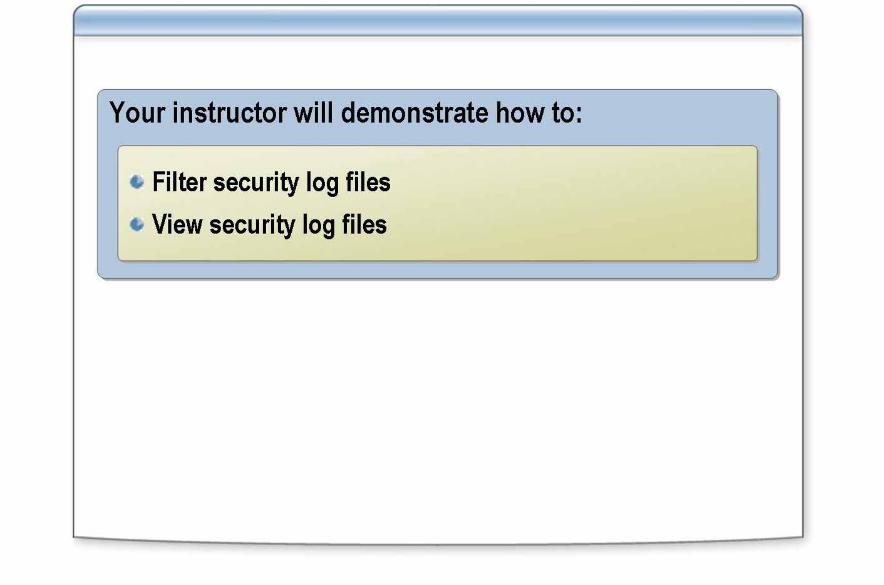
1. In Computer Management, in the console tree, expand **System Tools and Event Viewer**.
2. Right-click a log file, and then click **Properties**.
3. In the **Properties** dialog box, you can do the following:
   - Configure the maximum log file size
   - Configure overwrite behavior
   - Clear the log file

Procedure for using a GPO

To manage security log file information through a GPO:

1. Edit a GPO.
2. In Group Policy Object Editor, in the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, and then expand **Event Log**.
3. Define a parameter for the following Group Policy settings:
   - **Log size**
   - **Prevent local guest from accessing logs**
   - **Retain Log**
   - **Retention method for Log**

How to View Security Log Events



Your instructor will demonstrate how to:

- Filter security log files
- View security log files

Introduction

Security logs can get rather large, and viewing large logs or finding specific types of events in the log may be difficult. You can set a filter on the log to view specific types of events or events from specific users or groups.

Procedure for filtering the security logs

To filter the security logs:

1. In Event Viewer, in the console tree, right-click **Security**, click **View**, and then click **Filter**.
2. In the **Security Properties** dialog box, define your filter criteria, and then click **OK**.

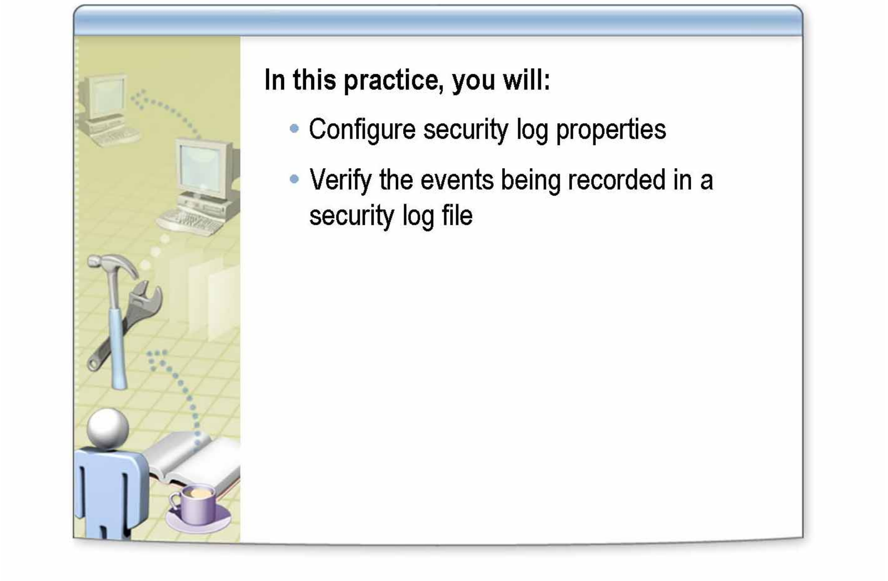
Procedure for viewing security logs

To view security logs:

1. In Event Viewer, in the console tree, click **Security**.
2. The details pane lists individual security events.

   If you want to see more details about a specific event, in the details pane, double-click the event.

Practice: Managing Log File Information



In this practice, you will:

- Configure security log properties
- Verify the events being recorded in a security log file

Objective

In this practice, you will:

- Configure security log properties.
- View security log events.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with the **Run as** command.

  Use the user account Nwtraders\ComputerNameAdmin (Example: LondonAdmin).
- Review the procedures in this lesson that describe how to perform this task.

Scenario

The network security team at Northwind Traders tells you that the security log file must have the following properties on your *ComputerName* server:

- The maximum log size must be 30,016 KB.
- The overwrite behavior is **Do not overwrite events (clear log manually)**.

They also ask you to review your security log file to determine if the security events are being logged for the folder D:\HR Reports.

Practice

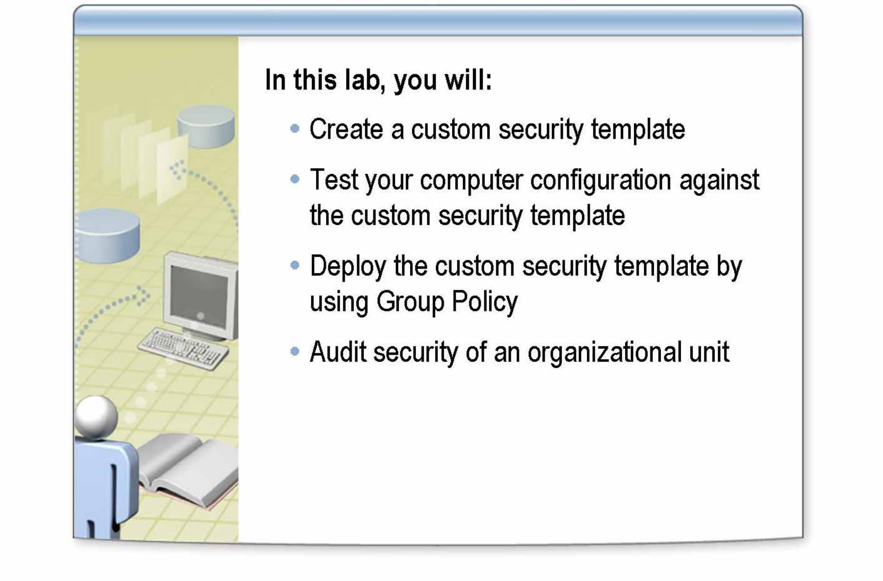
► Configure the security log properties

1. Change the maximum log size to 30,016 KB.
2. Change the overwrite behavior to **Do not overwrite events (clear log manually)**.

► Verify that security events are being logged for D:\HR Reports

1. Create a security log filter that filters the following types of events:
   - Success events and failure events
   - Security
   - Object access
2. Browse through the security log to see success and failure events for D:\HR Reports.

Lab A: Managing Security Settings



In this lab, you will:

- Create a custom security template
- Test your computer configuration against the custom security template
- Deploy the custom security template by using Group Policy
- Audit security of an organizational unit

Objectives

After completing this lab, you will be able to:

- Create a custom security template.
- Test your computer configuration against the custom security template.
- Deploy a custom template by using a GPO.
- Configure and test security auditing of organizational units.

Instructions

Before you begin this practice:

- Log on to the domain by using the *ComputerName*User account.
- Open CustomMMC with **Run as** command.

  Use the user account NWTraders\ComptuerNameAdmin (Example: LondonAdmin).
- Ensure the CustomMMC has the following snap-ins:
  - Security Templates
  - Group Policy Management
  - Security Configuration and Analysis
  - Active Directory Users and Computers
  - Computer Management (Local)
  - Computer Management (London)

Estimated time to complete this lab: 35 minutes

Exercise 1
Creating a Custom Template

In this exercise, you will create a custom security template.

Scenario

The security team has finished testing the security requirements for Northwind Traders. They have given you security requirements that you must use to create a custom security template called *ComputerName* Server Policy.

Tasks	Special instructions
1. Create a new custom security template.	▪ Security template name: *ComputerName* **Server Policy**
2. Enable audit policies.	▪ Enable the following audit policies for failure: • **Audit account logon events** • **Audit logon events** ▪ Enable the following audit policies for success and failure: • **Audit account management events** • **Audit object access events** • **Audit policy change events** • **Audit privilege use events** • **Audit system events**
3. Set event log properties.	▪ Set the following event log properties: • Set maximum application log size to 99,840 KB • Set maximum security log size to 99,840 KB • Retain security log for 7 days • Retain system log for 7 days
4. Save the template.	▪ Save the template *ComputerName* Server Policy.

Exercise 2
Testing a Custom Template

In this exercise, you will compare a custom security template to your server's current security policy.

Tasks	Special instructions
1. Create a new configuration and analysis baseline database.	▪ Database name: *ComputerName* **Security Test** ▪ Template: *ComputerName* **Server Policy Settings.inf**
2. Analyze your server.	▪ Analysis log name: *ComputerName* **Security Test.log**
3. Review the results of the audit policy analysis.	▪ Circle Y if your computer setting matches the database. Circle N if your computer setting differs from the database. • **Audit account logon events** (Y / N) • **Audit account management events** (Y / N) • **Audit logon events** (Y / N) • **Audit object access events** (Y / N) • **Audit policy change events** (Y / N) • **Audit privilege use events** (Y / N) • **Audit system events** (Y / N)
4. Review the results of the event log analysis.	▪ Circle Y if your computer setting matches the database. Circle N if your computer setting differs from the database. • **Maximum application log size** (Y / N) • **Maximum security log size** (Y / N) • **Retain security log** (Y / N) • **Retain system log** (Y / N)

Exercise 3
Deploying a Custom Template Using a GPO

In this exercise, you will import a custom template to a GPO and deploy the template to your computer. You will then test your computer to determine if you received the GPO.

Tasks	Special instructions
1. Create and link a GPO.	▪ Organizational unit to link to GPO: Locations/*ComputerName*/Computers ▪ GPO name: *ComputerName* **Security Settings**
2. Import a security template to a GPO.	▪ Template name: *ComputerName* Server Policy.inf
3. Disable **Block Policy inheritance**.	▪ Expand all organizational units of **Locations/*ComputerName*** and remove any blocking of inheritance of all sub organizational units.
4. Verify that the computer account is in the proper organizational unit.	▪ Verify that the computer named *ComputerName* is in the organizational unit Locations/*ComputerName*/Computers. ▪ If *ComputerName* is not in the Locations/*ComputerName*/Computers organizational unit, move it there.
5. Update your Group Policy settings.	▪ Run **gpupdate /force**.
6. Analyze the local computer security policy.	▪ Run **Analyze Computer Now** in Security Configuration and Analysis.
7. Review the results of the audit policy analysis.	▪ Circle Y if your computer setting matches the database. Circle N if your computer setting differs from the database. • **Audit account logon events** (Y / N) • **Audit account management events** (Y / N) • **Audit logon events** (Y / N) • **Audit object access events** (Y / N) • **Audit policy change events** (Y / N) • **Audit privilege use events** (Y / N) • **Audit system events** (Y / N)
8. Review the results of the event log analysis.	▪ Circle Y if your computer setting matches the database. Circle N if your computer setting differs from the database. • **Maximum application log size** (Y / N) • **Maximum security log size** (Y / N) • **Retain security log** **(** Y / N) • **Retain system log** (Y / N)

Exercise 4
Configuring and Testing Security Audits of Organizational Units

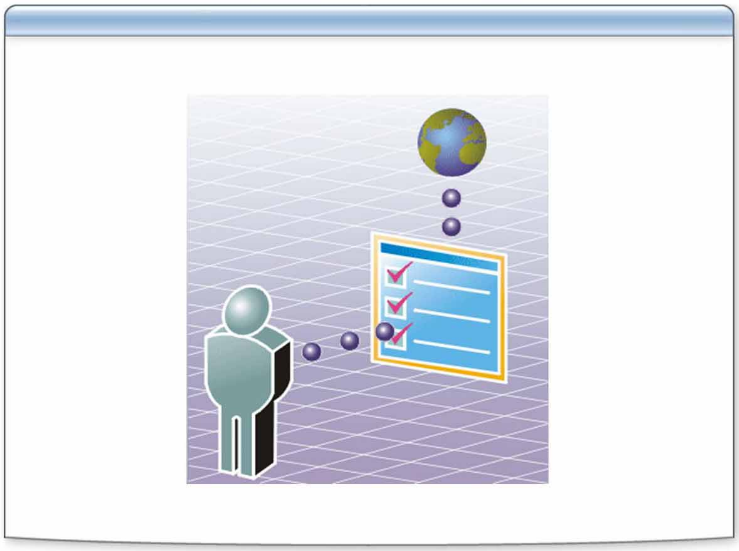
In this exercise, you will configure and test security audits of organizational units.

Scenario

Northwind Traders wants to configure security on the Location/*ComputerName* organizational units to monitor the G IT Admins group. You must configure and test auditing for failed attempts to delete user and computer accounts.

Tasks	Special instructions
1. Enable auditing for an organizational unit.	■ Audit the organizational unit Locations/*ComputerName* ■ Remove inheritable auditing entries ■ Remove all noninherited auditing entries ■ Audit the Everyone group ■ Audit the access of **Delete Computer Objects** for **Failed** access ■ Apply policy to **This object and all child objects**
2. Try to delete computer account with an unauthorized account.	■ Tool: DSRM a. Open a command prompt with runas b. runas /user:nwtraders\ComputerNameUser cmd c. Password: P@ssw0rd ■ Use DSRM to try and delete the computer *ComputerName* • Dsrm CN=*ComputerName*,OU=Computers,OU=*ComputerName*,OU=Locations,DC=nwtraders,DC=msft ■ You should get an access is denied error message
3. Filter the London security log.	■ Tool: Computer Management (London) ■ Filter security policy for: • Event types: **Failure audit** • Event source: **Security** • Category: **Directory Service Access** • User: *ComputerName***User**
❓	What was *ComputerName*User trying to do?

Course Evaluation



Your evaluation of this course will help Microsoft understand the quality of your learning experience.

To complete a course evaluation, go to http://www.CourseSurvey.com.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.