EXAM OBJECTIVES

Professional ▶

Exam 70-210

- Implement, configure, manage, and troubleshoot local user settings
  - Implement, configure, manage, and troubleshoot auditing.
- Implement, configure, manage, and troubleshoot a security configuration.

Server ▶

Exam 70-215

- Implement, configure, manage, and troubleshoot auditing.
- Implement, configure, manage, and troubleshoot security by using the Security Configuration Tool Set.

Directory Services ▶

Exam 70-217

- Configure and troubleshoot security in a Directory Services infrastructure.
  - Create, analyze and modify security configurations by using Security Configuration and Analysis and Security Templates.
  - Implement an audit policy.
- Monitor and analyze security events.

CHAPTER

13 Auditing and Security

This chapter is all about managing auditing and security on your Windows 2000 computer and on your Windows 2000 network. First, I'll show you how to enable and configure auditing. You'll learn how to audit Active Directory objects as well as files, folders, and printers. Next, I'll explain how you can use Event Viewer to view, monitor, and analyze audit and security events.

From there, I'll explore how to use the Security Templates snap-in to create and implement a security template that can be used to apply a predefined security policy to one or more computers. Next, I'll introduce you to another snap-in, Security Configuration and Analysis, that you can use to compare a computer's existing security policy settings against a predefined set of security policy settings. I'll also tell you about a command-line version of this snap-in that can make security analysis on your network easier for you. Finally, I'll give you some helpful tips for troubleshooting auditing and security problems.

Chapter Pre-Test

1. What are the two areas Windows 2000 auditing is divided into?
2. What types of objects you can audit in Windows 2000?
3. What Windows 2000 tool can you use to view the results of auditing?
4. What is a security template?
5. What MMC snap-in can you use to create, edit, and manage security templates?
6. What are the two primary ways to implement a security template?
7. What MMC snap-in can you use to compare a computer's security configuration settings against the predefined security configuration settings in a security template?

Managing Auditing

When enabled, *auditing* produces a log of specified security events and activities that occur on a Windows 2000 computer. By default, auditing is not enabled.

Windows 2000 auditing is divided into two areas: auditing of access to the system and auditing of access to objects. System access auditing primarily involves tracking accesses and attempted accesses to the Windows 2000 operating system. Object access auditing involves tracking accesses and attempted accesses to specific objects, such as Active Directory objects (including users, groups, computers, OUs, domains, and so on), files, folders, and printers.

You must be a member of the Administrators group to enable and configure auditing. In the next sections, I'll show you how to enable and configure both system access and object access auditing.

Enabling and Configuring System Access Auditing

Enabling and configuring system access auditing is done by configuring Audit Policy. You can configure an audit policy that is applied to an individual computer, or, depending on the tool you use, you can configure an audit policy that is applied to all of the Windows 2000 computers in an Active Directory container, such as a site, a domain, or an OU.

You can use a number of tools used to configure Audit Policy. The tool you use to configure an audit policy depends on which computers you want the audit policy to apply to:

- To configure an audit policy for the local Windows 2000 computer, use the Local Security Policy tool in Administrative Tools. (Select Start ➪ Settings ➪ Control Panel, then double-click Administrative Tools, then double-click Local Security Policy.)
- To configure an audit policy for all Windows 2000 computers in a domain, use the Domain Security Policy tool in Administrative Tools. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.

CAUTION

Auditing is disabled by default in the Default Domain Controllers Policy GPO. Even if you enable auditing for all Windows 2000 computers in a domain, auditing will *not* be enabled on domain controllers until you enable it in the Default Domain Controllers Policy GPO by using the Domain Controller Security Policy tool.

- To configure an audit policy for all domain controllers in a domain, use the Domain Controller Security Policy tool in Administrative Tools. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Controller Security Policy.) This tool modifies the security settings in the Default Domain Controllers Policy GPO. This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.
- To configure an audit policy for all Windows 2000 computers located in a particular OU or domain, use Active Directory Users and Computers to configure a Group Policy object (GPO) for the OU or the domain. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.) This tool is available on Windows 2000 domain controllers or on other Windows 2000 computers that have the ADMINPAK installed.
- To configure an audit policy for all Windows 2000 computers located in a particular site, use Active Directory Sites and Services to configure a Group Policy object (GPO) for the site. (Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Sites and Services.) This tool is available on Windows 2000 domain controllers, or on other Windows 2000 computers that have the ADMINPAK installed.

Audit Policy, like all other Windows 2000 policies, can be configured at several different levels: at the local computer level, at the OU level, at the domain level, and so on. Because of this, it's possible that the settings in an audit policy can conflict with settings in an audit policy set at another level. The point to remember is that when audit policy settings conflict, the audit policy that is applied *last* is the audit policy that takes precedence. Audit Policy is applied in the same order as Group Policy.

CROSS-REFERENCE

If you need refreshing on Group Policy, see Chapter 10.

Now I'll show you how to configure an audit policy for all Windows 2000 computers in the domain by using the Domain Security Policy tool. Because the Windows 2000 user interfaces for the Domain Security Policy tool, the Domain Controller Security Policy tool, and the Local Security Policy tool are substantially similar, you can use these same steps to configure an audit policy for domain controllers or for the local Windows 2000 computer — all you need to do is start the appropriate tool and follow the steps in the next section.

STEP BY STEP

CONFIGURING AN AUDIT POLICY FOR WINDOWS 2000 COMPUTERS IN A DOMAIN

1. Start the Domain Security Policy tool. (Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Security Policy.)
2. In the left pane of the Domain Security Policy dialog box, click the + next to Security Settings. Then click the + next to Local Policies. Highlight Audit Policy. A list of specific audit policies that you can configure is displayed in the right pane, as shown in Figure 13-1.

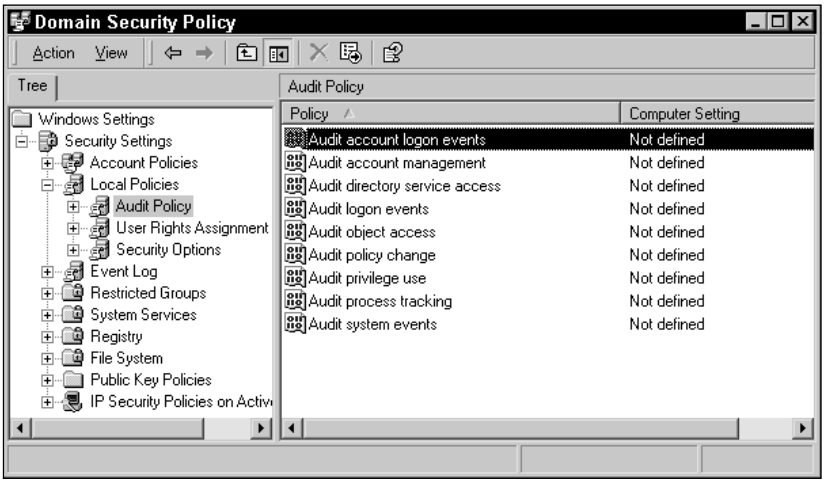

FIGURE 13-1 Configuring Audit Policy

3. In the right pane, double-click the audit policy you want to configure.

STEP BY STEP *Continued*

4. A Security Policy Setting dialog box for the audit policy you selected appears, as shown in Figure 13-2.

FIGURE 13-2 Defining an individual audit policy

Figure 13-2 shows the Security Policy Setting dialog box for the "Audit account logon events" audit policy. However, the dialog boxes for each of the other audit policies are identical to this one.

Select the check box next to "Define these policy settings." Then, select either the check box next to Success, Failure, or both.

When the Success check box is selected, Windows 2000 generates an audit event each time a user successfully performs the audited task (in this case, each time a user logs on).

When the Failure check box is selected, Windows 2000 generates an audit event each time a user attempts to perform an audited task but fails (usually because of a lack of permissions or user rights).

When both the Success and Failure check boxes are selected, an audit event is generated each time a user attempts to perform an audited task, whether successfully or unsuccessfully.

Click OK.

5. The Domain Security Policy dialog box reappears. Repeat Steps 3 and 4 to configure additional audit policies as necessary. Close the Domain Security Policy dialog box.

Table 13-1 lists and describes the types of Windows 2000 system events you can audit.

TABLE 13-1 Auditable System Events in Windows 2000

Event	Description
Account logon events	A domain controller receives an account validation request.
Account management	A user account or group is created, modified, or deleted; or, a user account is renamed, disabled, or enabled, or a user's password is changed.
Directory service access	A user accesses an Active Directory object (such as a user, group, computer, OU, domain, and so on) that is also configured for auditing. Note: To audit access to an Active Directory object, you *must* enable auditing of Directory service access events *and* configure auditing on the specific Active Directory object.
Logon events	A user logs on to or logs off the Windows 2000 computer.
Object access	A user accesses a file, folder, or printer that is configured for auditing. Note: To audit access to a file, folder, or printer, you *must* enable auditing of object access events *and* configure auditing on the specific file, folder, or printer.
Policy change	The user rights, security, audit, or trust relationship policies are modified.
Privilege use	A user exercises an assigned user right (other than the "Log on locally" or "Access this computer from the network" user rights).
Process tracking	An event, such as program activation, some forms of handle duplication, indirect object accesses, or process exit occurs. This event is not often selected for audit by administrators.
System events	A user restarts or shuts down the Windows 2000 computer, or a system security or Security Log event occurs.

TIP

Carefully consider which events you need to audit. If you choose to audit everything, the computer's performance will be slowed significantly, your Security Log will fill up quickly, and you'll find yourself sifting through volumes of useless information to find the auditing data you need.

Enabling and Configuring Object Access Auditing

As I mentioned earlier, object access auditing makes it possible for you to track access and attempted access to specific objects, such as Active Directory objects (including users, groups, computers, OUs, domains, and so on), files, folders, and printers.

Enabling object access auditing is a two-part process:

- You must enable and configure either the directory service access or object access audit policy for the Windows 2000 computer on which the object you want to audit access to is stored. (I explained how to enable and configure system access auditing for these events in the previous section.)
- You must configure auditing for the specific object you want to audit access and attempted access to. Object access auditing is configured in the Properties dialog box for the specific object. The exception to this rule is auditing of Active Directory objects. Auditing of all Active Directory objects in an Active Directory domain is configured by default.

It doesn't really matter which order you perform these two tasks in.

EXAM TIP

A favorite exam-writer trick is to tell you that auditing has been configured for an object, but that no audit events are being written to the Security Log. Remember that system access auditing (for either directory service access or object access) must also be enabled and configured before object auditing will occur.

In the next sections I'll show you how to configure auditing of Active Directory objects, files, folders, and printers.

Configuring Auditing of Active Directory Objects

You can configure auditing of access and attempted access to Active Directory objects and their properties. You can configure auditing for any Active Directory object, including users, groups, computers, OUs, domains, sites, and so on.

When you configure auditing of Active Directory objects, remember to take inheritance into account. All of the rules you learned about inheritance and blocking inheritance in Chapter 8 apply to auditing of Active Directory objects, as well.

By default, auditing is configured for the domain, and this auditing configuration is inherited by all Active Directory objects in the domain. This means that, once system access auditing of directory service access is enabled, all actions that modify objects in the domain are audited. You can modify this auditing configuration to meet your needs.

To modify the auditing configuration of most Active Directory objects, you can use Active Directory Users and Computers. To modify the auditing configuration of a site, use Active Directory Sites and Services.

STEP BY STEP

MODIFYING THE AUDITING CONFIGURATION OF ACTIVE DIRECTORY OBJECTS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, click the + next to the name of the domain that contains the Active Directory object for which you want to modify the auditing configuration. Continue expanding containers until the object for which you want to modify auditing is displayed in the right pane. In the right pane, double-click the object for which you want to modify auditing. Or, you can right-click the object, and select Properties from the menu that appears.
3. The object's Properties dialog box appears. Click the Security tab.
4. On the Security tab, click Advanced.
5. An Access Control Settings dialog box for the object appears. Click the Auditing tab.
6. The Auditing tab for the object is displayed, as shown in Figure 13-3. Notice that in this case the Active Directory object selected is a user named Alan R. Carter. Also notice that the check box next to "Allow inheritable auditing entries from parent to propagate to this object" is selected—this is the default setting.

   Finally, notice that this object has an auditing entry for the Everyone group. This entry, which was created by default during the installation of Active Directory, is inherited from the domain.

   To modify an auditing entry, highlight the entry and click View/Edit. Then skip to Step 8.

   To remove an auditing entry, highlight the entry and click Remove.

STEP BY STEP *Continued*

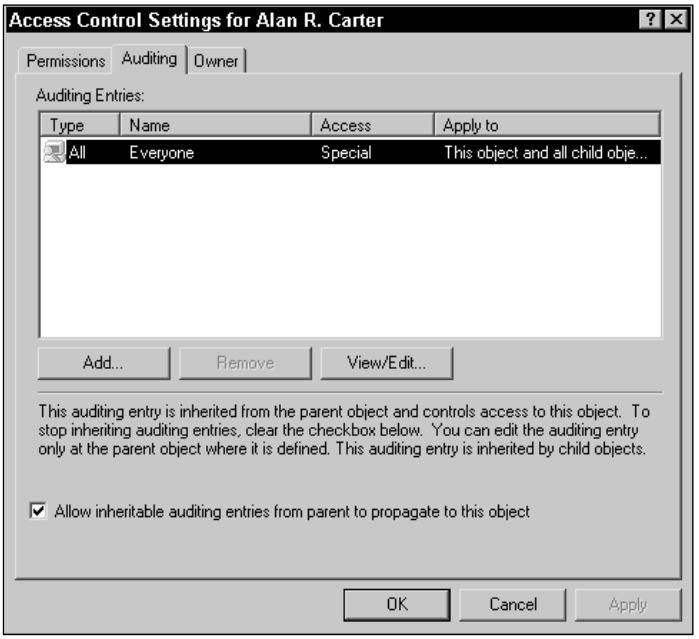

FIGURE 13-3 The Auditing tab

TIP

You can't remove auditing entries that are inherited from parent objects.

To add an auditing entry, click Add.

7. In the Select User, Computer, or Group dialog box, double-click the user, computer, or group for which you want to audit access to this Active Directory object.
8. The Auditing Entry dialog box for the object appears, as shown in Figure 13-4. Notice there are two tabs in this dialog box: Object and Properties.

   On the Object tab, configure auditing for accesses to the Active Directory object itself. You can configure successful accesses, failed accesses, or both, for each type of access.

   On the Properties tab, configure auditing for accesses to the properties of the Active Directory object. Again, you can configure successful accesses, failed accesses, or both, for each type of access.

   When you are finished configuring the auditing entry, click OK.

STEP BY STEP *Continued*

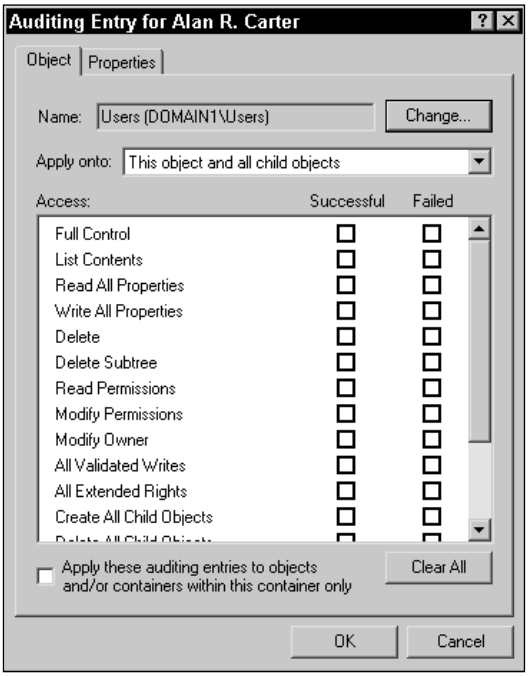

FIGURE 13-4 Configuring an auditing entry

9. In the Access Control Settings dialog box for the object, click OK.
10. In the object's Properties dialog box, click OK.
11. Close Active Directory Users and Computers.

TIP

Remember, you must also enable and configure system access auditing for directory service access before object auditing of Active Directory objects will occur.

Configuring Auditing of Files and Folders

You can configure auditing of files and folders located on NTFS volumes on Windows 2000 computers. You can't configure auditing of files and folders located on FAT or FAT32 volumes. By default, auditing is not configured on any files or folders on a Windows 2000 computer.

When configuring auditing of files and folders, make sure that you take inheritance into account. When auditing is configured for a volume or a folder, all files and folders in that volume or folder inherit the auditing settings configured on the parent object.

The task of configuring auditing of files and folders is normally performed by using Windows Explorer, as the following steps explain.

STEP BY STEP

CONFIGURING AUDITING OF FILES OR FOLDERS

1. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
2. In the left pane, click the + next to My Computer, then expand volumes and folders until the file or folder for which you want to configure auditing is displayed in the right pane.
3. In the right pane, right-click the file or folder for which you want to configure auditing, and select Properties from the menu that appears.
4. In the file or folder's Properties dialog box, click the Security tab.
5. On the Security tab, click Advanced.
6. In the Access Control Settings dialog box for the file or folder, click the Auditing tab.
7. On the Auditing tab, click Add to add an auditing entry for the file or folder.
8. In the Select User, Computer, or Group dialog box, double-click the user, computer, or group for which you want to audit access to this file or folder.
9. The Auditing Entry dialog box for the file or folder appears, as shown in Figure 13-5. Notice the "Apply onto" drop-down list box.

   Select the appropriate option from the "Apply onto" drop-down list box. This setting determines how the auditing entries you set in this dialog box will be inherited. The possible selections are:

   - This folder, subfolders and files—this is the default setting
   - This folder only
   - This folder and subfolders
   - This folder and files
   - Subfolders and files only
   - Subfolders only
   - Files only

STEP BY STEP *Continued*

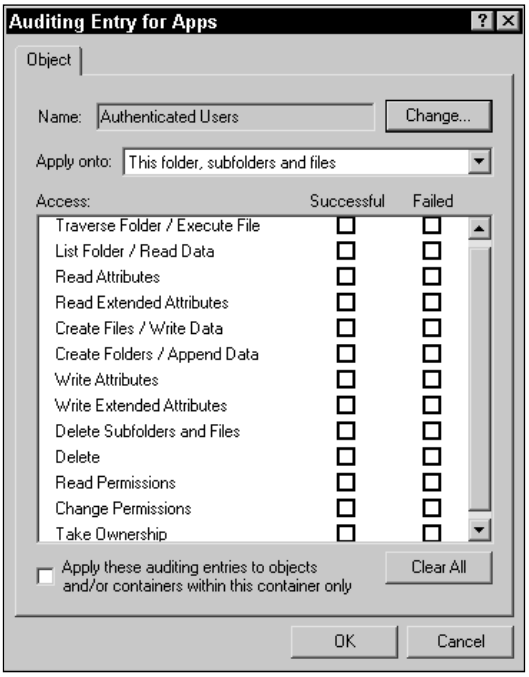

FIGURE 13-5 Configuring an auditing entry for the Apps folder

The selection you make in this drop-down list box works in conjunction with the "Apply these auditing entries to objects and/or containers within this container only" check box at the bottom of the dialog box. If you select this check box (and any option in the "Apply onto" box that includes subfolders), the auditing entries you set will be applied to the subfolder, but *will not be applied to any files or folders within the subfolder*.

Next, configure auditing for accesses to the file or folder. You can configure successful accesses, failed accesses, or both, for each type of access.

When you're finished configuring audit entries, click OK.

10. In the Access Control Settings dialog box for the file or folder, click OK.
11. If system access auditing of object access has not yet been enabled for this computer, Windows 2000 displays a Security dialog box, as shown in Figure 13-6. Click OK, and remember to enable auditing of object access after you complete these steps.

STEP BY STEP *Continued*

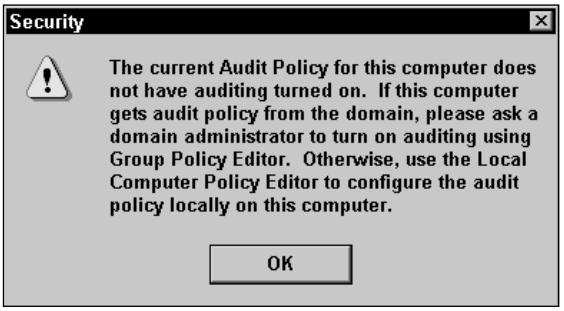

FIGURE 13-6 Security warning message

12. In the file or folder's Properties dialog box, click OK.
13. Close Windows Explorer.

Configuring Auditing of Printers

You can configure auditing of printers on Windows 2000 computers. By default, auditing is not configured on printers. In addition, there are no inheritance issues to worry about when configuring auditing for printers on a Windows 2000 computer.

Configuring auditing of printers is normally done by using the `Printers` folder, as the following steps explain.

STEP BY STEP

CONFIGURING AUDITING OF PRINTERS

1. Open the `Printers` folder. (Select Start ➪ Settings ➪ Printers.)
2. In the right pane of the Printers dialog box, right-click the printer for which you want to configure auditing, and select Properties from the menu that appears.
3. In the printer's Properties dialog box, click the Security tab.
4. On the Security tab, click Advanced.
5. In the Access Control Settings dialog box for the printer, click the Auditing tab.
6. On the Auditing tab, click Add.

STEP BY STEP *Continued*

7. In the Select User, Computer, or Group dialog box, double-click the user, computer, or group for which you want to audit accesses to this printer.
8. The Auditing Entry dialog box for the printer appears, as shown in Figure 13-7. Notice the "Apply onto" drop-down list box.

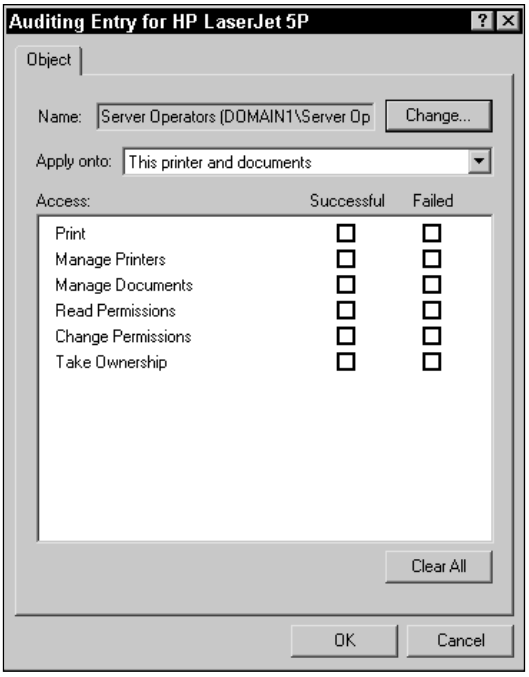

FIGURE 13-7 Configuring an auditing entry for a printer

Select the appropriate option in the "Apply onto" drop-down list box. In this list box you can choose whether to apply these auditing settings to this printer only, to this printer's documents only, or to this printer and its documents.

Next, configure auditing for accesses to the printer. You can configure successful accesses, failed accesses, or both, for each type of access.

When you're finished configuring printer auditing, click OK.

9. In the Access Control Settings dialog box for the printer, click OK.
10. In the printer's Properties dialog box, click OK.
11. Close the `Printers` folder.

Monitoring and Analyzing Security Events

You can use Event Viewer to view, monitor, and analyze the results of the auditing you have configured. Event Viewer has several logs, including the System Log, the Application Log, and the Security Log. The Security Log contains the data generated by auditing.

You can view the Security Log in its entirety, or you can filter events by date and type of audit event. You can clear the Security Log when it is full; and you can save (archive) the log to be analyzed at a later date by using Event Viewer, a text editor, or a spreadsheet or database program. You can also configure the maximum size of the log and event log wrapping (how the log handles additional auditing data when it becomes full).

An important consideration, from an administrative standpoint, is scheduling time to regularly monitor and analyze auditing events in the Security Log. The data gathered by auditing is of no value if it is not used.

The sections that follow explain how to access the Security Log in Event Viewer, how to view security events, how to filter security events, how to archive and clear the Security Log, and finally, how to configure the maximum size of the Security Log and Security Log wrapping.

STEP BY STEP

VIEWING SECURITY EVENTS IN EVENT VIEWER

1. Start Event Viewer. (Select Start ➪ Programs ➪ Administrative Tools ➪ Event Viewer.)
2. The Event Viewer dialog box appears. In the left pane, highlight the Security Log. Figure 13-8 shows the Security Log on a Windows 2000 computer. Notice that some events are marked with keys (these designate successful events) and that some events are marked with locks (these designate unsuccessful [failed] events).

   To view the details of an event, double-click the event.
3. The Event Properties dialog box appears, as shown in Figure 13-9.

   Notice the types of information included in this dialog box. Click OK.

STEP BY STEP *Continued*

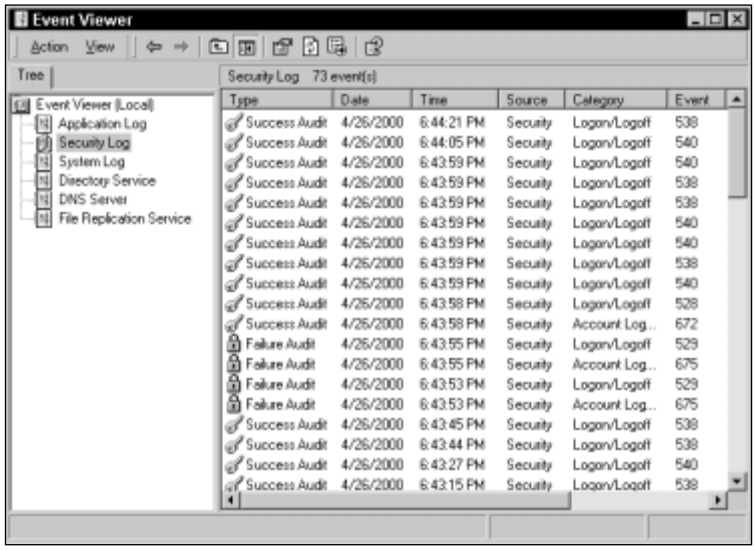

FIGURE 13-8 The Security Log in Event Viewer

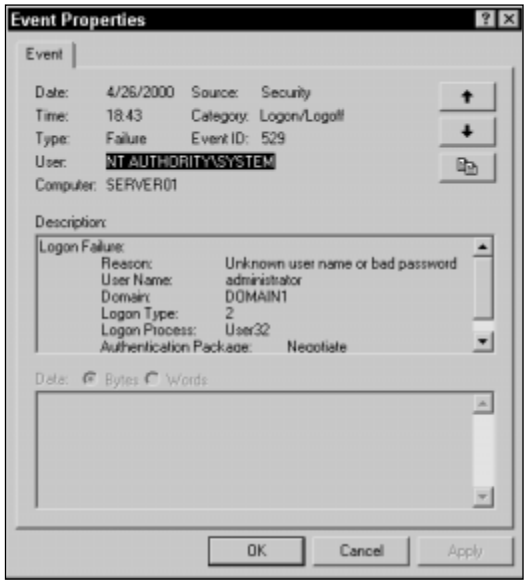

FIGURE 13-9 Viewing the details of a Security Log event

When you first open the Security Log, there may be so many events listed that you despair of ever locating the event you're looking for. To make it easier to locate specific events, you can filter the Security Log so that only events of the type(s) you select are displayed. Filtering Security Log events can help you to analyze the specific type(s) of events you want to monitor.

STEP BY STEP

FILTERING SECURITY LOG EVENTS

1. Start Event Viewer. (Select Start ➪ Programs ➪ Administrative Tools ➪ Event Viewer.)
2. The Event Viewer dialog box appears. In the left pane, highlight the Security Log. Select View ➪ Filter.
3. The Security Log Properties dialog box appears with the Filter tab on top, as shown in Figure 13-10. Notice the event types that you can select.

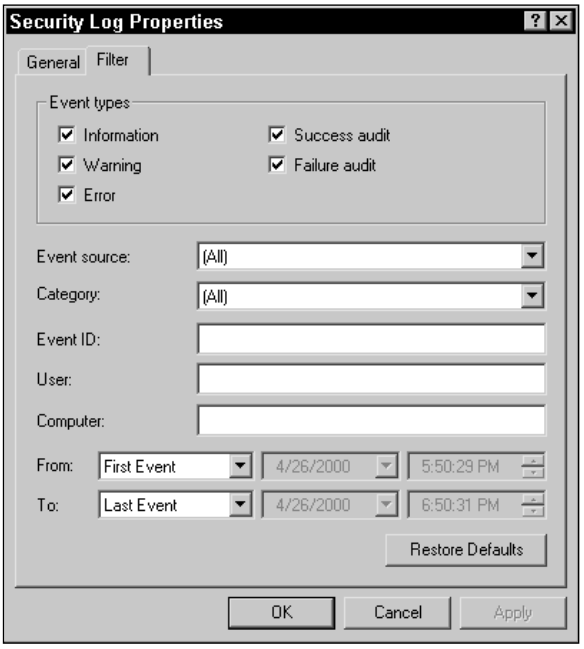

FIGURE 13-10 Filtering events

Select the check box next to the event type(s) you want displayed in the Security Log.

STEP BY STEP *Continued*

Then, select the event source from the "Event source" drop-down list box. Generally, the default selection of All is appropriate. However, if you only want to view security events from a specific source, such as Directory Services, select the appropriate source from this drop-down list box.

Finally, if you want to view only those events that occurred during a specific time period, you can configure the time period by selecting Events On in the From and To drop-down list boxes, and then specifying a start and stop date and time.

When you finish configuring filtering, click OK.

4. The Security Log in Event Viewer reappears. Only the events that meet the criteria you configured on the Filter tab are displayed.

If you want to archive the events in the Security Log, you can save them by using Event Viewer. After you archive the log, you should clear it so that the archived events are no longer displayed, and there is room for the log to accumulate new events.

STEP BY STEP

ARCHIVING AND CLEARING THE SECURITY LOG

1. Start Event Viewer. (Select Start ➪ Programs ➪ Administrative Tools ➪ Event Viewer.)
2. The Event Viewer dialog box appears. In the left pane, highlight the Security Log. Select Action ➪ Save Log File As.
3. In the Save "Security Log" As dialog box, select the folder in which you want to save the Security Log from the "Save in" drop-down list box. Then, in the "File name" text box, type in a name for the Security Log data you are saving.

   Finally, in the "Save as type" drop-down list box, select the appropriate file type. Select a file type of `.evt` if you plan to view this file later by using Event Viewer. Select a file type of `.txt` if you want to view the file later by using a text editor. Select a file type of `.csv` if you plan to export this data for later analysis in a spreadsheet or database program.

   Click Save.
4. After you've saved the Security Log, you may want to clear it. In the Event Viewer dialog box, select Action ➪ Clear all Events.

STEP BY STEP *Continued*

5. Event Viewer asks if you want to save the Security Log before you clear it. Because you just saved the Security Log, click No to continue.
6. Windows 2000 clears the Security Log and creates a success audit event with a description that states "The audit log was cleared." The description of this audit event also includes the user name of the user who cleared the log.

There are a couple of additional settings you may want to configure on the Security Log. You can configure the maximum size of the log, and the action that Windows 2000 will take when the log becomes full.

STEP BY STEP

CONFIGURING SECURITY LOG PROPERTIES

1. Start Event Viewer. (Select Start ➪ Programs ➪ Administrative Tools ➪ Event Viewer.)
2. The Event Viewer dialog box appears. In the left pane, highlight the Security Log. Select Action ➪ Properties.
3. The Security Log Properties dialog box appears, as shown in Figure 13-11.

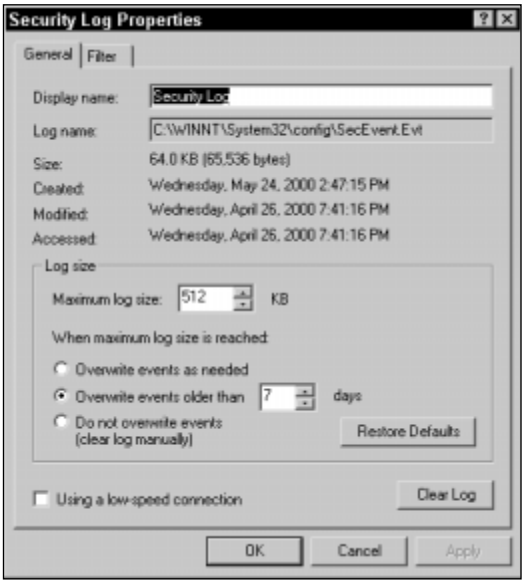

FIGURE 13-11 Configuring Security Log properties

STEP BY STEP *Continued*

In this dialog box, configure the maximum size of the Security Log. The default maximum log size is 512K, which may be much smaller than you need if you plan to audit multiple security events.

Next, select one of the three options to choose the action that Windows 2000 will take when the maximum log size is reached. Click OK.

4. Close Event Viewer.

Using Security Templates

A *security template* is a text-based `.inf` file that contains predefined security settings that can be applied to one or more computers. A security template can also be used to compare a computer's existing security configuration against a predefined, standard security configuration. Security templates are particularly useful on large networks. An administrator can create a single security configuration that can be applied to multiple computers, instead of having to manually create the security configuration on each and every computer.

Security templates can be created, edited, and managed by using the Security Templates snap-in to the MMC. You must be a member of the Administrators group to create, save, and implement security templates.

TIP

The Security Templates snap-in was originally included as part of the Security Configuration Tool Set, but Microsoft split this tool set into two components: the Security Templates snap-in and the Security Configuration and Analysis snap-in.

Microsoft has included several predefined security templates with Windows 2000. These templates are stored, by default, in *`SystemRoot`*`\Security\Templates`. Some of the most commonly used templates include:

- Default workstation (`basicwk.inf`)
- Default server (`basicsv.inf`)
- Default domain controller (`basicdc.inf`)
- Compatible workstation or server (`compatws.inf`)

- Secure workstation or server (`securews.inf`)
- Highly secure workstation or server (`hisecws.inf`)
- Secure domain controller (`securedc.inf`)
- Highly secure domain controller (`hisecdc.inf`)

In the next two sections I'll explain how to create and implement a security template.

Creating a Security Template

Before you can create a security template, you should create an MMC console that contains the Security Templates snap-in. This snap-in is then used to create a security template.

STEP BY STEP

CREATING A NEW MMC CONSOLE

1. From the desktop, select Start ➪ Run.
2. In the Run dialog box, type **mmc** and click OK.
3. A new MMC console, named Console1, is displayed. Select Console ➪ Add/Remove Snap-in.
4. In the Add/Remove Snap-in dialog box, click Add.
5. In the Add Standalone Snap-in dialog box, scroll down and highlight Security Templates. Click Add. Then click Close.
6. In the Add/Remove Snap-in dialog box, click OK.
7. In the Console1 (Console Root) dialog box, select Console ➪ Save As.
8. In the Save As dialog box, type a name for your security console (such as Security Console) in the "File name" text box, and click Save. By default, Windows 2000 saves this new MMC console to your `Administrative Tools` folder.
9. Close your security console.

There are two ways to create a security template. You can either edit then save one of the predefined security templates, or you can create a security template from scratch. By far the most common technique used is modifying an existing security template.

STEP BY STEP

CREATING A NEW SECURITY TEMPLATE BY EDITING AN EXISTING TEMPLATE

1. Open the security console you created in the previous set of steps. (Select Start ➪ Programs ➪ Administrative Tools ➪ *Security Console*.)
2. In the left pane of the security console, click the + next to Security Templates. Then click the + next to `C:\WINNT\Security\Templates`. All of the security templates on your computer, including the predefined security templates, are displayed in the left pane, as shown in Figure 13-12.

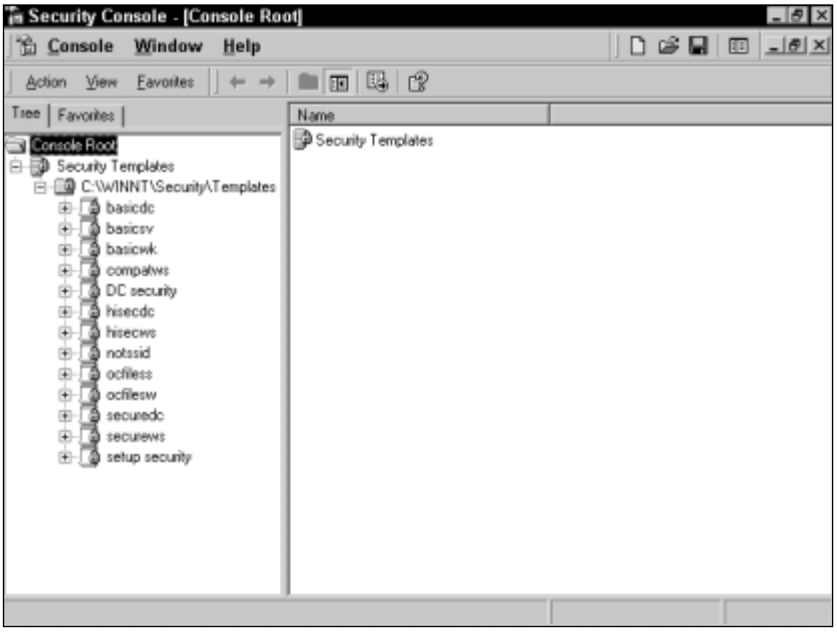

FIGURE 13-12 Security templates

Highlight the existing security template you want to modify. Select Action ➪ Save As.

3. In the Save As dialog box, type in the name you want to assign to the new template you're creating in the "File name" text box. Click Save.
4. In the left pane of the security console, click the + next to the name of the security template you just created. Further expand the components of the security template as necessary. Figure 13-13 shows the contents of a new security template I created. Notice that the configurable settings in a security template are the same as the configurable settings available in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

STEP BY STEP *Continued*

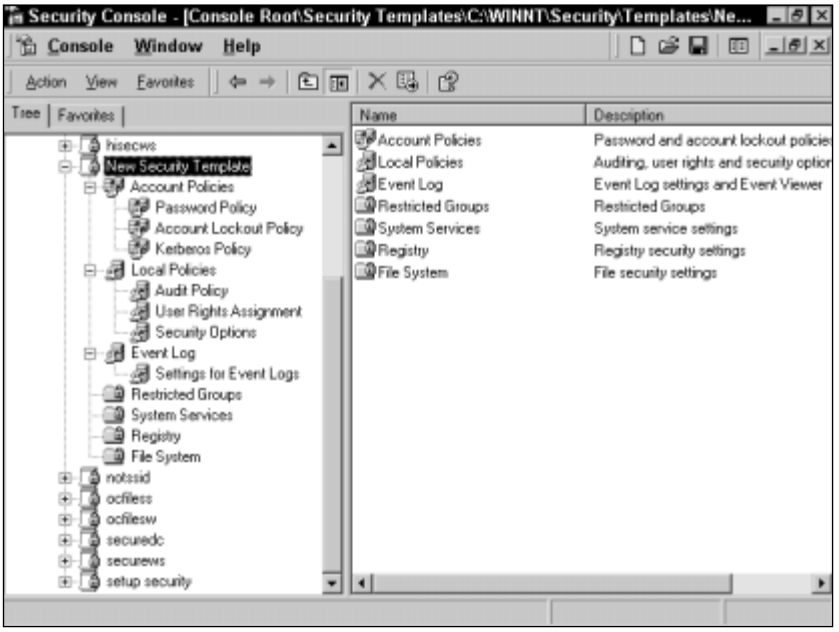

FIGURE 13-13 Contents of a security template

Modify the individual security settings in the template to meet your needs.

5. When you're finished configuring the security template, highlight the name of your security template in the left pane, and select Action ➪ Save.
6. Close the security console. If prompted, click Yes to save console settings to your security console.

You may decide you want to create a security template from scratch. The following steps explain how to perform this process.

STEP BY STEP

CREATING A NEW SECURITY TEMPLATE FROM SCRATCH

1. Open the security console you created earlier in this chapter. (Select Start ➪ Programs ➪ Administrative Tools ➪ *Security Console*.)
2. In the left pane of the security console, click the + next to Security Templates. Then click the + next to `C:\WINNT\Security\Templates`.

STEP BY STEP *Continued*

To create a new security template, highlight `C:\WINNT\Security\Templates`, and select Action➪New Template.

3. In the C:\WINNT\Security\Templates dialog box, type a name for your new security template in the "Template name" text box. You can also enter a description for the new template if you want to. Click OK.
4. In the right pane of the security console dialog box, double-click the new security template you just created.
5. Modify the individual security settings in the new security template to meet your needs.
6. When you finish configuring the security template, highlight the name of your security template in the left pane, and select Action➪Save.
7. Close the security console. If prompted, click Yes to save console settings to your security console.

Implementing a Security Template

Once you've chosen a security template to use (either one of the preconfigured ones or one that you've created), you need to implement it. There are two primary ways to implement a security template: you can either apply the security template directly to the local computer; or you can import the security template into a Group Policy object (GPO) in Active Directory, where it will be applied to all computers affected by that GPO.

To apply a security template to the local computer, use the Local Security Policy tool, as explained in the following steps.

STEP BY STEP

APPLYING A SECURITY TEMPLATE TO THE LOCAL COMPUTER

1. Select Start➪Programs➪Administrative Tools➪Local Security Policy.
2. In the Local Security Settings dialog box, select Action➪Import Policy.
3. In the Import Policy From dialog box, the security templates on this computer are displayed. Double-click the security template you want to apply to the local computer.
4. Close the Local Security Settings dialog box.

When you apply a security template to the local computer, it's important to keep in mind how the security settings in Group Policy are applied. If the computer you are applying the security template to is a member of a domain, it may be affected by other security settings configured at the domain level or set in various GPOs in Active Directory.

CROSS-REFERENCE

For more information on how Group Policy is applied, see Chapter 10.

If you want a security template to be applied to a group of computers, you might consider importing that security template into a GPO that affects those computers. The next set of steps explains how to import a security template into a GPO associated with a domain or an OU.

STEP BY STEP

IMPORTING A SECURITY TEMPLATE INTO A GPO

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
2. In the left pane of the Active Directory Users and Computers dialog box, expand domains and OUs as necessary until the domain or OU associated with the GPO to which you want to import a security template is displayed in the left pane. Highlight the domain or OU, then select Action ➪ Properties.
3. In the domain or OU's Properties dialog box, click the Group Policy tab.
4. On the Group Policy tab, highlight the GPO to which you want to import a security template and click Edit. (Or, you can double-click the GPO.)
5. The Group Policy dialog box appears. Click the + next to the `Windows Settings` folder in the Computer Configuration section. Then highlight the Security Settings container. Select Action ➪ Import Policy.
6. In the Import Policy From dialog box, the security templates on this computer are displayed. Double-click the security template you want to import into the GPO.
7. Close the Group Policy dialog box.
8. In the domain or OU's Properties dialog box, click OK.
9. Close Active Directory Users and Computers.

Using Security Configuration and Analysis

Security Configuration and Analysis is another snap-in to the MMC. You can use this snap-in to compare the security configuration on a Windows 2000 computer against a predefined security configuration in a security template that is loaded into the Security Configuration and Analysis snap-in. You can also use this snap-in to apply a security template's settings to the local computer. Like the Security Templates snap-in, you must be a member of the Administrators group to use the Security Configuration and Analysis snap-in.

EXAM TIP

Both the Server and Directory Services exams have objectives relating to security configuration and analysis. Make sure you are very comfortable with both the Security Templates and the Security Configuration and Analysis snap-ins before you take these exams.

Before you can use the Security Configuration and Analysis snap-in, you'll probably want to add it to the security console you created earlier in this chapter.

STEP BY STEP

ADDING THE SNAP-IN TO YOUR SECURITY CONSOLE

1. Open the security console you created earlier in this chapter. (Select Start ➪ Programs ➪ Administrative Tools ➪ *Security Console*.)
2. In the security console dialog box, select Console ➪ Add/Remove Snap-in.
3. In the Add/Remove Snap-in dialog box, click Add.
4. In the Add Standalone Snap-in dialog box, scroll down and highlight Security Configuration and Analysis. Click Add. Then click Close.
5. In the Add/Remove Snap-in dialog box, click OK.
6. In the security console dialog box, select Console ➪ Save.
7. Close the security console dialog box.

I'll show you how to use the Security Configuration and Analysis snap-in in the following sections.

Creating and Opening a Database

Before you can use the Security Configuration and Analysis snap-in to analyze a computer's security configuration, you must first create or open a database within the snap-in. This database will contain the settings from a security template against which the computer's security configuration will be compared.

STEP BY STEP

CREATING AND OPENING A DATABASE

1. Open the security console you created earlier in this chapter. (Select Start➪ Programs➪ Administrative Tools➪ *Security Console*.)
2. In the left pane of the security console, highlight Security Configuration and Analysis. Select Action➪ Open database. (Or, you can right-click Security Configuration and Analysis and select Open database from the menu that appears.)
3. The Open database dialog box appears. The contents of the `Database` folder on this computer are displayed. By default, this folder is empty.

   To open a database that you have previously created, double-click the database.

   To create a new database, type in a name for the database in the "File name" text box, and click Open.
4. In the Import Template dialog box, the security templates on this computer are displayed. Double-click the security template you want to import into the database.
5. Windows 2000 creates the database and returns you to the security console dialog box. Leave this dialog box open if you plan to analyze or configure your computer.

Analyzing a Computer

Once you've created a database (or opened an existing database) in the Security Configuration and Analysis snap-in, you're ready to use this snap-in to analyze your computer. What really happens here is that the Security Configuration and Analysis snap-in compares your computer's security configuration settings against the security configuration settings in the security template you've loaded into the database.

Once the analysis is performed, you can view the results of the analysis by using the Security Configuration and Analysis snap-in, and determine whether your computer meets the security standards specified in the security template.

STEP BY STEP

ANALYZING A COMPUTER'S SECURITY CONFIGURATION

1. Open the security console you created earlier in this chapter. (Select Start ➪ Programs ➪ Administrative Tools ➪ *Security Console*.)
2. If you haven't already done so, follow the steps in the previous section to create or open a database.
3. In the left pane of the security console, highlight Security Configuration and Analysis. Select Action ➪ Analyze Computer Now.
4. In the Perform Analysis dialog box, click OK to accept the default error log file path.
5. Security Configuration and Analysis analyzes the computer.
6. To view the results of the analysis, in the left pane of the security console dialog box, click the + next to Security Configuration and Analysis. Then continue expanding containers and folders until the container or folder that contains the security settings for which you want to view the analysis results is displayed in the left pane. Highlight that container or folder.
7. The analysis results are displayed in the right pane of the security console, as shown in Figure 13-14. Notice the symbols used to indicate compliance or noncompliance with the security settings in the database. An X in a red circle indicates noncompliance, and a check mark in a white circle indicates compliance.

   Also notice the Database Setting and Computer Setting columns. The Database Setting column displays the desired security settings, as specified by the security template settings contained in the database. The Computer Setting column displays the computer's actual security settings.
8. When you finish viewing the results of the analysis, close the security console. Or, if you want to apply the security settings in the database to the computer, leave the security console open—I'll show you how to apply these settings to your computer in the next section.

STEP BY STEP *Continued*

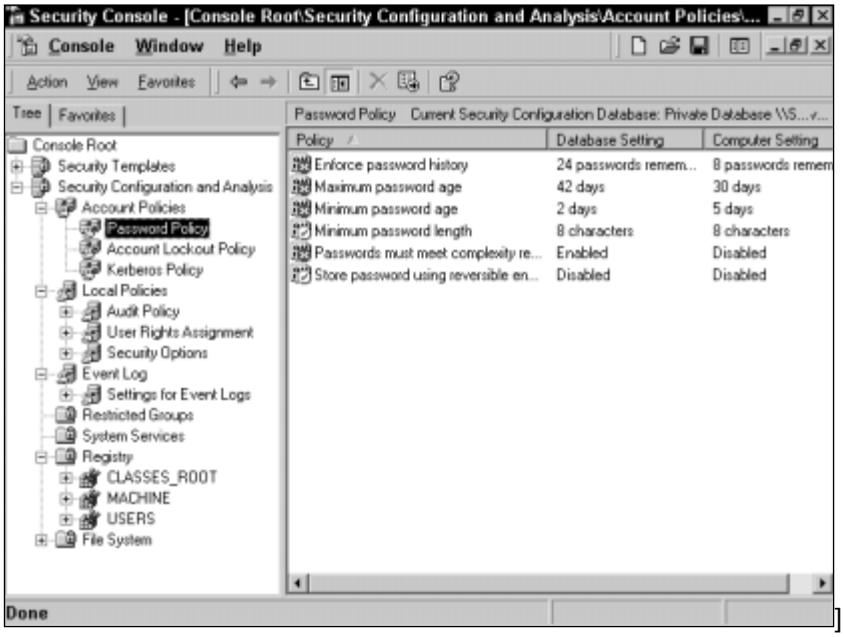

FIGURE 13-14 Viewing analysis results

Configuring a Computer

Once you've analyzed your computer against a predefined set of security settings, you may decide that you want to apply the security template settings contained in the Security Configuration and Analysis database to the local computer. For example, if the results of the analysis show that your computer doesn't meet your company's security settings standard (as set forth in the security template you used in the database to analyze the computer), you may need to use the Security Configuration and Analysis snap-in to apply the settings in the template to the noncompliant computer.

STEP BY STEP

APPLYING SECURITY SETTINGS TO THE LOCAL COMPUTER

1. Open the security console you created earlier in this chapter. (Select Start➪ Programs➪ Administrative Tools➪ *Security Console*.)
2. If you haven't already done so, follow the steps in the previous section to create or open a database. Make sure you select a database that contains the security settings you want to apply to this computer.

   Optionally, you may want to analyze the computer to compare its security settings with those contained in the database.
3. In the left pane of the security console, highlight Security Configuration and Analysis. Select Action➪ Configure Computer Now.
4. In the Configure System dialog box, click OK to accept the default error log file path.
5. Security Configuration and Analysis configures your computer's security settings. This takes a few minutes.
6. Close the security console dialog box. If prompted, click Yes to save settings to the security console.

Using the Command-Line Version of Security Configuration and Analysis

You can use a command-line version of the Security Configuration and Analysis snap-in, called `secedit.exe`, to perform the same tasks you can perform by using the snap-in. You can use `secedit.exe` to create and open a database, analyze a computer, and apply security settings to a computer. In addition to performing security configuration and analysis tasks, you can use `secedit.exe` to force an immediate refresh of Group Policy settings on the local computer.

So why would you want to use a command-line version of a tool when you can use a nice, GUI version? Well, let me ask you, do you want to sit down at each and every computer on your network and perform security analysis? Or would you rather configure a computer startup script that includes `secedit.exe` commands to analyze the computer's security configuration for you automatically? You can even specify the network location where `secedit.exe` will store the results of the analysis, so you can view the log files at a later time.

The syntax and parameters for `secedit.exe` are beyond the scope of this book. However, you can easily access the Windows 2000 Help for the `secedit.exe` command-line utility.

STEP BY STEP

ACCESSING HELP FOR SECEDIT.EXE

1. Select Start ➪ Run.
2. In the Run dialog box, type **secedit /?** in the Open text box, and click OK.
3. The Automating Security Configuration Management Help dialog box appears, which contains extensive information on using `secedit.exe`.

Troubleshooting Auditing and Security

Auditing and security problems are sometimes difficult to diagnose. Often, you don't even know a problem exists until someone violates your network's security. Auditing and security problems typically fall into one of two categories: either a user who is supposed to have access to a particular network resource is unable to access that resource, or a user who isn't supposed to be able to access a resource has somehow been able to breach your security and gain access.

No matter which category your auditing and security problem falls into, the troubleshooting approach you use to solve it is the same. I recommend that you first identify, as clearly as possible, your problem, including which user(s) and resource(s) are affected by the problem. Once you've clearly identified your problem, I recommend that you analyze the security configuration for the resource in question and determine the cause of the problem. Finally, you can take the appropriate steps to resolve the problem.

That said, here are a few tips to help you diagnose and resolve auditing and security problems.

- If you've configured object access auditing in the Properties dialog box of an object, but no events are appearing in the Security Log, ensure that you have also enabled the appropriate type of system

access auditing (either auditing of object access or auditing of directory service access, depending on the object you want to audit). Remember that until auditing is configured in *both* places, object access auditing won't occur.

- Suppose that you've enabled system access auditing, and you've also enabled object access auditing for a specific object. You log on as a user with no permissions to access the object and try to gain access to the object multiple times. However, when you view the Security Log, no audit events indicating your attempts to access the object are displayed. In this situation, ensure that the Failure check box is selected for system access auditing, and also that the Failed check box is selected for all types of access to the object. These check boxes will produce audit events for unsuccessful attempted accesses to the object.
- Suppose that you've applied an audit policy to a Windows 2000 computer (that is a member of a domain) by using Local Security Policy, but when you view the effective audit policy settings in Local Security Policy, the effective settings are listed as "No auditing." In this case, you should check the audit policy settings that may be set at another level of the network, including the audit policy settings in each Group Policy object that affects this computer. Remember the Group Policy inheritance rules, and that the Group Policy applied last is the one that takes precedence.
- If you're concerned that users and other administrators have modified security settings on their Windows 2000 computers away from the company's standard security settings, you can use the Security Configuration and Analysis snap-in to compare these computers against the predefined security settings adopted by your company. If differences are detected, you can also use Security Configuration and Analysis to apply the company's security settings to noncompliant computers.
- If you've imported security templates into a GPO to provide security for your Directory Services infrastructure, but the template isn't being applied the way you thought it would be applied, ensure that inheritance is not preventing the application of the security settings in the GPO.

KEY POINT SUMMARY

This chapter introduced several important auditing and security topics:

- When enabled, auditing produces a log of specified security events that occur on a Windows 2000 computer. Audited events are written to the Security Log in Event Viewer. By default, auditing is not enabled.
- Windows 2000 auditing is divided into two areas: system access auditing and object access auditing. If you want to perform object access auditing, you must also enable system access auditing.
- There are a number of tools you can use to configure Audit Policy, including Local Security Policy, Domain Security Policy, Domain Controller Security Policy, Active Directory Users and Computers, and so on. The tool you use depends on which computer(s) you want the audit policy to apply to.
- To modify the auditing configuration of Active Directory Objects, use Active Directory Users and Computers (or Active Directory Sites and Services, if you want to modify the auditing configuration of a site).
- Use Windows Explorer to configure auditing of files or folders.
- Use the `Printers` folder to configure auditing of printers.
- You can use Event Viewer to view, monitor, and analyze the results of the auditing.
- A security template is a text-based `.inf` file that contains predefined security settings that can be applied to one or more computers. You can use the Security Templates snap-in to the MMC to create, edit, and manage security templates.
- You can either apply a security template directly to the local computer, or you can import a security template into a GPO where it will be applied to all computers affected by that GPO.
- The Security Configuration and Analysis snap-in is used to compare the existing security configuration of a Windows 2000 computer against a predefined security configuration in a security template.
- There is a command-line version of the Security Configuration and Analysis snap-in—it's called `secedit.exe`.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about auditing and security, and to help you prepare for the Professional, Server, and Directory Services exams:

- **Assessment Questions:** These questions test your knowledge of the auditing and security topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenarios, you are asked to troubleshoot auditing and security problems and answer the questions following each problem. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab Exercises: T**hese exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice managing auditing and security in Windows 2000.

Assessment Questions

1. You want to enable system access auditing on a Windows 2000 Server computer that is a domain controller. Which tool should you use?
   A. System
   B. Windows Explorer
   C. Domain Security Policy
   D. Domain Controller Security Policy
2. You want to enable auditing of several folders on a Windows 2000 Professional computer. You have already enabled system access auditing. Which tool should you use?
   A. Local Security Policy
   B. Windows Explorer
   C. Folder Options
   D. System

3. Three days ago you configured auditing of a printer on a Windows 2000 computer that is a member of a domain, but no audit events are being written to the Security Log, even though you know that users have printed more than 100 documents to this printer. What should you do to resolve the problem?
   A. Either wait for the audit policy to be propagated to this computer, or use `secedit.exe` to force a refresh of audit policy on this computer.
   B. Enable system access auditing on the Windows 2000 computer.
   C. Configure the filter on the Security Log so that both "Success audit" and "Failure audit" events are displayed.
   D. Shut down and restart the computer so the audit policy will take effect.
4. Which Event Viewer log can you use to view the results of auditing?
   A. Application Log
   B. Security Log
   C. System Log
   D. Directory Service log
5. You recently used Domain Security Policy to set Audit Policy for all of the Windows 2000 computers in a domain. However, the Audit Policy settings are not being applied to your domain controller. In fact, when you configured object access auditing for folders on the domain controller, you received a Security message indicating that "the current Audit Policy for this computer does not have auditing turned on." What should you do to resolve the problem?
   A. Use Add/Remove Programs to add and enable the auditing feature on the domain controller.
   B. Use Local Security Policy to enable auditing on the domain controller.
   C. Use Domain Controller Security Policy to enable auditing on the domain controller.
   D. Wait until the Audit Policy is propagated from the domain to the domain controller. Then reconfigure object access auditing to the folders.

6. Which tasks can you perform by using the Security Templates snap-in to the MMC? (Choose all that apply.)
   A. Create security templates.
   B. Edit security templates.
   C. Import security templates.
   D. Compare a computer's security configuration settings against the security configuration settings in a specific security template.
7. What is the name of the command-line utility you can use to perform the same tasks as you can perform by using Security Configuration and Analysis?
   A. `gpedit.msc`
   B. `secpol.msc`
   C. `poledit.exe`
   D. `secedit.exe`
8. You are archiving a Security Log for later analysis in a spreadsheet. Which file type should you assign to the log when you save it?
   A. `.evt`
   B. `.txt`
   C. `.csv`
   D. `.exe`

Scenarios

Troubleshooting auditing and security on a Windows 2000 computer or a Windows 2000 network can be a painstaking, though necessary, task. For each of the following troubleshooting problems, consider the given facts and answer the questions that follow.

1. You recently configured object access auditing for multiple files and folders on a Windows 2000 Server computer, but no auditing events are appearing in the Security Log.
   a. What is the most likely cause of this problem?
   b. What should you do to resolve this problem?

2. You recently configured a security policy on a Windows 2000 Professional computer (that is a member of a domain) by using Local Security Policy. You also configured security policy settings in multiple GPOs in Active Directory that apply to various computers throughout the domain. However, when you view the effective settings for Security Options in Local Security Policy, the effective settings are listed as "Not defined."
   a. What is the most likely cause of this problem?
   b. What should you do to resolve this problem?

Lab Exercises

Lab 13-1 Managing Auditing and Security

- Professional
- Server
- Directory Services

The purpose of this lab is to provide you with an opportunity to manage auditing and security in a Windows 2000 environment.

There are four parts to this lab:

- Part 1: Implementing Auditing and Audit Policy
- Part 2: Monitoring and Analyzing Security Events
- Part 3: Implementing Security by Using a Security Template
- Part 4: Analyzing and Applying a Security Configuration

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Implementing Auditing and Audit Policy

In this part, you implement a domain audit policy, refresh your computer's policy settings, and then configure auditing of a folder, a printer, and an Active Directory object.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Domain Controller Security Policy.

2. In the left pane of the Domain Controller Security Policy dialog box, click the + next to Security Settings. Then click the + next to Local Policies. Highlight Audit Policy.
3. In the right pane, double-click "Audit directory service access."
4. In the Security Policy Setting dialog box, select the check box next to "Define these policy settings." Then, ensure that the check boxes next to Success and Failure are both selected. Click OK.
5. In the right pane, double-click "Audit logon events."
6. In the Security Policy Setting dialog box, select the check box next to "Define these policy settings." Then ensure that the check boxes next to Success and Failure are both selected. Click OK.
7. In the right pane, double-click "Audit object access."
8. In the Security Policy Setting dialog box, select the check box next to "Define these policy settings." Then ensure that the check boxes next to Success and Failure are both selected. Click OK.
9. Close the Domain Controller Security Policy dialog box.
10. Select Start ➪ Run.
11. In the Run dialog box, type

    ```
    secedit /refreshpolicy machine_policy
    ```

    and click OK.
12. Start Windows Explorer. (Select Start ➪ Programs ➪ Accessories ➪ Windows Explorer.)
13. In the left pane, click the + next to My Computer, then highlight Local Disk (C:).
14. In the right pane, right-click the `Program Files` folder and select Properties from the menu that appears.
15. In the Program Files Properties dialog box, click the Security tab.
16. On the Security tab, click Advanced.
17. In the Access Control Settings for Program Files dialog box, click the Auditing tab.
18. On the Auditing tab, click Add.
19. In the Select User, Computer, or Group dialog box, double-click the Authenticated Users group.

20. In the Auditing Entry for Program Files dialog box, select the Successful and Failed check boxes next to List Folder/Read Data. Click OK.
21. In the Access Control Settings for Program Files dialog box, click OK.
22. In the Program Files Properties dialog box, click OK.
23. In the left pane, scroll down and click the + next to Control Panel. Then highlight the `Printers` folder.
24. In the right pane, right-click the AGFA-AccuSet v52.3 printer, and select Properties from the menu that appears.
25. In the AGFA-AccuSet v52.3 Properties dialog box, click the Security tab.
26. On the Security tab, click Advanced.
27. In the Access Control Settings for AGFA-AccuSet v52.3, click the Auditing tab.
28. On the Auditing tab, click Add.
29. In the Select User, Computer, or Group dialog box, double-click the Everyone group.
30. In the Auditing Entry for AGFA-AccuSet v52.3, select the Successful and Failed check boxes next to Print. (The Read Permissions check boxes are automatically checked when you select the Print check boxes.) Click OK.
31. In the Access Control Settings for AGFA-AccuSet v52.3 dialog box, click OK.
32. In the AGFA-AccuSet v52.3 Properties dialog box, click OK.
33. Close the `Printers` folder.
34. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
35. In the left pane of the Active Directory Users and Computers dialog box, highlight `domain1.mcse`. Select Action ➪ Properties.
36. In the domain1.mcse Properties dialog box, click the Security tab.
37. On the Security tab, click Advanced.
38. In the Access Control Settings for domain1 dialog box, click the Auditing tab.

39. On the Auditing tab, double-click the default auditing entry named Everyone.
40. In the Auditing Entry for domain1 dialog box, notice the default settings on both the Object and Properties tabs. Then, on the Object tab, select the Successful and Failed check boxes next to List Contents. Click OK.
41. In the Access Control Settings for domain 1 dialog box, click OK.
42. In the domain1.mcse Properties dialog box, click OK.
43. Close Active Directory Users and Computers.

Part 2: Monitoring and Analyzing Security Events

In this part, you create a failure audit event, and then use Event Viewer to view, filter, and analyze auditing and security events.

1. Select Start ➪ Shut Down.
2. In the Shut Down Windows dialog box, select Log off Administrator from the drop-down list box. Click OK.
3. Press Ctrl + Alt + Delete. In the Log On to Windows dialog box, type in a user name of **Administrator**, a password of **wrongo**, and click OK.
4. In the Logon Message dialog box, click OK.
5. In the Log On to Windows dialog box, type in a user name of **Administrator**, a password of **password**, and click OK.
6. Select Start ➪ Programs ➪ Administrative Tools ➪ Event Viewer.
7. In the left pane of the Event Viewer dialog box, highlight the Security Log. Notice the large number of events that appear in the right pane. Select View ➪ Filter.
8. In the Security Log Properties dialog box, clear the check boxes next to Information, Warning, Error, and Success audit. Click OK.
9. The Security Log in Event Viewer reappears. Notice that now only failure audit events are listed in the right pane. In the right pane, double-click the most recent failure audit event. (This is the event at the top of the list.)

10. In the Event Properties dialog box, read the detailed information about the audit event. Notice that the failure event is a logon failure due to an unknown user name or a bad password. (This is the event you generated in Step 3.) Click OK.
11. Close Event Viewer.

Part 3: Implementing Security by Using a Security Template

In this part, you add the Security Templates snap-in and the Security Configuration and Analysis snap-in to an MMC console. Then you use the Security Templates snap-in to create a new security template. Finally, you apply the new security template to both the local computer and to a GPO in Active Directory.

1. From the desktop, select Start ➪ Run.
2. In the Run dialog box, type **mmc** and click OK.
3. A new MMC console, named Console1, is displayed. Maximize the Console Root dialog box within the Console 1 dialog box. Select Console ➪ Add/Remove Snap-in.
4. In the Add/Remove Snap-in dialog box, click Add.
5. In the Add Standalone Snap-in dialog box, scroll down and double-click Security Templates. Then double-click Security Configuration and Analysis. Then click Close.
6. In the Add/Remove Snap-in dialog box, click OK.
7. In the Console1 (Console Root) dialog box, select Console ➪ Save As.
8. In the Save As dialog box, type **Security Configuration Tool Set** in the "File name" text box, and click Save.
9. In the left pane of the console, click the + next to Security Templates. Then click the + next to `C:\WINNT\Security\Templates`. All of the security templates on your computer, including the predefined security templates, are displayed in the left pane. Highlight `basicsv`. Then select Action ➪ Save As.
10. In the Save As dialog box, type **My Security Template** in the "File name" text box. Click Save.
11. In the left pane of the console, click the + next to `My Security Template`. Then click the + next to Local Policies. Highlight Security Options. In the right pane, double-click "Clear virtual memory pagefile when system shuts down."

12. In the Template Security Policy Setting dialog box, select the check box next to "Define this policy setting in the template." Then select the Enabled option. Click OK.
13. In the left pane of the console, highlight `My Security Template`, and select Action ➪ Save.
14. Close the Security Configuration Tool Set dialog box. When prompted, click Yes to save console settings to the Security Configuration Tool Set.
15. Select Start ➪ Programs ➪ Administrative Tools ➪ Local Security Policy.
16. In the Local Security Settings dialog box, select Action ➪ Import Policy.
17. In the Import Policy From dialog box, double-click `My Security Template`.
18. Close the Local Security Settings dialog box.
19. Select Start ➪ Programs ➪ Administrative Tools ➪ Active Directory Users and Computers.
20. In the left pane of the Active Directory Users and Computers dialog box, highlight `domain1.mcse`. Select Action ➪ Properties.
21. In the domain1.mcse Properties dialog box, click the Group Policy tab.
22. On the Group Policy tab, highlight the Default Domain Policy GPO, and click Edit.
23. In the Group Policy dialog box, click the + next to the `Windows Settings` folder in the Computer Configuration section. Then highlight the Security Settings container. Select Action ➪ Import Policy.
24. In the Import Policy From dialog box, double-click `My Security Template`.
25. Close the Group Policy dialog box.
26. In the domain1.mcse Properties dialog box, click OK.
27. Close Active Directory Users and Computers.

Part 4: Analyzing a Security Configuration

In this part, you use Security Configuration and Analysis to analyze your Windows 2000 Server computer's current security configuration.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Security Configuration Tool Set.

2. In the left pane of the console, highlight Security Configuration and Analysis. Select Action ➪ Open database.
3. In the Open database dialog box, type **My Database** in the "File name" text box, and click Open.
4. In the Import Template dialog box, double-click `hisecdc`.
5. Windows 2000 creates the database and returns you to the console dialog box. In the left pane of the console, highlight Security Configuration and Analysis. Select Action ➪ Analyze Computer Now.
6. In the Perform Analysis dialog box, click OK to accept the default error log file path.
7. Security Configuration and Analysis analyzes the computer.
8. To view the results of the analysis, in the left pane of the console, click the + next to Security Configuration and Analysis. Click the + next to Local Policies. Then highlight Security Options.
9. The analysis results are displayed in the right pane. Notice that this computer is not compliant with the security settings in the `hisecdc` security template. Close the Security Configuration Tool Set dialog box. If prompted, click Yes to save console settings to the Security Configuration Tool Set.

Answers to Chapter Questions

Chapter Pre-Test

1. Windows 2000 auditing is divided into two areas: auditing of access to the system (often called system access auditing) and auditing of access to objects (often called object access auditing).
2. You can audit a number of different objects in Windows 2000, such as Active Directory objects (including users, groups, computers, OUs, domains, and so on), files, folders, and printers.
3. Event Viewer
4. A security template is a text-based `.inf` file that contains predefined security settings that can be applied to one or more computers. A security template can also be used to compare a computer's existing security configuration against a predefined, standard security configuration.

5. You can use the Security Templates snap-in to create, edit, and manage security templates.
6. There are two primary ways to implement a security template: you can either apply the security template directly to the local computer; or you can import the security template into a Group Policy object (GPO) in Active Directory, where it will be applied to all computers affected by that GPO.
7. The Security Configuration and Analysis snap-in

Assessment Questions

1. **D.** Using Domain Controller Security Policy is the best choice. You can set audit policy in Domain Security Policy, but auditing will *not* be enabled on domain controllers until you enable it in the Default Domain Controllers Policy GPO by using either the Domain Controller Security Policy tool, Active Directory Users and Computers, or the Group Policy snap-in to the MMC.
2. **B.** Once system access auditing has been enabled, you can enable object access auditing of folders by configuring the folders' Properties dialog boxes in Windows Explorer.
3. **B.** The most likely cause of the lack of audit events in the Security Log is that system access auditing has not yet been enabled on this Windows 2000 computer. To audit access to an object, such as a printer, you must not only configure object access auditing, you must configure system access auditing as well.
4. **B.** Audited events are written to the Security Log in Event Viewer.
5. **C.** Because the domain controller's Audit Policy is being overridden by the Default Domain Controllers Policy GPO, you should use Domain Controller Security Policy (or Active Directory Users and Computers) to modify this GPO and thereby enable auditing on the domain controller.

6. **A, B.** You can create, edit, delete, and save security templates by using the Security Templates snap-in. However, if you want to import a security template you'll need to use another tool, such as Local Security Policy or Active Directory Users and Computers. If you want to compare a computer's security configuration against the configuration of a specific template, you'll need to use Security Configuration and Analysis.
7. **D.**
8. **C.** Saving the Security Log as a comma-delimited file is probably the best choice if you want to analyze the data later in a spreadsheet.

Scenarios

1. The most likely cause of this problem is that system access auditing for object access has not been enabled on the Windows 2000 Server computer. To resolve the problem, use the appropriate tool (Local Security Policy, Domain Security Policy, Domain Controller Security Policy, and so on) to enable system access auditing on the Windows 2000 Server computer. Then auditing of the files and folders will occur, and the audit events will be written to the Security Log.
2. The most likely cause of this problem is that security policy settings in a GPO are overriding the security policy settings you set on this Windows 2000 Professional computer by using Local Security Policy. Check the security policy settings set at other levels of the network, including each GPO that may affect this computer. Remember the Group Policy inheritance rules, and that the Group Policy applied last is the one that takes precedence.

MCSE
EXAM
MATERIAL