**<CHN>CHAPTER SIX**

**<CHT>HOST, APPLICATION, AND DATA SECURITY**

**<COOT>Labs included in this chapter**

* <COOH1>Lab 6.1 Exploring the Windows Server 2016 Group Policy Management
* Lab 6.2 Creating a Security Template
* Lab 6.3 Analyzing Security Configurations
* Lab 6.4 Applying Security Settings from a Security Template and Verifying System Compliance
* Lab 6.5 Auditing Object Access

<COOBT>CompTIA Security+ Exam Objectives

<COOBL>Domain Lab

<COOB>Network Security 6.1, 6.2, 6.3, 6.4, 6.5

Application, Data and Host Security 6.1, 6.2, 6.3, 6.4, 6.5

Access Control and Identity Management 6.4, 6.5

# <H1>Lab 6.1 Exploring the Windows Server 2016 Group Policy Management

**<H2>Objectives**

<TX1>You can use the Group Policy Management Console in Windows Server 2016 to create policies at different account levels, an essential maintenance and configuration task. The Group Policy Management dialog provides easy access to important security settings.

The policies found within the management console can also be accessed from the server’s hard drive, but the console simplifies the process of policy creation. Note that the previous tool of choice for this job, the Security Configuration Wizard, has been deprecated in favor of the Group Policy Management Console.

<TX2>After completing this lab, you will be able to:

* <BL>Describe the functions available in the Windows Server 2016 Group Policy Management Console
* Use the Windows Server 2016 Group Policy Management Console to create and apply a policy

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Completion of Lab 6-1
* Windows 10 VM (Called *Win10*)

**<H2>Activity**

<FE1TX1>Estimated completion time: **20–30 minutes**

In this lab, you configure your server to apply a policy that can be applied to any computer connected to the domain.

1. <NL\_FIRST>Load the *Windows Server* VM. Click **Tools**, then click **Active Directory Users and Computers**.
2. <NL\_MID>Right click the **TESTDOMAIN.local** server and select **New/Organizational Unit**. Name the OU **Test OU**. Then click **OK**.
3. Verify that the OU appears in the list below the TESTDOMAIN.local AD tree.
4. Right click **Test OU** and select **New/Organizational Unit**. Name the OU **Groups**, and then click **OK**. Repeat this process to make two more OUs under Test OU. Name them **Users** and **Servers**.
5. Create a policy on the *Windows Server* as follows: click Start, select **Windows** Administrative Tools, and click Group Policy Management.
6. Expand the tree until you see the Test OU item under TESTDOMAIN.local. Expand the **Test OU** and confirm that Groups, Servers, and Users all appear.
7. Right click **Test OU** and select **Create a GPO in this domain, and link it here**. Name the GPO **Test Settings** and click **OK**.
8. Expand the Group Policy Object under the TESTDOMAIN.local tree and verify that **Test Settings** now exists.
9. Under the Group Policy Object, right click **Test Settings** and select **Edit**. Note that the Test Settings configuration tree has two sections, Computer Configuration and User Configuration.
10. In both sections, look for Policies and Preferences. Note that there is a distinct difference between a policy and a preference. Policies are refreshed every 90 minutes and preferences are enforced at logon. You must decide when you want the policies enforced. If you want to make a suggestion and allow the user to be able to change the default setting, then you would use preferences. Many times, when you set a configuration in the Policies area, the relevant control will be greyed out at the user level.
11. Explore the policies folders under both the Computer Configuration and the User Configuration.
12. Expand **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **All settings**.
13. Find and double-click **Add Logoff to the Start Menu**.
14. Click **Enabled**, click **Apply**, and then click **OK**.

[BEGIN NOTE]

<B1TX1>Any computer connected to the domain TESTDOMAIN.local will now have the option of Logoff added to their Start Menu.

[END NOTE]

1. To make sure the policy is enforced right away, open a command window on the *Windows Server* and enter the command **gpupdate /force**.
2. Launch the *Win10* VM and validate that the Logoff option is now part of the Start Menu.
3. Close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.8 Explain how resiliency and automation strategies reduce risk.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.
* 5.1 Explain the importance of policies, plans, and procedures related to organizational security.

**<H2>Review Questions**

1. <MULT>The Group Policy Management Console has two main sections: Computer Configuration and User Configuration. Which of the following statements about these sections is false?
   1. <MULTA>If you create a policy at the Computer Configuration level, it will affect all computers connected to the domain.
   2. **If you make a policy at the User Configuration level, it will drill down into whichever computer the user logs into and changes the default settings of the computer.**
   3. The User Configuration level can be used to configure the control panel and start menu for all users logged into the given domain.
   4. A preference policy is only enforced at login.
2. <TF>A group policy will be enforced if a user uses remote administration to control a computer. **True** or False?
3. <MULT>Which of the following is not an option for Policy settings?
   1. **<MULTA>Configured**
   2. Enabled
   3. Not Configured
   4. Disabled
4. <TF>The Security Management Console exists in Windows Server 2016. True or **False**?
5. <TF>Configuration of a group policy should be done at the highest possible level in the domain tree. **True** or False?

# <H1>Lab 6.2 Creating a Security Template

**<H2>Objectives**

<TX1>Creating a policy template can help streamline server configuration as well as any other network configuration. You can use the Microsoft Management Console (MMC) to create templates that you can then import into the Group Policy Management Console. The MMC can play a large role in replication of policies across multiple servers. You can create the policy in the MMC and then export it to many different servers. If the servers are correctly configured to inherit their settings, you can implement the policy at the root node and allow the network to propagate itself with the proper policies.

<TX2>After completing this lab, you will be able to:

* <BL>Explain the general types of security settings available in the MMC
* Create security templates using the MMC
* Import the template into the Group Policy Management Console

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Completion of Lab 6.1

**<H2>Activity**

<FE1TX1>Estimated completion time: **15 minutes**

<TX1>In this lab, you create a security template that has a single policy. This single policy will enable Audit Logs to log any failed login attempts.

1. <NL\_FIRST>Launch the Windows Server VM.
2. <NL\_MID>Open a command prompt window, type mmc, and then press Enter. This launches a Microsoft Management Console, a utility that allows the creation of custom tool sets.
3. From the File menu, click Add/Remove Snap-in.
4. In the Available snap-ins box, scroll down and select Security Templates, and then click Add. The Security Templates tool appears in the Selected snap-ins box, as shown in Figure 6-1.

**[Insert Figure 6-1 Here]**

1. From the **File** menu, select Save As. In the File name box, type **Audit** Template and save the console to your desktop.
2. If necessary, expand the Security Templates node in the left pane to show the Test Template folder, as shown in Figure 6-2.

**[Insert Figure 6-2 Here]**

1. Expand the **Local Policies** tree, click **Audit Policy**, double-click the Audit logon events.
2. Select the **Define these policy settings in the template** checkbox, then select **Failure**. Click **Apply**, and then click **OK**.
3. Click the **File** menu, and then click **Save**.
4. Open the Group Policy Management Console. Launch Server Manager, click **Tools**, and then click **Group Policy Management** as shown in Figure 6-3.

**[Insert Figure 6-3 Here]**

1. Locate the Test OU from Lab 6.1. Expand the **Test OU** tree, right-click **Test Setting**, and then click **Edit**.
2. Expand the tree in the Group Policy Editor until you see the Security Settings under “Computer Configuration.”
3. Right-click **Security Settings** and select **Import Policy**. Navigate to the location where you saved Test Template and click **OK**.
4. Verify that the Audit logon events policy is set to Failure.
5. Open the MMC and create a second policy that restricts the icons that appear on the desktop of the computer. Import it into the Group Policy Management console when you are finished creating it.
6. Close all windows. If prompted, click Yes to save the console settings, and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>3.8 Explain how resiliency and automation strategies reduce risk.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.
* 5.1 Explain the importance of policies, plans, and procedures related to organizational security.

**<H2>Review Questions**

1. <MULT>Which of the following policies can be configured in Security Templates? (Choose all that apply.)
   1. **<MULTA>Local Policies\Audit Policy\Audit object access**
   2. **Local Policies\User Rights Assignment\Deny logon locally**
   3. **Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation**
   4. **Local Policies\Security Options\Accounts: Rename administrator account**
2. <FIB>In Security Templates, the Registry node allows an administrator to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. **<FIBA>set permissions on registry keys and subkeys**
   2. automate backups of specific registry keys and subkeys
   3. modify the value of registry keys and subkeys
   4. add and delete registry keys and subkeys
3. <MULT>Which of the following policies can be configured in Security Templates? (Choose all that apply.)
   1. **<MULTA>Account Policies\Kerberos Policy\Maximum lifetime for user ticket**
   2. **Account Policies\Account Lockout Policy\Reset account lockout counter after**
   3. Event Log\Create new log
   4. Restricted Logon\Bypass user account control
4. <MULT>Which of the following statements about Account Policy\Kerberos Policy\Maximum lifetime for service ticket is correct? (Choose all that apply.)
   1. **<MULTA>The unit of measurement for this setting is minutes.**
   2. This security setting determines the maximum number of services that a granted session ticket can be used to access.
   3. **Session tickets are used to authenticate new connections with servers.**
   4. **If a session ticket expires during a session, ongoing operations are not interrupted.**
5. <MULT>Which of the following statements is true about the Reset account lockout counter after policy (which is found in Account Policies\Account Lockout Policy)?
   1. <MULTA>This setting determines how long a user must wait before attempting to log on after an account lockout.
   2. The maximum duration of this setting is 10,000 minutes.
   3. **The Reset account lockout value must be less than or equal to the Account lockout duration if an account lockout threshold is defined.**
   4. This setting applies only to Windows 7 clients.

# <H1>Lab 6.3 Analyzing Security Configurations

**<H2>Objectives**

<TX1>Security Templates contains over 250 security policies (for example, Account lockout duration), and that does not include the thousands of custom settings that an administrator can configure in the Restricted Groups, Registry, and File System nodes. Obviously, it would be impractical for administrators to manually investigate each setting on each computer to determine whether any particular setting was correctly configured.

<TX2>The Group Policy Management Console in Windows Server 2016 makes it easier to configure policies from previous version of the OS. The console provides the ability to work with templates created in the MMC and other user-based role definitions.

<TX2>After completing this lab, you will be able to:

* <BL>Use the Group Policy Management Console to import a policy created in the MMC.

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Completion of Lab 6.1
* Completion of Lab 6.2

**<H2>Activity**

<FE1TX1>Estimated completion time: **20 minutes**

<TX1>In this lab, you modify a domain user account and then compare your server’s current security settings with those in the security template you created in Lab 6.2.

1. <NL\_FIRST>Launch the Windows Server VM. In the Server Manager, click **Tools**, then click the Active Directory Users and Computers console.
2. <NL\_MID>Create a user named **Martin T. Sheppard** and add him to the user group under the Test OU/Users folder by doing the following: right-click the **Users** folder, select **New** andthen select **User**. Fill in the appropriate information. Set the password to never expire and remove the option for the user to change the password at next logon.
3. Click the Users container, right-click the account of Martin Sheppard, and select Add to a group.
4. Type Enterprise Admins and click Check Names. When the Enterprise Admins group appears underlined, click OK.
5. Click OK in the Active Directory Domain Services window.
6. Double-click the Enterprise Admins group, click the Members tab, verify that Martin Sheppard is a member of the Enterprise Admins group as shown in Figure 6-4, and then click OK. Close Active Directory Users and Computers.

**[Insert Figure 6-4 Here]**

1. Open the Security Templates console.
2. Right-click Security Templates, select New Template Search Path, navigate to C:\Users\Administrator\Documents\Security, select the Templates directory, and click OK.
3. In the left pane under the Console Root, right-click Restricted Groups and then select Add Group.
4. Click **Browse**, enter **Enterprise Admins** and then click **Check Names**. After the group is found, click **OK**, and then click **OK** three times to close the windows.
5. Notice that the Enterprise Admins appear in the center pane under the restricted groups. With the current settings, Martin Sheppard could not access the domain and the policies would not be enforced on his account.
6. To save the Security Template, click **File** and then click **Save**.
7. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <MULT>In this lab, which policy would not be enforced on the Martin Sheppard account?
   1. **<MULTA>Local Policies\Audit Policy\Audit logon events**
   2. Account Policies\Password Policy\Maximum password age
   3. Account Policies\Account Lockout Policy\Account lockout threshold
   4. Local Policies\Security Options\Accounts: Guest account status
2. <MULT>You are a network administrator and have been tasked with implementing a workstation backup procedure. You must use a backup program that cannot back up open files. You have set logon hours for all users and have asked users to log off when their logon hours expire, but many do not do so or leave work without logging off and with files left open. You want to apply a security policy that will automatically log off users when their logon hours expire. Which policy should you configure?
   1. <MULTA>Account Policies\Account Lockout Policy\Force user logoff
   2. Account Policies\Account Lockout Policy\Force logoff when logon hours expire
   3. **Local Policies\Security Options\Network Security: Force logoff when logon hours expire**
   4. Local Policies\Security Options\Interactive logon: Force logoff when logon hours expire
3. <MULT>You are a network administrator and have hired a consultant to develop drivers to interface between Windows Server 2016 and peripheral devices that were developed in-house. These devices will be connected directly to the Windows Server 2016 servers. You created a user account for the consultant that will expire when his contract is completed. His account is a member of the Domain Users security group. The consultant has completed quality assurance testing of the drivers on his test server. Now he needs to test them in your production environment. He must log on directly to your Windows Server 2016 server to complete the tests. When he comes to the server room and logs on with his account, the following error appears: “You cannot log on because the logon method you are using is not allowed on this computer. Please see your network administrator for more information.” Your organization’s security policies do not permit you to make the consultant’s account a member of any administrative security group, even temporarily. Your goal is to allow the developer to log on locally to your server using his own account. What section of the security settings contains the policy that you must configure to meet your goal?
   1. **<MULTA>User Rights Assignment**
   2. Account Lockout Policy
   3. Kerberos Policy
   4. Restricted Groups
4. <MULT>Which of the following statements is true of the following policy: Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services? (Choose all that apply.)
   1. <MULTA>This setting applies both to local and remote logon.
   2. **This setting has no effect on Windows 2000, Service Pack 1 computers.**
   3. **By default, this setting, when applied to workstations or servers that are not domain controllers, permits members of the Administrators and Remote Desktop Users security groups to log on through Remote Desktop Services.**
   4. This setting, when applied to a system that does not have Terminal Services installed, will install Terminal Services.
5. <TF>The Security Configuration and Analysis console is available on both Windows 10 and Windows Server 2016. True or **False**?

# <H1>Lab 6.4 Applying Security Settings from a Security Template and Verifying System Compliance

**<H2>Objectives**

<TX1>Servers do not generally fall out of compliance with security policy requirements by themselves. Although file corruption or memory errors could theoretically cause these settings to change, it is usually the actions of server administrators that result in alterations of security settings. Sometimes, software installation requires temporary changes in registry permissions. The application of updates and patches can also require temporary changes in security settings. Whatever the reason for deviations from the required security setting, the server administrator is the person to assure that the server is in compliance with security policy requirements. Using the Group Policy Management Console and the Microsoft Management Console, administrators can both audit the compliance of their servers and apply the required settings with a few mouse clicks.

<TX2>After completing this lab, you will be able to:

* <BL>Use the Group Policy Management tool to apply the settings of a security template to a server
* Use the Group Policy Management tool to analyze a system’s compliance with a security template

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Completion of Lab 6.3

**<H2>Activity**

<FE1TX1>Estimated completion time: **10 minutes**

<TX1>In this lab, you apply a setting from a security template to a server and then verify that it completed successfully.

1. <NL\_FIRST>Launch the Windows Server VM
2. <NL\_MID>Open the MMC console you created in Lab 6.3.
3. From the **File** menu, click **Add/Remove Snap-in**.
4. Select **Security Configuration and Analysis**, click **Add**, and then click **OK**.
5. In the left pane under the Console Root, right-click Security Configuration and Analysis and select Open Database. Name the Database **TestDB** and click **Open**. When prompted for a template, select **Test Template**, whichyou created in Lab 6.2.
6. Right-click the Security Configuration and Analysis node, click Analyze Computer Now, and click OK to accept the Error log file path.
7. Under “Security Configuration and Analysis,” click the Restricted Groups node. Notice the green circle with the white check mark inside it, which indicates that the server’s current configuration for this setting is now consistent with the settings in the Restricted Enterprise Admins Group security template.
8. Double-click the Enterprise Admins group listing and verify that the server’s settings and the database settings are compliant. Note that the mtsheppard account is no longer listed as being in the Enterprise Admins group. Close the Enterprise Admins Properties window, close the Security Configuration and Templates console, and save the console settings if prompted.
9. Does Martin Sheppard still have Enterprise Admin privileges on your server? Verify your answer by doing the following to examine Active Directory Users and Computers: Click Start, click Administrative Tools, and open Active Directory Users and Computers.
10. Open the Users container, double-click Martin Sheppard’s account, and click the Member Of tab. The Restricted Groups setting that you configured in the security template has been applied to the server, and it has enforced the setting that states only the Administrator can be a member of the Enterprise Admins group.
11. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <TF>As a result of the steps in this lab, any attempt to add Martin Sheppard to the Enterprise Admins group again would result in an error and the action would not be permitted. True or **False**?
2. <FIB>Preconfigured security templates that ship with Windows Server 2016 and that are used to configure member servers and workstations \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. **<FIBA>can be applied only to Windows Server 2016 systems**
   2. are found in C:\Documents and Settings\All Users\Documents\Security\Templates
   3. are found in C:\Users\Administrator\Documents\Security\Templates
   4. do not exist
3. <MULT>Which of the following statements regarding Security Configuration and Analysis is correct? (Choose all that apply.)
   1. <MULTA>When using Security Configuration and Analysis, once you have created and used a database for applying settings to a server, it cannot be used again; a new, identical database must be created.
   2. **When using Security Configuration and Analysis, you can import multiple security templates into the same database.**
   3. Security Configuration and Analysis can be used to revert to the original, default settings by importing the Setup Security template.
   4. Administrators can create scripts that perform the same function as the Security Configuration and Analysis console using the *scwcmd* command.
4. <MULT>Which of the following statements regarding security settings is correct? (Choose all that apply.)
   1. <MULTA>After installing Services for Macintosh in a Windows Server 2016 system, the Windows server can enforce security settings on a network system running the OS X operating system.
   2. **The System Services node in a security template allows administrators to specify the startup types and permissions for system services.**
   3. **The command-line utility secedit can perform the same function as the Security Configuration and Analysis tool.**
   4. **After the installation of Active Directory on a Windows Server 2016, a default security template is created in C:\Windows\Security\Templates.**
5. <FIB>You have been promoted to Senior Server Administrator. You are transferred to the corporate office and are assigned to administer 45 Windows Server 2016 servers. Unfortunately, the previous administrator did not document the system configurations. You want to determine whether the current security settings on the servers are properly configured. You can do this by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
6. **<FIBA>using Security Configuration and Analysis to analyze each computer, followed by right-clicking Security Configuration and Analysis, and selecting Export Template**
7. right-clicking Security Templates and selecting Export current settings
8. right-clicking the search path node under Security Templates and selecting Export current settings
9. none of the above

# <H1>Lab 6.5 Auditing Object Access

**<H2>Objectives**

<TX1>Hardening a server generally involves keeping current with updates and patches, removing unneeded services and user accounts, and so on. Another important task, especially if the server is in the demilitarized zone (DMZ), is to configure logging of authentication attempts, service events, and users’ access of resources. Of course, logging itself is not enough; the log files need to be reviewed regularly.

<TX2>The oversight of server events is called auditing. By configuring auditing, administrators specify what types of events should be logged. Frequently, it is important to know who accessed an object on a server and what he or she did with it. In Windows Server 2016, objects that can be audited for access include files, folders, drives, and printers. Unlike all other auditing in Windows Server 2016, object access auditing is not functional simply after enabling it in a local security policy or in a group policy. Once object access auditing is activated, the administrator must then specify which objects are to be audited.

<TX2>Auditing can be configured to a granular level for both event failures and event successes. Although it might seem obvious why an administrator would want to audit failures, it may not be as obvious why auditing object access successes is useful; the information resulting from the auditing of successes can be used to assess resource usage and help determine the need for system upgrades.

<TX2>After completing this lab, you will be able to:

* <BL>Create domain user and group accounts
* Configure NTFS permissions on a folder
* Enable object access auditing
* Configure auditing object access on resources
* Examine security logs for access successes and failures

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016 VM
* Completion of Lab 6.2
* Completion of Lab 6.4

**<H2>Activity**

<FE1TX1>Estimated completion time: **40–50 minutes**

<TX1>In this lab, you configure auditing.

1. <NL\_FIRST>Log on to Windows Server as Administrator.
2. <NL\_MID>Click File Explorer, then double-click Local Disk (C:).
3. In the right pane, right-click in a blank area and select New, click Folder, and name the folder Sales.
4. Open the Sales folder. In the right pane, right-click in a blank area, select New, click Text Document, and name the document Sales Report.
5. Open the Sales Report document and enter the following text: Please enter your sales estimates for this quarter here.
6. From the File menu, select Exit and click Save.
7. Close the Sales window.
8. Click Start, click Administrative Tools, and double-click Active Directory Users and Computers. If necessary, expand your domain (Teamx.net), right-click the Users container, click New, click User, and create two users configured as shown in Table 6-1.

**[Start Table 6-1 Here]**

|  |  |  |  |
| --- | --- | --- | --- |
| <TBCH>Full Name | User Logon Name | Password | User Must Change Password at Next Logon</TBCH> |
| <TBTX1>Martin Sheppard | mtsheppard | Pa$$word | unchecked |
| Anthony Newman | anewman | Pa$$word | Unchecked</TBTX1> |

**<TBN>Table 6-1** User account configuration

**[End Table 6-1 Here]**

1. Right-click the Users container, click New, and click Group. Verify that the Group scope is set to Global and that the Group type is set to Security. In the Group name box, type Sales Managers and click OK. Repeat this procedure to create a second global security group named Sales Associates.
2. Double-click the Sales Managers group, click the Members tab, and click the Add button. In the Enter the object names to select box, type Martin and click the Check Names button. When the Martin Sheppard account appears underlined, click OK, then click OK on the Sales Managers Properties window. Repeat this procedure to make Anthony Newman a member of the Sales Associates global group, and then close Active Directory Users and Computers.
3. Click **File Explorer**, then double-click Computer, open Local Disk (C:), right-click the Sales directory, click Properties, click the Security tab, click Edit, select the Users group, and click Remove. Read the error message that appears. Inheritance of permissions set at the root of C: must be blocked before you can remove the Users group.
4. Click OK on the error message and close the Permissions window. In the Sales Properties window, click the Advanced button. In the Advanced Security Settings for Sales window, click the **Disable inheritance** button, click the convert inherited permissions into explicit permissions on this object option, click OK in the Advanced Security Settings for Sales window, and click OK again.
5. In the Sales Properties window, click Edit, select the Users group, and click Remove. Click the Add button. In the Enter the object names to select box, type Sales, and then click Check Names. Holding the Ctrl key, select both the Sales Associates and Sales Managers groups, release the Ctrl key, and click OK. Click OK in the Select Users, Computers, Service Accounts or Groups window. In the Permissions for Sales window, select Sales Associates and check the Full control box in the Allow column. Sales Associates should now have Full control, Modify, Read & execute, List folder contents, Read, and Write checked.
6. Click Sales Managers and verify that users in this group have only the following permissions: Read & execute, List folder contents, and Read checked. Note that members of the Sales Managers group will be able to read documents in the Sales folder but will not be allowed to write to the files or directory or delete anything in it. Click OK in the Permissions for Sales window, and click OK in the Sales Properties window.
7. To allow non-administrative accounts to log on locally to the domain controller so that you can test the new users’ permissions, do the following: in Server Manager, click **Tools**, double-click Group Policy Management, expand the Forest, expand Domains, expand your domain, expand the Domain Controllers, right-click the Default Domain Controllers Policy, and click Edit.
8. Under Computer Configuration, expand Policies, expand Windows Settings, expand Security Settings, expand Local Policies, and click User Rights Assignment. In the right pane, double-click the policy Allow log on locally, and click Add User or Group. In the Add User or Group window, click Browse, and in the Enter the object names to select box, type Domain, click Check Names, select Domain Users, click OK, and click OK three more times. Now, domain users can log on to your domain controller interactively instead of just over the network.
9. In the left pane, click Audit Policy. In the right pane, double-click Audit object access, place a check mark in the Define these policy settings box, place a check mark in the Failure box, and click OK. Close Group Policy Management Editor and Group Policy Management.
10. Open a command prompt, and enter gpupdate /force. Now, the policies that allow Domain Users to log on locally to the domain controller and that enable auditing of object access are activated. (They should have updated automatically within 5 minutes—the default time for domain controllers to refresh their policies.) However, enabling audit access does not mean that you can track accesses to the Sales folder yet. You still have to configure auditing on each object you want to track. If setting the policy to audit object access resulted in all system objects being audited, the system would bog down and stop because of all the logging being done. Close the command prompt.
11. Enable auditing of object access on the Sales folder as follows: right-click C:\Sales, click Properties, click the Security tab, click Advanced, and click the Auditing tab.
12. In the Advanced Security Settings for Sales, click the Add button. Click **Select a principal**.In the Enter the object name to select box, type Everyone, click Check Names, and when the Everyone group appears underlined, click OK.
13. The Auditing Entry for Sales window appears. Select the **Fail** option from the Type drop-down list in the top portion of the window, then click **Show advanced properties**, and place check marks in the boxes for Create files / write data, Delete subfolders and files, and Delete, as shown in Figure 6-5. Click OK three times to complete auditing configuration on the Sales folder. Close all windows and log off.

**[Insert Figure 6-5 Here]**

1. Log on as **anewman**. Click **File Explorer**, double-click Computer, double-click Local Disk (C:), open the Sales folder, open Sales Report, and add this line: These figures are due Monday, July 4th. Save the file, close all windows, and log out.
2. Log on as **mtsheppard**. Click **File Explorer**, double-click Computer, double-click Local Disk (C:), open the Sales folder, open Sales Report, and add this line: Please include sales from accounts that have closed. Save the file. What happens? Assume that you have logged in as a regular user and that you do not know the administrative password. Cancel the attempt to save the file. Try to delete the Sales Report document. What happens? You do not have delete permissions. Cancel the attempt to delete the file. Try to delete the Sales folder. Again, you do not have the delete permissions. Close all windows and log out.
3. Log on as Administrator. In Server Manager, click **Tools**, then select Event Viewer, expand Windows Logs, and click Security. There are likely to be a lot of events. The logged events that have a key icon indicate successful actions. Those with padlocks indicate an account’s failed attempts to perform a prohibited action. In the Actions pane on the right, click Filter Current Log. Click the drop-down arrow in the Logged box, select Last hour, and click OK. You will need to scroll down in the upper window to see what object was accessed (the folder or file) and what action was attempted (delete). Explore the failure events by double-clicking them and find evidence that Martin Sheppard attempted to write to the Sales Report file, attempted to delete the Sales Report file, and attempted to delete the Sales folder, as shown in Figure 6-6.

**[Insert Figure 6-6 Here]**

1. Close all windows and log off.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>1.2 Given a scenario, use secure network administration principles.
* 4.3 Given a scenario, select the appropriate solution to establish host security.
* 5.3 Install and configure security controls when performing account management, based on best practices.

**<H2>Review Questions**

1. <FIB>The reason to audit the Everyone group is that \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
2. <FIBA>by default, non-administrators are not audited for object access
3. **you do not know who may be attempting to perform actions that are prohibited by access controls**
4. the Everyone group does not include users who are logged on locally
5. there are no other options
6. <MULT>Which of the following statements about auditing is correct? (Choose all that apply.)
7. **<MULTA>In this lab, the Sales Report file inherited the auditing configuration you set on the Sales folder.**
8. **Object access auditing settings on a file may not conflict with the object access auditing settings on the parent folder.**
9. User auditing can be set on the Profile tab of the user account properties.
10. **Auditing should be used sparingly to avoid decreases in system performance.**
11. <TF>Object access auditing prevented Martin Sheppard from deleting the Sales folder. True or **False**?
12. <FIB>In this lab, auditing was configured in the group policy object of the Default Domain Controllers OU because \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
13. **<FIBA>auditing will then apply to all domain controllers in the Default Domain Controllers OU**
14. the Audit object access setting is not available in the Local Security Policy console
15. local administrators on domain controllers are not able to configure Local Security Policy settings unless they are also members of the Domain Admins group
16. if auditing were set at the Local Security Policy, it would be effective only when users logged on locally
17. <TF>Object access auditing is an effective means of tracking accidental file deletion. **True** or False?