* [e](https://lms.godeploy.it/Labs/DelegateLab/9dbbd30d-5fb9-ed11-9561-00155d800002)
* [Lab Guide](https://lms.godeploy.it/Labs/DelegateLab/9dbbd30d-5fb9-ed11-9561-00155d800002)

 Lab Guide

Lab 1 - Introduction to Configuration Management



Lab 1: Introduction to Configuration Management

Exercise 1: Starting the Alpha VM and exploring the domain configuration

In this exercise, you will start the Alpha VM and examine the existing Group Policy configuration. Alpha is a Windows Server 2016 Domain Controller, DHCP, and DNS Server. This server will be the basis for the lab Active Directory environment.

Task 1: Explore the current domain configuration

In this task, you will examine the current domain layout prior to working with Group Policy.

1. Select the [**Alpha**](urn:it:godeploy:lab-guide:action-link:select-vm?=603f68c6-8dbb-ea11-abef-00155d10e510) VM.

**Note**: You will see a CTRL+ALT+DEL prompt for logon. Since you are using a virtual machine, this key sequence will not pass through. Instead, select the appropriate option in the virtual machine interface to send the CTRL+ALT+DEL sequence.

In some cases, you might be able to use the keyboard shortcut: CTRL+ALT+END to send the key sequence.

1. Log on as [***HQ\Administrator***](urn:it:godeploy:lab-guide:action-link:paste-vm-username?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=HQ%5CAdministrator) with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. After you have successfully logged on to the Alpha VM, in Server Manager, click **Tools** > **Active Directory Users and Computers**.
3. Right‐click hq.local and select the **Raise domain functional level** option.
4. What is the current domain functional level?
5. Do not make any changes here now. Click the Close button.
6. Expand hq.local in the left section of the window and then click the **Computers** container.
7. Do you see any computers listed?
8. Select the **Domain Controllers** container.
9. What domain controller is listed?
10. Open the **Accounts OU**.
11. Expand the **Engineering OU** and list the user accounts that you see:
12. Expand the **IT OU** and list the user accounts that you see:
13. Expand the **Management OU** and list the user accounts that you see:
14. Expand the **Sales OU** and list the user accounts that you see:
15. Open the Users container and double‐click the Domain Admins group.
16. Click the **Members** tab.
17. Who are the members of this group?
18. Double‐click the **Enterprise Admins** group.
19. Click the **Members** tab.
20. Who are the members of this group?
21. Close Active Directory Users and Computers.
22. Send a [**CTRL+ALT+DEL**](urn:it:godeploy:lab-guide:action-link:send-vm-key-combo?=CTRL%2BALT%2BDEL) key sequence to the VM.
23. Click Sign Out.
24. Send a [**CTRL+ALT+DEL**](urn:it:godeploy:lab-guide:action-link:send-vm-key-combo?=CTRL%2BALT%2BDEL) key sequence to the VM again.
25. Click Other user and log on as **Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
26. In the Server Manager, click **Tools** > **Group Policy Management**.

**Note**: Usually the Group Policy Management Console will open behind the Server Manager. Look for a flashing icon in the taskbar and click on it to bring the GPMC to the foreground.

1. In the Group Policy Management Console, navigate to **Forest: hq.local > Domains > hq.local > Group Policy Objects**.
2. What Group Policy Objects are already present?

Task 2: Analyze a few of the default policy settings

In this task, you will examine the current domain policy settings.

1. In the Group Policy Management Console, navigate to **Forest: hq.local > Domains > hq.local**.
2. Right‐click Default **Domain Policy** and select the Edit option.
3. Under Computer Configuration, expand Policies, Windows Settings, Security Settings, Account Policies, and then click Password Policy.
4. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies**, expand **Local Policies**, and then click the **Security Options** node.
2. Double‐click **Accounts: Block Microsoft accounts**.
3. Select the **Define this policy setting** check box, and then from the drop‐down list select **Users can't add or log on with Microsoft accounts**.
4. Click **OK**.
5. Browse through the remaining policy settings within the Security Options section to determine what is configured.
6. Close the Group Policy Management Editor.
7. In the **Group Policy Management Console**, select **Default Domain Policy** in the left window pane.
8. In the message box that appears, select the **Do not show this message again** check box, then click **OK**.
9. In the right window pane, click the **Settings** tab.
10. Click the **Security Settings** section to expand it, then expand each of the sub‐sections to display all of the configured items.

**Note**: This is a read‐only mode that is more convenient for viewing the items that are configured when you do not want to make changes.

1. Close the **Group Policy Management Console**.

Exercise 2: Viewing the policies of a domain joined server

In this exercise, you will start the Bravo VM and analyze its current Group Policies. Bravo is a Windows Server that is a member of the Domain, but is not yet a Domain Controller.

Task 1: Explore the server's local policies

In this task, you will start the Bravo VM and explore the local policies of the server, which is already a domain member.

1. Switch to the [**Bravo**](urn:it:godeploy:lab-guide:action-link:select-vm?=b112fbf6-8dbb-ea11-abef-00155d10e510) VM.
2. Send a [**CTRL+ALT+DEL**](urn:it:godeploy:lab-guide:action-link:send-vm-key-combo?=CTRL%2BALT%2BDEL) key sequence to the VM.
3. Log on as **Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
4. Click the **Start button** in the lower‐left corner.
5. Type **gpedit.msc** and then press **ENTER**.
6. Under **Computer Configuration**, expand **Windows Settings > Security Settings > Account Policies** and then click **Password Policy**.

**Note**: Look at the icons next to the policy settings. This icon indicates that the settings came from policies inherited from Active Directory and not the local machine.

1. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**, expand **Local Policies**, and then click the **Security Options** node.
2. Write the values for the following policy setting: **Accounts: Block Microsoft accounts**
3. Where is the Block Microsoft accounts setting coming from?
4. Close the Local Group Policy Editor without making any changes.

Exercise 3: Preparing Windows 10 Client for domain policies

In this exercise, you will start and configure the Echo VM. Echo is a Windows 10 Client that is not yet joined to the Domain.

Task 1: Explore the local policies before joining the domain

In this task, you will start the Echo VM and explore the local policies on the VM before joining it to the domain.

1. Switch to the [**Echo**](urn:it:godeploy:lab-guide:action-link:select-vm?=941bdf51-8ebb-ea11-abef-00155d10e510) VM.
2. Log on as [**Student**](urn:it:godeploy:lab-guide:action-link:paste-vm-username?=941bdf51-8ebb-ea11-abef-00155d10e510&i=1&d=Student) with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=941bdf51-8ebb-ea11-abef-00155d10e510&i=1&d=Pa%24%24w0rd).

**Note**: A Network Location dialog box may appear at some point. Select **Work Network** if it does. Click **Close** after it is done.

1. Click the **Start button** in the lower‐left corner.
2. Type **gpedit.msc** and then press ENTER.
3. Under **Computer Configuration**, expand **Windows Settings** > **Security Settings** > **Account Policies** and then click **Password Policy**.

**Note**: Look at the icons next to the policy settings. The icon you see indicates that the settings came from policies on the local machine and were not inherited from Active Directory. This is because the device is not a member of the Domain yet.

1. Write the values for the following policy settings: Enforce password history
   * Maximum passwor: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**, expand **Local Policies** and then click the **Security Options** node.
2. Write the values for the following policy setting: **Accounts: Block Microsoft accounts**
3. Close the Local Group Policy Editor without making any changes.

Task 2: Join the hq.local domain

In this task, you will join the VM to the hq.local domain.

1. Click the **Start button** and type **PowerShell**.
2. In the search results, right‐click the Windows PowerShell link and select **Run as administrator**.
3. On the User Account Control dialog box, click **Yes**.
4. In the PowerShell window, type the command below, and press ENTER:

Add-Computer -DomainName hq.local -Restart

**Note**: You can also join the domain using the graphical interface. We are using PowerShell in this case as an alternative.

1. In the credentials dialog box, type **Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd) and click OK.

**Note**: You will see a CTRL+ALT+DEL prompt for logon. Since you are using a virtual machine, this key sequence will not pass through. Instead, select the appropriate option in the virtual machine interface to send the CTRL+ALT+DEL sequence.

In some cases, you might be able to use the keyboard shortcut: CTRL+ALT+END to send the key sequence.

1. After rebooting, send the [**CTRL+ALT+DEL**](urn:it:godeploy:lab-guide:action-link:send-vm-key-combo?=CTRL%2BALT%2BDEL) sequence, or click the background image to bring up the logon screen.
2. Click the Switch user icon (the left arrow) on the logon screen. Click Other user and log on as **Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).

Task 3: Explore the local policies after joining the domain

In this task, you will explore the local policies on the VM after joining it to the domain.

1. On the [**Echo**](urn:it:godeploy:lab-guide:action-link:select-vm?=941bdf51-8ebb-ea11-abef-00155d10e510) VM, click the Start button, type gpedit.msc, and then press ENTER.
2. Under **Computer Configuration**, expand **Windows Settings > Security Settings > Account Policies** and then click **Password Policy**.
3. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies** expand **Local Policies**, and then click the **Security Options** node.
2. Write the value for the following policy setting: Accounts: Block Microsoft accounts
3. Close the **Local Group Policy Editor** without making any changes.
4. How are the above settings different from what you saw before you joined the Echo VM to the domain?

Exercise 4: Preparing Windows 8.1 Client for domain policies

In this exercise, you will start and configure the Delta VM. Delta is a Windows 8.1 Client that has not yet been joined to the domain.

Task 1: Explore the local policies before joining the domain

In this task, you will start the Delta VM and explore the local policies on the VM before joining it to the domain.

1. Switch to the [**Delta**](urn:it:godeploy:lab-guide:action-link:select-vm?=7aa29128-8ebb-ea11-abef-00155d10e510) VM.
2. Log on as [**Student**](urn:it:godeploy:lab-guide:action-link:paste-vm-username?=7aa29128-8ebb-ea11-abef-00155d10e510&i=1&d=Student) with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=7aa29128-8ebb-ea11-abef-00155d10e510&i=1&d=Pa%24%24w0rd).

**Note**: A Network Location dialog box may appear at some point. Select **Work Network** if it does. Click **Close** after it is done.

1. Click the **Start button** in the lower‐left corner.
2. Type **gpedit.msc** and then press ENTER.
3. Under **Computer Configuration**, expand **Windows Settings > Security Settings > Account Policies** and then click **Password Policy**.

**Note**: Look at the icons next to the policy settings. The icon you see indicates that the settings came from policies on the local machine and were not inherited from Active Directory. This is because the device is not a member of the Domain yet.

1. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**, expand **Local Policies**, and then click the **Security Options** node.
2. Write the values for the following policy setting: **Accounts: Block Microsoft accounts**
3. Close the Local Group Policy Editor without making any changes.

Task 2: Join the hq.local domain

In this task, you will join the VM to the hq.local domain.

1. Click the **Start button** and type **PowerShell**.
2. In the search results, right‐click the Windows PowerShell link and select **Run as administrator**.
3. On the User Account Control dialog box, click **Yes**.
4. In the PowerShell window, type the command below, and press **ENTER**:

Add-Computer -DomainName hq.local -Restart

**Note**: You can also join the domain using the graphical interface. We are using PowerShell in this case as an alternative.

1. In the credentials dialog box, type **Speck** with a password of **Pa$$w0rd** and click OK.

**Note**: You will see a CTRL+ALT+DEL prompt for logon. Since you are using a virtual machine, this key sequence will not pass through. Instead, select the appropriate option in the virtual machine interface to send the CTRL+ALT+DEL sequence.

In some cases, you might be able to use the keyboard shortcut: CTRL+ALT+END to send the key sequence.

1. After rebooting, send the [**CTRL+ALT+DEL**](urn:it:godeploy:lab-guide:action-link:send-vm-key-combo?=CTRL%2BALT%2BDEL) sequence, or click the background image to bring up the logon screen.
2. Click the Switch user icon (the left arrow) on the logon screen. Click Other user and log on as Speck with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=7aa29128-8ebb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).

Task 3: Explore the local policies after joining the domain

In this task, you will explore the local policies on the VM after joining it to the domain.

1. On the [**Delta**](urn:it:godeploy:lab-guide:action-link:select-vm?=7aa29128-8ebb-ea11-abef-00155d10e510) VM, click the Start button, type **gpedit.msc**, and then press **ENTER**.
2. Under **Computer Configuration**, expand **Windows Settings > Security Settings > Account Policies**, and then click **Password Policy**.
3. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**, expand **Local Policies**, and then click the **Security Options** node.
2. Write the value for the following policy setting: **Accounts: Block Microsoft accounts**
3. Close the Local Group Policy Editor without making any changes.
4. How are the above settings different from what you saw before you joined the Delta VM to the domain?

Exercise 5: Preparing Windows 7 for domain policies

In this exercise, you will start and configure the Kilo VM. Kilo is a Windows 7 operating system that has not yet been joined to the domain.

Task 1: Explore the local policies before joining the domain

In this task, you will start the Kilo VM and explore the local policies on the VM before joining it to the domain.

1. Switch to the [**Kilo**](urn:it:godeploy:lab-guide:action-link:select-vm?=8156fc71-8ebb-ea11-abef-00155d10e510) VM.
2. Log on as [**Student**](urn:it:godeploy:lab-guide:action-link:paste-vm-username?=7aa29128-8ebb-ea11-abef-00155d10e510&i=1&d=Student) with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=7aa29128-8ebb-ea11-abef-00155d10e510&i=1&d=Pa%24%24w0rd).

**Note**: A Network Location dialog box may pop up at some point. Select **Work Network** if it does. Click **Close** after it is done.

1. Click **Start**, type **gpedit.msc** in the Search box, and then press **ENTER**.
2. Under **Computer Configuration**, expand **Windows Settings > Security Settings > Account Policies** and then click **Password Policy**.
3. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**, expand **Local Policies**, and then click the **Security Options** node.
2. Does the following policy option exist? **Accounts: Block Microsoft Accounts**
3. Why?
4. Close the Local Group Policy Editor without making any changes.

Task 2: Join the hq.local domain

In this task, you will change the VM name on the Kilo VM and join it to the hq.local domain.

1. Click **Start**, right‐click **Computer**, and then select **Properties**.
2. Click the **Change settings** link and then click the **Change** button in **System Properties**.
3. Make sure **Kilo** is the name in the Computer name text box, type **hq.local** in the Member of Domain text box, and then click **OK**.
4. Type **Speck** and a password of **Pa$$w0rd** when credentials are asked for, and then click **OK**.
5. On the Welcome dialog box, click **OK**, and on the Restart message, click **OK**.
6. Click Close to exit the System Properties dialog box and then click **Restart Now**.

**Note**: You will see a CTRL+ALT+DEL prompt for logon. Since you are using a virtual machine, this key sequence will not pass through. Instead, select the appropriate option in the virtual machine interface to send the CTRL+ALT+DEL sequence.

1. After rebooting, send the [**CTRL+ALT+DEL**](urn:it:godeploy:lab-guide:action-link:send-vm-key-combo?=CTRL%2BALT%2BDEL) sequence, then click Switch User on the logon screen. Click Other User and log on as Speck with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=7aa29128-8ebb-ea11-abef-00155d10e510&i=1&d=Pa%24%24w0rd).

Task 3: Explore the local policies after joining the domain

In this task, you will explore the local policies on the VM after joining it to the domain.

1. On the [**Kilo**](urn:it:godeploy:lab-guide:action-link:select-vm?=8156fc71-8ebb-ea11-abef-00155d10e510) VM, click **Start**, type **gpedit.msc** in the Search box, and then press **ENTER**.
2. Under **Computer Configuration**, expand **Windows Settings > Security Settings > Account Policies** and then click **Password Policy**.
3. Write the values for the following policy settings: Enforce password history
   * Maximum password: **age**
   * Minimum password: **age**
   * Minimum password: **length**

Password must meet complexity requirements

1. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**, expand **Local Policies** and then click the **Security Options** node.
2. Confirm that the following option still does NOT exist: **Accounts: Block Microsoft accounts**
3. Close the Local Group Policy Editor without making any changes.
4. How are the above settings different from what you saw before you joined the Kilo VM to the domain?

Exercise 6: Examining the location of the computer objects

In this exercise, you will examine where the computer objects have been created.

Task 1: Examine the new computer objects with ADUC

In this task, you will find out where the computer objects are placed after joining them to the domain by using the Active Directory Users and Computers tool.

1. Switch to [**Alpha**](urn:it:godeploy:lab-guide:action-link:select-vm?=603f68c6-8dbb-ea11-abef-00155d10e510) and log on as **Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. In Server Manager, click **Tools > Active Directory Users and Computers**.
3. Open hq.local, Computers.
4. What computers do you see listed?

Task 2: Examine the new computer objects with ADAC

In this task, you will find out where the computer objects are placed after joining them to the domain by using the Active Directory Administrative Center tool.

1. In **Server Manager**, click **Tools > Active Directory Administrative Center**.
2. In the upper‐left portion of the tool, just above Overview, are two icons. One of them is the Tree View icon. Click **Tree View**.
3. Expand **hq.local, Computers**.
4. What computers do you see listed?

Task 3: Examine the new computer objects with PowerShell

In this task, you will find out where the computer objects are placed after joining them to the domain by using Windows PowerShell.

1. In **Server Manager**, click **Tools > Windows PowerShell**.
2. Type the following command:

Get-ADComputer -Filter \* -SearchBase "CN=Computers,DC=hq,DC=local" | Format-Table Name

1. What computers do you see listed?

**Results**: You have completed this lab.

Module 9: Configuring and Troubleshooting Resource Access

Lab: Configuring and Troubleshooting Resource Access

**Scenario**

Your users need access to file and printer resources. You’ve been tasked configuring and sharing these resources. Because some of your users work from home, the IT manager has tasked you with creating a sync share for Work Folders to enable the Sales team to access their work content while out of the office. When you return to the helpdesk, a user has reported the loss of some files. You are assigned the ticket for resolution.

**Objectives**

After completing this lab, you will be able to:

* Configure and troubleshoot file access
* Configure Work Folders
* Recover files

Exercise 1: Configuring and troubleshooting file access

**Scenario**

In this exercise, you will create a folder structure for the Marketing and IT departments. After you review the default permissions, you will share folders for both departments, and then test the differences in permissions when using Network File and Folder Sharing and Advanced Sharing.

The main tasks for this exercise are as follows:

1. Create a folder structure.
2. Review default permissions.
3. Configure permissions for the IT and Marketing folders.
4. Review configured permissions.
5. Test local file permissions.
6. Test share permissions.

Task 1: Create folders

1. On [**LON-CL1**](urn:gd:lg:a:select-vm), sign in as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. On the taskbar, click **File Explorer**.
3. In File Explorer, in the navigation pane, expand **This PC**,and then click **Local Disk (C:)**. In the details pane, right-click the empty space, select **New**, select **Folder**, and then type [**Data**](urn:gd:lg:a:send-vm-keys) for the new folder's name.
4. In File Explorer, in the navigation pane, expand **Local Disk (C:)**, click **Data**. In the details pane, right-click the empty space, select **New**, select **Folder**, and then type [**Marketing**](urn:gd:lg:a:send-vm-keys) for the new folder's name.
5. In File Explorer, in the details pane, right-click the empty space, select **New**, select **Folder**, and then type [**IT**](urn:gd:lg:a:send-vm-keys) for the new folder's name.

Task 2: Review default permissions

1. On **LON-CL1**, in File Explorer, in the navigation pane, double-click **Data** below **Local Disk (C:)**, right-click **IT**, and then select **Properties**.
2. In the **IT Properties** window, click the **Security** tab, and then click **Edit**.
3. In the **Permissions for IT** dialog box, verify that **Authenticated Users** is selected in the **Group or user names** section, and then click **Remove**. Read the text in the **Windows Security** dialog box that appears, which explains why you cannot remove an authenticated user. Click **OK**,and then click **Cancel**.
4. In the **IT Properties** window, on the **Security** tab, click **Advanced**.
5. In the **Advanced Security Settings for IT** dialog box, verify that all permissions entries are inherited from C:\. Also, verify that **Users (LON-CL1\Users)** have **Read & execute** access, while **Authenticated Users** have **Modify** access. Click **OK** twice.
6. In File Explorer, in the navigation pane, right-click **Marketing**, and then select **Properties**.
7. In the **Marketing Properties** window, click the **Security** tab, and then click **Advanced**.
8. In the **Advanced Security Settings for Marketing** dialog box, verify that all permissions entries are inherited from C:\. Also, verify that **Users (LON-CL1\Users)** have **Read & execute** access, while **Authenticated Users** have **Modify** access. Click **OK** twice.

Task 3: Configure permissions for the IT and Marketing folders

1. On **LON-CL1**, in File Explorer, in the navigation pane, right-click the **IT** folder, click **Show more options**, select **Give access to**, and then select **Specific people**.
2. In the **Network access** dialog box, verify that **AdatumAdmin** is displayed with **Owner** permissions.
3. In the **Type a name and then click Add, or click the arrow to find someone** text box, type [**IT**](urn:gd:lg:a:send-vm-keys), and then click **Add**.
4. Verify that **IT** is added and selected. Click **Read** in the **Permission Level** column, select **Read/Write**,click **Share**, and then click **Done**.
5. In File Explorer, in the navigation pane, right-click **Marketing**,and then select **Properties**.
6. In the **Marketing Properties** dialog box, select the **Sharing** tab. In the **Network File and Folder Sharing** section, verify that **Marketing** is not shared, and then in the **Advanced Sharing** section, click **Advanced Sharing**.
7. In the **Advanced Sharing** dialog box, select the **Share this folder** check box. Verify that the share name is **Marketing** (the same as the folder name), and that **Limit the number of simultaneous users to** is set to **20**. Click **Permissions**.
8. In the **Permissions for Marketing** dialog box, click **Remove**. Click **Add**, in the **Enter the object names to select (examples)** box, type [**Marketing**](urn:gd:lg:a:send-vm-keys), and then click **OK**. In the **Permissions for Marketing** section, select the **Change** check box in the **Allow** column, and then click **OK** twice.
9. In the **Marketing Properties** dialog box, in the **Network File and Folder Sharing** section, verify that **Marketing** is now shared as **\\LON-CL1\Marketing**, and then click **Close**.
10. Right-click the **Start** icon, and then select **Windows Terminal (Admin)**. Click **Yes** at the **User Account Control** prompt.
11. At the command prompt, view shares created on **LON-CL1** by running **net view \\lon-cl1**. Close the command prompt.
12. Right-click the **Start** icon, and then select **Computer Management**.
13. In Computer Management, in the navigation pane, expand **Shared Folders**, and then click **Shares**. In the details pane, verify that you see **IT** and **Marketing** shares, and the default Windows 11 shares. Close Computer Management.

Task 4: Review configured permissions

1. On **LON-CL1**, in File Explorer, in the navigation pane, right-click **IT**, and then select **Properties**.
2. In the **IT Properties** window, click the **Security** tab, and then click **Advanced**.
3. In the **Advanced Security Settings for IT** dialog box, verify that all the permissions entries are set explicitly at this level, because their permission inheritance is set to **None**.
4. Verify that only an **AdatumAdmin**, **Administrators (LON-CL1\Administrators)** group, **SYSTEM** and **IT (ADATUM\IT)** group have access to the IT folder. These settings match the permissions that you configured in the **Network access** dialog box.
5. In the **Advanced Security Settings for IT** dialog box, click **OK**.
6. In the **IT Properties** dialog box, select the **Sharing** tab, in the **Network File and Folder Sharing** section, verify that **IT** now is shared as **\Lon-cl1\it**, and then click **Advanced Sharing**.
7. In the **Advanced Sharing** dialog box, click **Permissions**. In the **Permissions for IT** dialog box, verify that the **Everyone** and **Administrators** groups have Full Control permissions to the share, click **OK** twice, and then click **Close**.

**Note:** If you share a folder by using the **Network access** dialog box, you will modify the local file permissions to match your configuration, while the Everyone and Administrators groups will have the Full Control share permission.

1. In File Explorer, in the navigation pane, right-click **Marketing**, and then select **Properties**.
2. In the **Marketing Properties** window, click the **Security** tab, and then click **Advanced**.
3. In the **Advanced Security Settings for Marketing** dialog box, verify that all of the permissions entries are inherited from C:\. Also verify that **Users (LON-CL1\Users)** have **Read & execute** access, while **Authenticated Users** have **Modify** access, which are the same file permissions as before you shared the **Marketing** folder. Click **OK** twice.

**Note:** If you share a folder by using the Advanced Sharing feature, this does not modify local file permissions. You only modify share permissions if you use Advanced Sharing.

1. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.

Task 5: Test local file permissions

1. On **LON-CL1**, sign in as **[Adatum\Bill](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Bill is a member of the Marketing group, but is not a member of the IT group.
2. On the taskbar, click **File Explorer**. In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Data**, and then select **Marketing**.
3. In the details pane, right-click the empty space, select **New**, select **Text Document**,and then type [**File10**](urn:gd:lg:a:send-vm-keys) as the name of the file.

**Note:** Bill has local file permissions to create a new file in the Marketing folder, because permissions were configured by using the Advanced Sharing feature. This modified only the share permissions, while the default local file permissions were not modified. By default, Authenticated Users have the Modify permission.

1. In File Explorer, in the navigation pane, select **IT**, and then click **Cancel**.

**Note:** You will get an error, because Bill does not have local file permissions to the IT folder. Permissions were configured by Network access, and only members of the IT group have local file permissions to the folder.

1. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.
2. On [**LON-CL1**](urn:gd:lg:a:select-vm), sign in as **[Adatum\Beth](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Beth is member of the IT group, and she is not member of the Marketing group.
3. On the taskbar, click **File Explorer**. In File Explorer, in the navigation pane, expand **This PC**, expand **Local Disk (C:)**, expand **Data**, and then select **Marketing**.
4. In the details pane, verify that you can see **File10** that was created by Bill. Right-click the empty space, select **New**, select **Text Document**,and then type [**File20**](urn:gd:lg:a:send-vm-keys) as the name of the file.

**Note:** Beth has local file permissions to create a new file in the Marketing folder because you configured permissions by using the Advanced Sharing feature. This modified only the share permissions, while the default local file permissions were not modified. By default, Authenticated Users have the Modify permission.

1. In File Explorer, in the navigation pane, select **IT**.In the details pane, right-click the empty space, select **New**, select **Text Document**,and then type [**File21**](urn:gd:lg:a:send-vm-keys) as the name of the file.

**Note:** Beth is able to create a file, because you configured permissions by using Network access. Members of the IT group have local file permissions to the IT folder.

**Note:** Be aware that Network File and Folder Sharing modifies file permissions and share permissions. However, the Advanced Sharing feature does not modify file permissions, and only sets share permissions.

1. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.

Task 6: Test share permissions

1. On [**LON-CL2**](urn:gd:lg:a:select-vm), sign in as **[Adatum\Bill](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Bill is a member of the Marketing group, but he is not a member of the IT group.
2. On the taskbar, click **File Explorer**. In File Explorer, click the arrow in the Address bar, type [**\\LON-CL1**](urn:gd:lg:a:send-vm-keys),and then press Enter.
3. Verify that you can see the **IT** and **Marketing** shares in the details pane. Double-click **Marketing**. Verify that you can see the files that Bill and Beth created locally.
4. In the details pane, right-click the empty space, select **New**, select **Text Document**,and then type [**File30**](urn:gd:lg:a:send-vm-keys) as the name of the file. Bill has permissions to create a new file in the Marketing share because he is a member of the Marketing group.
5. In File Explorer, click **LON-CL1** in the address bar. In the details pane, double-click **IT**. Read the text in the **Network Access** dialog box, and then click **Close**.

**Note:** Bill is not a member of the IT group, so he does not have permissions to the IT share.

1. Right-click the **Start** icon, select **Shut down or sign out**, and then select **Sign out**.
2. Sign in as **[Adatum\Beth](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Beth is a member of the IT group, but she is not a member of the Marketing group.
3. On the taskbar, click **File Explorer**. In File Explorer, click the arrow in the Address bar, type [**\\LON-CL1**](urn:gd:lg:a:send-vm-keys),and then press Enter.
4. Verify that you can see the **IT** and **Marketing** shares in the details pane. Double-click **Marketing**.
5. Read the text in the **Network Access** dialog box. Beth is not a member of the Marketing group, so she does not have permissions to the Marketing share. Click **Close**.
6. In the details pane, double-click **IT**. Right-click the empty space in the details pane, select **New**, select **Text Document**,and then type [**File40**](urn:gd:lg:a:send-vm-keys) as the name of the file. Beth has permissions to create a new file in the IT share because she is a member of the IT group.

**Note:** Users can connect only to shares that were shared for groups in which they are members, regardless of whether they were shared by Network access or Advanced Sharing.

**Results**: After completing this exercise, you will have created a folder structure for the Marketing and IT departments, shared their folders, and tested local and share permissions.

Exercise 2: Configuring Work Folders

**Scenario**

Work Folders enables users to access their work content from both domain-joined computers, standalone computers, and other devices, such as iOS and Android smartphones. In this exercise, you'll setup and configure Work Folders for Adatum users.

The main tasks for this exercise are as follows:

1. Install the Work Folders feature.
2. Configure the Work Folders website.
3. Configure domain-joined Work Folders clients.
4. Configure and test a standalone computer.

Task 1: Install the Work Folders feature

1. Sign in to [**LON-DC1**](urn:gd:lg:a:select-vm) as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. Right-click **Start**, and then click **Windows PowerShell (Admin)**.
3. In Windows PowerShell, enter the following cmdlet:
4. Install-WindowsFeature FS-SyncShareService
5. Run **services.msc**, and in Services, locate and start the **Windows Sync Share** service.
6. Minimize the Windows PowerShell window, and switch to **Server Manager**.
7. In Server Manager, in the navigation pane, select **File and Storage Services**, and then select **Work Folders**.
8. In the **WORK FOLDERS** section, select **TASKS**, and then select **New Sync Share**.
9. In the **New Sync Share Wizard**, on the **Before you begin** page, select **Next**.
10. On the **Select the server and path** page, in the **Enter a local path** text box, enter [**C:\syncshare1**](urn:gd:lg:a:send-vm-keys), select **Next**, and if **New Sync Share Wizard** page appears, then click **OK**.
11. On the **Specify the structure for user folders** page, verify that **User alias** is selected, and then select **Next**.
12. On the **Enter the sync share name** page, click **Next** to accept the default sync share name.
13. On the **Grant sync access to groups** page, click **Add**, and in the **Enter the object name to select** text box, enter [**Marketing**](urn:gd:lg:a:send-vm-keys). Select **OK**, and then select **Next**.
14. On the **Specify security policies for PCs** page, verify the two available options. Clear the **Automatically lock screen, and require a password** check box, and then select **Next**.
15. On the **Confirm selections** page, select **Create**.
16. On the **View Results** page, select **Close**.
17. In Server Manager, in the **WORK FOLDERS** section, verify that **syncshare1** is listed, and that in the **USERS** section, the user **Naomi Booth** is listed.

Task 2: Configure the Work Folders website

1. In Server Manager, select **Tools**, and then select **Internet Information Services (IIS) Manager**.
2. In the **Microsoft Internet Information Services (IIS) Manager**, in the navigation pane, expand **LON-DC1 (ADATUM\AdatumAdmin)**. Expand **Sites**, right-click **Default Web Site**, and then select **Edit Bindings**.
3. In the **Site Bindings** dialog box, click **Add**.
4. In the **Add Site Binding** dialog box, in the **Type** list, select **https**. In the **SSL certificate** list, select **LON-DC1.Adatum.com**, click **OK**, and then click **Close**.
5. Close the IIS Manager.

Task 3: Configure domain-joined Work Folders clients

1. On LON-DC1, in **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the **Group Policy Management Console**, in the navigation pane, expand **Forest: Adatum.com**, expand Domains, select **Adatum.com**, and then select **Marketing**.
3. Right-click **Marketing**, and then click **Create a GPO in this domain, and Link it here**. In the **Name** text box, enter [**Deploy Work Folders**](urn:gd:lg:a:send-vm-keys), and then select **OK**.
4. Right-click **Deploy Work Folders**, and then select **Edit**.
5. In the **Group Policy Management Editor**, under **User Configuration**, in the navigation pane, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then select the **Work Folders** node.
6. In the details pane, right-click **Specify Work Folder settings** , and then click **Edit**.
7. In the **Specify Work Folder settings** dialog box, select **Enabled**. In the **Work Folders URL** text box, enter [**https://lon-dc1.adatum.com**](urn:gd:lg:a:send-vm-keys), select the **Force automatic setup** check box, and then click **OK**.
8. Close the Group Policy Management Editor.
9. Sign in to [**LON-CL1**](urn:gd:lg:a:select-vm) as [**ADATUM\AdatumAdmin**](urn:gd:lg:a:send-vm-keys) with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
10. If necessary, sign out of LON-CL1 and sign in as **[adatum\Naomi](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** by using the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
11. On the toolbar, select the **File Explorer** icon.
12. In the navigation pane, select **Work Folders**.

**Note:** If the Work Folders node doesn't display, open **Windows Terminal** and run **GPupdate /force**. If necessary, sign out and then back in.

1. Right-click in the details pane, click **New**, select **Text Document**, and then name the file **On LON-CL1**.

Task 4: Configure and test a standalone computer

1. Sign in to [**LON-CL4**](urn:gd:lg:a:select-vm) as [**Admin**](urn:gd:lg:a:send-vm-keys) with the password of [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). This is a local account.
2. On the taskbar, right-click **Start** and then click **Run**.
3. In the **Run** dialog box, enter [**\\lon-dc1.adatum.com\c$**](urn:gd:lg:a:send-vm-keys).
4. In the **Enter Network credentials** dialog box, enter the user name as **[adatumadmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** and the password as [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys). Select **OK**.
5. Double-click **Adatum.cer**.
6. In the **Certificate** dialog box, select **Install Certificate**.
7. On the **Certificate Import Wizard**, select **Local Machine**, and then select **Next**.
8. On the **User Account Control** dialog box, select **Yes**.
9. On the **Certificate Store** page, select **Place all certificates in the following store**, and then select **Browse**.
10. On the **Select Certificate Store** page, select **Trusted Root Certification Authorities**, and then select **OK**.
11. On the **Certificate Store** page, select **Next**.
12. On the **Certificate Import Wizard** page, select **Finish**.
13. After the **Certificate Import Wizard** opens, select **OK**, and then in the **Certificate** window, select **OK**.
14. Restart LON-CL4, and then sign in to LON-CL4 as [**Admin**](urn:gd:lg:a:send-vm-keys) by using the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
15. On LON-CL4, open **Control Panel**.
16. In Control Panel, in the **Search Control Panel** text box, enter [**work**](urn:gd:lg:a:send-vm-keys), and then select **Work Folders**.
17. On the **Manage Work Folders** page, select **Set up Work Folders**.
18. On the **Enter your work email address** page, select **Enter a Work Folders URL instead**.
19. On the **Enter a Work Folders URL** page, in the **Work Folders URL** text box, enter [**https://lon-dc1.adatum.com**](urn:gd:lg:a:send-vm-keys), and then select **Next**.
20. In the **Windows Security** dialog box, in the **User name** text box, enter **[adatum\Naomi](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)**, and in the **Password** text box, enter [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys), and then select **OK**.
21. On the **Introducing Work Folders** page, review the local Work Folders location, and then select **Next**.
22. On the **Security policies** page, select the **I accept these policies on my PC** check box, and then click **Set up Work Folders**.
23. On the **Work Folders has started syncing with this PC** page, select **Close**.
24. On the Work Folders page, verify that the On LON-CL1.txt file displays.

**Results**: After completing this exercise, you will have successfully deployed and tested Work Folders for users in the Marketing department.

Exercise 3: Recovering files

**Scenario**

In this exercise, you will explore how File History works. First, you will configure it to store backups of the protected folders periodically to the network location, and verify which folders are protected by default. You will then make sure that you can recover deleted files.

The main tasks for this exercise are as follows:

1. Create a shared folder for File History.
2. Configure and use File History and Previous Versions.

Task 1: Create a shared folder for File History

1. On [**LON-DC1**](urn:gd:lg:a:select-vm), sign in as **[Adatum\AdatumAdmin](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** with the password [**Pa55w.rd**](urn:gd:lg:a:send-vm-keys).
2. On **LON-DC1**, on the taskbar, click **File Explorer**. In the navigation pane, click **Local Disk (C:)**.
3. In File Explorer,in the details pane, right-click an empty space, point to **New**, and then click **Folder**. Type **[FileHistory](urn:gd:lg:a:send-vm-keys" \o "Paste text into VM)** as the folder name, and then press Enter.
4. Right-click the **FileHistory** folder, and then click **Properties**.
5. In the **FileHistory Properties** dialog box, on the **Security** tab, click **Edit**. Click **Add**, in the **Enter the object names to select** box, type [**Domain**](urn:gd:lg:a:send-vm-keys), and then click **OK**.
6. Click **Domain Users** , and then click **OK**.
7. In the **Permissions for Domain Users** section, in the **Allow** column, select the **Full control** check box,and then click **OK**.
8. On the **Sharing** tab, click **Advanced Sharing**.
9. Select the **Share this folder** check box, and then click **Permissions**. In the **Permissions for Everyone** section, in the **Allow** column, click **Full Control** , and then click **OK** twice.
10. In the **FileHistory Properties** dialog box, click **Close**.

Task 2: Configure and use File History and Previous Versions

1. On [**LON-CL1**](urn:gd:lg:a:select-vm), open **File Explorer**.
2. In File Explorer, in the navigation pane, expand **This PC** ,and then click **Documents**. In the details pane, right-click an empty space, point to **New**, click **Text Document**, and then enter [**Report**](urn:gd:lg:a:send-vm-keys) as the name of the file.
3. Double-click **Report.txt**, and in Notepad, type [**This is a report**](urn:gd:lg:a:send-vm-keys). Close the Notepad file, and then click **Save** to save the changes.
4. Click **Start**, type [**file history**](urn:gd:lg:a:send-vm-keys), and then click **Restore your files with File History**.
5. In the **Home - File History** window, click **Configure File History** settings.
6. In the **File History** window, in the navigation pane, click **Select drive**.
7. In the **Select Drive** dialog box, click **Add network location**.
8. In the **Folder** box, type [**\\LON-DC1\FileHistory**](urn:gd:lg:a:send-vm-keys), click **Select Folder** , and then click **OK**.
9. In the **File History** window, in the details pane, click **Turn on**.
10. In the navigation pane, click **Advanced settings** , review the default values for how often to save copies of files and how long to keep them, and then click **Cancel**.
11. In File Explorer, in the navigation pane, click **Documents**, right-click **Report.txt**, and then click **Delete**.
12. In File Explorer, in the navigation pane, right-click **Documents** and then click **Properties**.
13. Select the **Previous Versions** tab, and then click **Documents** in the **Folder versions** list.
14. Click the down arrow next to **Open** and then click **Open in File History**.
15. Click the circular **Restore to original location** button.
16. File Explorer opens. Double-click **Documents**.
17. Verify that **Report.txt** has been recovered to the original location.
18. Double-click **Report.txt** , confirm that it contains the text that you typed, close Notepad, and then close File Explorer.
19. In the **Report.txt - File History** window, on the left of the address box, click the upward-pointing arrow twice.

**Results** : After completing this exercise, you will have configured and used File History.

**Congratulations!** You have now completed this lab. To continue to the next lab click End Lab in the Tools Menu . If you wish to contiue with this lab at a later date ensure you save the lab environment rather than ending it.

Lab 2: Using Group Policy Management Tools

Exercise 1: Working with multiple local policies

In this exercise, you will implement multiple local policies.

Task 1: Implement multiple local policies on Windows 10 Client

Windows Vista and later support the usage of multiple policies on the local machine. In this task, you will implement multiple local policies on the Windows 10 client VM.

1. Log on to the [**Echo**](urn:it:godeploy:lab-guide:action-link:select-vm?=941bdf51-8ebb-ea11-abef-00155d10e510) VM as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=941bdf51-8ebb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. If you are on the Start screen, click the Desktop.
3. Right‐click the Start button, and select Computer Management.
4. Expand System Tools, Local Users and Groups, and then click Users.
5. Right‐click Users and select New User.
6. In the New User dialog box, type LocalTest1 in the User name text box and Pa$$w0rd in the Password and Confirm password text boxes.
7. Clear the User must change password at next logon check box, click Create, and then click Close.
8. Close the Computer Management Console.
9. Open the Start screen, type mmc.exe and then press ENTER.
10. Click Yes if a User Account Control prompt appears.
11. Expand the console and the inner window to full screen.
12. Select File, Add/Remove Snap‐in from the menu bar.
13. Select the Group Policy Object Editor snap‐in, and then click Add.
14. Click the Browse button.
15. Click the Users tab.
16. Select the LocalTest1 user from the list and then click OK.
17. Click Finish and then click OK.
18. Expand Local Computer\LocalTest1 Policy, User Configuration, Administrative Templates, and then click Control Panel.
19. Click Prohibit access to the Control Panel and PC Settings option.
20. Click the Enabled radio button and then click OK.
21. Close the MMC and do not save the console.
22. Who will the Control Panel restriction apply to?
23. Is this a local user or a domain user?
24. Log off and log back on as the .\LocalTest1 user with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=9833cfe3-8fbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
25. Can you access Control Panel?
26. Log off and log back on as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).

Exercise 2: Installing the RSAT on a member server

Member servers do not include the GPMC or other RSAT tools by default. Domain Controllers have the GPMC, but not all of the other RSAT tools. This exercise will demonstrate how to install all of the RSAT tools that are available.

Some administrators may find themselves administering other servers in the environment from the console of a central server that they Remote Desktop into for security reasons. In other cases, administration can be performed from the console of the Windows Client with RSAT installed.

Task 1: Install the RSAT using the graphical interface

In this task, you will install the RSAT on Windows Server.

1. Switch to the [**Alpha**](urn:it:godeploy:lab-guide:action-link:select-vm?=603f68c6-8dbb-ea11-abef-00155d10e510) VM and log in as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=b112fbf6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. In Server Manager, click the Tools option and review the tools that are available. (Do not open any tools, just look at them for future comparison.)
3. In Server Manager, click Add roles and features.
4. Click Next four times until you reach the Select features screen.
5. Is the Group Policy Management feature installed on Alpha?
6. Scroll down and expand Remote Server Administration Tools.
7. Expand Feature Administration Tools and select the following features: BitLocker Drive Encryption Administration Utilities, Failover Clustering Tools, Network Load Balancing Tools.
8. Expand Role Administration Tools.
9. What tools appear to have been installed already?
10. Select the following features: Hyper‐V Management Tools, Remote Desktop Services Tools, File Services Tools, Print and Document Services Tools, Volume Activation Tools
11. Click Next, then click Install.
12. Wait for the installation to finish, then click Close.
13. In Server Manager, click Tools.
14. Do you see the new Administrative Tools?

Task 2: Install the RSAT using PowerShell

In this task, you will install the RSAT on Windows Server using Windows PowerShell.

1. On the [**Alpha**](urn:it:godeploy:lab-guide:action-link:select-vm?=603f68c6-8dbb-ea11-abef-00155d10e510) VM, if you are not already logged in, log in as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. Right‐click the PowerShell icon in the start menu, then choose more > Run as Administrator.
3. Click Yes on the UAC prompt.
4. Type the command below followed and press ENTER:

Get‐WindowsFeature ‐ComputerName Bravo

1. Scroll through the results and find the Group Policy Management option.
2. Is there an "X" next to it?
3. Scroll through the results and find the Remote Server Administration Tools section.
4. What items are enabled from this listing?
5. Type the command below and press ENTER:

Install‐WindowsFeature ‐Computer Bravo ‐Name gpmc,rsat ‐IncludeAllSubFeature

1. Wait for the installation to finish. It may take a few minutes.
2. Type the command below and press ENTER:

Get‐WindowsFeature ‐ComputerName Bravo

1. Scroll through the results.
2. Do the GPMC and all of the RSAT items show as Installed now?
3. Switch to the [**Bravo**](urn:it:godeploy:lab-guide:action-link:select-vm?=b112fbf6-8dbb-ea11-abef-00155d10e510) VM and log in as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=941bdf51-8ebb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
4. In Server Manager, click the Tools option and scan through the tools that are available.
5. Do you see all of the tools that you just installed?

Exercise 3: Installing the GPMC on Windows 10 Client

Windows 10 Client does not include the GPMC by default. It must be enabled as part of the RSAT pack. For the bulk of these labs, you will be using the Echo VM as your management console for the lab Active Directory Environment.

Task 1: Install the RSAT on Windows 10 Client

In this task, you will install the RSAT on the Windows 10 Client VM.

**Note**: If you get an error similar to the following while installing, please temporarily enable the Windows Update Service to ensure installation is successful.

"Installer encountered an error: 0x80070422  
The service cannote be started, etiher because it is disabled or because it has no enabled devices associated with it."

1. Switch to the [**Echo**](urn:it:godeploy:lab-guide:action-link:select-vm?=941bdf51-8ebb-ea11-abef-00155d10e510) VM and if you are not already logged in, log in as **HQ/Speck** with a password of [***Pa$$w0rd***](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=7aa29128-8ebb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. Open File Explorer and navigate to D:\LabFiles\Install\Win10.
3. Double‐click RSAT‐Windows10.msu.
4. Click YES to install the package. (This will take several minutes to complete. It is a fairly large update.)
5. Click I accept in the license window. (Again, be patient. This installation will take a few minutes.)
6. Click Close in the Installation Complete window.

Task 2: Verify the installation of the RSAT and GPMC tools

In this task, you will verify that the RSAT and GPMC tools have been installed correctly.

1. Click the Start button and note the newly installed RSAT tools.
2. Click the Start button and type Server Manager.
3. Right‐click the Server Manager icon in the search results and select Pin to Start.

**Note**: You can pin other frequently used items to the Start menu. However, the Server Manager has almost everything you need to administer your environment.

1. Open the Server Manager.
2. Click Add Other Servers to Manage, then click Find Now.
3. Hold the CTRL key and select Alpha and Bravo from the list on the left, then click the Arrow in the middle to add them to the list on the right, then click OK.
4. Select All Servers and you should now see Alpha and Bravo listed.
5. Click the Tools menu option, then select Group Policy Management.
6. Expand Forest:hq.local, Domains, and hq.local.
7. What items do you see listed under the hq.local domain?

Exercise 4: Installing the GPMC on Windows 8.1 Client

Windows 8.1 Client does not include the GPMC by default. It must be enabled as part of the RSAT pack.

**Caution**: Creating and editing policies from a Windows 8.1 or Server 2012 R2 console may leave out certain new policy settings that are available only in the Group Policy Management Editor on Windows 10 Client and Windows Server 2016. If you do use Windows 8.1 or Server 2012 R2 to edit policies, make sure you implement the ADMX Central Store discussed later in this course.

Task 1: Install the RSAT on Windows 8.1 Client

In this task, you will install the RSAT on the Windows 8.1 Client VM.

1. Log on to the [**Delta**](urn:it:godeploy:lab-guide:action-link:select-vm?=7aa29128-8ebb-ea11-abef-00155d10e510) VM as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=603f68c6-8dbb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. Mount the GroupPolicy‐LabFiles.iso using the lab interface.
3. Open File Explorer and navigate to D:\LabFiles\Install\Win8.1
4. Double‐click RSAT‐Windows8.1.msu.
5. Click YES to install the package. (This will take several minutes to complete. It is a fairly large update.)
6. Click I accept in the license window. (Again, be patient. This installation will take a few minutes.)
7. Click Close in the Installation Complete window.

Task 2: Verify the installation of the RSAT and GPMC tools

In this task, you will verify that the RSAT and GPMC tools have been installed correctly.

1. Move your mouse to the lower‐left corner of the screen, right‐click the Start tile that appears, then click Control Panel.
2. Click Programs.
3. Under Programs and Features, click Turn Windows features on or off.
4. Expand Remote Server Administration Tools.
5. Examine the items under the RSAT section. They should all be selected by default (unlike in Windows 7 where you have to turn them all on by hand).
6. Close Control Panel.
7. Open the Start screen and move your mouse to the lower‐right corner until the Charms bar appears.
8. Click Settings, then select Tiles.
9. Notice that the Show Administrative Tools option is set to Yes. (This is a known issue. The tools are not really visible until you change this option to No, then back to Yes.)
10. Click the slider to change the option to No and then click on the Start screen background.
11. Move your mouse to the lower‐right corner until the Charms bar appears.
12. Click Settings, then select Tiles.
13. Click the slider next to Show Administrative Tools to change the option back to Yes.
14. Click the Start screen background.
15. Click the down arrow in the bottom left corner of the screen. (You are now in the Apps view.)
16. Next to "Apps" at the top of the screen, click the drop‐down arrow and choose by category.
17. Scroll to the right and you will see all of the Administrative Tools.
18. Right‐click the Server Manager icon and select Pin to Start.

**Note**: You can pin other frequently used items to the Start menu. However, the Server Manager has almost everything you need to administer your environment.

1. Open the Server Manager.
2. Click Add Other Servers to Manage, then click Find Now.
3. Hold the CTRL key and select Alpha and Bravo from the list on the left, then click the Arrow in the middle to add them to the list on the right, then click OK.
4. Select All Servers and you should now see Alpha and Bravo listed.
5. Click the Tools menu option, then select Group Policy Management.
6. Expand Forest:hq.local, Domains, and hq.local.
7. What items do you see listed under the hq.local domain?

Exercise 5: Installing the GPMC on Windows 7

Windows 7 behaves the same as Windows 10 Client when it comes to the GPMC. It must be enabled as part of the RSAT pack.

**Caution**: Creating and editing policies from a Windows 7 or Server 2008 console may leave out certain new policy settings that are available only in the Group Policy Management Editor on Windows 8 Client and Windows Server 2012. If you do use Windows 7 to edit policies, make sure you implement the ADMX Central Store discussed later in this course.

It is STRONGLY recommended that you always edit policies from the newest version of Windows available in the environment.

Task 1: Install the RSAT on Windows 7

In this task, you will install the RSAT on the Windows 7 VM.

1. Log on to [**Kilo**](urn:it:godeploy:lab-guide:action-link:select-vm?=8156fc71-8ebb-ea11-abef-00155d10e510) as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=7aa29128-8ebb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. Mount GroupPolicy‐LabFiles.iso using the lab interface.
3. Open Windows Explorer and navigate to D:\LabFiles\Install\Win7.
4. Double‐click RSAT‐Windows7.msu.
5. Click YES to install the package. (This will take several minutes to complete. It is a fairly large update.)
6. Click I accept in the license window. (Again, be patient. This installation will take a few minutes.)
7. Click Close in the Installation Complete window.
8. Close the Help window that appears at the end of the installation.

Task 2: Enable the RSAT and GPMC tools

In this task, you will enable the RSAT and GPMC tools.

1. Click Start, Control Panel.
2. Click Programs.
3. Under Programs and Features, click Turn Windows features on or off.
4. Expand Remote Server Administration Tools.
5. Expand Feature Administration Tools and Role Administration Tools and select *all* the check next to each component. (You will have to expand several sub‐nodes as well. Unfortunately, there is not a faster way to do this.)
6. Click OK and wait for the installation to finish. (This will take a couple of minutes.)
7. To configure the Start menu to display the Administration Tools shortcut, right‐click Start, click Properties, and then click Customize.
8. In the Customize Start Menu dialog box, scroll down to System administrative tools, and then click the Display on the All Programs menu and the Start menu radio button. (This option may already be selected.)
9. Click OK and then click OK again.
10. Click Start and Administrative Tools. You should now see all of the tools available for managing the domain environment, including the Group Policy Management Console.
11. Open the Group Policy Management console.
12. Expand Forest:hq.local, Domains, and hq.local.
13. What items do you see listed under the hq.local domain?

Exercise 6: Performing basic Group Policy management

In this exercise, you will be introduced to a few basic Group Policy Management techniques.

Task 1: Use the Group Policy Management Console

In this task, you will use the Group Policy Management Console.

1. Switch to the [**Echo**](urn:it:godeploy:lab-guide:action-link:select-vm?=941bdf51-8ebb-ea11-abef-00155d10e510) VM and log on as **HQ/Speck** with a password of [**Pa$$w0rd**](urn:it:godeploy:lab-guide:action-link:paste-vm-password?=941bdf51-8ebb-ea11-abef-00155d10e510&i=0&d=Pa%24%24w0rd).
2. Open the Start menu, type Server Manager and then press ENTER. (Or click the Server Manager shortcut you previously created.)
3. In Server Manager, click the All Servers option on the left.
4. Right‐click All Servers and select Add Servers.
5. Click Find Now, hold CTRL and click Alpha and Bravo.
6. Click the right‐arrow in the middle of the window, then click OK.
7. In All Servers you should now see Alpha and Bravo listed.

**Note**: You can now right‐click Alpha or Bravo to get a context‐sensitive menu of options that are pertinent to that particular machine. It is not required to add theses servers in order to use the Administrative Tools, but it is more convenient and provides you will status and event log details from those servers within the Server Manager console.

1. In Server Manager, click Tools, Group Policy Management.
2. Expand Forest:hq.local, Domains, and hq.local.
3. Click Default Domain Policy. (Click Do not show this message again, then click OK if you see a GPMC popup message appear.)
4. Click the Settings tab to get a report of all settings within this policy. (If an Internet Explorer security warning appears, click Add, then click Add and click OK to add this site to the list of trusted sites.)
5. Expand Security Settings and browse around the Account Policies and Local Policies.
6. Can you modify any of the settings directly within this interface?
7. Right‐click Default Domain Policy (in the left section of the window) and select Edit.
8. Under Computer Configuration, expand Policies, Windows Settings, Security Settings, Account Policies, and Password Policy.
9. Does it appear that you can change these values?
10. Do not make any changes. Close the Group Policy Management Editor and return to the Group Policy Management Console.
11. Expand the Domain Controllers OU and select Default Domain Controllers Policy.
12. Click the Settings tab.
13. Browse around the Security Settings\Local Policies\User Rights Assignment and Security Options. You will notice that settings configured here are very different from those configured on the Default Domain Policy.
14. Expand the Group Policy Objects container. (You should see the same two policies listed.)
15. What is the difference between these policies and the ones you just examined?
16. Right‐click Group Policy Objects and click New.
17. In the New GPO dialog box, type Taskbar Policy Settings in the Name box and then click OK.
18. Select the Taskbar Policy Settings GPO.

Task 2: Configure policy settings and filter the display

In this task, you will configure the policy settings and filter the display.

1. Right‐click the Taskbar Policy Settings GPO and click Edit.
2. Expand User Configuration, Policies, Administrative Templates, and then click Start Menu and Taskbar.
3. Double‐click the Lock the Taskbar setting.
4. What is the current setting?

**What does it mean?**

1. Select Enabled and then click OK. (The OK button may be hidden if you have 800 x 600 as your screen resolution. Maximize the dialog box to view the OK button.)
2. Double‐click the Do not allow pinning programs to the Taskbar setting.
3. Select Enabled and then click OK. (The OK button may be hidden if you have 800 x 600 as your screen resolution. Maximize the dialog box to view the OK button.)
4. In the left section of the window, click the All Settings container.
5. How many settings are available?
6. Click the State column heading to sort by that column.
7. Do you see the options that you just configured near the top of the list?
8. Right‐click All Settings and select Filter Options.
9. From the Configured drop‐down list select Yes and then click OK.
10. Now how many settings do you see?
11. Right‐click All Settings and clear the Filter On check mark.
12. Close the Group Policy Management Editor and return to the Group Policy Management Console.
13. Will these policy settings apply to anyone yet?
14. Why?

**Note**: If your lab VMs are running on the local machine and not through the Remote Labs interface, you should create a Checkpoint (Snapshot) of the Alpha, Bravo, Echo, Delta and Kilo VMs. Check with your instructor if you are unsure of how to do this. If your labs are being accessed remotely, you may ignore this note.

**Results**: You have completed this lab.