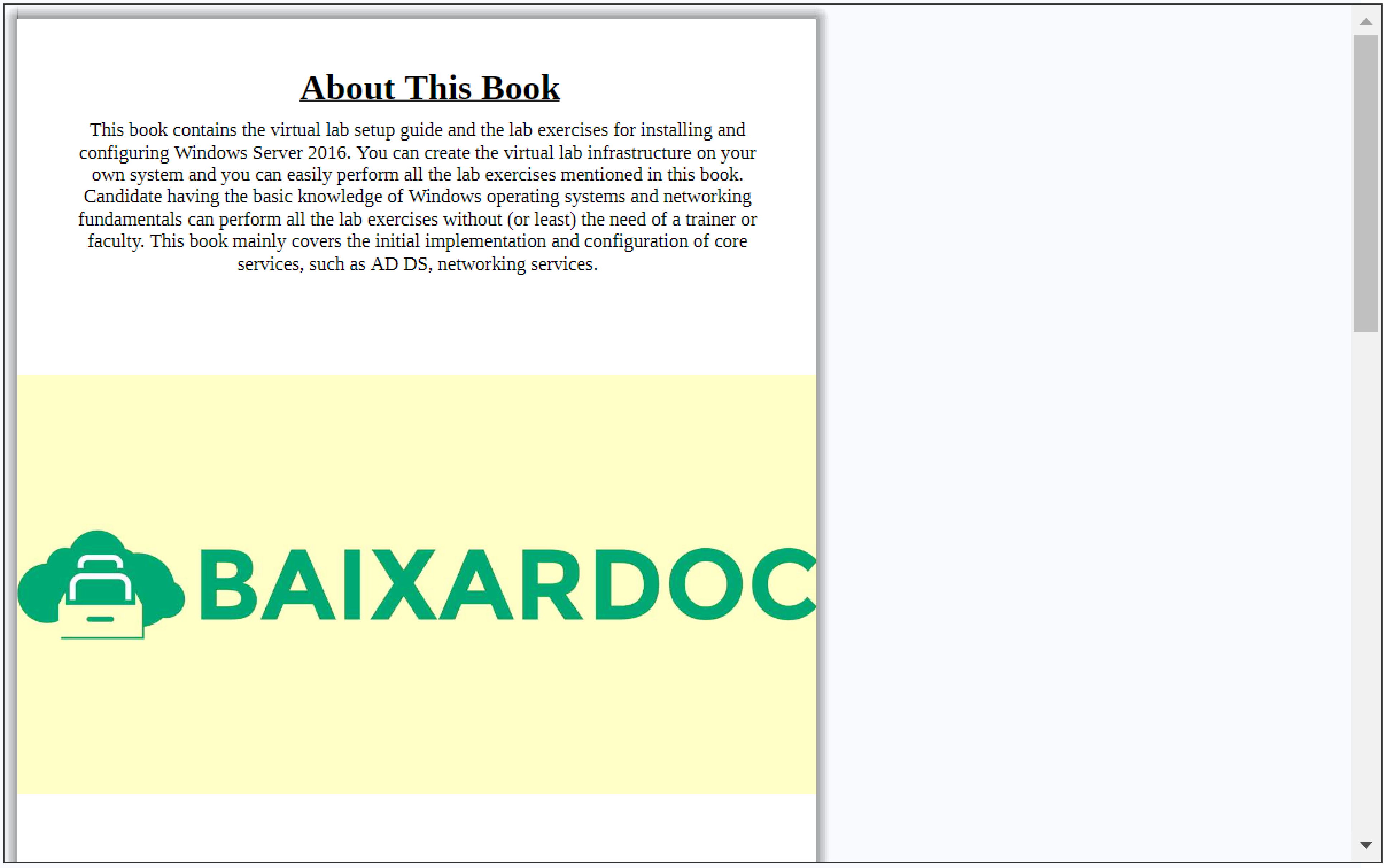
/ Installing And Configuring Windows Server

Preview only show first 10 pages with watermark. For full document please download



About This Book

This book contains the virtual lab setup guide and the lab exercises for installing and configuring Windows Server 2016. You can create the virtual lab infrastructure on your own system and you can easily perform all the lab exercises mentioned in this book. Candidate having the basic knowledge of Windows operating systems and networking fundamentals can perform all the lab exercises without (or least) the need of a trainer or faculty. This book mainly covers the initial implementation and configuration of core services, such as AD DS, networking services.

Installing And Configuring Windows Server

DOWNLOAD EMBED

Rating	
Date	June 2018
Size	6.7MB
Views	6,600
Categories	Active Directory Ip Address Domain Name System Group Policy Computer Network

Share

Transcript

Installing and Configuring Windows Server 2016 (Hands-on Guide)

Copyright The author holds all the rights of publishing and reproducing to this book. The content of this book cannot be reproduced or copied in any form or by any means or reproduced without the prior written permission of the author. About This Book This book contains the virtual lab setup guide and the lab exercises for installing and configuring Windows Server 2016. You can create the virtual lab infrastructure on your own system and you can easily perform all the lab exercises mentioned in this book. Candidate having the basic knowledge of Windows operating systems and networking fundamentals can perform all the lab exercises without (or least) the need of a trainer or faculty. This book mainly covers the initial implementation and configuration of core services, such as AD DS, networking services. Audience and Candidates Prerequisites This book is intended for the candidates who have basic operating system knowledge, and want to gain the hands-on practice skills and knowledge necessary to implement the core infrastructure services. In addition, this book is also helpful for the candidate who are looking for certification in the Windows Server 2016 platform. The candidates should have the basic knowledge of the networking fundamentals, Windows-based operating systems, and virtualization platforms to perform the hands-on practices. Disclaimer We made almost every effort to avoid errors or omissions in this guide. However, errors may slink in. Any mistake, error or discrepancy noted by the readers are requested to share with us, which will be highly appreciable. The contents and images in this guide could include technical inaccuracies or typographical errors. Author(s) or publisher makes no representations about the accuracy of the information contained in the guide. Virtual Machines The virtual machines that will be used throughout this book are listed in the following table. S. No. VM Name Operating System 1 DC1 Windows Server 2016 2 SERVER1 Windows Server 2016 3 CLIENT1 Windows 8.1/10 4 ROUTER Windows

Server 2016 5 SERVER2 Windows Server 2016 To prepare the virtual machines mentioned in the preceding table, you need ISO images. You can download the evaluation ISO images (Windows Server 2016 (Technical Preview) and Windows 8.1/10) from the Microsoft download center. To perform the step by step lab exercises, download the ISO images and place them under the D:\ISOs folder on the host machine. You can setup the virtual lab infrastructure on the VMware or Hyper-V platform. Each virtual machine will act as a separate machine with the unique GUID, SID, and IP address. The following table lists the IP addresses and roles of the respective VMs. S. No. VM Name IP Address Role 1 DC1 10.0.0.100 Domain controller of the mcsalab.local domain. 2 SERVER1 10.0.0.101 Member server of the mcsalab.local domain. 3 CLIENT1 10.0.0.102 Client machine of the mcsalab.local domain. 4 ROUTER Internal Subnet: 10.0.0.1 Router server to perform the LAN routing. External Subnet: 192.168.0.1 5 SERVER2 192.168.0.2 Workgroup server in the external subnet. Preparing Virtual Machines To create the virtual machines, you need to perform the following tasks on the host machine: 1. 2. 3. 4. 5. 6. Install VMware Workstation or Player. Install and configure the DC1 virtual machine Install and configure the SERVER1 virtual machine Install and configure the CLIENT1 virtual machine Install and configure the ROUTER virtual machine Install and configure the SERVER2 virtual machine Task 1: Installing VMware Workstation on the Host Machine To Install VMware Workstation or VMware Player, first you need to download it. Once it is downloaded, just double-click the setup file, and follow the simple steps to complete the installation process. Task 2: Installing and Configuring the DC1 Virtual Machine To install and configure the DC1 virtual machine, you need to perform the following steps: 1. 2. 3. Make sure that the VMware console is active. Select File and then select New Virtual Machine. On the New Virtual Machine Wizard, click Next. 4. On the Guest Operating System Installation page, select the Installer disc image file (iso): radio button, browse the location of the Server 2016 ISO image file, and then click Next. 5. Note: If you use the VMware platform that automatically detects the version of the Windows server, you may asked to set the following settings: Product key Operating system edition Administrator password Otherwise, you may skip it. 6. On the Select a Guest Operating System page, select the highest supported version of Windows server (in this case Windows Server 2012 but it will still support Windows Server 2016), and then click Next. 7. 8. On the Name and Virtual Machine page, type DC1 in the Virtual machine name field. In the Location field, navigate the location where you want to save the virtual machine, such as H:\VMs\2k16\DC1, and then click Next. 9. On the Specify Disk Capacity page, select Store virtual disk as a single file, optionally you can also set the disk size as well, and then click Next. 10. On the Ready to Create Virtual Machine page, click Customize Hardware. 11. On the Hardware window, select Network Adapter in the left pane. Select the Host only radio button, and then click Close. 12. 13. 14. Click Finish. On the VMware console, power on the DC1 virtual machine. On the Windows Setup page, click Next, and then click Install Now. 15. On the Select the operating system you want to install page, select the Windows Server 2016 Desktop Experience, and then click Next. 16. 17. 18. On the License terms page, select the I accept the license terms check box, and then click Next. On the Which type of installation do you want page, select the Custom option, and then click Next. On the Where do you want to install Windows page, click Next. 19. The Installation process will begin, after 10-15 minutes the Customize settings screen will display. 20. Set Administrator password as Password@123. Task 2.1: Configuring the DC1 Virtual Machine 1. 2. Sign in to DC1 with the Administrator account. Open the System Properties (sysdm.cpl) and set the computer name as DC1. 3. 4. 5. 6. Restart and sign in to the system with the Administrator account. After some time, the Server Manager console will display. Open the Run dialog box, type ncpa.cpl, and then press Enter. Select and right-click the active network adapter, and then select Properties. Set the following TCP/IP settings: IP address: 10.0.0.100. Subnet mask: 255.0.0.0. Default gateway: 10.0.0.1. Preferred DNS server: 10.0.0.100. 7. Close the Network Connections console. Task 2.2: Promoting the DC1 Virtual Machine as a Domain Controller To promote the DC1 virtual machine as a domain controller, you need to perform the following steps: 1. 2. 3. 4. 5. 6. Open the Server Manager console. Click the Add roles and features link. On the Before you begin page, click Next. On the Select installation type page, click Next. On the Select destination server page, click Next. On the Select server roles page, select the Active Directory Domain Services check box, as shown in the following figure. 7. 8. 9. 10. Accept the default selections through rest of the wizard and complete the installation process. Click Close, once the installation succeeds on DC1. On the Server Manager console, click the Notifications icon. Click the Promote this server to a domain controller link, as shown in the following figure. 11. 12. On the Deployment Configuration page, select the Add a new forest radio button. In the Root domain name text box, type mcsalab.local, as shown in the following figure, and then click Next. 13. On the Domain Controller Options page, make sure that the Domain Name System (DNS) server check box is selected, as shown in the following figure. 14. In the Password and Confirm password text boxes, type the Password@123, and then click Next. 15. On the DNS Options page and then click Next. 16. On the Additional Options page, click Next. 17. On the Paths page, as shown in the following figure, review the default location for the AD DS database file, and then click Next. 18. On the Review Options page, click Next. 19. On the Prerequisites Check page, as shown in the following figure, review the prerequisites, and then click Install. 20. After some time, the system will restart automatically, sign in to DC1 with the MCSALAB\Administrator account. 21. Do not shut down the DC1 virtual machine. Task 3: Installing and Configuring the SERVER1 Virtual Machine To install and configure the SERVER1 virtual machine, you can follow the simple steps as you used to install and configure the DC1 virtual machine. 1. 2. 3. 4. 5. 6. 7. 8. During the installing SERVER1 virtual machine, make sure that you use the following settings and options: Virtual machine name: SERVER1. Operating system version: Windows Server 2016. Memory: 2048 MB Hard disk size: 50 GB Network Adapter: Host only (click Customize Hardware before clicking the Finish button.) Password: Password@123 Once you installed the SERVER1 virtual machine with the preceding settings, configure the following TCP/IP settings: IP address: 10.0.0.101 Subnet mask: 255.0.0.0 Default gateway: 10.0.0.1 Preferred DNS server: 10.0.0.100 Once you configured the preceding TCP/IP settings, open the System Properties dialog box and click Change. On the Computer Name/Domain Changes dialog box, in the Computer name text box, type SERVER1. Select the Domain radio button, in the Member of section, and then type mcsalab.local, and then click OK. On the Windows Security dialog box, provide the credentials of the DC1 server, and restart the SERVER1 virtual machine. Sign in to SERVER1 with the Administrator account. Shut down the SERVER1 virtual machine. Task 4: Installing and Configuring the CLIENT1 Virtual Machine To install and configure the CLIENT1 virtual machine, you can follow the simple steps as you used to install and configure the DC1 virtual machine. 1. 2. 3. 4. 5. 6. 7. 8. During the installing CLIENT1 virtual machine, make sure that you use the following settings and options: Virtual machine name: CLIENT1. Operating system version: Windows 8.1/10. Memory: 1024 MB Hard disk size: 50 GB Network Adapter: Host only (click Customize Hardware before clicking the Finish button.) Password: Password@123 Once you installed the CLIENT1 virtual machine with the preceding settings, configure the following TCP/IP settings: IP address: 10.0.0.102 Subnet mask: 255.0.0.0 Default gateway: 10.0.0.1 Preferred DNS server: 10.0.0.100 Once you configured the preceding TCP/IP settings, open the System Properties dialog box, and click Change. On the Computer Name/Domain Changes dialog box, in the Computer name text box, type CLIENT1. Select the Domain radio button in the Member of section, type mcsalab.local, and then click OK. On the Windows Security dialog box, provide the credentials of the DC1 server, and restart the CLIENT1 virtual machine. Sign in to CLIENT1 with the Administrator account. Shut down the CLIENT1 virtual machine. Task 5: Installing and Configuring the ROUTER Virtual Machine To install and configure the ROUTER virtual machine, you can follow the simple steps as you used to install and configure the DC1 virtual machine. 1. 2. During the creating ROUTER virtual machine, make sure that you use the following settings and options: Virtual machine name: ROUTER. Operating system version: Windows Server 2016. Memory: 1024 MB Hard disk size: 50 GB Network Adapter: Host only Once you created the ROUTER virtual machine with the preceding settings, select the ROUTER virtual machine, click Edit virtual machine settings, as shown in the following figure. 3. On the Virtual Machine Settings dialog box, click Add. 4. On the Add Hardware Wizard, select Network Adapter, and then click Next. 5. On the Network Adapter Type page, select VMnet2 under the Custom option. 6. 7. 8. 9. Click Finish and then click OK button. Power on the ROUTER virtual machine. Follow the simple steps to install the ROUTER virtul machine. Use Password@123 as Administrator password. Once you installed the ROUTER virtual machine with the preceding settings, configure the following TCP/IP settings on the first network adapter (connected to the Host only network): IP address: 10.0.0.1 Subnet mask: 255.0.0.0 Preferred DNS server: 10.0.0.100 10. Configure the following TCP/IP settings on the second network adapter (connected to the VMnet2 network): IP address: 192.168.0.1 Subnet mask: 255.255.255.0 11. 12. 13. Once you configured the preceding TCP/IP settings, open the System Properties dialog box, set the computer name as ROUTER, and restart the ROUTER virtual machine. Open the Command Prompt window, type ping 10.0.0.100, and then press Enter. You should be able to communicate (ping) with the DC1 server. Note: If you are unable to communicate with the DC1 server, you may need to interchange the TCP/IP settings of the network adapters. 14. Do not shut down the ROUTER virtual machine. Task 6: Creating and Configuring the SERVER2 Virtual Machine To install and configure the SERVER2 virtual machine, you can follow the simple steps as you used to install and configure the DC1 virtual machine. 1. 2. 3. 4. 5. 1. During the installing SERVER2 virtual machine, make sure that you use the following settings and options: Virtual machine name: SERVER2. Operating system version: Windows Server 2016. Memory: 1024 MB Hard disk size: 50 GB Network Adapter: VMnet2 Password: Password@123 Once you installed the SERVER2 virtual machine with the preceding settings, configure the following TCP/IP settings: IP address: 192.168.0.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.0.1 Preferred DNS server: 10.0.0.100 Once you configured the preceding TCP/IP settings, open the System Properties dialog box, set the computer name as SERVER2, and restart the SERVER2 virtual machine. Sign in to SERVER2 with the Administrator account. Shut down the SERVER2 virtual machine. Shut down the DC1 virtual machine. Task 7: Creating Snapshots of Virtual Machines Once you installed and configured all the virtual machines, you need to create the snapshots/checkpoints for each virtual machine. Snapshot will help you to revert a virtual machine to its previously used state (at the point when you had created it). To create a snapshot, you need to perform the following tasks: 1. Make sure that the all virtual machines are turned off. 2. Select and right-click any virtual machine, select Snapshot, and then select Take snapshot. After few seconds, the snapshot will be created. 3. Using the preceding method, create snapshots of all the virtual machines. Task 8: Working with Windows Server 2016 Desktop Experience GUI interface of Windows Server 2016 is almost has similar functions as used in windows Server 2012 R2. However, there are some new feature have been added to make the user experience more interesting. Some of the basic GUI features are: Start button Task Manager Task View Start button 1. Sign in to DC1 and click the Start button. It will show you the various options, such as Server Manager, Settings, PowerShell, and Calculator that can be accessed directly. 2. If you right-click the Start button, it will show you few more options, as shown in the following figure. Task Manager The Task Manager in Windows Server 2016 is much similar to the Task Manager that has been used in Windows Server 2012 R2. Task View Task View allows you to view and switch between different active windows. This feature was not available in Windows Server 2012 R2. Task 9: What's New in Windows Server 2016? In Windows Server 2016, there are many new roles and features have been added. Some of the major new roles and features are: Host Guardian Service Multipoint Services Windows Server Essentials Experience Setup and Boot Event Collections SMB Bandwidth Limit Windows Biometric Framework BitLocker Network Unlock Host Guardian Service The Host Guardian Service (HGS) is a server role introduced in Windows Server 2016. It provides the Attestation and Key Protection services that allow Guarded Hosts to run shielded virtual machines. The Attestation service validates guarded host identity and configuration. The Key Protection service allows transport keys to enable guarded hosts to unlock and run shielded virtual machines. Multipoint Services It allows multiple users to simultaneously share one computer and each user has their own independent and familiar Windows experience. Windows Server Essentials Experience This is a role service that sets up the IT infrastructure and offers powerful functions, such as "PC backups" that helps organizations' to protect data, and "Remote Web Access" that helps access business information from anywhere, virtually. It also helps you to simply and rapidly connect to cloud-based applications and services to extend the functionality of the servers. Setup and Boot Event Collections It is a feature that enables the collection and logging of setup and boot events from other computers on the network. SMB Bandwidth Limit This feature provides a mechanism to track SMB traffic per category and allows you to limit the amount of traffic allowed for a given category. It is commonly used to limit the bandwidth used by live migration over SMB. Windows Biometric Framework This feature allows fingerprint devices to be used to identify and verify identities and to sign in to Windows. BitLocker Network Unlock This feature enables a network-based key protector to be used to automatically unlock BitLocker-protected operating system drives in domain-joined computers, when the computer is restarted. Exercise 1: Installing and Configuring Windows Server 2012 R2 Core Machine In this exercise, you will install and configure a Windows Server 2012 R2 core machine. The installation process for the server core option and full GUI option is almost identical. However, server core option requires less hardware resources and it is more secure than the full GUI option. In this exercise, you will use the following virtual machines: DC1 CORE1 To install and configure the Windows Server 2012 R2 core machine, you need to perform the following tasks: Task 1: Installing Windows Server 2012 R2 Core Machine. 1. 2. Create a virtual machine with the following settings: During the creating the virtual machine, make sure that you use the following settings and options: Virtual machine name: CORE1. Operating system version: Windows Server 2016. Memory: 512 MB Hard disk size: 20 GB Network Adapter: Host only Password: Password@123 3. 4. 5. 6. Once the virtual machine is created, power on the CORE1 virtual machine. After some time, the Windows Setup screen will display. Click Next and then click Install now. If the Activate Windows screen is displayed, click I don't have a product key link. 7. On the Select the operating system you want to install page, select Windows Server 2016 Technical Preview 4, and then click Next. 8. On the License terms page, select the I accept the license terms check box, and then click Next. 9. On the Which type of installation do you want? page, click Custom: Install Windows only (advanced), as shown in the following figure. 10. On the Where do you want to install Windows? page, click Next. 11. The installation process will start. 12. After some time, the sign in screen will display, and you will be asked to change the Administrator password. 13. Set the Administrator password as Password@123. Task 2: Configuring the Windows Server 2016 Core Machine. To configure the Windows Server 2016 core machine, you need to perform the following steps: 1. 2. Sign in to CORE1 with the Administrator account. On the Command Prompt window, type sconfig.cmd, and then press Enter. The Server Configuration options will display, as shown in the following figure. 3. 4. To change the system Date and Time, type 9, and then press Enter. On the Date and Time dialog box, as shown in the following figure, click Change time zone. 5. 6. Select the desired time zone, and then click OK. In the Date and Time dialog box, click Change Date and Time, and verify the date and time, and then click OK. 7. On the Command Prompt window, type 8, and then press Enter to configure Network Settings. 8. Type the index number (in our example it is 10) of the network adapter, as shown in the following figure, and then press Enter. 9. On the Network Adapter Settings page, type 1, to set the Network Adapter Address, as shown in the following figure, and then press Enter. 10. To set static IP address, type S, as shown in the following figure, and then press Enter. 11. At the Enter static IP address: prompt, type 10.0.0.103, and then press Enter. 12. At the Enter subnet mask: prompt, accept the default value, and then press Enter. 13. At the Enter default gateway: prompt, type 10.0.0.1, and then press Enter, as shown in the following figure. 14. On the Network Adapter Settings option, type 2, to configure the DNS server address, and then press Enter. 15. At the Enter new preferred DNS server prompt, type 10.0.0.100, and then press Enter. 16. On the Network Settings message box, as shown in the following figure, click OK. 17. Press Enter to not configure an alternate DNS server address. 18. At the Select option: prompt, type 4, and then press Enter to return to the main menu. 19. At the Enter number to select an option: prompt, type 15, and then press Enter to exit the sconfig.cmd utility. 20. On the Command Prompt window, type ping dc1.mcsalab.local to verify the connectivity between DC1 and CORE1. Task 3: Adding CORE1 to Domain 1. On the Command Prompt window, type sconfig.cmd, and then press Enter. 2. At the Enter number to select an option: prompt, type 2, and then press Enter. 3. At the Enter a new computer name: prompt, type CORE1, and then press Enter. 4. On the Restart dialog box, click Yes. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. The system will restart and after some time the Sign in screen will display. Sign in to CORE1 with the Administrator account. On the Command Prompt window, type hostname, and then press Enter to verify the computer's name. On the Command Prompt window, type sconfig.cmd, and then press Enter. Type 1 to change the Domain/Workgroup settings, and then press Enter. Type D to join a domain, and then press Enter. At the Name of domain to join prompt, type mcsalab.local, and then press Enter. At the Specify an authorized domain\user prompt, type Administrator, and then press Enter. At the Type the password associated with the domain user prompt, type Password@123, and then press Enter. At the Change Computer Name message box, as shown in the following figure, click No. 15. On the Restart dialog box, click Yes. The system will restart. After some time, the sign in screen will display. 16. Sign in to CORE1 with the MCSALAB\Administrator account. Results: After completing this exercise, you will have configured a Windows Server 2016 server core machine. Do not turn off or shut down the DC1 and/or CORE1 virtual machine(s) as these virtual machines will be required to perform the next exercise. Exercise 2: Managing Servers Remotely In this exercise, you will manage the server core machine from the remote location. In addition, you will also deploy roles and features on the server core machine. Further, you will manage the services on the server core machine. Before starting to perform this exercise, make sure that the DC1 and CORE1 virtual machines are running, and you have not reverted them in the previous exercise. Task 1: Creating and Managing the Server Group 1. 2. 3. 4. 5. Sign in to DC1 with the MCSALAB\Administrator account. On the Server Manager console, make sure that Dashboard is selected in the left pane, and then click Create a server group. On the Create Server Group dialog box, click the Active Directory tab, and then click Find Now. In the Server group name text box, select the CORE1 and SERVER1 servers, and then add CORE1 and SERVER1 to the server group. In the Server group name text box, type ServerGroup1, as shown in the following figure. 6. 7. Click OK to close the Create Server Group dialog box. On the Server Manager console, select ServerGroup1 in the left pane. Verify that the both servers are listed in the Servers pane, as shown in the following figure. Task 2: Deploying Roles and Features on CORE1 Machine 1. Sign in to DC1 with the MCSALAB\Administrator account. 2. On the Server Manager console, click ServerGroup1 in the left pane. 3. Scroll to the top of the pane, select and right-click CORE1, and then select Add Roles and Features, as shown in the following figure. 4. On the Add Roles and Features Wizard, click Next. 5. On the Select installation type page, click Next. 6. On the Select destination server page, make sure that CORE1.mcsalab.local is selected, as shown in the following figure, and then click Next. 7. On the Select server roles page, select the DHCP Server check box, as shown in the following figure, and then click Next. 8. On the Add Roles and Features dialog box, click Next. 9. Click Next, until the Confirm install selections page is displayed. 10. On the Confirm installation selections page, select the Restart the destination server automatically if required check box, as shown in the following figure, and then click Install. 11. Click Close to close the Add Roles and Features Wizard, once the installation is completed. Task 3: Managing Services on the CORE1 Machine 1. Switch to as Other user and sign in to CORE1 with the MCSALAB\Administrator account. 2. On the Command Prompt window, type the following command, and then press Enter, as shown in the following figure. netsh.exe firewall set service remoteadmin enable ALL 3. Switch back and sign in to DC1 with the MCSALAB\Administrator account. 4. On the Server Manager console, select ServerGroup1. 5. Select and right-click CORE1, and then click Computer Management. 6. On the Computer Management console, expand the Services and Applications node, and then select Services. 7. Select and right-click the DHCP Server service, and then click Properties, as shown in the following figure. 8. 9. On the Properties dialog box, on the General tab, make sure that the Startup type is set to Automatic. Select the Recovery tab, configure the following settings, as shown in the following figure. First failure: Restart the Service Second failure: Restart the Service Subsequent failures: Restart the Computer Reset fail count after: 1 days Restart service after: 1 minute 10. On the Properties dialog box, click Restart Computer Options. 11. On the Restart Computer Options dialog box, in the Restart computer after box, type 2, and then click OK. 12. Click OK to close the Properties dialog box. 13. Close the Computer Management console. Results: After completing this exercise, you have created a server group, deployed roles and features, and managed a service remotely. Shut down and revert the DC1 and CORE1 virtual machines to prepare for the next exercise. Exercise 3: Using Windows PowerShell to Manage Servers In this exercise, you will use the Windows PowerShell to manage the Window Server 2016. Windows PowerShell is a command-line interface that is similar to command prompt. It is designed to execute the scripts similar to UNIX/Linux operating systems. Start the DC1 virtual machine to perform this exercise. Task 1: Using the Windows PowerShell to Connect Remotely to Servers and View Information 1. Sign in to DC1 with the MCSALAB\Administrator account. 2. On the Server Manager console, select ServerGroup1. 3. Select and right-click CORE1, and then select Windows PowerShell. 4. At the Windows PowerShell prompt, type cd\ and then press Enter. 5. Type Import-Module ServerManager, and then press Enter. 6. Type Get-WindowsFeature and then press Enter to view the installed roles and features on CORE1, as shown in the following figure. 7. Type the following command to view the running services on CORE1 and then press Enter, as shown in the following figure. Get-service | where-object {$_.status -eq "Running"} 8. Type the following command and then press Enter to view a list of processes on CORE1, as shown in the following figure. Get-Process 9. Type the following command to view the IP addresses of the CORE1 machine, and then press Enter, as shown in the following figure. Get-NetIPAddress | Format-table 10. Type the following command to view the most recent 5 security logs, and then press Enter, as shown in the following figure. Get-EventLog Security -Newest 5 11. Close Windows PowerShell. Task 2: Using Windows PowerShell to Manage Roles and Features Remotely 1. 2. 3. 4. On DC1, on the taskbar, click the Windows PowerShell icon. At the Windows PowerShell prompt, type the following command, and then press Enter. Import-Module ServerManager To verify that the WINS Server feature is not installed on CORE1, type the following command, and then press Enter, as shown in the following figure. Get-WindowsFeature -ComputerName CORE1 5. 6. To install the WINS Server feature on CORE1, type the following command, and then press Enter, as shown in the following figure. Install-WindowsFeature WINS -ComputerName CORE1 7. Verify that the Exit Code status displays as the success text. Results: After completing this exercise, you have managed the servers using Windows PowerShell. Shut down and revert the DC1 and CORE1 virtual machines. Exercise 04: Installing and Configuring Domain Controllers The system that holds the Active Directory Domain Services role acts as a domain controller. A domain controller is a server that is used to manage and control the clients on a network. In this exercise, you will learn how to configure a domain controller on Windows Serve 2016. In addition, you will also learn how to configure a server as a Global Catalog server. Start the DC1 and SERVER1 virtual machines to perform this exercise. Task 1: Adding the AD DS Role on a Member Server 1. 2. 3. 4. Sign in to DC1 with the MCSA\Administrator account. On the Server Manager console, in the left pane, select and right-click All Servers, and then select Add Servers. On the Add Servers dialog box, in the Name (CN) text box, type SERVER1, and then click Find Now. In the name list area, select SERVER1, and then click the arrow to add the server to the Selected column, as shown in the following figure. 5. 6. Click OK to close the Add Servers dialog box. On the Server Manager console, in the Servers pane, wait until the Manageability status displays as Online – Performance counters not started, as shown in the following figure. 7. Select and right-click SERVER1, and then select Add Roles and Features. 8. On the Add Roles and Features Wizard, click Next. 9. On the Select installation type page, click Next. 10. On the Select destination server page, make sure that the Select a server from the server pool radio button is selected. 11. In the Server Pool area, make sure that SERVER1.mcsalab.local is selected, as shown in the following figure, and then click Next. 12. On the Select server roles page, select the Active Directory Domain Services check box. 13. On the Add Roles and Features dialog box, click Add Features, and then click Next. 14. The Select server roles page is returned, make sure that the Active Directory Domain Services check box is selected, as shown in the following figure, and then click Next. 15. Click Next, until the Confirm installation selections page is displayed. 16. On the Confirm installation selections page, select the Restart the destination server automatically if required check box, and then click Install. 17. The installation process will start. Click Close to close the Add Roles and Features Wizard, once the installation is completed. Task 2: Configuring SERVER1 Server as a Domain Controller 1. On DC1, on the Server Manager console, click the Notifications button. 2. On the Post-deployment Configuration box, click the Promote this server to a domain controller link, as shown in the following figure. 3. 4. On the Deployment Configuration page, of the Active Directory Domain Services Configuration Wizard, make sure that the Add a domain controller to an existing domain radio button is selected. In the Domain text box, make sure that the mcsalab.local text is written, as shown in the following figure. 5. In the Supply the credentials to perform this operation section, click Change. 6. On the Windows Security dialog box, in the Username text box, type MCSALAB\Administrator, in the Password box, type Password@123, as shown in the following figure. 7. 8. Click OK and then click Next. On the Domain Controller Options page, make sure that Domain Name System (DNS) server check box is selected, and then clear the Global Catalog (GC) check box. 9. In the Type the Directory Services Restore Mode (DSRM) password section, type Password@123, in the Password and Confirm password text boxes, as shown in the following figure, and then click Next. 10. Click Next, until the Prerequisites Check page is displayed. 11. On the Prerequisites Check page, review the warnings, and then click Install. 12. The installation process will start, click Close, once the installation is completed. 13. The server will restart. Wait for server to restart. Task 3: Configuring SERVER1 as a Global Catalog Server 1. 2. Switch and sign in to SERVER1 with the MCSALAB\Administrator account On the Server Manager console, click Tools, and then click Active Directory Sites and Services. 3. On the Active Directory Sites and Services console, expand Sites\DefaultFirst-Site-Name\Servers, and then click SERVER1, as shown in the following figure. 4. In the left pane, select and right-click NTDS Settings, and then select Properties. 5. On the NTDS Settings Properties dialog box, select the Global Catalog check box, as shown in the following figure, and then click OK. 6. Close the Active Directory Sites and Services console. Results: After completing this exercise, you will have explored the Server Manager console and promoted a member server to be a domain controller. Shut down and revert the DC1 and SERVER1 virtual machines to prepare for the next exercise. Exercise 5: Installing a Domain Controller by Using IFM In this exercise, you will learn how to configure a domain controller using the IFM data file. The Install From Media (IFM) is a feature that allows you to configure a server as a domain controller. This feature helps you to reduce the network bandwidth consumption used during the additional domain controller configuration. IFM allows you to export the Active Directory database file (NTDS) to an external media which can be used to configure an additional domain controller. Start the DC1 and SERVER1 virtual machines to perform this exercise. Task 1: Generating a IFM Data File 1. Sign in to DC1 with the MCSA\Administrator account. 2. Open the Run dialog box, in the Open text box, type cmd, and then press Enter. 3. On the Command Prompt window, type the following commands, and then press Enter after each one, as shown in the following figure. Ntdsutil Activate instance ntds IFM Create sysvol full C:\IFM Task 2: Adding the AD DS Role to the Member Server 1. 2. Switch and sign in to SERVER1 with the MCSALAB\Administrator account. Open the Command Prompt window, type the following command, and then press Enter, as shown in the following figure. Net use Z: \DC1\c$\IFM 3. Open the Server Manager console, if required. 4. In the left pane, select Local Server. 5. In the toolbar, click Manage, and then click Add Roles and Features, as shown in the following figure. 6. 7. 8. 9. 10. 11. 12. 13. 14. On the Before you begin page of the Add Roles and Features Wizard, click Next. On the Select installation type page, make sure that the Role-based or featurebased installation radio button is selected, and then click Next. On the Select destination server page, make sure that the SERVER1 server is selected, and then click Next. On the Select server roles page, select the Active Directory Domain Services check box. On the Add Roles and Features Wizard dialog box, click Add Features, and then click Next. On the Select Features page, click Next. On the Active Directory Domain Services page, click Next. On the Confirm installation selections page, select the Restart the destination server automatically if required check box. On the Add Roles and Features Wizard message box, as shown in the following figure, read the message, and then click Yes. 15. 16. On the Confirm installation selections page, click Install. The installation process will start. Click Close, once the installation is completed. Note: If you see a warning regarding the DNS server delegation, click OK. Task 3: Configuring SERVER1 as a New Domain Controller Using the IFM Data File 1. 2. On SERVER1, open the Command Prompt window, if required. On the Command Prompt window, type the following commands, and then press Enter, as shown in the following figure. Robocopy Z: C:\IFM /copyall /s 3. Close the Command Prompt window, once the copying process is completed. 4. On the Server Manager console, click the Notifications button. 5. In the Post-deployment Configuration box, click the Promote this server to a domain controller link. 6. On the Deployment Configuration page, make sure that the Add a domain controller to an existing domain radio button is selected. 7. Make sure that the mcsalab.local text is written in the Domain text box, as shown in the following figure. 8. In the Supply the credentials to perform this operation section, click Change. Note: If you are already logged in as MCSA\Administrator account, you don’t need to change the credentials on this page. If so, move directly to the Domain Controller Options page. 9. On the Windows Security dialog box, in the Username text box, type MCSALAB\Administrator, in the Password text box, type Password@123. 10. Click OK, and then click Next. 11. On the Domain Controller Options page, make sure that the Domain Name System (DNS) server and Global Catalog (GC) check boxes are selected. 12. Under the DSRM password section, type Password@123 in the Password and Confirm password text boxes and then click Next. 13. 14. 15. On the DNS Options page, click Next. On the Additional Options page, select the Install from media check box. In the Path text box, type C:\IFM, as shown in the following figure. 16. 17. 18. 19. Click Verify. Once the path has been verified, click Next. On the Paths page, click Next. On the Review Options page, click Next. On the Prerequisites Check page, click Install. The installation process will start and the server will restart, once the configuration is completed. Wait for the server to restart. Results: After completing this exercise, you will have installed an additional domain controller for the branch office by using IFM. Shut down and revert the DC1 and SERVER1 virtual machines to prepare for the next exercise. Exercise 6: Managing Organizational Units and Groups in AD DS Active Directory objects are used to access the various network resources for the various purposes. Once you configured a domain controller, you need to create and manage Active Directory objects, such as OUs, groups, and users. You can delegate the administrative permissions to the Active Directory objects. In this exercise, you will learn how to create Active Directory objects, how to delegate the permissions, and how to configure home folders. In addition, you will also learn how to reset and rejoin the computer accounts. Start the DC1 and CLIENT1 virtual machines to perform this exercise. Task 1: Managing Organizational Units and Groups 1. 2. 3. Sign in to DC1 with the MCSALAB\Administrator account. On the Server Manager console, click Tools, and then click Active Directory Users and Computers. On the Active Directory Users and Computers console, select and right-click mcsalab.local, and then select New, and then click Organizational Unit, as shown in the following figure. 4. On the New Object – Organizational Unit dialog box, in the Name text box, type Training, as shown in the following figure, and then click OK. 5. Select and right-click the Training OU in the left pane, and then select New, and then click Group. 6. On the New Object – Group dialog box, in the Group name text box, type Students, as shown in the following figure, and then click OK. 7. Select and right-click mcsalab.local, in the left pane, and then select New, and then click Organizational Unit. 8. On the New Object – Organizational Unit dialog box, in the Name text box, type Development, and then click OK. 9. Select and right-click the Development OU, and then select New, and then click Group. 10. On the New Object – Group dialog box, in the Group name text box, type Trainers, and then click OK. 11. Select and right-click the Development OU, and then select New, and then click Group. 12. On the New Object – Group dialog box, in the Group name text box, type Managers, and then click OK. 13. In the right pane, select and right-click the Trainers group, and then select Move, as shown in the following figure. 14. On the Move dialog box, select the Training OU, as shown in the following figure, and then click OK. 15. In the left pane, select the Training OU. 16. In the right pane, select and right-click Trainers, and then select Delete. 17. On the Active Directory Domain Services message box, click Yes. Make sure that the Trainers group is deleted. Task 2: Delegating the Permissions 1. Make sure that the Active Directory Users and Computers console is active on DC1. 2. In the left pane, select and right-click the Training OU, and then select Delegate Control, as shown in the following figure. 3. On the welcome page of the Delegation of Control Wizard, and click Next. 4. On the Users or Groups page, click Add. 5. On the Select Users, Computers, or Groups dialog box, in the Enter the object names to select (examples) text box, type Students, as shown in the following figure, and then click OK. 6. 7. 8. On the Users or Groups page, click Next. On the Tasks to Delegate page, make sure that the Delegate the following common tasks radio button is selected. Select the Create, delete, and manage user accounts check box, as shown in the following figure, and then click Next. 9. 10. On the Completing the Delegation of Control Wizard page, click Finish. Select and right-click the Training OU, and then select New, and then click User. 11. On the New Object - User dialog box, type Marsh, in the First name and User logon name text boxes, as shown in the following figure, and then click Next. 12. 13. In the Password and Confirm password text boxes, type Password@123. Clear the User must change password at next logon check box, select the Password never expires check box, as shown in the following figure. 14. 15. Click Next, and then click Finish. Minimize the Active Directory Users and Computers console. Task 3: Configuring Home Folders for User Accounts 1. On DC1, create a folder named Marsh Data, under the C:\Users\Public folder, as shown in the following figure. 2. 3. Select and right-click the Marsh Data folder, and then select Properties. On the Marsh Data Properties dialog box, select the Sharing tab, as shown in the following figure. 4. Click Advanced Sharing. 5. On the Advanced Sharing dialog box, select the Share this folder check box, as shown in the following figure. 6. Click Permissions. 7. On the Permissions for Marsh Data dialog box, in the Permissions for Everyone section, select the Full Control check box, as shown in the following figure. 8. Click Apply, and then click OK. 9. Click OK to close Advanced Sharing dialog box, and then click Close. 10. Close the Windows Explorer window. 11. Switch to the Active Directory Users and Computers console. 12. Select and right-click the Marsh user, and then select Properties. 13. On the Marsh Properties dialog box, select the Profile tab. 14. Under the Home folder section, select the Connect radio button. 15. In the To text box, type \DC1\Marsh Data\Marsh, as shown in the following figure, and then click Apply. Note: By default all the domain users are denied to sign in to the Domain Controller server. In the next steps, we are going to make Marsh as the member of Print Operators group to sign in to Domain Controller to test the exercise. You will learn more about the user rights and permissions in the upcoming exercises. 16. 17. Select the Member Of tab, and then click Add. On the Select Groups dialog box, in the Enter the object names to select (example) text box, type Print Operators, as shown in the following figure. 18. 19. 20. 21. Click Check Names, and then click OK. On the Member Of tab, and click again Add. On the Select Groups dialog box, in the Enter the object names to select (example) text box, type Students. Click Check Names, and then click OK. Note: You have added the Marsh user to Students group to test the delegated permissions. 22. 23. Click OK to close the Marsh Properties dialog box. Close the Active Directory Users and Computers console. Task 4: Testing and Verifying the Home Folders and Delegated Permissions 1. On DC1, open the Run dialog box, type logoff and then click OK to sign out from the MCSALAB\Administrator account, as shown in the following figure. 2. Switch to Other user and Sign in as Marsh with the password as Password@123, as shown in the following figure. 3. Press the Windows+E keys to open the Windows Explorer window. 4. Verify that drive Z is mapped to (\DC1\Marsh Data), as shown in the following figure. 5. Double-click Marsh (\DC1\Marsh Data) (Z:). Note: You should be able to access this drive without any errors. If you receive no errors, you have been successful. 6. 7. 8. 9. Close the Windows Explorer window. Open the Run dialog box, type dsa.msc, in the Open text box, and then press Enter. On the User Account Control dialog box, in the User name text box, type Marsh. In the Password text box, type Password@123, as shown in the following figure, and then click Yes. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. On the Active Directory Users and Computers console, expand mcsalab.local. Select and right-click Training, and then click New, and then click User. On the New Object – User dialog box, in the First name and User logon name text boxes, type Test User2, and then click Next.

In the Password and Confirm password text boxes, type Password@123. Click Next, and then click Finish. Make sure that the Test User1 account is created, under the Training OU. Select and right-click Development, and then click New, and then click User. On the New Object – User dialog box, in the First name and User logon name text boxes, type Test User2, and then click Next. In the Password and Confirm password text boxes, type Password@123, click Next, and then click Finish. Make sure that you get the following error message. 20. 21. 22. Click OK, and then click Cancel. Close the Active Directory Users and Computers console. Sign out from the Marsh user. Task 5: Resetting the Computer Accounts 1. 2. Sign in to DC1 with the MCSALAB\Marsh account. On the Server Manager console, click Tools, and then click Active Directory Users and Computers. 3. On the Active Directory Users and Computers console, expand mcsalab.local. 4. In the left pane, select Computers. 5. In the right pane, select and right-click CLIENT1, and then click Reset Account, as shown in the following figure. 6. On the Active Directory Domain Services message box, click Yes, and the click OK. Task 6: Examining the Behavior when a User Logins on Client. 1. 2. Try to Sign in to CLIENT1 with the MCSALAB\Marsh account. A message displays stating that The trust relationship between this workstation and the primary domain failed, as shown in the following figure. Task 7: Rejoining the Domain to Reconnect the Computer Account 1. 2. 3. Sign in to CLIENT as CLIENT1\Administrator with the password as Password@123. Open the System Properties dialog box, click Network ID. On the Select the option that describes your network page, as shown in the following figure, click Next. 4. 5. 6. 7. 8. On the Is your company network on a domain? page, click Next. On the You will need the following information page, click Next. On the Type your user name, password, and domain name for your domain account page, in the User name text box, type Administrator. In the Password text box, type Password@123. In the Domain name text box, type MCSALAB.LOCAL, as shown in the following figure, and then click Next. 9. 10. 11. 12. 13. 14. On the User Account and Domain Information dialog box, click Yes. On the Do you want to enable a domain user account on this computer? page, select the Do not add a domain user account radio button, and then click Next. Click Finish, and then click OK. On the Microsoft Windows dialog box, click Restart Now. Wait for system to restart. Sign in as MCSALAB\Marsh with the password as Password@123. Make sure that you are able to sign in. Results: After this exercise, you have successfully created and tested Organizational Units, Groups, Users, Home Folders, and the Delegation of Control Wizard. In addition, you should also have successfully reset a trust relationship Shut down and revert the DC1 and CLIENT1 virtual machines to prepare for the next exercise. Exercise 7: Using Windows PowerShell to Create User Accounts and Groups As discussed earlier, Window PowerShell is a command-line interface used to manage Windows servers and clients. You can also use Windows PowerShell to manage the Active Directory objects. In this exercise, you will learn how to manage Active Directory objects using Window PowerShell. In addition, you will also learn how to export and import the Active Directory objects using Window PowerShell. Start the DC1 and CLIENT1 virtual machines to perform this exercise. Task 1: Creating a User Account Using Windows PowerShell 1. 2. 3. 4. Sign in to DC1 with the MCSALAB\Administrator account. On the taskbar, click the Windows PowerShell icon. At the Windows PowerShell prompt, type cd\ and then press Enter. To create an Organizational Unit named BranchOffice, type the following command, and then press Enter: New-ADOrganizationalUnit BranchOffice 5. To create a user named Peter under the BranchOffice OU, type the following command, and then press Enter: New-ADUser -Name Peter -DisplayName “Peter Mark” -Path “ou=BranchOffice,dc=mcsalab,dc=local” 6. To set the password for Peter user, type the following command, and then press Enter: Set-ADAccountPassword Peter When prompted for the current password, press Enter. When prompted for the desired password, type Password@123, and then press Enter. When prompted to repeat the password, type Password@123, and then press Enter. 7. To enable the Peter user, type the following command, and then press Enter. Enable-ADAccount Peter 8. Switch to the CLIENT1 virtual machine. 9. 10. On CLIENT1, sign in as Peter with the password as Password@123. Verify that sign in is successful, and then sign out of CLIENT1. Task 2: Creating Groups Using Windows PowerShell 1. 2. Switch back to DC1. At the Windows PowerShell prompt, type the following command to create a new security (global) group named BranchUsers, and then press Enter. New-ADGroup BranchUsers -Path “ou=BranchOffice,dc=mcsalab,dc=local” 3. At the GroupScope prompt: type Global and then press Enter, as shown in the following figure. 4. To add the Peter user as member of the BranchUsers group, type the following command, and then press Enter. Add-ADGroupMember BranchUsers -Members Peter 5. To view the members of the BranchUsers group, type the following command, and then press Enter. Get-ADGroupMember BranchUsers Task 3: Exporting User Accounts Using the ldifde Tool 1. At the Windows PowerShell prompt, type the following command, and then press Enter, as shown in the following figure. ldifde -f MyUsers 2. 3. At the Windows PowerShell prompt, type notepad MyUsers and then press Enter. Review the MyUsers file and close the Notepad. Results: After completing this exercise, you have managed AD DS objects using Windows PowerShell. Shut down and revert the DC1 and CLIENT1 virtual machines to prepare for the next exercise. Exercise 8: Installing and Configuring the DHCP Server Role Dynamic Host Configuration Protocol (DHCP) is as service that is used to provide TCP/IP settings, such as IP address, subnet mask, default gateway, and DNS server to the clients, automatically. In a large enterprise network, it is difficult to manage IP addresses manually. Hence, DHCP can be a useful feature to manage the IP addresses in a large enterprise network. In this exercise, you will learn how to install the DHCP server role and how to configure the DHCP scope. In addition, you will also learn how to use the DHCP reservation feature to reserve a specific IP address for a specific client. Start the DC1 and CLIENT1 virtual machines to perform this exercise. Task 1: Installing the DHCP Server Role 1. Sign in to DC1 with MCSALAB\Administrator account. 2. Open the Server Manager console, if required. 3. On the Server Manager console, click the Add roles and features link. 4. On the Add Roles and Features Wizard, click Next. 5. On the Select installation type page, make sure that the Role-based or featurebased installation radio button is selected, and then click Next. 6. On the Select destination server page, click Next. 7. On the Select server roles page, select the DHCP Server check box. 8. On the Add Roles and Features Wizard dialog box, click Add Features. 9. The Select server roles page is returned, as shown in the following figure, click Next. 10. Complete the installation process. Task 2: Configuring the DHCP Scope 1. 2. 3. On the Server Manager console, click Tools, and then click DHCP. On the DHCP console, in the left pane, expand dc1.mcsalab.local. Select and right-click dc1.mcsalab.local, and then select Authorize. 4. Select and right-click dc1.mcsalab.local, and then click Refresh. Notice that the icons next to IPv4 IPv6 changes color from red to green, as shown in the following figure. 5. 6. 7. On the DHCP console, select and right-click IPv4, and then select New Scope. On the welcome page of the New Scope Wizard, click Next. On the Scope Name page, in the Name text box, type DHCPScope1, as shown in the following figure, and then click Next. 8. On the IP Address Range page, provide the following information, as shown in the following figure, and then click Next. Start IP address: 10.0.0.225 End IP address: 10.0.0.250 Length: 8 Subnet mask: 255.0.0.0 9. On the Add Exclusions and Delay page, exclude the following IP address range, as shown in the following figure. Start IP address: 10.0.0.225 End IP address: 10.0.0.230 10. Click Add, and then click Next. 11. On the Lease Duration page, review the default lease duration limit, and then click Next. 12. On the Configure DHCP Options page, make sure that the Yes, I want to configure these option now radio button is selected, as shown in the following figure, and then click Next. 13. On the Router (Default Gateway) page, in the IP address text box, type 10.0.0.1, as shown in the following figure. 14. 15. Click Add, and then click Next. On the Domain Name and DNS Servers page, make sure that 10.0.0.100 is written under the IP address column, as shown in the following figure, and then click Next. 16. 17. On the WINS Servers page, click Next. On the Activate Scope page, make sure that the Yes, I want to activate this scope now radio button is selected, as shown in the following figure, and then click Next. 18. 19. 20. On the Completing the New Scope Wizard page, click Finish. Select and right-click IPv4, and then select Refresh. Make sure that the IPv4 node is marked with the green color, as shown in the following figure. Task 3: Configuring DHCP Client 1. 2. 3. Open the Network Connections window, select and right-click the active network adapter and then select Properties. On the Properties dialog box, scroll down, select Internet Protocol Version 4 (TCP/IPv4), and then click Properties. On the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, select the Obtain an IP address automatically radio button, select the Obtain DNS server address automatically radio button, as shown in the following figure. 4. 5. 6. Click OK, and then click Close. Open the Run dialog box, type cmd, and then press Enter. On the Command Prompt window, type ipconfig /renew, as shown in the following figure, and then press Enter. 7. Type the ipconfig /all command and verify that CLIENT1 has received TCP/IP settings, such as IP address, subnet mask, default gateway, and DNS server's IP address, as shown in the following figure. Task 4: Configuring DHCP Reservation 1. On CLIENT1, on the Command Prompt window, type ipconfig /all, and then press Enter. 2. Find and write down the Physical Address of the CLIENT1 network adapter, in this case it is 00-15-5D-77-D6-0B, as shown in the following figure. Note: The physical address is a unique 48 bit address, which is assigned by IEEE and network adapter's vendor. 3. Switch and sign in (if required) to DC1 with the MCSALAB\Administrator account. 4. Make sure that the DHCP console is active. If not, open the DHCP console. 5. On the DHCP console, expand dc1.mcsalab.local, and then click IPv4. 6. Select and right-click Reservations, and then select New Reservation, as shown in the following figure. 7. 8. 9. On the New Reservation dialog box, in the Reservation Name text box, type CLIENT1. In the IP address text box, type 10.0.0.240. In the MAC address text box, type the physical address of the CLIENT1 machine (00-15-5D-77-D6-0B), as shown in the following figure. Note: Replace the physical address text with the actual physical address of your CLIENT1 machine. 10. 11. 12. Click Add, and then click Close. Switch back and sign in to CLIENT1. On the Command Prompt window, type ipconfig /release, and then press Enter to release the existing IP address. 13. On the Command Prompt window, type ipconfig /renew, and then press Enter to obtain a new IP address. 14. On the Command Prompt window, verify that IP address of CLIENT1 is now 10.0.0.240, as shown in the following figure. 15. Close the Command Prompt window. Results: After completing this exercise, you should have configured DHCP scope, DHCP options, and DHCP reservation. Shut down and revert the DC1 and CLIENT1 virtual machines to prepare for the next exercise. Exercise 9: Installing and Configuring DNS Domain Name System (DNS) is a service that is used to perform the name resolution. Name resolution is a process to map domain names in to IP addresses and vice versa. The systems communicate to each other using the IP addresses, however it is difficult to remember the IP addresses of each client in a large enterprise network. DNS service allows you to communicate with the systems using the domain names, which is easier to remember than IP addresses. In this exercise, you will learn how to install and configure the DNS server role. In addition, you will also learn how configure DNS forwarder and how to manage DNS cache. Start the DC1, SERVER1, and CLIENT1 virtual machines to perform this exercise. Task 1: Configuring SERVER1 as a Domain Controller without Installing the DNS Server Role 1. 2. 3. Sign in to SERVER1 with the Administrator account. On the Server Manager console, click the Add roles and features link. On the Before you begin page of the Add Roles and Features Wizard, click Next. 4. On the Select installation type page, click Next. 5. On the Select destination server page, make sure that SERVER1.mcsalab.local is selected, and then click Next. 6. On the Select server roles page, select the Active Directory Domain Services check box. 7. On the Add Roles and Features Wizard dialog box, click Add Features, and then click Next. 8. On the Select features page, click Next. 9. On the Active Directory Domain Services page, click Next. 10. On the Confirm installation selections page, click Install. 11. The installation process will start. Click Close, once the installation succeeded. 12. On the Server Manager console, click the Notifications icon, and then click the Promote this server to a domain controller link, as shown in the following figure. 13. On the Deployment Configuration page of the Active Directory Domain Services Configuration Wizard, make sure that the Add a domain controller to an existing domain radio button is selected. 14. Under the Supply the credentials to perform this operation section, click Change. 15. On the Windows Security dialog box, in the User name text box, type MCSALAB\Administrator. In the Password text box, type Password@123. 16. The Deployment Configuration page is returned, as shown in the following figure. Review the selected options, and then click Next. 17. On the Domain Controller Options page, clear the Domain Name System (DNS) server check box. 18. Under the DSRM password section, type Password@123 in the Password and

Confirm password text boxes, as shown in the following figure, and then click Next. 19. Click Next, until the Prerequisites Check page is displayed. 20. On the Prerequisites Check page, click Install. 21. The installation process will start and the server will restart automatically. After SERVER1 restarts, sign in to SERVER1 with the MCSALAB\Administrator account. Task 2: Creating and Configuring the Myzone.local Zone on DC1 1. 2. 3. Sign in to DC1 with the MCSALAB\Administrator account. On the Server Manager console, click Tools, and then click DNS. On the DNS Manager console, expand DC1, select and right-click Forward Lookup Zones, and then select New Zone, as shown in the following figure. 4. 5. On the welcome page of the New Zone Wizard, click Next. On the Zone Type page, make sure that the Primary zone radio button is 6. selected. Clear the Store the zone in Active Directory check box, as shown in the following figure, and then click Next. 7. On the Zone Name page, in the Zone name text box, type Myzone.local, as shown in the following figure, and then click Next. 8. 9. On the Zone File page, click Next. On the Dynamic Update page, make sure that the Do not allow dynamic updates radio button is selected, as shown in the following figure, and then click Next. 10. On the Completing the New Zone Wizard page, as shown in the following figure, review the zone configuration options, and then click Finish. 11. On the DNS Manager console, expand Forward Lookup Zones. 12. Select and right-click the Myzone.local zone, and then select New Host (A or AAAA), as shown in the following figure. 13. On the New Host dialog box, in the Name text box, type www. In the IP address text box, type 10.0.0.101, as shown in the following figure, and then click Add Host. 14. 15. 16. On the DNS message box, click OK. On the New Host dialog box, click Done. Leave the DNS Manager console active. Task 3: Adding the DNS Server Role on the SERVER1 1. 2. 3. Switch and Sign in to SERVER1 with the MCSALAB\Administrator account. On the Server Manager console, click the Add roles and features link. On the Before you begin page of the Add Roles and Features Wizard, click Next. 4. On the Select installation type page, click Next. 5. On the Select destination server page, make sure that SERVER1.mcsalab.local is selected, and then click Next. 6. On the Select server roles page, select the DNS Server check box. 7. On the Add Roles and Features Wizard dialog box, click Add Features. 8. The Select Server roles page is returned, as shown in the following, click Next. 9. On the Select Features page, click Next. 10. On the DNS Server page, click Next. 11. On the Confirm installation selections page, click Install. 12. The installation process will start. Click Close, once the installation succeeded. Task 4: Verifying Replication of the mcsalab.local Zone 1. 2. 3. 4. On SERVER1, on the Server Manager console, click Tools, and then click DNS. On the DNS Manager console, expand SERVER1, and then expand Forward Lookup Zones. Right-click Forward Lookup Zone and then select Refresh. Make sure that the _msdcs.mcsalab.local and mcsalab.local zones are displayed. Note: If the zone list is empty, proceed to the next step, otherwise close the DNS Manager console. 5. 6. 7. On SERVER1, switch back to the Server Manager console, click Tools, and then click Active Directory Sites and Services. On the Active Directory Sites and Services console, expand Sites, and then click Default-First-Site-Name, and then click Servers, and then click DC1. Select NTDS Settings, in the right pane, select and right-click the SERVER1 replication connection, and select Replicate Now, as shown in the following figure. Note: If you receive an error message, proceed to the next step, and then retry this step after 5 minutes. 8. 9. In the left pane, expand SERVER1, and then select NTDS Settings. In the right pane, select and right-click the DC1 replication connection, select 10. 11. 12. Replicate Now, and then click OK. Switch back to the DNS Manager console, select and right-click Forward Lookup Zones, and then click Refresh. Make sure that the _msdcs.mcsalab.local and mcsalab.local zones are displayed. Close the DNS Manager console. Task 5: Configuring DNS Forwarder 1. 2. 3. Switch and sign in to DC1. Open the DNS Manager console. On the DNS Manager console, select and right-click DC1, and then select Properties, as shown in the following figure. 4. On the DC1 Properties dialog box, select the Forwarders tab, as shown in the following figure. 5. On the Forwarders tab, click Edit. 6. On the Edit Forwarders dialog box, type 10.0.0.101, as shown in the following figure, and then click OK. 7. 8. On the DC1 dialog box, click OK. On the DNS Manager console, select and right-click DC1, and then click All Tasks, and then click Restart. 9. Switch and sign in to CLIENT1. 10. Open the Command Prompt window. 11. On the Command Prompt window, type ping www.myzone.local, and the 12. press Enter. Make sure that you are able to resolve the www.myzone.local FQDN successfully, as shown in the following figure. 13. On the Command Prompt window, type nslookup, and then press Enter. 14. At the nslookup prompt, type www.myzone.local, and then press Enter. 15. Make sure that you receive an IP address for this host, as shown in the following figure. 16. Leave the Command Prompt window active. Task 6: Managing the DNS Cache 1. On CLIENT1, on the Command Prompt window, type the following command and then press Enter, as shown in the following figure. ipconfig /displaydns 2. Examine the output and close the Command Prompt window. 3. Press the Windows key, and then type cmd. 4. Select and right-click Command Prompt, and then select Run as administrator as shown in the following figure. 5. 6. On the User Account Control dialog box, click Yes. On the Command Prompt window, type the following command to clear the DNS cache, and then press Enter. ipconfig /flushdns 7. On the Command Prompt window, type the following command and verify that the DNS cache has been cleared, and then press Enter. ipconfig /displaydns 8. Close the Command Prompt window. Results: After completing this exercise, you should have deployed DNS server, DNS zone, DNS forwarder, and DNS cache. Shut down and revert the DC1, SERVER1, and CLIENT1 virtual machines to prepare for the next exercise. 10: Implementing LAN Routing LAN routing is a Window feature that enables you to communicate between different subnets. To communicate between different subnets, typically a device called router is used, but you can also use a Windows server, such as Windows Server 2016 server to perform the LAN routing. However, Windows Server 2016 does not support all the features supported by a router. It is typically helpful for a small network with the limited number of subnets. In this exercise, you will learn how to use a Windows Server 2016 server as a software router to enable LAN routing between two or more subnets. Start the DC1, ROUTER, and SERVER2 virtual machines to perform this exercise. Task 1: Installing the LAN Routing Feature on ROUTER 1. 2. 3. Sign in to ROUTER with the Administrator account. On the Server Manager console, click the Add roles and features link. On the Before you began page of the Add Roles and Features Wizard, click Next. 4. On the Select installation type page, click Next. 5. On the Select destination server page, click Next. 6. On the Select Server roles page, select the Remote Access check box, as shown in the following figure, and then click Next. 7. 8. 9. On the Select features page, click Next. On the Remote Access page, click Next. On the Select roles services page, select the Routing check box. 10. On the Add Roles and Features Wizard dialog box, click Add Features. 11. The Select role services page is returned, as shown in the following figure, click Next. Note: The DirectAccess and VPN (RAS) check box will be selected automatically. 12. 13. 14. 15. On the Web Server Role (IIS) page, click Next. On the Select role services page, click Next. On the Confirm installation selection page, click Install. Click Close, once the installation succeeded. Task 2: Configuring the LAN Routing Service on ROUTER 1. On the Server Manager console, click Tools, and then click Remote and Routing Access. 2. On the Routing and Remote Access console, select and right-click ROUTER (local), and then select Configure and Enable Routing and Remote Access, as shown in the following figure. 3. 4. On the welcome page of the Routing and Remote Access Server Setup Wizard, click Next. On the Configuration page, select the Custom configuration radio button, as shown in the following figure, and then click Next. 5. On the Custom Configuration page, select the LAN routing check box, as shown in the following figure. 6. 7. 8. Click Next, and then click Finish. On the service message box, click Start Service. Make sure that the ROUTER (local) node's color changes red to green, as shown in the following figure. 9. Close the Routing and Remote Access console. 10. On the ROUTER virtual machine, open the Run dialog box, type firewall.cpl in the Open text box, and then press Enter. 11. On the Windows Firewall window, in the left pane, click the Turn Windows Firewall on or off link. 12. On the Customize Settings window, select the Turn off Windows Firewall (not recommended) radio button for each profile, as shown in the following figure. 13. Close the Customize Settings window. Task 3: Testing the Connectivity between DC1 and SERVER2 Servers 1. Switch and sign in to SERVER2 with the Administrator account. 2. Open the Run dialog box, type firewall.cpl, in the Open text box, and then press Enter. 3. On the Windows Firewall window, in the left pane, click the Turn Windows Firewall on or off link. 4. On the Customize Settings window, select the Turn off Windows Firewall (not recommended) radio button for each firewall profiles 5. Close the Customize Settings window. 6. Switch and sign in to DC1 with MCSALAB\Administrator account. 7. Open the Command Prompt window, on the Command Prompt window, type the following commands and then press Enter after each one. Ping 10.0.0.1 Ping 192.168.0.1 Ping 192.168.0.2 8. You should be able to communicate to all systems successfully, as shown in the following figure. 9. Close the Command Prompt window. Results: After completing this exercise, you will have configured LAN routing between DC1 and SERVER2 servers. Do not shut down or revert any virtual machine, as these will be used in the next exercise. Exercise 11: Configuring IPv6 Addressing IPv6 addressing scheme provides more unique addresses and is more secure than traditional IPv4 addressing scheme. An IPv6 address comprises of eight blocks and each block can contain 16 (bit) hexadecimal digits. You can enable communication between IPv4 and IPv6 nodes using the various techniques, such as Teredo, ISATAP, and 6to4 tunneling. In this exercise, you will learn how to configure IPv6 addresses on Window-based systems. Make sure that the DC1, ROUTER, and SERVER2 virtual machines are running before start this exercise. Task 1: Disabling IPv6 Address on DC1 1. 2. 3. 4. Switch and Sign in to SERVER2 with the Administrator account. On the taskbar, click the Windows PowerShell icon. At the Windows PowerShell prompt, type ping 10.0.0.100, and then press Enter. Verify that you are able communicate with the DC1 (10.0.0.100) server, as shown in the following figure. 5. Switch and Sign in to DC1 with the MCSALAB\Administrator account. 6. On the Server Manager console, in the left pane, click Local Server. 7. In the Properties pane, click the 10.0.0.100, IPv6 enabled link, as shown in the following figure. 8. On the Network Connections window, select and right-click your network adapter, and then select Properties, as shown in the following figure. 9. On the network adapter's properties dialog box, clear the Internet Protocol Version 6 (TCP/IPv6) check box, as shown in the following figure, and then click OK. 10. 11. Close the Network Connections window. On the Server Manager console, verify that your network adapter lists only 10.0.0.100, as shown in the following figure. You may need to refresh the Server Manager console. Notice that DC1 is now an IPv4-only host. Task 2: Disabling IPv4 Address on SERVER2 1. 2. 3. 4. Switch and Sign in to SERVER2 with the Administrator account. On the Server Manager console, in the left pane, click Local Server. In the Properties pane, click the 192.168.0.2, IPv6 enabled link. On the Network Connections window, select and right-click active network 5. adapter, and then select Properties. On the network adapter's properties dialog box, clear the Internet Protocol Version 4 (TCP/IPv4) check box, as shown in the following figure, and then click OK. 6. Close the Network Connections window. 7. On the Server Manager console, verify that network adapter now lists only IPv6 enabled, as shown in the following figure. You may need to refresh the Server Manager console. Notice that SERVER2 is now an IPv6-only host. Task 3: Configuring an IPv6 Network on ROUTER 1. 2. 3. Switch and Sign in to ROUTER with the Administrator account. On the taskbar, click the Windows PowerShell icon. To configure a network address that will be used on the IPv6 network, at the Windows PowerShell prompt, type the following cmdlet, and then press Enter, as shown in the following figure. New-NetRoute -InterfaceAlias "Ethernet1" -DestinationPrefix 2001:AABB:0:1::/64 -Publish Yes Note: Ethernet1 is the name of the network adapter connected to the external subnet. 4. To allow clients to obtain the IPv6 network address automatically from ROUTER, at the Windows PowerShell prompt, type the following cmdlet, and then press Enter, as shown in the following figure. Set-NetIPInterface -InterfaceAlias "Ethernet1" -AddressFamily IPv6 Advertising Enabled 5. At the Windows PowerShell prompt, type ipconfig.exe, and then press Enter. Notice that Ethernet1 now has an IPv6 address on the 2001:AABB:0:1::/64 network, as shown in the following figure. This address will be used for communication on the IPv6-only network. Task 4: Verifying IPv6 Address on SERVER2 1. 2. 3. Switch and Sign in to SERVER2 with the Administrator account. On the taskbar, click the Windows PowerShell icon. At the Windows PowerShell prompt, type ipconfig.exe, and then press Enter. Notice that your network adapter now has an IPv6 address on the on the 2001:AABB:0:1::/64 network, as shown in the following figure. 4. The network address was obtained from the router through the stateless configuration. Results: After completing the exercise, you will have configured an IPv6-based network. Shut down and revert the DC1, SERVER2 and ROUTER virtual machines to prepare for the next exercise. Exercise 12: Installing and Configuring Disk Storage Disks are used to store the system data as well as personnel data. There are various storage technologies, such as SATA, IDE, iSCSI, and Fibre Channel that can be used to store the data. In a virtualized environment, you can add additional virtual hard disks to the virtual machines, and then you can create additional volumes on these disks. In this exercise, you will learn how to manage disks on a Window server. Further, you will learn how to shrink and extend volumes. Task 1: Adding New Virtual Disks to DC1 1. 2. 3. Make sure that the DC1 virtual machine is powered off. On your host machine, on the VMware console, select and right-click the DC1 virtual machine, and then select Settings. On the virtual machine's setting dialog box, ensure that Hard Disk is selected, and then click Next. 4. 5. On the Select a Disk Type page, accept the default selection (SCSI), and then click Next. On the Select a Disk page, make sure that the Create a new virtual disk radio button is selected, and then click Next. . 6. On the Specify Disk Capacity page, set the disk size as 10 GB, select the Store virtual disk as a single file radio button, and then click Next. 7. On the Specify Disk File page, accept the default file name, and then click Finish. 8. Add one more new virtual disk with following settings: Store virtual disk as a single file. Size: 10 GB. File name : Accept default. Task 2: Initializing the Added Disks 1. 2. 3. 4. Power on the DC1 virtual machine. Open the Server Manager console. On the Server Manager console, click Tools, and then click Computer Management. On the Computer Management console, under the Storage node, select Disk Management. 5. In the Disks pane, select and right-click Disk 1, and then select Online, as shown in the following figure. 6. 7. Select and right-click Disk 1, and then select Initialize Disk. On the Initialize Disk dialog box, make sure that the Disk 1 check box is selected, select the GPT (GUID Partition Table) radio button, and then click OK. Note: The GPT partition table supports more features than the traditional MBR partition table. 8. 9. In the Disks pane, select and right-click Disk 2, and then select Online. Select and right-click Disk 2, and then select Initialize Disk. 10. On the Initialize Disk dialog box, make sure that the Disk 2 check box is selected, select the GPT (GUID Partition Table) radio button, and then click OK. Task 3: Creating and Formatting Simple Volumes 1. On the Computer Management console, under the Disk Management node, select and right-click the Unallocated space of Disk 1, and then select New Simple Volume, as shown in the following figure. 2. 3. On the Welcome to the New Simple Volume Wizard page, click Next. On the Specify Volume Size page, in the Simple volume size MB value box, type 5000, as shown in the following figure, and then click Next. 4. On the Assign Drive Letter or Path page, make sure that the Assign the following drive letter check box is selected, accept the default drive letter, as shown in the following figure, and then click Next. 5. On the Format Partition page, in the Volume label text box, type Volume1, as shown in the following figure, and then click Next. 6. On the Completing the New Simple Volume Wizard page, click Finish. 7. On the Disk Management console, select and right-click the Unallocated space of Disk 2, and then select New Simple Volume. 8. On the Welcome to the New Simple Volume Wizard page, click Next. 9. On the Specify Volume Size page, in the Simple volume size in MB value box, type 5000, and then click Next. 10. On the Assign Drive Letter or Path page, make sure that the Assign the following drive letter check box is selected, accept the default drive letter, and 11. 12. 13. 14. 15. then click Next. On the Format Partition page, in the Volume label text box, type Volume2, and then click Next. On the Completing the New Simple Volume Wizard page, click Finish. Leave the Computer Management console active. Press the Windows+E keys to open the Windows Explorer window. Verify that the Volume1 and Volume2 are created, as shown in the following figure. 16. Close the Windows Explorer window. Task 4: Shrinking the Volumes 1. 2. On DC1, switch to the Computer Management console. On the Computer Management console, under the Disk Management node, select and right-click Volume1, and then select Shrink Volume, as shown in the following figure. 3. On the shrink dialog box, in the Enter the amount of space to shrink in MB value box, type 1000, as shown in the following figure, and then click Shrink. Task 5: Extending the Volumes 1. 2. 3. On the Computer Management console, under the Disk Management node, select and right-click Volume2, and then select Extend Volume. On the Welcome to the Extended Volume Wizard page, click Next. On the Select Disks page, in the Select the amount of space in MB value box, type 3000, as shown in the following figure, and then click Next. 4. On the Completing the Extended Volume Wizard page, click Finish. 5. Press the Windows+E keys to open the Windows Explorer window, verify that the volumes' sizes are reflected. Results: After completing this exercise, you should have initialized new disks, and created and formatted simple volumes. In addition, you should also have shrink and extended the volumes. Do not shut down or revert the DC1 virtual machine, as it will be used in the next exercise. Exercise 13: Configuring a Redundant Storage Space Redundant Array of Inexpensive Disk (RAID) is a storage technology that allows you to combine multiple hard disks in a single large hard disk. It also provides redundancy and fault tolerance in the event of a disk failure. RAID can be configured either as a hardware RAID (which requires a hardware controller device) or as a software RAID (which does not require any specific hardware device). RAID can be divided in to various RAID levels and each RAID level supports various features and limitations. In this exercise, you will learn how to create storage pools, how to create and test a mirrored volume. Ensure that the DC1 virtual machine is running and you have not reverted it in the previous state. Task 1: Creating a Storage Pool 1. 2. Sign in to DC1 and open the Server Manager console. Open the Disk Management console, select and right-click Disk 1, and then delete the created volume. Also delete the volume for Disk 2, as shown in the following figure. 3. On the Server Manager console, in the left pane, select File and Storage Services, and then select Storage Pools. 4. In the STORAGE POOLS pane, click TASKS, and then click Rescan Storage. 5. Click again TASKS, and then click New Storage Pool, as shown in the following figure. 6. 7. On the Before you begin page, click Next. On the Specify a storage pool name and subsystem page, in the Name text box, type MyStoragePool1, as shown in the following figure, and then click Next. 8. On the Select physical disks for the storage pool page, select the all available disk check boxes, as shown in the following figure, and then click Next. 9. 10. On the Confirm selections page, click Create. On the View results page, click Close, once the task is competed. Task 2: Creating a Mirrored Virtual Disk 1. 2. On DC1, on the Server Manager console, in the Storage Spaces pane, select MyStoragePool1.

On the VIRTUAL DISKS pane, click TASKS, and then click New Virtual Disk, as shown in the following figure. 3. 4. 5. On the Before you begin page, click Next. On the Select the storage pool page, make sure that MyStoragePool1 is selected, and then click Next. On the Specify the virtual disk name page, in the Name text box, type Mirrored Disk1, as shown in the following figure, and then click Next. 6. On the Select the storage layout page, in the Layout section, select Mirror, as shown in the following figure, and then click Next. 7. On the Specify the provisioning type page, select the Thin radio button, as shown in the following figure, and then click Next. 8. On the Specify the size of the virtual disk page, in the Virtual disk size box, type 5, as shown in the following figure, and then click Next. 9. 10. 11. On the Confirm selections page, click Create. On the View results page, wait until the task completes. Make sure that the Create a volume when this wizard closes check box is selected, and then click Close. 12. On the Before you begin page of the New Volume Wizard, click Next. 13. On the Select the server and disk page, in the Disk section, select the Mirrored Disk1 virtual disk, as shown in the following figure, and then click Next. 14. On the Specify the size of the volume page, click Next. 15. On the Assign to a drive letter or folder page, notice the Drive letter, as shown in the following figure, and then click Next. 16. 17. On the Select file system settings page, in the File system drop-down menu, ensure that ReFS is selected. In the Volume label text box, type Mirrored Volume1, as shown in the following figure, and then click Next. Note: ReFS is a new file system that supports more features than NTFS file system. 18. 19. On the Confirm selections page, click Create. On the Completion page, click Close, once the task completes. Task 3: Creating a File in to Mirrored Volume1 1. 2. Open the Windows Explorer window, double-click Mirrored Volume1. Create the MyTextFile1 file under Mirrored Volume1, as shown in the following figure. 3. Close the Windows Explorer window. Task 4: Removing a Physical Drive 1. On your host machine, on the VMware console, select and right-click DC1, and then select Settings. 2. On the Virtual Machine Settings dialog box, select Hard Disk 2 hard drive, as shown in the following figure. 3. In the right pane, click Remove, and then click OK. Task 5: Verifying the File Availability 1. On DC1, switch to the Computer Management console or open it if required. 2. Make sure that the Disk Management node is selected, verify that the Disk 2 is disappeared from the disk list, as shown in the following figure. 3. 4. 5. 6. Open the Windows Explorer window. On the Windows Explorer window, double-click Mirrored Volume1. Verify that the MyTextFile1 file is still available. Close the Windows Explorer window. Results: After completing this exercise, you should have created a storage pool and added some disks to it. Then you should have created a mirrored virtual disk from the storage pool. In addition, after removing a physical drive, you should have verified that the virtual disk was still available and accessible. Shut down and revert the DC1 virtual machine to prepare for the net exercise. Exercise 14: Implementing File Sharing File sharing allows you to share and access the files on a network. You can also set the desired permissions (NTFS and shared permissions) on a file share for the various users. In addition, you can enable the access-based enumeration feature on a file share, which allows users to access only those shared files for which they have the access permission. Start the DC1, SERVER1, and CLIENT1 virtual machines to perform this exercise. Task 1: Creating the Folder Structure for the New Share Before start to this exercise, you need to create Peter and Shawn user accounts on the DC1 virtual machine. To do this, you need to perform the following steps: 1. Sign in to DC1 with the MCSALAB\Administrator account. 2. Open the Active Directory Users and Computers console, and then expand the mcsalab.local node. 3. Select and right-click Users in the left pane, select New, and then click User. 4. Follow the simple steps to create the Peter and Shawn user accounts. 5. The following figure displays the Active Directory Users and Computers console. Peter and Shawn user accounts are listed under the Users node. Note: If you face problems to create user accounts, you may refer the exercise 6 and 7. 6. Switch and Sign in to SERVER1 with the MCSALAB\Administrator account. 7. Open the Windows Explorer window, in the navigation pane, double-click Local Disk (C:). 8. Create a folder named MyData. 9. Double-click the MyData folder. 10. Create the Marketing and Sales folders under it, as shown in the following figure. Task 2: Configuring NTFS Permissions on the Folder Structure 1. 2. 3. On SERVER1, on the Windows Explorer window, navigate to drive Local Drive (C:). Select and right-click the MyData folder, and then select Properties. On the MyData Properties dialog box, select Security, and then click Advanced, as shown in the following figure. 4. 5. On the Advanced Security Settings for MyData dialog box, click Disable Inheritance. On the Block Inheritance dialog box, as shown in the following figure, select the Convert inherited permissions into explicit permissions on this object option, and then click OK. 6. 7. 8. 9. Click OK twice to close the MyData Properties dialog box. On the Windows Explorer window, double-click the MyData folder. Select and right-click the Marketing folder, and then select Properties. On the Marketing Properties dialog box, click Security, and then click Advanced. 10. On the Advanced Security Settings for Marketing dialog box, click Disable Inheritance. 11. On the Block Inheritance dialog box, select the Convert inherited permissions into explicit permissions on this object option. 12. Remove the Read & Execute and Special permissions for Users (SERVER1\Users), as shown in the following figure, and then click OK. 13. On the Security tab, click Edit. 14. On the Permissions for Marketing dialog box, click Add. 15. On the Select Users, Computers, Service Accounts, and Groups dialog box, type Peter, click Check Names, as shown in the following figure, and then click OK. Note: You may asked to provide Domain administrator credentials. 16. On the Permissions for Marketing dialog box, select the Modify check box under the Allow section, as shown in the following figure. 17. 18. Click OK to close the Permissions for Marketing dialog box. Click OK to close the Marketing Properties dialog box. Task 3: Sharing the Folder 1. On SERVER1, select and right-click the MyData folder, and then select Properties. 2. On the MyData Properties dialog box, select the Sharing tab, and then click Advanced Sharing. 3. On the Advanced Sharing dialog box, select the Share this folder check box, as shown in the following figure, and then click Permissions. 4. On the Permissions for MyData dialog box, as shown in the following figure, and then click Add. 5. On the Select Users, Computers, Service Accounts, or Groups dialog box, in the Enter the object names to select (examples): text area, type Authenticated Users. 6. Click Check Names, and then click OK. 7. On the Permissions for MyData dialog box, make sure that the Authenticated Users is selected in the Share

Permissions section, and then select the Change check box under the Allow section, as shown in the following figure. 8. 9. 10. Click OK to close the Permissions for MyData dialog box. Click OK to close the Advanced Sharing window. Click Close to close the MyData Properties dialog box. Task 4: Accessing the Shared Folder 1. 2. 3. Switch and Sign in to CLIENT1 with the MCSALAB\Peter account. Open the Run dialog box, type \SERVER1\MyData, and then press Enter. Double-click the Marketing folder. Note: Peter should be able to access to the Marketing folder. 4. Sign out of CLIENT1. Task 5: Enabling Access-based Enumeration 1. Switch back and Sign in to SERVER1 with the MCSALAB\Administrator account. 2. Open the Server Manager console, on the Server Manager console, in the left pane, select File and Storage Services. 3. On the File and Storage Services page, click Shares. 4. In the Shares pane, select and right-click MyData, and then click Properties, as shown in the following figure. 5. On the MyData Properties dialog box, in the left pane, select Settings, and then select the Enable access-based enumeration check box, as shown in the following figure. 6. 7. Click OK to close the MyData Properties dialog box. Close the Server Manager console. Task 6: Testing the Access-based Enumeration Configuration 1. Switch back and sign in to CLIENT1 with the MCSALAB\Shawn account. 2. Click the Desktop tile. 3. Open the Run dialog box, in the Open text box, type \SERVER1\MyData, and then press Enter. Note: Shawn should only be able to view the Sales folder, the folder for which he has been assigned permissions. 4. Sign out of CLINET1. Results: After completing this exercise, you should have created and tested a file share. In addition, you should also have tested the access-based enumeration feature for the shared folder. Shut down and revert the DC1, SERVER1, and CLIENT1 virtual machines to prepare for the next exercise. Exercise 15: Implementing Shadow Copies Shadow copy is a feature that allows you to recover the files (including the shared files) which are accidently overwritten or deleted. First, you need to enable this feature (on a desired disk) then you can create multiple shadow copy versions on a disk. However, shadow copy cannot be considered as an alternate of the Window backup feature, because it only works until the system is working on which you have enabled it. If the system goes down or crashed accidently, shadow copy cannot be used to recover the system or system's data. In this exercise, you will learn how to use the shadow copy feature to recover the accidently deleted files. Start the DC1 and SERVER1 virtual machines to perform this exercise. Task 1: Configuring Shadow Copies 1. 2. 3. 4. 5. 6. 7. Sign in to SERVER1 with the MCSALAB\Administrator account. Open the Windows Explorer window. Select and right-click Local Disk (C:), and then click Configure Shadow Copies. On the Shadow Copies dialog box, make sure that C:\ volume is selected, and then click Enable. On the Enable Shadow Copies message box, click Yes. On the Shadow Copies dialog box, click Settings. On the Settings dialog box, as shown in the following figure, click Schedule. 8. On the C:\ schedule dialog box, review the various schedule options, and then click OK. 9. On the Settings dialog box, click OK. 10. Click OK to close the Settings dialog box. 11. On the Shadow Copies dialog box, click OK. Task 2: Recovering a Deleted File Using Shadow Copy 1. 2. 3. 4. 5. 6. On SERVER1, switch to the Windows Explorer window. Navigate to Local Disk (C:), and then click Users. Select and right-click Public, and then click Delete. Also delete the Public folder from Recycle Bin. On the Windows Explorer window, select and right-click the Users folder, and then click Properties. On the Users Properties dialog box, click the Previous Versions tab, as shown in the following figure. 7. 8. Select the folder version for the Users folder, and then click Open. Verify that the Public is listed in the folder, select and right-click Public, and then click Copy. 9. On the other Windows Explorer window, navigate to the Local Disk (C:)\Users folder, and then click Paste. 10. Close the Windows Explorer window. 11. Click OK and close all open windows. Results: After completing this exercise, you should have configured the Shadow Copies feature to recover the accidently deleted file. 12. Shut down and revert the DC1 and SERVER1 virtual machines to prepare for the next exercise. Exercise 16: Implementing Network Printing A printer is a hardware device which translate the soft copies in to hard copies. A single printer can be shared on a network and then it can be accessed by multiple clients to send the print jobs. Once you shared a printer on a network, you need to connect it on each clients in order to send the print jobs. However, in a large enterprise network, where multiple printers are used to handle a number of thousand print jobs, you may need to configure the printer pool for ease print management. In this exercise, you will learn how to install, share, and manage a network printer on a Windows-based network. Start the DC1, SERVER1, and CLIENT1 virtual machines to perform this exercise. Task 1: Installing the Print and Document Services Server Role 1. Sign in to SERVER1 as MCSALAB\Administrator. 2. On the Server Manager console, click Manage, and then click Add Roles and Features. 3. On the Before you begin page of the Add Roles and Features Wizard, click Next. 4. On the Select installation type page, make sure that the Role-based or featurebased installation radio button is selected, and then click Next. 5. On the Select destination server page, click Next. 6. On the Select Server Roles page, as shown in the following figure, select the Print and Document Services check box. If the Add Roles and Features Wizard dialog box displays, click Add Features, and then click Next. 7. 8. On the rest of the pages, click Next until the Confirm Installation Selections page displays. Click Install to install the required role services, and then click Close once the installation succeeded. Task 2: Installing a New Printer 1. 2. 3. On the Server Manager console, click Tools, and then click Print Management. On the Print Management console, expand Printer Servers, and then click SERVER1 (Local). Select and right-click Printers, and then click Add Printer, as shown in the following figure. 4. On the Network Printer Installation Wizard page, select the Add a new printer using an existing port radio button, as shown in the following figure, and then click Next. 5. On the Printer Driver page, make sure that the Install a new printer radio button is selected, and then click Next. 6. On the Printer Installation page, select Canon in the Manufacture list. 7. Select any of the printer model in the Printers list in the right pane, as shown in the following figure, and then click Next. 8. 9. On the Printer Name and Sharing Settings page, click Next. On the Printer Found page, click Next, and then click Finish. Task 3: Configuring Printer Pooling 1. On the Print Management console, select and right-click the recently added printer, and then click Properties. 2. On the printer properties dialog box, click the Sharing tab, select the List in the directory check box, as shown in the following figure, and then click Apply. 3. On the printer properties dialog box, click the Ports tab, select the Enable printer pooling check box, and then select the LPT2: check box to select it as an additional port, as shown in the following figure. 4. 5. Click OK to close the printer properties dialog box. Close the Print Management console. Task 4: Connecting a Printer on a Client 1. Switch and Sign in to CLIENT1 as MCSALAB\Administrator with the password as Password@123. 2. Open Control Panel, on the Control Panel window, click the Add a device link under Hardware and Sound. 3. On the Add a device window, select the discovered printer, as shown in the following figure, and then click Next. 4. On the Control Panel window, click the View devices and printers link, under Hardware and Sound. 5. Make sure that the recently added printer is listed. Results: After completing this exercise, you should have installed and configured a network printer. In addition, you should also have configured the printer pooling. Shut down and revert the DC1, SERVER1, and CLIENT1 virtual machines to prepare for the next exercise. Exercise 17: Implementing Group Policy Objects A Group Policy Object (GPO) is a collection of security policies and settings that are used to control the users' and computers' behavior on a network. You can use various security policies to restrict the Active Directory objects from accessing the unwanted resources, such as features, services, files, or tools. Once you promote a server as a domain controller, the Default Domain Policy and Default Domain Controller Policy GPOs are created by default on the domain controller. These GPOs contain various preconfigured policies that are applied on the domain controllers and computers. However, you can create a new GPO with the custom security policies and settings using the Group Policy Management console. In this exercise, you will learn how to create a GPO and how to configure a GPO to prevent Active Directory objects from accessing the resources on a Windows-based domain network. Start the DC1 and CLIENT1 virtual machines to perform this exercise. Task 1: Creating a New GPO 1. 2. 3. Sign in to DC1 with the MCSALAB\Administrator. Open the Server Manager console, if required. On the Server Manager console, click Tools, and then click Group Policy Management. 4. On the Group Policy Management console, expand Forest: mcsalab.local, and then click Domains. 5. Select and right-click mcsalab.local, and then select Create a GPO in this domain, as shown in the following figure. 6. On the New GPO dialog box, in the Name text box, type Internet Explorer GPO, and then click OK. Task 2: Configuring the Internet Explorer GPO 1. 2. 3. On DC1, on the Group Policy Management console, select and right-click Internet Explorer GPO, and then click Edit. On the Group Policy Management Editor console, navigate to User Configuration\Policies\Administrative Templates. Select and right-click All Settings, and then select Filter Options, as shown in the following figure. 4. 5. On the Filter Options dialog box, select the Enable Keyword Filters check box. In the Filter for word(s): text box, type General, as shown in the following figure, and then click OK. 6. In the Settings pane in the right hand, select and right-click Disable the General page, and then select Edit, as shown in the following figure. 7. 8. On the Disable the General page dialog box, select the Enabled radio button, and then click OK. Close the Group Policy Management Editor console. Task 3: Creating a Domain User to Test the GPO 1. 2. On DC1, open the Command Prompt window. Execute the following command, as shown in the following figure (type Password@123 when you are prompted for password). dsadd user cn=User1,"cn=users,dc=mcsalab,dc=local" –disabled no –pwd * 3. Close the Command Prompt window. Task 4: Testing the Internet Explorer GPO 1. 2. 3. Switch and Sign in to CLIENT1 as MCSALAB\User1 with the password as Password@123. Open the Run dialog box, type control in the Open text box, and then press Enter. On the Control Panel window, click Network and Internet. 4. On the Network and Internet window, as shown in the following figure, click Change your homepage. 5. When you click the Change your home page link, you will get a message, as shown in the following figure. 6. 7. Click OK to close the Internet Control Panel message box. On the Control Panel window, click Internet Options. Notice that, in the Internet Properties dialog box, the General tab is not available, as shown in the following figure. 8. Close all open windows and sign out. Task 5: Configuring Security Filtering to Exempt a User from the Internet Explorer GPO 1. 2. 3. 4. 5. 6. 7. Switch and sign to DC1. Open the Group Policy Management console, if required. On the Group Policy Management console, select and right-click Internet Explorer GPO. In the right pane, click the Delegation tab. On the Delegation tab, click the Advanced button. On the Internet Explorer GPO Security Settings dialog box, click Add. On the Select Users, Computers, Service Accounts, or Groups text box, type User1, as shown in the following figure, and then click OK. 8. 9. On the Internet Explorer GPO Security Settings dialog box, in the Security section, select User1. In the Permissions for User1 section, select the Deny check box, as shown in the following figure, and then click OK. 10. 11. On the Windows Security dialog box, click Yes. Close the Group Policy Management console. Task 6: Testing the Internet Explorer GPO 1. 2. 3. 4. 5. Switch and Sign in to CLIENT1 as MCSALAB\User1 with the password as Password@123. Open the Run dialog box, type control in the Open text box, and then press Enter. On the Control Panel window, click Network and Internet. On the Network and Internet dialog box, click Change your homepage. Notice that the General tab is available on the Internet Properties dialog box. Close all open windows, and sign out. Results: After completing this exercise, you should have configured and tested a GPO. Shut down and revert the DC1 and CLIENT1 virtual machines. Exercise 18: Implementing AppLocker and Firewall Using Group Policy AppLocker is a security feature that allows you to restrict specific applications for specific groups or users. In the exercise, you will learn how to control an application using the AppLocker feature. Further, you will also learn how to manage Windows Firewall using the Group Policy Management console. Start the DC1 virtual machine to perform this exercise. Task 1: Restricting an Application Using AppLocker 1. 2. 3. 4. 5. 6. 7. Sign in to DC1 as MCSALAB\Administrator with the password as Password@123. Open the Group Policy Management console. Navigate to Forest: mcsalab.local\Domains\mcsalab.local. Select and right-click Group Policy Objects, and then select New. On the New GPO dialog box, in the Name text box, type Software Policy, and then click OK. Right-click Software Policy, and then select Edit. On the Group Policy Management Editor console, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker, as shown in the following figure. 8. Expand AppLocker, right-click Executable Rules, and then select Create New Rule. 9. On the Before You Begin page, select Next. 10. On the Permissions page, under the Users or Groups box, select Deny, and then select Next. 11. On the Conditions page, select the Path radio button, as shown in the following figure, and then click Next. 12. On the Path page, click Browse Files, browse to C:\Windows\System32\calc.exe, click Open, as shown in the following figure, and then select Next. 13. 14. On the Exceptions page, select Next. On the Name and Description page, in the Name text box, type Block Calculator, and then click Create. 15. If the AppLocker dialog box appears and prompts to create default rules, click Yes. 16. On the Group Policy Management Editor console, as shown in the following figure, notice the default executables rules. 17. Select the AppLocker node in the left pane, and then click the Configure rule enforcement link, as shown in the following figure. 18. On the Enforcement tab of the AppLocker Properties dialog box, under 19. Executable rules, select the Configured check box. Make sure that the Enforce rules option is selected in the drop-down list, as shown in the following figure, and then click OK. 20. 21. 22. Close the Group Policy Management Editor console. On the Group Policy Management console, select and right-click Domain Controllers, and then select Link an Existing GPO. On the Select GPO dialog box, select Software Policy, and then click OK. 23. Under the Link Group Policy Objects tab, select Software Policy, and then click Link Order to move this policy to top. 24. Open the Run dialog box, type services.msc, and then press Enter. 25. On the Services console, select and right-click Application Identity, and then select Properties. 26. On the Application Identity Properties (Local Computer) dialog box, set the Startup type as Automatic, click Start, as shown in the following figure, and then click OK. Note: If you get an error, just close the Service Manager window. 27. Open the Command Prompt window, type gpupdate /force, and then press Enter. 28. Sign out from to DC1 and Sign in back to DC1 as MCSALAB\Administrator. 29. Open the Run dialog box, type calc.exe in the Open text box, and then press Enter. 30. You should get an error as shown in the following figure. Note: If you are still able to open the Calculator application, restart the DC1 server, and then try again. Task 2: Configuring Windows Firewall Rules Using Group Policy 1. 2. Sign in to DC1 and open the Group Policy Management console, if required. Navigate to Forest: mcsalab.local\Domains\mcsalab.local\Group Policy Objects. 3. Right-click the Group Policy Objects node, and then select New, as shown in the following figure. 4. In the Name text box type Firewall GPO, and then click OK. 5. Expand Group Policy Objects, right-click Firewall GPO, and then select Edit. 6. On the Group Policy Management Editor console, navigate to Computer Configuration\Policies\Windows Settings\Security Settings. 7. Under the Security Settings node, expand Windows Firewall with Advanced Security, and then expand the Windows Firewall with Advanced Security – LDAP node, as shown in the following figure. 8. Select and right-click Inbound Rules, and then select New Rule, as shown in the following figure. 9. On the New Inbound Rule Wizard, on the Rule Type page, the select Predefined radio button. 10. In the drop-down list, select Remote Desktop, as shown in the following figure, and then click Next. 11. On the Predefined Rules page, click Next. 12. On the Action page, select the Block the connection radio button, as shown in the following figure, and then click Finish to close New Inbound Rule Wizard. 13. Close the Group Policy Management Editor console. 14. Open the Command Prompt window and type gpupdate /force, and then press Enter. 15. Close the Command Prompt window. 16. On the Group Policy Management console, select Firewall GPO in the left pane. 17. If displayed, on the Internet Explorer dialog box click Close 18. In the right pane, select the Settings tab and verify that the Inbound Rules are configured, as shown in the following figure. 19. Close the Group Policy Management console. Results: After completing this exercise, you should have configured AppLocker and Windows Firewall rules using the Group Policy Management console. Shut down and revert the DC1 virtual machine. Hope, you have enjoyed a great learning experience with this learning guide and hope you will provide great rating to this lab guide.