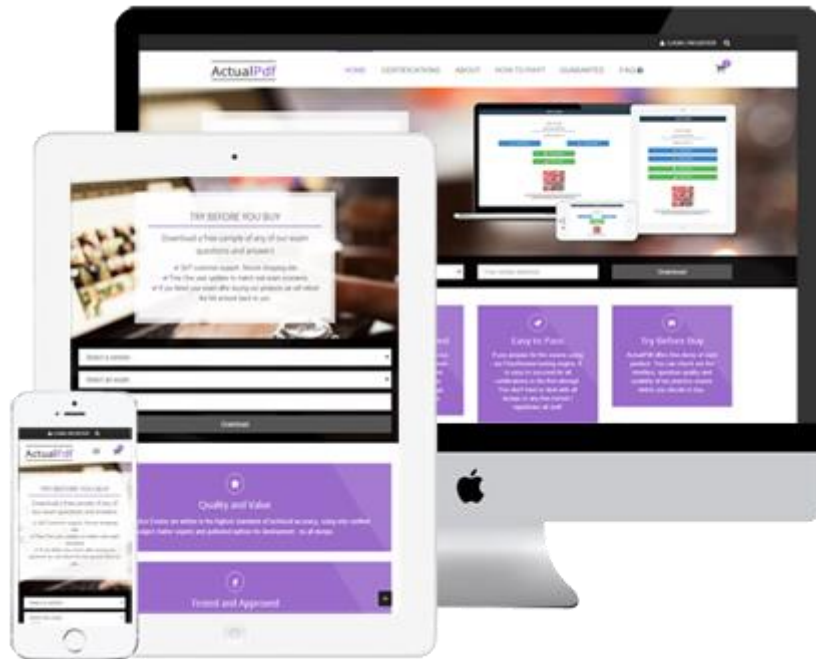


ActualPDF



| | |
|----------------------|---------------------|
| Select a vendor... ▼ | Select an exam... ▼ |
| Your email address | Free Download |

<http://www.actualpdf.com>

Unlimited Lifetime Access to 5000+ Certification Actual Exams PDF

Exam : **070-697**

Title : **Configuring Windows Devices**

Vendor : **Microsoft**

Version : **DEMO**

NO.1 You have a Windows 10 Enterprise computer named Computer1 that has the Hyper-V feature installed.

Computer1 hosts a virtual machine named VM1. VM1 runs Windows 10 Enterprise. VM1 connects to a private virtual network switch.

From Computer1, you need to remotely execute Windows PowerShell cmdlets on VM1.

What should you do?

- A. Run the Invoke-Command cmdlet and specify the -VMName parameter.
- B. Run the Powershell.exe command and specify the -Command parameter.
- C. Run the winrm.exe command and specify the -s parameter.
- D. Run the Receive-PSSession cmdlet and specify the -Name parameter.

Answer: A

Explanation

We can use Windows PowerShell Direct to run PowerShell cmdlets on a virtual machine from the Hyper-V host. Because Windows PowerShell Direct runs between the host and virtual machine, there is no need for a network connection or to enable remote management.

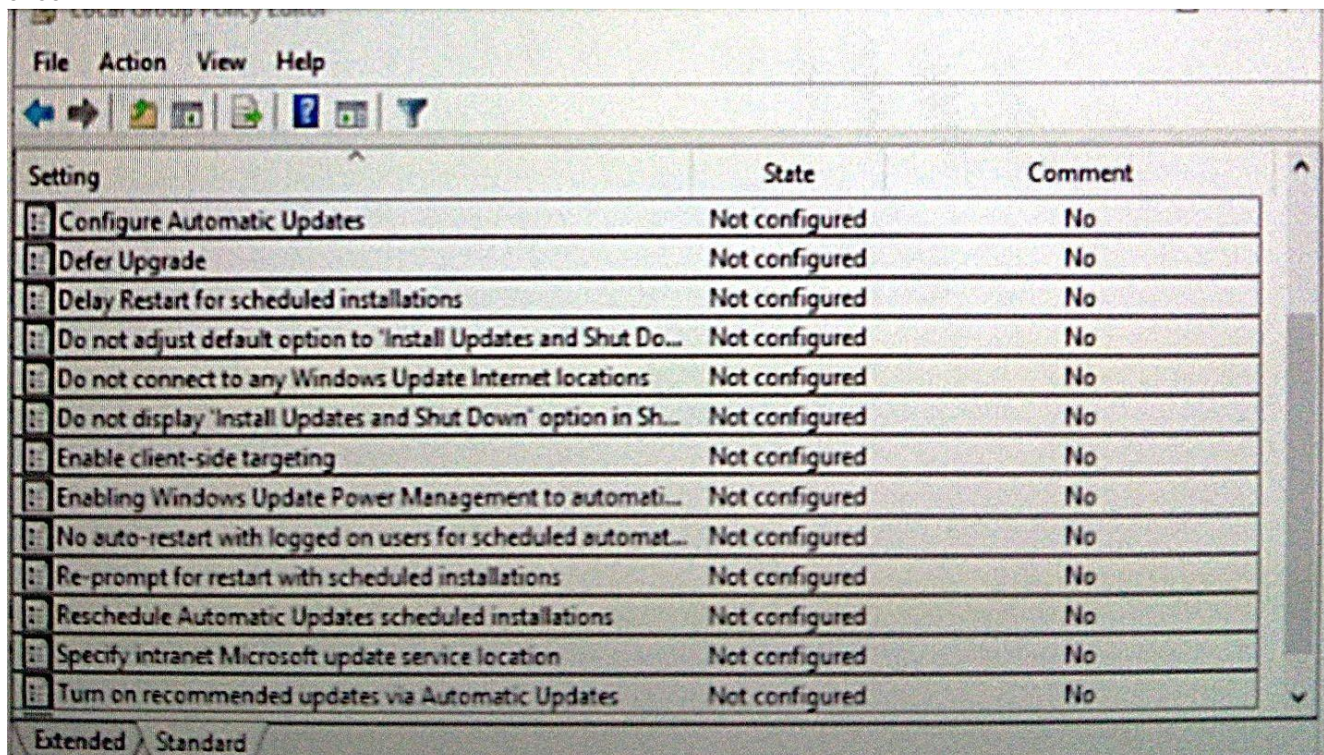
There are no network or firewall requirements or special configuration. It works regardless of your remote management configuration. To use it, you must run Windows 10 or Windows Server Technical Preview on the host and the virtual machine guest operating system.

To create a PowerShell Direct session, use one of the following commands:

NO.2 You have an Active Directory domain. All of the client computers in the domain run Windows 10 Enterprise.

You need to configure the client computers to download updates from a Windows Server Update Service server.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.



| Setting | State | Comment |
|---|----------------|---------|
| Configure Automatic Updates | Not configured | No |
| Defer Upgrade | Not configured | No |
| Delay Restart for scheduled installations | Not configured | No |
| Do not adjust default option to 'Install Updates and Shut Do... | Not configured | No |
| Do not connect to any Windows Update Internet locations | Not configured | No |
| Do not display 'Install Updates and Shut Down' option in Sh... | Not configured | No |
| Enable client-side targeting | Not configured | No |
| Enabling Windows Update Power Management to automati... | Not configured | No |
| No auto-restart with logged on users for scheduled automat... | Not configured | No |
| Re-prompt for restart with scheduled installations | Not configured | No |
| Reschedule Automatic Updates scheduled installations | Not configured | No |
| Specify intranet Microsoft update service location | Not configured | No |
| Turn on recommended updates via Automatic Updates | Not configured | No |

Answer:

| Setting | State | Comment |
|---|----------------|---------|
| Configure Automatic Updates | Not configured | No |
| Defer Upgrade | Not configured | No |
| Delay Restart for scheduled installations | Not configured | No |
| Do not adjust default option to 'Install Updates and Shut Do... | Not configured | No |
| Do not connect to any Windows Update Internet locations | Not configured | No |
| Do not display 'Install Updates and Shut Down' option in Sh... | Not configured | No |
| Enable client-side targeting | Not configured | No |
| Enabling Windows Update Power Management to automati... | Not configured | No |
| No auto-restart with logged on users for scheduled automat... | Not configured | No |
| Re-prompt for restart with scheduled installations | Not configured | No |
| Reschedule Automatic Updates scheduled installations | Not configured | No |
| Specify intranet Microsoft update service location | Not configured | No |
| Turn on recommended updates via Automatic Updates | Not configured | No |

Explanation

Configure Automatic Updates

Specify intranet Microsoft update service location

NO.3 You are an IT professional for a bank. All of the user's files on the external drives are encrypted by using EFS.

You replace a user's computer with a new Windows 10 Enterprise computer. The user needs to connect her external hard drive to the new computer. You have the original computer's certificate and key.

You need to import the certificate and key onto the new computer.

Into which certificate store should you import the certificate and key?

- A. Personal
- B. Trusted Publishers
- C. Untrusted Certificates
- D. Trusted Root Certification Authorities

Answer: A

NO.4 Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

You have an application named App1 installed on a computer named Computer1. Computer1 runs Windows

10. App1 saves data to %UserProfile%\App1\Data.

You need to ensure that you can recover the App1 data if Computer1 fails.

What should you configure?

- A. application control policies

- B. software restriction policies
- C. NTFS permissions
- D. account policies
- E. Microsoft OneDrive
- F. Encrypting File System (EFS) settings
- G. HomeGroup settings
- H. share permissions

Answer: E

NO.5 You have a computer named Computer1 that runs Windows 10 Enterprise. You add a 1 TB hard drive and create a new volume that has the drive letter D.

You format the drive by using NTFS.

You need to limit the amount of space that each user can consume on D: to 200 GB. Members of the Administrators group should have no limit.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Run convert D: /FS:NTFS.
- B. Enable the Deny disk space to users exceeding quota limit setting.
- C. Add a quota entry.
- D. Set a default quota limit.
- E. Run fsutil quota violations D:.

Answer: B,D,E

Explanation

<https://msdn.microsoft.com/en-us/library/dd163561.aspx>

[https://technet.microsoft.com/en-us/library/cc788136\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc788136(v=ws.11).aspx)

NO.6 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a corporate network. All servers run Windows Server 2016. All servers and client devices are joined to an Active Directory Domain Services (AD DS) domain named adatum.com. The use of VPN servers on the network is strictly prohibited.

Users must be able to access the corporate network in addition to Work Folders when they work at home on Windows 10 devices. You install, configure, and publish the certificate revocation list (CRL) for an internal Active Directory Certificate Services (AD CS) server.

You need to configure the environment to allow your users to register devices.

Solution: You create a DNS CNAME record of enterpriseregistration.adatum.com. You deploy Active Directory Federation Services (AD FS) and point the DNS record to your AD FS server. You deploy a Web Application Proxy server for the clients to connect to establish Internet connectivity to the device registration connection.

Does the solution meet the goal?

- A. Yes

B. No

Answer: A

Explanation

References:

<https://blog.nextxpert.com/2013/11/27/publishing-work-folders-with-web-application-proxy-2/>

NO.7 You have 100 Windows computers that are managed by using Microsoft Intune. You need to ensure that when a new critical update is released, the update is approved automatically and deployed to the computers within 24 hours of approval.

What should you do from the Microsoft Intune administration portal?

A. From the Policy node, click Compliance Policies, and then create a new compliance policy.

B. From the Admin node, click Enrollment Rules, and then modify the device enrollment rules.

C. From the Policy node, click Configuration Policies, and then create a new Windows policy.

D. From the updates node, select Critical Updates, and then modify the Approval settings.

Answer: D

Explanation

References:

<https://docs.microsoft.com/en-us/intune/deploy-use/keep-windows-pcs-up-to-date-with-software-updates-in-micr>

NO.8 You have a computer named Computer1 that runs Windows 10 Enterprise.

You plan to implement File History on Computer1.

You need to identify the interface that can be used to perform File History management actions.

Which interface should you identify for each action? To answer, select the appropriate options in the answer area.

Add items to be included in the File History:

Backup section from the Settings app

File history item from Control Panel

Storage Spaces item from Control Panel

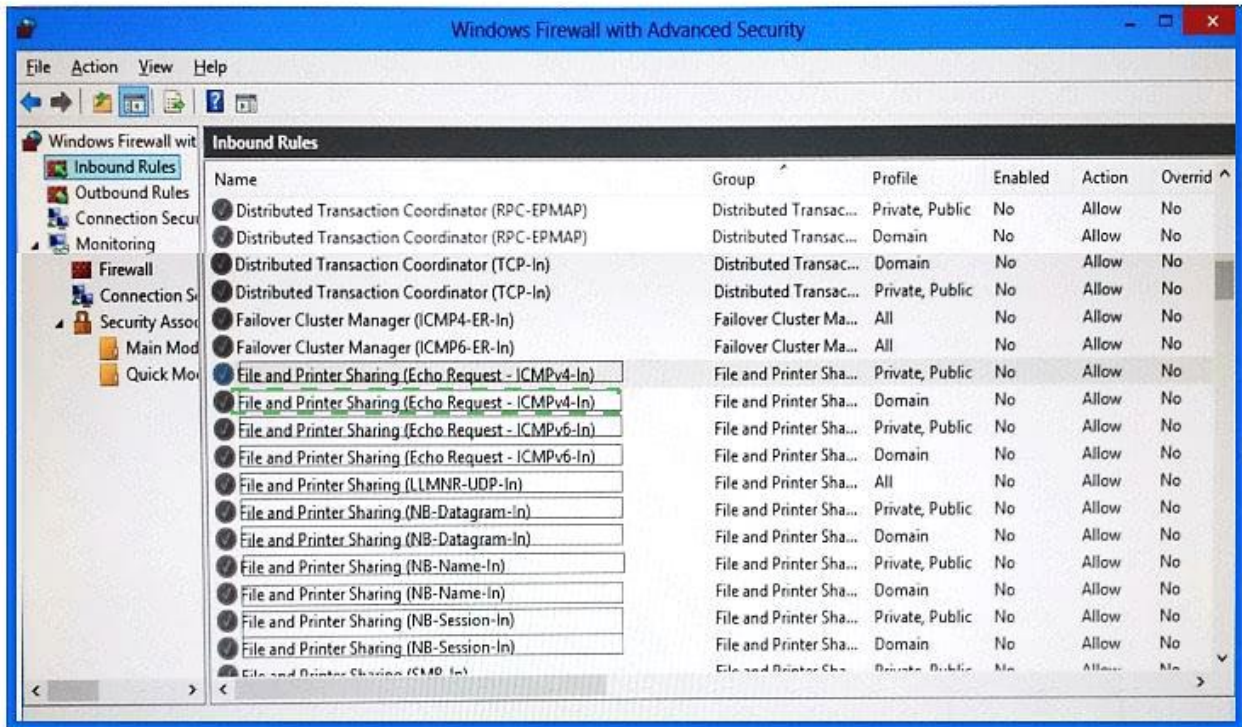
Configure File History to use a network location:

Backup section from the Settings app

File history item from Control Panel

Storage Spaces item from Control Panel

Answer:



Explanation

Add items to be included in the File History:

Backup section from the Settings app

File history item from Control Panel

Storage Spaces item from Control Panel

Configure File History to use a network location:

Backup section from the Settings app

File history item from Control Panel

Storage Spaces item from Control Panel

NO.9 You manage Microsoft Intune for a company named Contoso. You have 200 computers that run Windows 10.

The computers are Intune clients.

You need to configure software updates for the clients.

Which policy template should you use to configure each software updates setting? To answer, drag the appropriate policy templates to the correct settings. Each policy template may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Policy Templates

Microsoft Intune Agent Settings

Windows Configuration Policy

Windows Custom Policy (Windows 10 and Windows 10 Mobile)

Answer Area

Require automatic updates:

Policy template

Minimum classification of updates to install automatically:

Policy template

Allow immediate installation of updates that do not interrupt Windows:

Policy template

Answer:**Policy Templates**

Microsoft Intune Agent Settings

Windows Configuration Policy

Windows Custom Policy (Windows 10 and Windows 10 Mobile)

Answer Area

Require automatic updates:

Windows Configuration Policy

Minimum classification of updates to install automatically:

Windows Configuration Policy

Allow immediate installation of updates that do not interrupt Windows:

Microsoft Intune Agent Settings

Explanation**Policy Templates**

Microsoft Intune Agent Settings

Windows Configuration Policy

Windows Custom Policy (Windows 10 and Windows 10 Mobile)

Answer Area

Require automatic updates:

Windows Configuration Policy

Minimum classification of updates to install automatically:

Windows Configuration Policy

Allow immediate installation of updates that do not interrupt Windows:

Microsoft Intune Agent Settings

You must make use of the Microsoft Intune Windows general configuration policy to configure settings for enrolled devices. The system settings that can be configured using this policy include the following:

To configure the Allow immediate installation of updates that do not interrupt Windows update policy setting you have to configure and deploy a Microsoft Intune Agent Settings policy.

NO.10 Employees are permitted to bring personally owned portable Windows 10 Enterprise computers to the office.

They are permitted to install corporate applications by using the management infrastructure agent and access corporate email by using the Mail app.

An employee's personally owned portable computer is stolen.

You need to protect the corporate applications and email messages on the computer.

Which two actions should you perform? Each correct answer presents part of the solution.

A. Prevent the computer from connecting to the corporate wireless network.

B. Disconnect the computer from the management infrastructure.

C. Change the user's password.

D. Initiate a remote wipe.

Answer: C,D

Explanation

The personally owned portable Windows10Enterprise computers being managed by the management infrastructure agent enables the use of remote wipe. By initiating a remote wipe, we

can erase all company data including email from the stolen device.

Microsoft Intune provides selective wipe, full wipe, remote lock, and passcode reset capabilities. Because mobile devices can store sensitive corporate data and provide access to many corporate resources, you can issue a remote device wipe command from the Microsoft Intune administrator console to wipe a lost or stolen device.

Changing the user's password should be the first step. If the stolen computer is accessed before the remote wipe happens, the malicious user could be able to access company resources if the laptop has saved passwords.

NO.11 You administer Windows 10 Enterprise computers for a software development company. The marketing department is going to meet a potential customer to demonstrate the product. You want to configure a laptop that has a stand-alone virtual machine that runs Windows 10 Enterprise and the latest build of your software.

You need to enable BitLocker on the system drive of the virtual machine.

What should you do first.

- A. Join the virtual machine to an Active Directory Domain Services (AD DS) domain.
- B. Turn on the Require additional authentication at startup local policy.
- C. Turn off the Require additional authentication at startup local policy.
- D. Activate Windows.

Answer: B

NO.12 You are the system administrator for a company. All devices run Windows 10 and use a variety of Microsoft Store for Business apps. All user reports issues updating a Windows Store app. You need to troubleshoot the issue.

Winch three actions should you perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Use the Programs and Features Control Panel applet to repair the application.
- B. Run the repair-bde command.
- C. Run the SFC command.
- D. Run the Windows App Troubleshooter.
- E. Run the net start wuau servicing command.

Answer: A,C,D

NO.13 You have a desktop computer that runs Windows 8 Enterprise. You add three new 3-terabyte disks. You need to create a new 9-terabyte volume.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. From Disk Management, bring all disks offline.
- B. From PowerShell, run the Add-PhysicalDisk cmdlet.
- C. From PowerShell, run the New-VirtualDisk cmdlet.
- D. From Disk Management, create a new spanned volume.
- E. From Disk Management, convert all of the 3-terabyte disks to GPT.
- F. From Diskpart, run the Convert MBR command.

Answer: D,E

Explanation

B: GPT disks can grow to a very large size. The maximum partition (and disk) size is a function of the operating system version. Windows XP and the original release of Windows Server 2003 have a limit of 2TB per physical disk, including all partitions. For Windows Server 2003 SP1, Windows XP x64 edition, and later versions, the maximum raw partition of 18 exabytes can be supported.

A: A spanned volume is a dynamic volume consisting of disk space on more than one physical disk. If a simple volume is not a system volume or boot volume, you can extend it across additional disks to create a spanned volume, or you can create a spanned volume in unallocated space on a dynamic disk. You can make a spanned volume of GPT disks.

NO.14 Your network contains an Active Directory domain named contoso.com. Contoso.com is synchronized to a Microsoft Azure Active Directory. You have a Microsoft Intune subscription. Your company plans to implement a Bring Your Own Device (BYOD) policy. You will provide users with access to corporate data from their personal iOS devices.

You need to ensure that you can manage the personal iOS devices.

What should you do first?

- A. Set a DNS alias for the enrollment server address.
- B. Enroll for an Apple Push Notification (APN) certificate.
- C. Configure the Intune Service to Service Connector for Hosted Exchange.
- D. Create a device enrollment manager account.
- E. Install the Company Portal app from the Apple App Store.

Answer: B

Explanation

An Apple Push Notification service (APNs) certificate must first be imported from Apple so that you can manage iOS devices. The certificate allows Intune to manage iOS devices and institutes an accredited and encrypted IP connection with the mobile device management authority services.

NO.15 You administer the Windows 10 desktop environment for an organization. All desktop machines have Windows 10 Enterprise edition installed and are joined to the domain trey.com. All servers in trey.com run either Windows Server 2012 or Windows Server 2012 R2.

Users are permitted to bring their own devices. Users must be able to access their data from all devices including Apple iOS devices.

You need to implement a solution that provides the access to the data from all devices and synchronizes data across all devices without requiring subscription services.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. (Choose three.)

Actions

Deploy and configure the work folders client on all devices

Configure Offline Files and Folders on all devices

Configure a Sync share

Configure a Microsoft Intune subscription with device policies

Add the Work Folders role service on a Windows Server 2012 server

Add the Work Folders role service on a Windows Server 2012 R2 server

Configure the Device Registration service on a Windows Server 2012 R2 server

Answer Area

Three empty rectangular boxes with yellow borders, intended for the user to write their answer.

Answer:

Actions

Deploy and configure the work folders client on all devices

Configure Offline Files and Folders on all devices

Configure a Sync share

Configure a Microsoft Intune subscription with device policies

Add the Work Folders role service on a Windows Server 2012 server

Add the Work Folders role service on a Windows Server 2012 R2 server

Configure the Device Registration service on a Windows Server 2012 R2 server

Answer Area

Add the Work Folders role service on a Windows Server 2012 R2 server

Configure a Sync share

Deploy and configure the work folders client on all devices

Explanation

| Actions | Answer Area |
|--|--|
| | Add the Work Folders role service on a Windows Server 2012 R2 server |
| Configure Offline Files and Folders on all devices | Configure a Sync share |
| | Deploy and configure the work folders client on all devices |
| Configure a Microsoft Intune subscription with device policies | |
| Add the Work Folders role service on a Windows Server 2012 server | |
| | |
| Configure the Device Registration service on a Windows Server 2012 R2 server | |

References:

<https://docs.microsoft.com/en-us/windows-server/storage/work-folders/deploy-work-folders#step-5-create-securi>

<https://www.grouppolicy.biz/2013/07/how-to-setup-work-folder-using-group-policy/>

NO.16 You have an Active Directory domain named contoso.com that contains a deployment of Microsoft System Center 2012 Configuration Manager Service Pack 1 (SP1). You have a Microsoft Intune subscription that is synchronized to contoso.com by using the Microsoft Azure Active Directory Synchronization Tool (DirSync.) You need to ensure that you can use Configuration Manager to manage the devices that are registered to your Microsoft Intune subscription. Which two actions should you perform? Each correct answer presents a part of the solution.

- A. In Microsoft Intune, configure an Exchange Connector.
- B. Install and configure Azure Active Directory Synchronization Services (AAD Sync.)
- C. In Configuration Manager, configure the Microsoft Intune Connector role.
- D. In Microsoft Intune, create a new device enrollment manager account.
- E. In Configuration Manager, create the Microsoft Intune subscription.

Answer: C,E

Explanation

To allow Configuration Manager to manage mobile devices in the same context as other devices, it requires you to create a Windows Intune subscription and synchronize user accounts from Active Directory to Microsoft Online. to achieve that, you are required to complete the following tasks:

References:

<http://blogs.technet.com/b/configmgrteam/archive/2013/03/20/configuring-configuration-manager-sp1-to-manag>

NO.17 You have five computers that run Windows 10. You are the only user who uses the computers. All of the computers are members of the same domain.

You need to ensure that you can access any file on any of the computers over the Internet.

What should you configure?

- A. Encrypting File System (EFS) settings
- B. application control policies
- C. Microsoft OneDrive
- D. account policies
- E. software restriction policies
- F. HomeGroup settings
- G. share permissions
- H. NTFS permissions

Answer: C

NO.18 You configure VPN auto trigger for five Windows 10 Enterprise computers. When you test the computers, they trigger the VPN all the time, even in the office.

You need to configure VPN auto trigger to function only when VPN is required.

Which command should you use?

- A. Add -VpnConnectionTriggerApplication [-Name] <string> -ApplicationID <String[]> -PassThru
- B. Add -VpnConnectionTriggerTrusted Network [-Name] <string> [-DnsSuffix] <string[]>
- C. Set -VpnConnectionTriggerDnsConfiguration [-Name] <string> [-DnsSuffix <String>] [-DnsIPAddress <string[]>] [-DnsSuffixSearchList
- D. Add -VpnConnectionTriggerDnsConfiguration [-Name] <string> -DnsSuffix <String> [-DnsIPAddress <string[]>] -PassThru

Answer: B