Number: 70-697
Passing Score: 800
Time Limit: 120 min
File Version: 4.0

70-697

Configuring Windows Devices

Version 4.0

Sections

1. Manage identity
2. Plan desktop and device deployment
3. Plan and implement a Microsoft Intune device management solution
4. Configure networking
5. Configure storage
6. Manage data access and protection
7. Manage remote access
8. Manage apps
9. Manage updates and recovery

Exam A

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

Correct Answer: D
Section: Plan desktop and device deployment
Explanation

Explanation/Reference:
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:
Enter-PSSession -VMName VMName
Invoke-Command -VMName VMName -ScriptBlock { commands }

Incorrect Answers:
A: WinRM is Windows Remote Management. This is not required when using Windows PowerShell Direct.
B: Running PowerShell.exe with a PowerShell cmdlet will execute the PowerShell cmdlet on the local machine. It will not remotely execute the PowerShell cmdlet on the VM.
C: You could run the **Enter-PSSession** cmdlet with the **-VMName** parameter but the **Receive-PSSession** cmdlet with the **–Name** parameter will not work.

References:
https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/about/whats_new

QUESTION 2
You deploy several tablet PCs that run Windows 10 Enterprise.

You need to minimize power usage when the user presses the sleep button.

What should you do?

A. In Power Options, configure the sleep button setting to **Sleep**.
B. In Power Options, configure the sleep button setting to **Hibernate**.
C. Configure the active power plan to set the system cooling policy to **passive**.
D. Disable the C-State control in the computer's BIOS.

Correct Answer: B
Section: Plan desktop and device deployment
Explanation

Explanation/Reference:
Explanation:
We can minimize power usage on the tablet PCs by configuring them to use Hibernation mode. A computer in hibernation mode uses no power at all. Hibernation is a power-saving state designed primarily for laptops. While sleep puts your work and settings in memory and draws a small amount of power, hibernation puts your open documents and programs on your hard disk, and then turns off your computer. Of all the power-saving states in Windows, hibernation uses the least amount of power. On a laptop, use hibernation when you know that you won't use your laptop for an extended period and won't have an opportunity to charge the battery during that time.

Incorrect Answers:
A: Sleep is a power-saving state that allows a computer to quickly resume full-power operation. A sleeping computer draws a small amount of power whereas a hibernating computer uses no power.
C: A passive cooling policy slows down the processor before speeding up the processor's cooling fan to conserve power. However, this will still use more power than a hibernating tablet.
D: C-States are different modes of CPU clock speed used to conserve power when processors are idle. Disabling C-State control disables the ability to reduce the power consumption of the computer.

References:
http://windows.microsoft.com/en-gb/windows7/sleep-and-hibernation-frequently-asked-questions

QUESTION 3
You are the desktop administrator for a small company.

Your workgroup environment consists of Windows 10 Enterprise computers. You want to prevent 10 help desk computers from sleeping. However, you want the screens to shut off after a certain period of time if the computers are not being used.

You need to configure and apply a standard power configuration scheme for the 10 help desk computers on your network.

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

A. Import the power scheme by using POWERCFG /IMPORT on each of the remaining help desk computers. Set the power scheme to Active by using POWERCFG /S.
B. Use POWERCFG /X on one help desk computer to modify the power scheme to meet the requirements. Export the power scheme by using POWERCFG /EXPORT.
C. Use POWERCFG /S on one help desk computer to modify the power scheme to meet the requirements. Export the power scheme by using POWERCFG /EXPORT.
D. Import the power scheme by using POWERCFG /IMPORT on each of the remaining help desk computers. Set the power scheme to Active by using POWERCFG /X.

Correct Answer: AB
Section: Plan desktop and device deployment
Explanation

Explanation/Reference:
Explanation:
You can use the Powercfg.exe tool to control power settings and configure computers to default to Hibernate or Standby modes.

In this question, we use POWERCFG /X on one help desk computer to modify the power scheme to meet our requirements. After configuring the required settings, we can export the power scheme settings to a file by using POWERCFG /EXPORT.
We can then import the power scheme from the file on each of the remaining help desk computers by using POWERCFG /IMPORT. After importing the power scheme on the remaining computers, we need to set the new power scheme to be the active power scheme by using POWERCFG /S.

Incorrect Answers:
C: You need to use the /X switch to modify the power scheme, not the /S switch.
D: You need to use the /S switch to set the power scheme as active, not the /X switch.

References:
https://technet.microsoft.com/en-us/library/cc748940(v=ws.10).aspx

QUESTION 4
A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 10 Enterprise. Some computers have a Trusted Platform Module (TPM) chip.

You need to configure a single Group Policy object (GPO) that will allow Windows BitLocker Drive Encryption on all client computers.

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

A. Enable the Require additional authentication at startup policy setting.
B. Enable the Enforce drive encryption type on operating system drives policy setting.
C. Enable the option to allow BitLocker without a compatible TPM.
D. Configure the TPM validation profile to enable Platform Configuration Register indices (PCRs) 0, 2, 4, and 11.

Correct Answer: AC
Section: Plan desktop and device deployment
Explanation

Explanation/Reference:
Explanation:
We need to allow Windows BitLocker Drive Encryption on all client computers (including client computers that do not have Trusted Platform Module (TPM) chip).
We can do this by enabling the option to allow BitLocker without a compatible TPM in the group policy. The 'Allow BitLocker without a compatible TPM' option is a checkbox in the 'Require additional authentication at startup' group policy setting. To access the 'Allow BitLocker without a compatible TPM' checkbox, you need to first select Enabled on the 'Require additional authentication at startup' policy setting.

Incorrect Answers:
B: Enabling the 'Enforce drive encryption type on operating system drives' policy setting allows you to configure whether the entire drive or used space only is encrypted when BitLocker is enabled. However, it does not enable the use of BitLocker on computers without a TPM chip.
D: The Platform Configuration Register indices (PCRs) 0, 2, 4, and 11 are enabled by default for computers that use an Extensible Firmware Interface (EFI). Configuring the TPM validation profile does not enable the use of BitLocker on computers without a TPM chip.

References:
http://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/

QUESTION 5
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. Change the user's password.
C. Disconnect the computer from the management infrastructure.
D. Initiate a remote wipe.

Correct Answer: BD
Section: Plan desktop and device deployment
Explanation

Explanation/Reference:

Explanation:
The personally owned portable Windows 10 Enterprise 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.

Incorrect Answers:
A: Preventing the computer from connecting to the corporate wireless network will not offer much protection. The person in possession of the laptop would still be able to access all the data on the laptop and download emails. Furthermore, it is likely that the corporate applications can access corporate servers over any Internet connection.
C: Disconnecting the computer from the management infrastructure will not help. The person in possession of the laptop would still be able to access all the data on the laptop and download emails. This step would also remove the ability to perform a remote wipe. The computer will be disconnected from the management infrastructure when the remote wipe happens.

References:
https://technet.microsoft.com/en-gb/library/jj676679.aspx

QUESTION 6
You are an IT consultant for small and mid-sized business.

One of your clients wants to start using Virtual Smart Cards on its Windows 10 Enterprise laptops and tablets. Before implementing any changes, the client wants to ensure that the laptops and tablets support Virtual Smart Cards.

You need to verify that the client laptops and tablets support Virtual Smart Cards.

What should you do?

A. Ensure that each laptop and tablet has a Trusted Platform Module (TPM) chip of version 1.2 or greater.
B. Ensure that BitLocker Drive Encryption is enabled on a system drive of the laptops and tablets.
C. Ensure that each laptop and tablet can read a physical smart card.
D. Ensure that the laptops and tablets are running Windows 10 Enterprise edition.

Correct Answer: A
Section: Plan desktop and device deployment
Explanation

Explanation/Reference:
Explanation:
A Trusted Platform Module (TPM) chip of version 1.2 or greater is required to support Virtual Smart Cards.

Virtual smart card technology from Microsoft offers comparable security benefits to physical smart cards by using two-factor authentication. Virtual smart cards emulate the functionality of physical smart cards, but they use the Trusted Platform Module (TPM) chip that is available on computers in many organizations, rather than requiring the use of a separate physical smart card and reader. Virtual smart cards are created in the TPM, where the keys that are used for authentication are stored in cryptographically secured hardware.

Incorrect Answers:
B: BitLocker Drive Encryption does not need to be enabled on a system drive of the laptops and tablets to support Virtual Smart Cards.
C: The ability to read a physical smart card does not ensure support for Virtual Smart Cards.
D: Windows 10 Enterprise edition is not a requirement for Virtual Smart Cards; other versions of Windows 10 (and Windows 8) can use Virtual Smart Cards.

References:
https://technet.microsoft.com/en-GB/library/dn593708.aspx

QUESTION 7
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. Install the Company Portal app from the Apple App Store.
B. Create a device enrollment manager account.
C. Set a DNS alias for the enrollment server address.
D. Configure the Intune Service to Service Connector for Hosted Exchange.
E. Enroll for an Apple Push Notification (APN) certificate.

Correct Answer: E
Section: Plan and implement a Microsoft Intune device management solution
Explanation

Explanation/Reference:
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.

Incorrect Answers:
A: Users can only install the Company Portal app after they have been added as Intune users, which require the Apple Push Notification (APN)

certificate to be in place.
B: The device enrollment manager account is a special Intune account that has permission to enroll more than five corporate-owned devices. It is not used for BYOD.
C: The *Set a DNS alias for the enrollment server address* setting is an optional setting for enrolling Windows devices.
D: The *Configure Intune service to service connector for hosted Exchange* setting is used to connect Microsoft Intune and hosted Exchange without an on-premises infrastructure.

References:
https://technet.microsoft.com/library/dn408185.aspx
https://technet.microsoft.com/en-us/library/dn764961.aspx
https://technet.microsoft.com/en-us/library/mt346003.aspx
https://technet.microsoft.com/en-us/library/dn646988.aspx

QUESTION 8
You manage Microsoft Intune for a company named Contoso. Intune client computers run Windows 10 Enterprise.

You notice that there are 25 mandatory updates listed in the Intune administration console.

You need to prevent users from receiving prompts to restart Windows following the installation of mandatory updates.

Which policy template should you use?

A. Microsoft Intune Agent Settings
B. Windows Configuration Policy
C. Microsoft Intune Center Settings
D. Windows Custom Policy (Windows 10 and Windows 10 Mobile)

Correct Answer: A
Section: Plan and implement a Microsoft Intune device management solution
Explanation

Explanation/Reference:
Explanation:
To configure the *Prompt user to restart Windows during Intune client agent mandatory updates* update policy setting you have to configure the Microsoft Intune Agent Settings policy. Setting the *Prompt user to restart Windows during Intune client agent mandatory updates* setting to No would prevent users from receiving prompts to restart Windows following the installation of mandatory updates.

Incorrect Answers:
B: You make use of the Microsoft Intune Windows general configuration policy to configure settings for enrolled devices, but not the policy setting in question.
C: The Microsoft Intune Center allows users to get applications from the company portal, check for updates, manage Microsoft Intune Endpoint Protection, and request remote assistance. It does not allow users to configure settings to prevent users from receiving prompts to restart Windows following the installation of mandatory updates

D: You can make use of the Microsoft Intune custom configuration policy for Windows 10 and Windows 10 Mobile to deploy OMA-URI (Open Mobile Alliance Uniform Resource Identifier) settings.

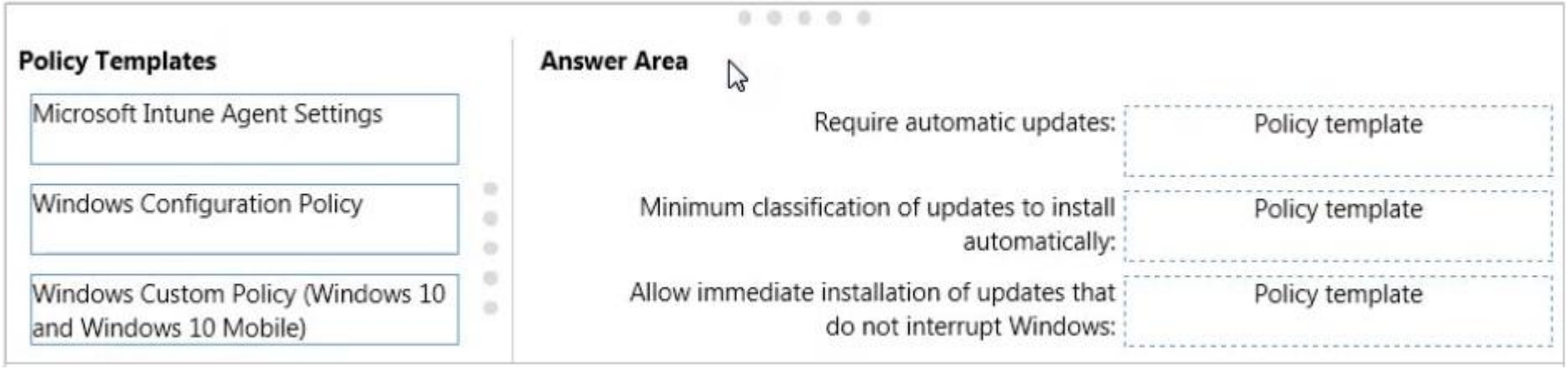
References:
http://blogs.technet.com/b/windowsintune/archive/2013/01/09/policy-settings-for-mandatory-updates.aspx
https://technet.microsoft.com/en-us/library/dn646989.aspx

QUESTION 9
You manage Microsoft Intune for a company named Contoso. You have 200 computers that run Windows 10. The computers are Intune clients.

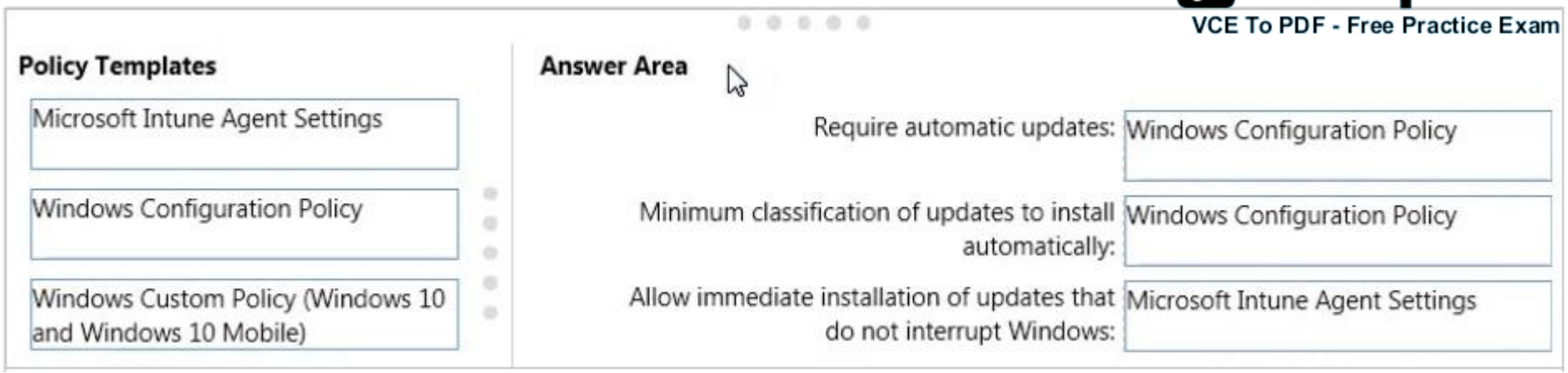
You need to configure software updates for the clients.

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.

Select and Place:



Correct Answer:



Section: Plan and implement a Microsoft Intune device management solution
Explanation

Explanation/Reference:
Explanation:
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:

- Require automatic updates.
- Require automatic updates – Minimum classification of updates to install automatically.
- User Account Control.
- Allow diagnostic data submission.

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.

Incorrect Answers:
You can make use of the Microsoft Intune custom configuration policy for Windows 10 and Windows 10 Mobile to deploy OMA-URI (Open Mobile Alliance Uniform Resource Identifier) settings, which can be used to control features on Windows 10 and Windows 10 Mobile devices.

References:
https://technet.microsoft.com/en-us/library/dn646968.aspx
https://technet.microsoft.com/en-us/library/mt147409.aspx

QUESTION 10
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, create a new device enrollment manager account.
B. Install and configure Azure Active Directory Synchronization Services (AAD Sync.)
C. In Microsoft Intune, configure an Exchange Connector.
D. In Configuration Manager, configure the Microsoft Intune Connector role.
E. In Configuration Manager, create the Microsoft Intune subscription.

Correct Answer: DE
Section: Plan and implement a Microsoft Intune device management solution
Explanation

Explanation/Reference:
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:

- Sign up for a Windows Intune organizational account
- Add a public company domain and CNAME DNS entry
- Verify users have public domain User Principal Names (UPNs)
- If you plan to use single sign-on, deploy and configure Active Directory Federated Services (ADFS)
- Deploy and Configure Active Directory Synchronization
- Reset users Microsoft Online password – If not using ADFS*
- Configure Configuration Manager for mobile device management
- **Create the Windows Intune Subscription in the Configuration Manager console**
- **Add the Windows Intune Connector Site System role**
- Verify that Configuration Manager successfully connects to Windows Intune

References:
http://blogs.technet.com/b/configmgrteam/archive/2013/03/20/configuring-configuration-manager-sp1-to-manage-mobile-devices-using-windows-intune.aspx

QUESTION 11
You have a Microsoft Intune subscription.

You have three security groups named Security1, Security2 and Security3. Security1 is the parent group of Security2. Security2 has 100 users.

You need to change the parent group of Security2 to be Security3.

What should you do first?

A. Edit the properties of Security1.
B. Edit the properties of Security2.
C. Delete security2.
D. Remove all users from Security2.

Correct Answer: C
Section: Plan and implement a Microsoft Intune device management solution
Explanation

Explanation/Reference:
Explanation:
You cannot change the parent group of a security group in Microsoft Intune. You can only delete the group and recreate another group with the correct parent.
Deleting a group does not delete the users that belong to that group. Therefore, you do not need to remove the users from the group; you can just delete the group and recreate it.

Incorrect Answers:
A: You cannot change the parent of a group by modifying the properties of the parent group.
B: You cannot change the parent of a group by modifying the properties of the group.
D: Deleting a group does not delete the users that belong to that group. Therefore, you do not need to remove the users from the group; you can just delete the group and recreate it.

References:
https://technet.microsoft.com/en-gb/library/dn646990.aspx

QUESTION 12
HOTSPOT
You have a network that contains Window 10 Enterprise computers.

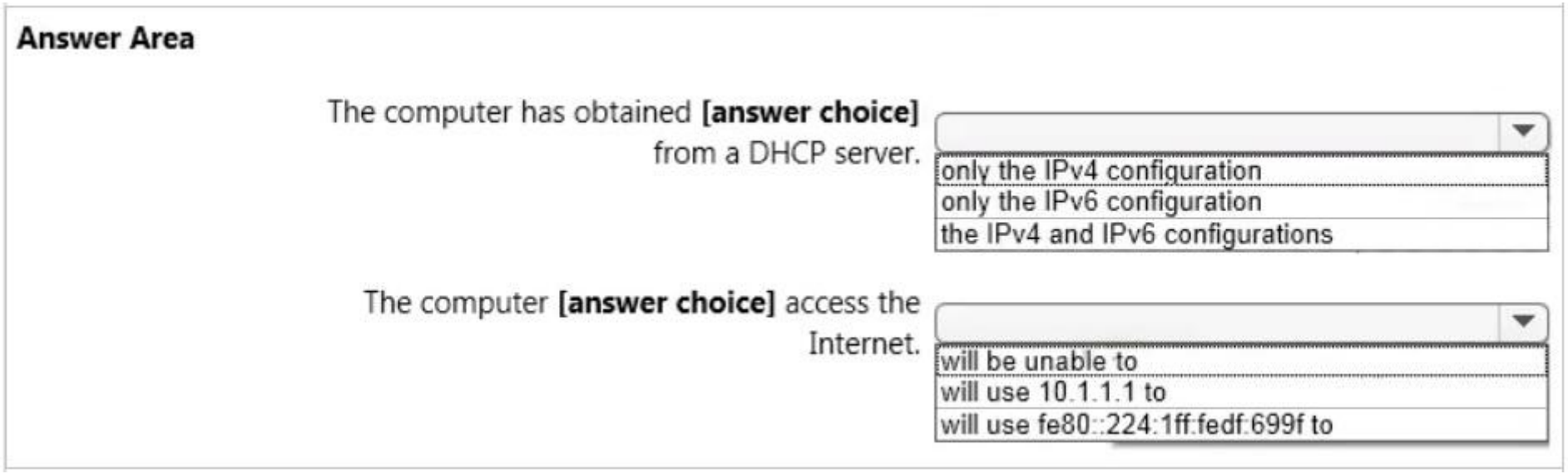
The network configuration of one of the computers is shown in the following output.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : Computer1
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #5
   Physical Address. . . . . . . . . : E8-B1-94-0A-8E-10
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Etheret adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : DisplayLink Network Adapter NCM#5
   Physical Address. . . . . . . . . : 00-50-2E-00-7D-F0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c4e9:416b:3ebe:a6cb%13(Preferred)
   Default Gateway . . . . . . . . . : fe80::224:1ff:fedf:699f%34
   DHCPv6 IAID . . . . . . . . . . . : 771772598
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1A-B8-FC-74-88-53-2E-00-7D-F0
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::1%2
                                       fec0:0:0:ffff::1%3
   NetBIOS over Tcpip. . . . . . . . : Disabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7260 #2
```

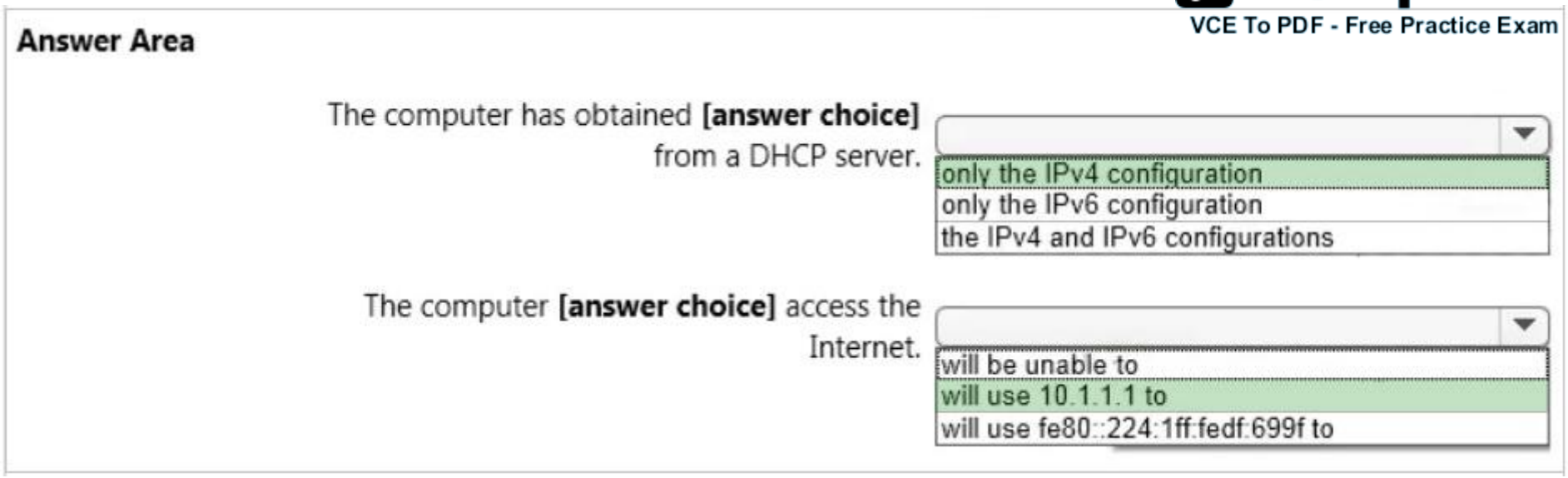
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the output.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Section: Configure networking
Explanation

Explanation/Reference:
Explanation:
The exhibit below shows that the computer obtained its IPv4 address from a DHCP server. It also shows when the DHCP lease was obtained and when it will expire.

```
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 10.1.1.133(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Thursday, August 13, 2015 12:01:10 PM
Lease Expires . . . . . . . . . . : Saturday, August 21, 2015 10:37:18 AM
```

The IPv6 address shown below starts with ‘fe80’. This is an auto-configuration address, not an address obtained from a DHCP server.

```
Link-local IPv6 Address . . . . . : fe80::c4e9:416b:3ebe:a6cb%13(Preferred)
```

The IP address of the Default Gateway is 10.1.1.1

QUESTION 13
A company has 100 client computers that run Windows 10 Enterprise.

A new company policy requires that all client computers have static IPv6 addresses.

You need to assign static IPv6 addresses to the client computers.

Which Network Shell (netsh) command should you run?

A. add address
B. set interface
C. set global
D. set address

Correct Answer: A
Section: Configure networking
Explanation

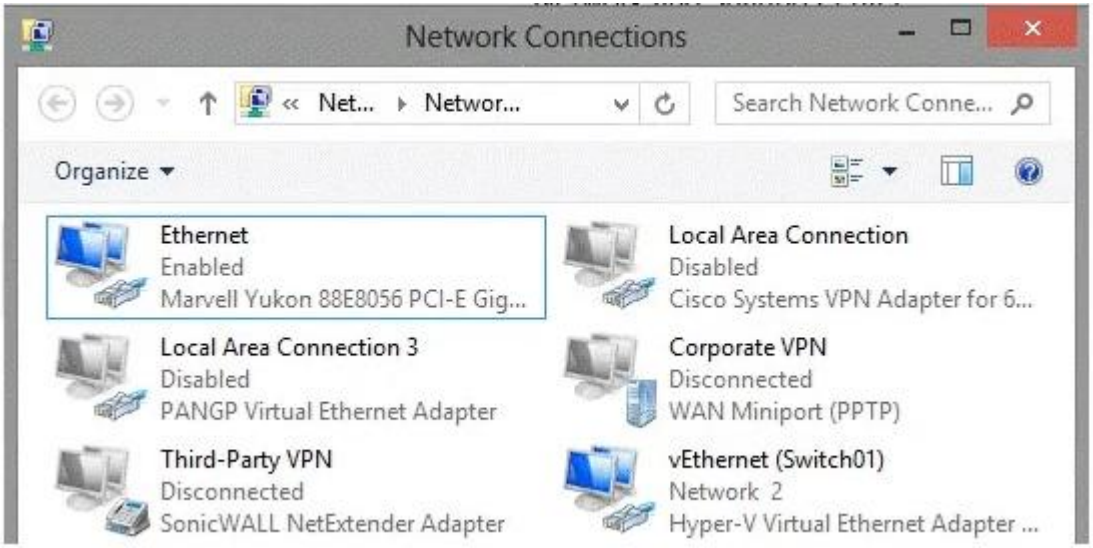
Explanation/Reference:
Explanation:
The *add address* Network Shell (netsh) command adds an IPv6 address to a specified interface.

Incorrect Answers:
B: The *set interface* Network Shell (netsh) command modifies interface configuration parameters.
C: The *set global* Network Shell (netsh) command modifies global configuration parameters.
D: The *set address* Network Shell (netsh) command modifies an IPv6 address on a specified interface.

References:
https://technet.microsoft.com/en-gb/library/cc740203(v=ws.10).aspx#BKMK_3

QUESTION 14
HOTSPOT
You are setting up a Windows 10 Enterprise computer.

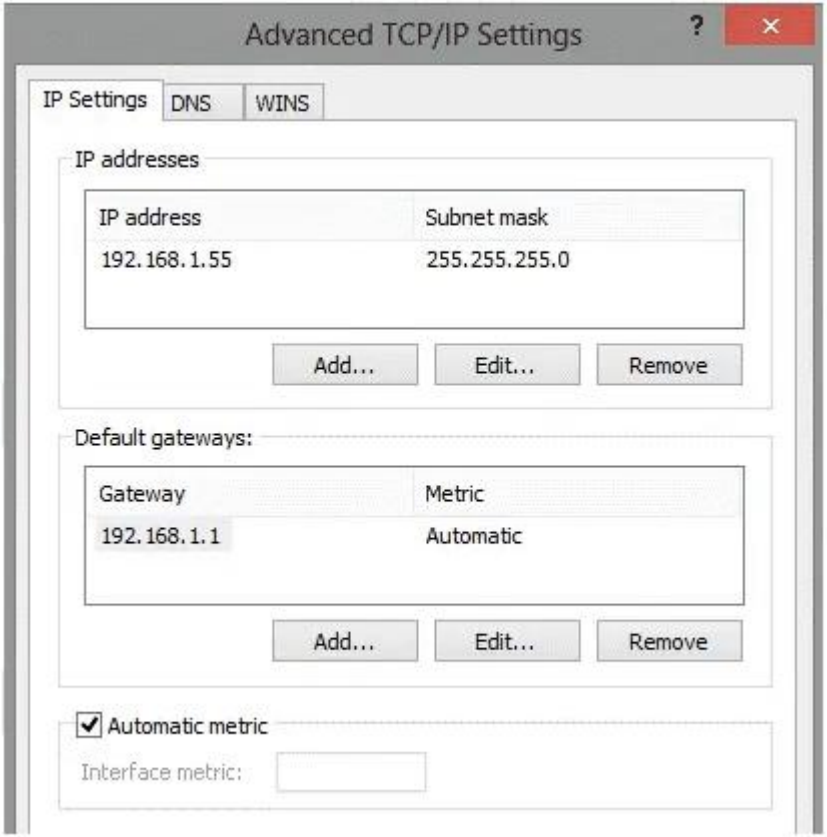
The computer's network connections are shown in the Network connections exhibit. (Click the Exhibit button.)



The computer's network settings are shown in the Network Settings exhibit. (Click the Exhibit button.)

```
Ethernet adapter vEthernet (Switch01):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter #2
   Physical Address. . . . . . . . . : BC-AE-C5-21-02-A3
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4ad:8811:98c6:5f2c%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.55(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 314355397
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-17-F7-1A-65-BC-AE-C5-21-02-A3
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Advanced TCP/IP settings are shown in the Advanced TCP/IP Settings exhibit. (Click the Exhibit button.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

	Yes	No
The computer is a Microsoft Hyper-V host.	○	○
The computer has a static IP address.	○	○
The computer is a Microsoft Hyper-V virtual machine.	○	○

Correct Answer:

Answer Area

	Yes	No
The computer is a Microsoft Hyper-V host.	○	○
The computer has a static IP address.	○	○
The computer is a Microsoft Hyper-V virtual machine.	○	○

Section: Configure networking
Explanation

Explanation/Reference:
Explanation:
The computer has a physical network adapter.

When you enable Hyper-V on a computer, a virtual network adapter connected to a virtual switch is added.

Therefore, the computer is a Hyper-V host.

The computer has an IP address. The text in the image below shows that the network connection is not DHCP enabled. Therefore, this is a static IP address.

The computer is a Hyper-V host, not a Hyper-V virtual machine.

QUESTION 15
A company has 10 portable client computers that run Windows 10 Enterprise.

The portable client computers have the network connections described in the following table.

Network name	Connection type	Network profile
CorpWired	Wired	Private
CorpWifi	Wireless	Public
HotSpot	Public hotspot	Public

None of the computers can discover other computers or devices, regardless of which connection they use.

You need to configure the connections so that the computers can discover other computers or devices only while connected to the CorpWired or CorpWifi connections.

What should you do on the client computers?

A. For the CorpWifi connection, select Yes, turn on sharing and connect to devices.
B. Turn on network discovery for the Public profile.
C. Change the CorpWired connection to public. Turn on network discovery for the Public profile. For the HotSpot connection, select **No, don't turn on sharing or connect to devices**.
D. For the CorpWired connection, select Yes, turn on sharing and connect to devices.
E. Turn on network discovery for the Private profile.

Correct Answer: C

Section: Configure networking
Explanation

Explanation/Reference:
Explanation:
Of the answers given, this is the only single answer that meets the requirements.
Network discovery is a network setting that affects whether your computer can see (find) other computers and devices on the network and whether other computers on the network can see your computer. By default, Windows Firewall blocks network discovery, but you can enable it.
When we change the CorpWired connection to public, all networks will be in the Public profile. Enabling network discovery for the Public profile will enable the computers to see other computers on each network (including HotSpot).
To prevent network discovery on the HotSpot network, we can select **No, don't turn on sharing or connect to devices** for that network. This will disable Network discovery for the computer's connection to the HotSpot network.

Incorrect Answers:
A: This solution would enable network discovery for the CorpWifi network, but not the CorpWired network.
B: This solution would enable network discovery for the CorpWifi and HotSpot networks, but not the CorpWired network.
D: This solution would enable network discovery for the CorpWired network, but not the CorpWifi network.
E: This solution would enable network discovery for the CorpWired network, but not the CorpWifi network.

QUESTION 16
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 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.

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

Correct Answer: BCD
Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
To limit the amount of space that each user can consume, you should enable the **Enable Quota Management** setting, and then enter the appropriate values in the Limit Disk Space To text box and the Set Warning Level To text box, and then select the Deny Disk Space To Users Exceeding Quota

Limit check box to enforce identical quota limits for all users.

Incorrect Answers:
A: The fsutil quota violations D: command will search the system and application logs and display a message to indicate that quota violations have been detected or that a user has reached a quota threshold or quota limit. It will not, however, set the quota limit.
E: The convert D: /FS:NTFS command will convert the volume to NTFS. It will not set the quota limit.
F: A default quota entry exists for administrators so answer F is not required.

Reference:
https://technet.microsoft.com/en-us/library/dd277427.aspx
https://technet.microsoft.com/en-us/library/cc788136.aspx
https://technet.microsoft.com/en-us/library/bb490885.aspx

QUESTION 17
You purchase a new Windows 10 Enterprise desktop computer. You have four external USB hard drives.

You want to create a single volume by using the four USB drives. You want the volume to be expandable, portable and resilient in the event of failure of an individual USB hard drive.

You need to create the required volume.

What should you do?

A. From Control Panel, create a new Storage Space across 4 USB hard drives. Set resiliency type to **Three-way mirror**.
B. From Control Panel, create a new Storage Space across 4 USB hard drives. Set resiliency type to **Parity**.
C. From Disk Management, create a new spanned volume.
D. From Disk Management, create a new striped volume.

Correct Answer: B
Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
Storage Spaces can combine multiple hard drives into a single virtual drive. To create a storage space, you'll have to connect two or more additional internal or external drives to your computer to create a storage pool. You can also specify an arbitrarily large logical size. When your existing drive begins to fill up and nears the physical limit, Windows will display a notification in the Action Center, prompting you to add additional physical storage space. Selecting the Parity resiliency type allows Windows to store parity information with the data, thereby protecting you from a single drive failure.

Incorrect Answers:
A: The Three-way mirror resiliency type allows Windows to store three copies of your data. Mirroring uses drive space less efficiently than parity.
C: Spanned volumes are not fault tolerant
D: Striped volumes are not fault tolerant

References:
http://www.howtogeek.com/109380/how-to-use-windows-8s-storage-spaces-to-mirror-combine-drives/
https://technet.microsoft.com/en-us/library/cc772180.aspx
https://technet.microsoft.com/en-us/library/cc732422.aspx

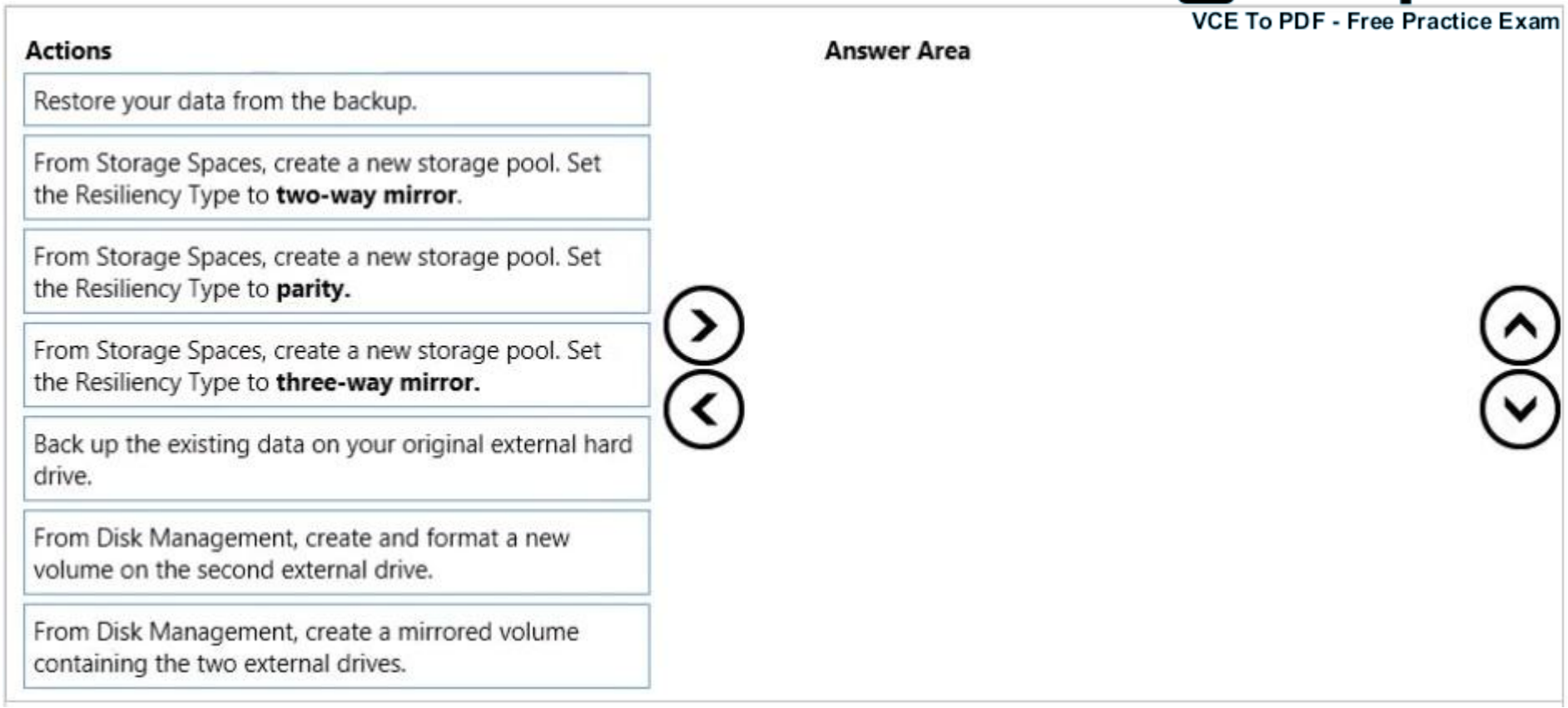
QUESTION 18
DRAG DROP
You have a Windows 10 Enterprise computer. You have a 1-terabyte external hard drive.

You purchase a second 1-terabyte external hard drive.

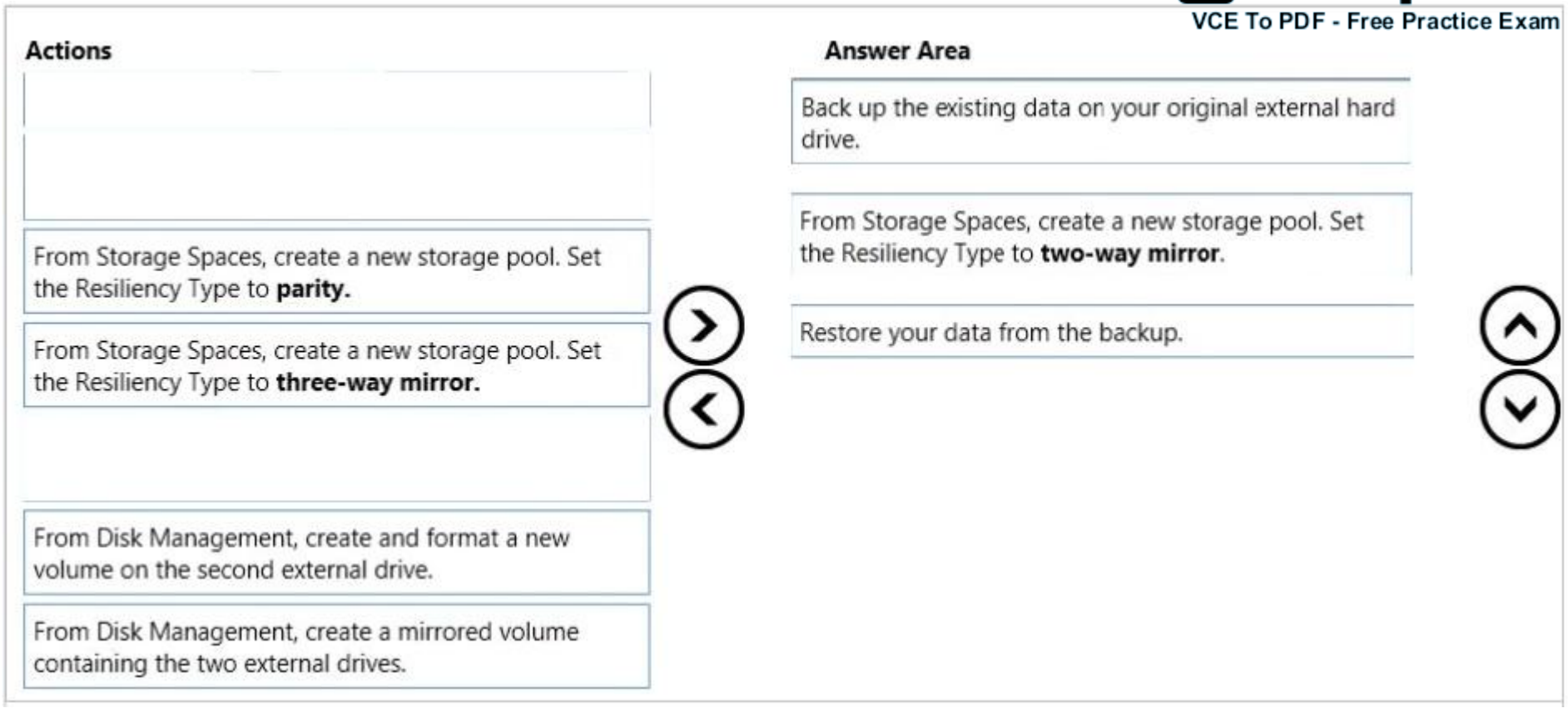
You need to create a fault-tolerant volume that includes both external hard drives. You also need to ensure that additional external hard drives can be added to the volume.

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.

Select and Place:



Correct Answer:



Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
Storage Spaces can combine multiple hard drives into a single virtual drive. To create a storage space, you'll have to connect two or more additional internal or external drives to your computer to create a storage pool. When creating the pool, any existing data on the disks will be lost. It is therefore important to back up the data if you do not want to lose it. You can also specify an arbitrarily large logical size. When your existing drive begins to fill up and nears the physical limit, Windows will display a notification in the Action Center, prompting you to add additional physical storage space. Selecting the Two-way mirror resiliency type allows Windows to store two copies of your data, so that you won't lose your data if one of your drives fails.

References:
http://www.howtogeek.com/109380/how-to-use-windows-8s-storage-spaces-to-mirror-combine-drives/

QUESTION 19
HOTSPOT
You manage 50 computers that run Windows 10 Enterprise.

You have a Windows To Go workspace installed on a USB drive named USB1.

You need to configure USB1 to meet the following requirements:

- When you run Windows To Go from USB1, you can see the contents of the computer's internal drives from File Explorer.
- When you connect USB1 to a computer that runs Windows 10, you can automatically view the content of USB1 from File Explorer.

In the table below, select the action that must be performed to achieve each requirement.

NOTE: Make only one selection in each column. Each correct selection is worth one point.

Hot Area:

Answer Area

Actions	When you run Windows To Go from USB1, you can see the contents of the computer's internal drives from File Explorer.	When you connect USB1 to a computer that runs Windows 10, you can automatically view the content of USB1 from File Explorer
From DiskPart, configure the **san policy** option.	○	○
From DiskPart, configure the **attributes volume** option.	○	○
From DiskPart, configure the **attributes disk** option	○	○
From fsutil, configure the **volume** option.	○	○
From fsutil, configure the **behavior** option.	○	○

Correct Answer:

Answer Area

Actions	When you run Windows To Go from USB1, you can see the contents of the computer's internal drives from File Explorer.	When you connect USB1 to a computer that runs Windows 10, you can automatically view the content of USB1 from File Explorer
From DiskPart, configure the **san policy** option.	○	○
From DiskPart, configure the **attributes volume** option.	○	○
From DiskPart, configure the **attributes disk** option	○	○
From fsutil, configure the **volume** option.	○	○
From fsutil, configure the **behavior** option.	○	○

Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
If you want to view the contents of the computer's internal drives from File Explorer when you run Windows To Go from USB1, you have to launch an elevated command prompt, run *diskpart* and then execute the *List disk* command. You now have to select the internal disk using the *sel disk* command, and then enter the *online disk* command.
Configuring the *attributes volume* option from DiskPart allows you to display, set, or clear the attributes of a volume.

Incorrect Answers:
Configuring the *attributes disk* option from DiskPart allows you to display, set, or clear the attributes of a disk.
Fsutil volume is used to dismount a volume, query to see how much free space is available on a disk, or find a file that is using a specified cluster.
Fsutil behavior is used to query or set NTFS volume behaviour.

References:
http://www.verboon.info/2012/12/how-to-access-data-from-the-local-disk-when-running-a-windows-to-go-workspace/
https://technet.microsoft.com/en-us/library/cc732970.aspx
https://technet.microsoft.com/en-us/library/cc753059.aspx

QUESTION 20
You support Windows 10 Enterprise computers that are members of an Active Directory domain. Recently, several domain user accounts have been configured with super-mandatory user profiles.

A user reports that she has lost all of her personal data after a computer restart.

You need to configure the user's computer to prevent possible user data loss in the future.

What should you do?

A. Remove the .man extension from the user profile name.
B. Configure Folder Redirection by using the domain group policy.
C. Configure the user's documents library to include folders from network shares.
D. Add the .dat extension to the user profile name.

Correct Answer: B
Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
Folder Redirection allows administrators to redirect the path of a folder to a new location, which can be a folder on the local computer or a directory on a network file share. Users can then work with documents on a server as if the documents were based on a local drive, but are available to the user from any computer on the network. Folder Redirection can be found under Windows Settings in the console tree by editing domain-based Group Policy via the Group Policy Management Console (GPMC).

Incorrect Answers:
A: A super mandatory profile is a roaming profile in which the profile path ends in .man. Removing the .man extension will create a roaming profile, which will not solve the problem.
C: A super mandatory profile prevents users from saving any changes to their profile, which includes the user's documents library.
D: A super mandatory profile is a roaming profile in which the profile path ends in .man. Adding the .dat extension will result in an error.

References:
https://technet.microsoft.com/en-gb/library/cc732275.aspx
http://windowsitpro.com/systems-management/inside-user-profiles

QUESTION 21
You have a client Windows 10 Enterprise computer. The computer is joined to an Active Directory domain. The computer does not have a Trusted Platform Module (TPM) chip installed.

You need to configure BitLocker Drive Encryption (BitLocker) on the operating system drive.

Which Group Policy object (GPO) setting should you configure?

A. Allow access to BitLocker-protected fixed data drives from earlier version of Windows.
B. Require additional authentication at startup.
C. Allow network unlock at startup.
D. Configure use of hardware-based encryption for operating system drives.

Correct Answer: B
Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
To make use of BitLocker on a drive without TPM, you should run the gpedit.msc command. You must then access the *Require additional authentication at startup* setting by navigating to *Computer Configuration\Administrative Templates\Windows Components\Bit Locker Drive Encryption\Operating System Drives* under Local Computer Policy. You can now enable the feature and tick the *Allow BitLocker without a compatible TPM checkbox*.

Incorrect Answers:
A: The *Allow access to BitLocker-protected fixed data drives from earlier version of Windows* policy setting is used to control whether access to drives is allowed via the BitLocker To Go Reader, and if the application is installed on the drive.
C: The *Allow network unlock at startup* policy allows clients running BitLocker to create the necessary network key protector during encryption.
D: The *Configure use of hardware-based encryption for operating system drives* policy controls how BitLocker reacts when encrypted drives are used as operating system drives

References:
http://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/
https://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_depopt4

QUESTION 22
You administer Windows 10 Enterprise desktop computers that are members of an Active Directory domain.

You want to create an archived copy of user profiles that are stored on the desktops. You create a standard domain user account to run a backup task.

You need to grant the backup task user account access to the user profiles.

What should you do?

A. Add the backup task account to the Remote Management Users group on a domain controller.
B. Add the backup task account to the Backup Operators group on every computer.
C. Add the backup task account to the Backup Operators group on a domain controller.
D. Set the backup task account as NTFS owner on all the profiles.

Correct Answer: B
Section: Configure storage
Explanation

Explanation/Reference:
Explanation:
The Local Backup Operators group can back up and restore files on a computer, regardless of any permission that protect those files.

Incorrect Answers:
A: The Remote Management Users group is normally used to allow users to manage servers via the Server Manager console.
C: Members of the Domain Backup Operators group will be able to back up all files and folders on all computers in the domain, not just the Windows 10 Enterprise desktop computers.
D: Setting the backup task account as NTFS owner on all the profiles will allow the backup task account to control how permissions are set on the NTFS volumes for those user profiles and to whom permissions are granted. You only need to grant the backup task user account access to the user profiles, not control over its permissions.

References:
https://technet.microsoft.com/en-us/library/cc771990.aspx
https://technet.microsoft.com/en-us/library/dn579255.aspx
https://technet.microsoft.com/en-us/library/cc779180(v=ws.10).aspx

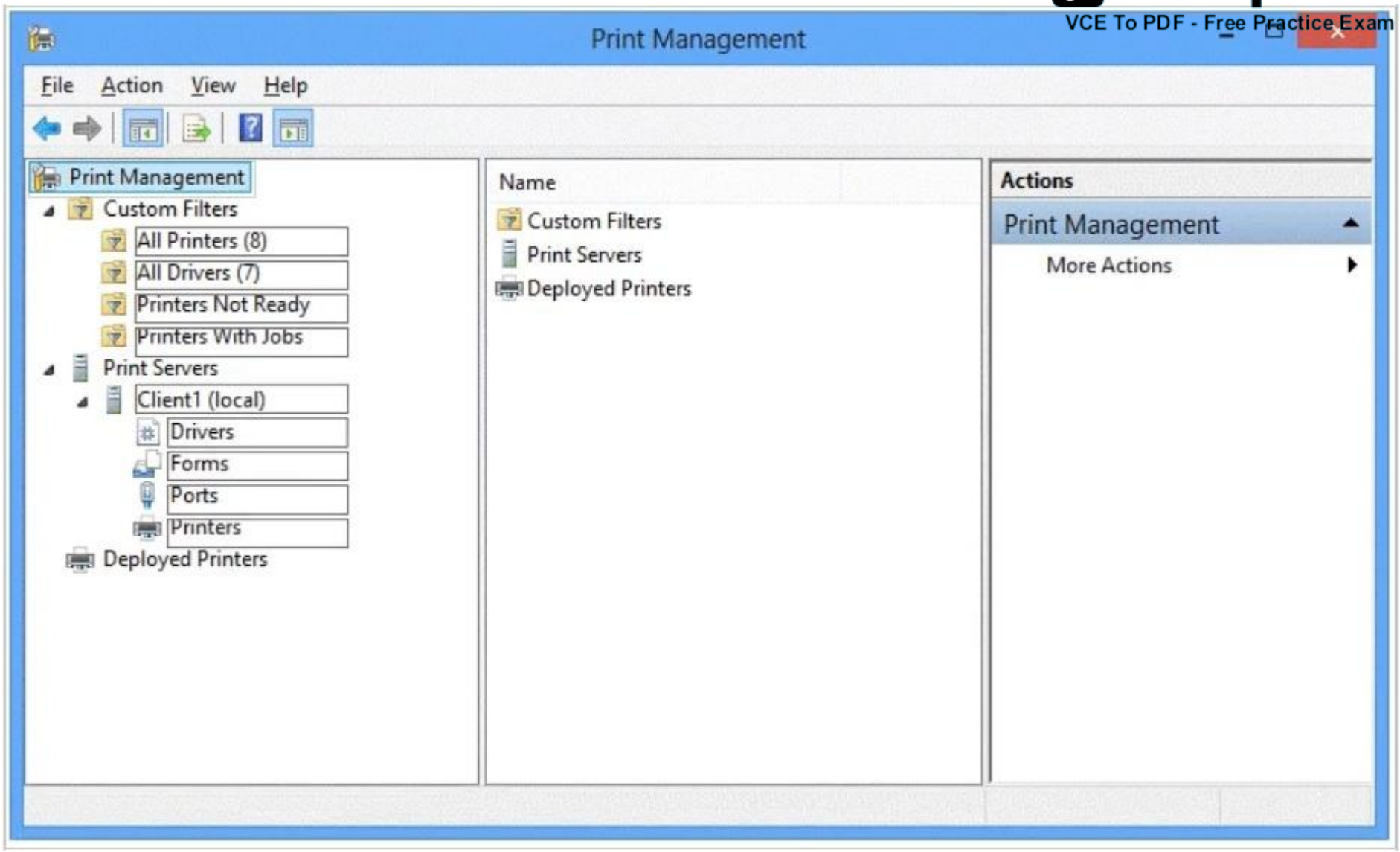
QUESTION 23
HOTSPOT
You administer Windows 10 Enterprise computers in your company network, including a computer named Wst1. Wst1 is configured with multiple shared printer queues.

Wst1 indicates hardware errors. You decide to migrate the printer queues from Wst1 to a new computer named Client1.

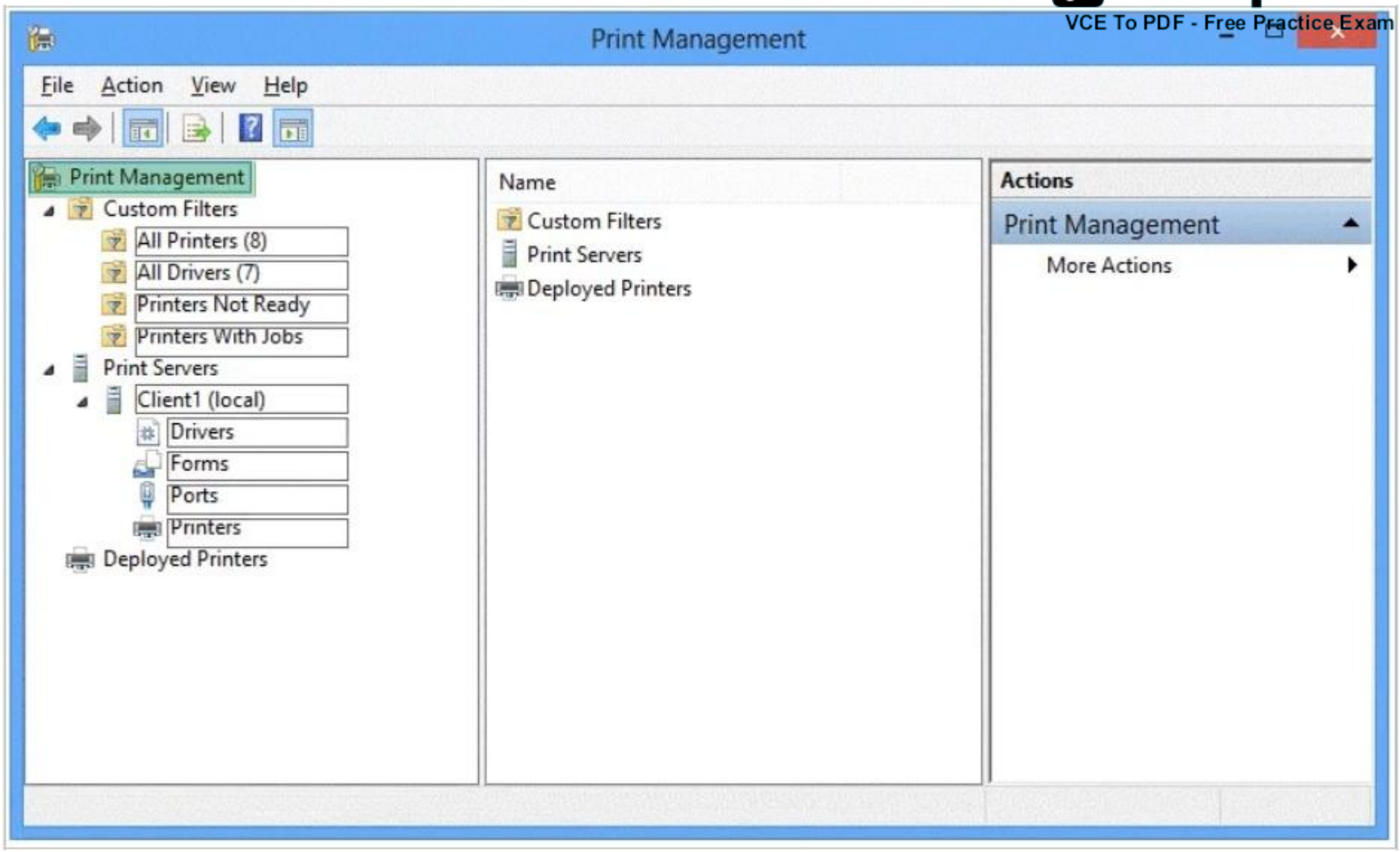
You export the printers on Wst1 to a file. You need to import printers from the file to Client1.

From the Print Management console, which Print Management node should you select? To answer, select the appropriate node in the answer area.

Hot Area:



Correct Answer:



Section: Manage data access and protection
Explanation

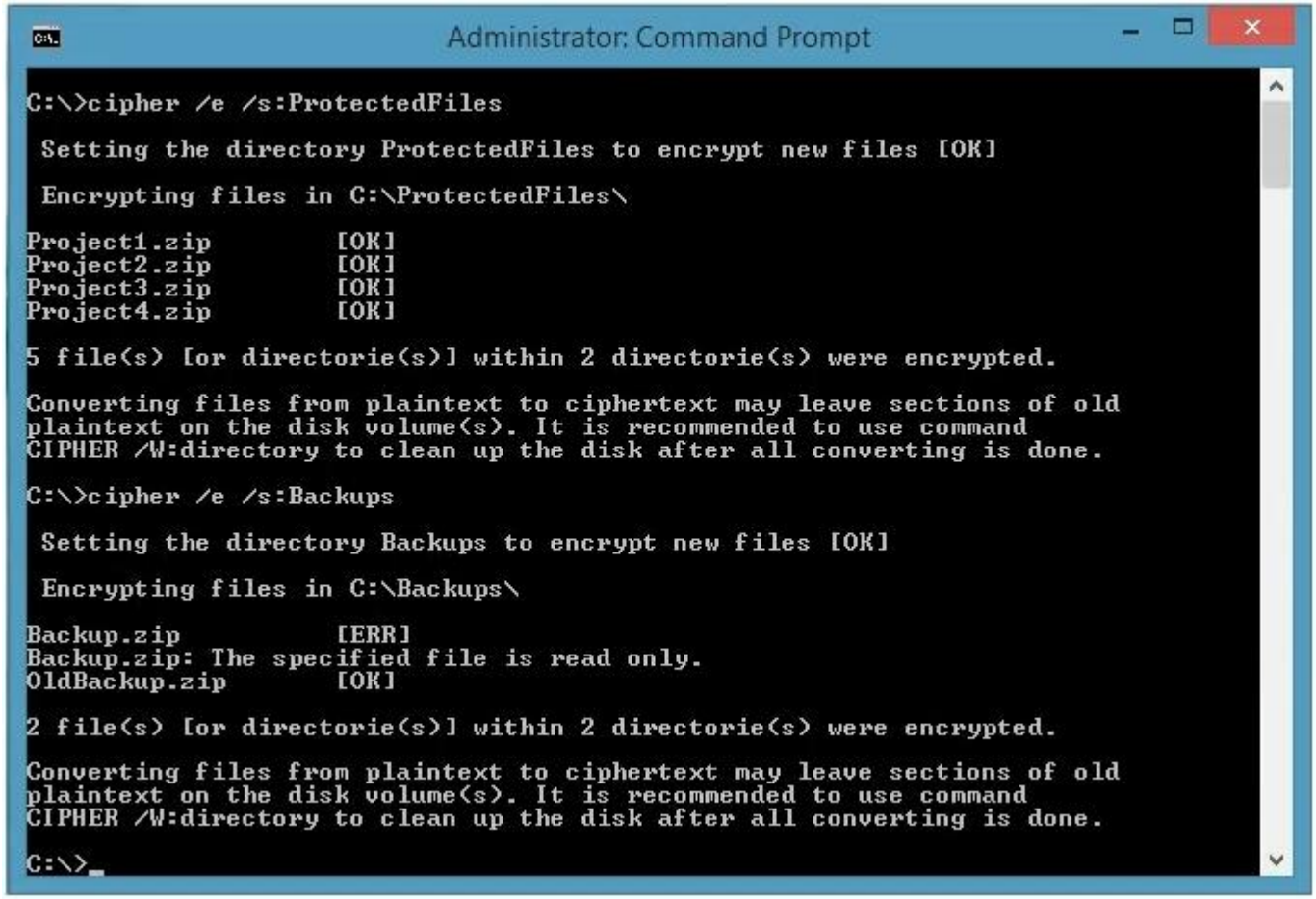
Explanation/Reference:

Explanation:
We have exported the printers on Wst1 to a file. To import printers from the file to Client1, we use the Printer Migration Wizard.
Right-click **Print Management**, and then click Migrate Printers to open the Printer Migration Wizard. Select Import printer queues and printer drivers from a file, and select the export file. Then complete the wizard.

References:
http://blogs.technet.com/b/canitpro/archive/2013/06/17/step-by-step-install-use-and-remove-windows-server-migration-tools.aspx

QUESTION 24
HOTSPOT
Your company upgrades a research and development department workstation to a Windows 10 Enterprise computer. Two of the workstation's folders need to be encrypted. The folders are named C:\ProtectedFiles and C:\Backups.

You attempt to encrypt the folders. The output is shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The attempt to encrypt the ProtectedFiles folder and files **[answer choice]**

- succeeded for all files and folders.
- succeeded for the files but not for the folder.
- will not finish until you run the command to clean up the disk.

The attempt to encrypt the Backups folder and files **[answer choice]**

- failed to encrypt the files and folders.
- encrypted the folder but not the files.
- failed to encrypt one of the files but encrypted the folder and the other file.

Correct Answer:

Answer Area

The attempt to encrypt the ProtectedFiles folder and files **[answer choice]**

- succeeded for all files and folders.
- succeeded for the files but not for the folder.
- will not finish until you run the command to clean up the disk.

The attempt to encrypt the Backups folder and files **[answer choice]**

- failed to encrypt the files and folders.
- encrypted the folder but not the files.
- failed to encrypt one of the files but encrypted the folder and the other file.

Section: Manage data access and protection
Explanation

Explanation/Reference:

Explanation:
We can see from the image below that all files and the ProtectedFiles folder were encrypted successfully (There are no errors and there is an [OK] message for each action).

```
C:\>cipher /e /s:ProtectedFiles

 Setting the directory ProtectedFiles to encrypt new files [OK]

 Encrypting files in C:\ProtectedFiles\

Project1.zip        [OK]
Project2.zip        [OK]
Project3.zip        [OK]
Project4.zip        [OK]

5 file(s) [or directorie(s)] within 2 directorie(s) were encrypted.
```

The image below shows that the folder was encrypted successfully (Setting the directory Backups to encrypt new files [OK]).
The file Backup.zip failed to encrypt because the file is read only. The other file, OldBackup.zip was encrypted successfully.

```
C:\>cipher /e /s:Backups

 Setting the directory Backups to encrypt new files [OK]

 Encrypting files in C:\Backups\

Backup.zip          [ERR]
Backup.zip: The specified file is read only.
OldBackup.zip       [OK]

2 file(s) [or directorie(s)] within 2 directorie(s) were encrypted.
```

References:
https://technet.microsoft.com/en-us/library/bb490878.aspx

QUESTION 25
DRAG DROP
You have a computer that runs Windows 10 Enterprise that contains the following folders:

You have a local user named User1. User1 has read and execute permission to Folder1.

You need to ensure that User1 can perform the following tasks.

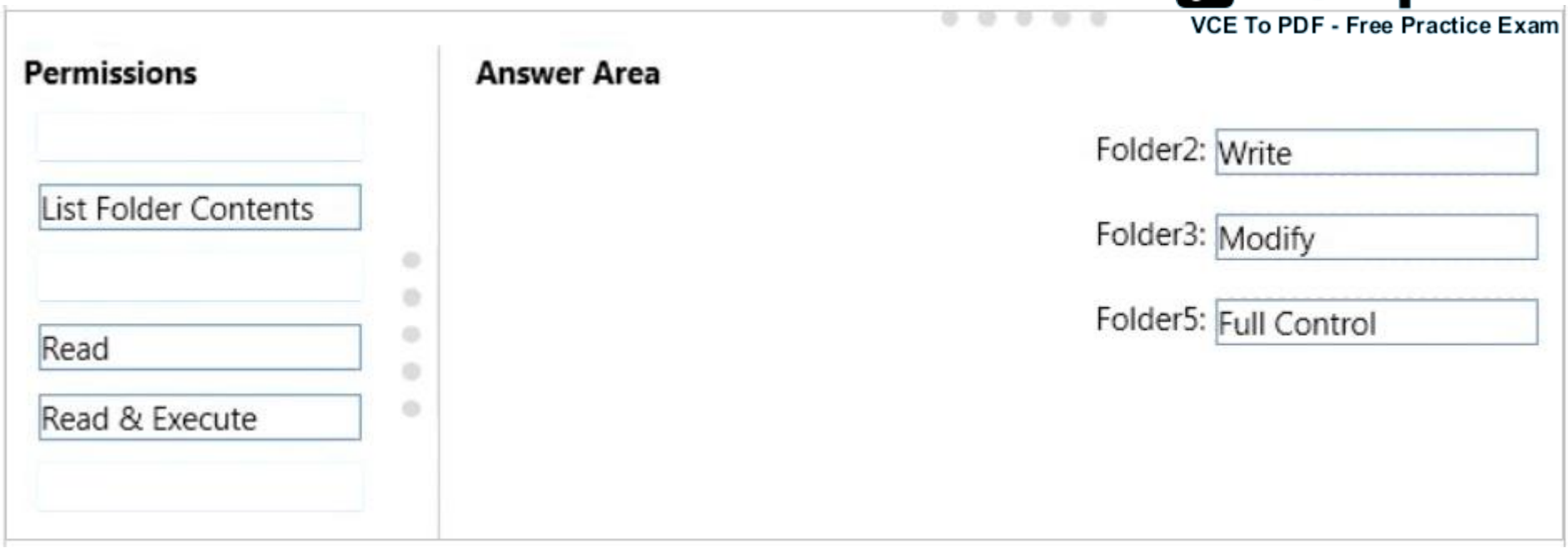
- Create new files in Folder2.
- Edit all files in Folder3.
- Change the permissions of files in Folder5.

The solution must use the principle of least privilege.

Which permissions should you assign to User1 on each folder? To answer, drag the appropriate permissions to the correct folders. Each permission 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.

Select and Place:

Correct Answer:



Section: Manage data access and protection
Explanation

Explanation/Reference:
Explanation:
Advanced permissions are detailed permissions that are grouped together to create the standard permissions. The permissions in this question are standard permissions.
Folder2: To create new files in a folder, you need Write permission to the folder. The 'Write' standard permission includes the 'Create files / write data' advanced permission.
Folder3: To edit existing files in a folder, you need Modify permission.
Folder5: To change the permissions of files in a folder, you need the 'Change Permissions' advanced permission. The Change Permission advanced permission is in the 'Full Control' standard permission group. Therefore, the answer for Folder5 is Full Control.

References:
http://windows.microsoft.com/en-gb/windows/before-applying-permissions-file-folder#1TC=windows-7

QUESTION 26
You have a Windows 10 Enterprise computer.

The computer has a shared folder named C:\Marketing. The shared folder is on an NTFS volume.

The current NTFS and share permissions are configured as follows.

Group name	NTFS permission	Shared folder permission
Everyone	Read and Execute	Read
Marketing	Modify	Full Control

UserA is a member of both the Everyone group and the Marketing group. UserA must access C:\Marketing from across the network. You need to identify the effective permissions of UserA to the C:\Marketing folder.

What permission should you identify?

A. Full Control
B. Read and Execute
C. Read
D. Modify

Correct Answer: D
Section: Manage data access and protection
Explanation

Explanation/Reference:
Explanation:
UserA is a member of both the Everyone group and the Marketing group and UserA must access C:\Marketing from across the network.
When accessing a file locally, you combine the NTFS permissions granted to your account either directly or by way of group membership. The 'least' restrictive permission is then the permission that applies.
In this question, the NTFS permission is the least restrictive of Read/Execute and Modify… so Modify is the effective permission.
When accessing a folder or file across the network, you combine the effective NTFS permissions (Modify in this case) with the effective Share permissions granted to your account either directly or by way of group membership (Full Control in this case). The 'most' restrictive permission is then the permission that applies. Modify is more restrictive than Full Control so Modify is the effective permission.

Incorrect Answers:
A: The effective permission is Modify, not Full Control.
B: The effective permission is Modify, not Read and Execute.
C: The effective permission is Modify, not Read.

QUESTION 27
DRAG DROP
You have a desktop computer and a tablet that both run Windows 10 Enterprise.

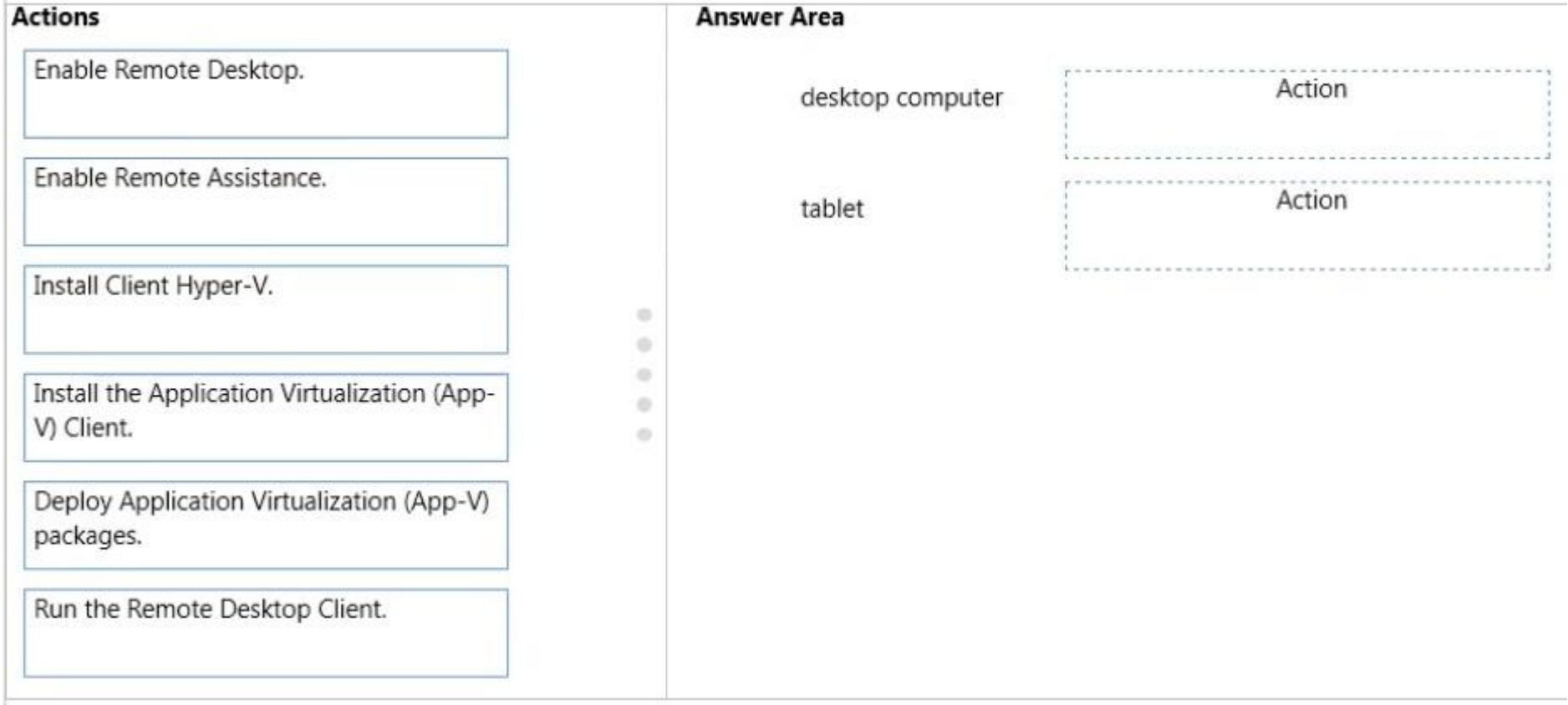
The desktop computer is located at your workplace and is a member of an Active Directory domain. The network contains an Application Virtualization (App-V) infrastructure. Several App-V applications are deployed to all desktop computers.

The tablet is located at your home and is a member of a workgroup. Both locations have Internet connectivity.

You need to be able to access all applications that run on the desktop computer from you tablet.

Which actions should you perform on each computer? To answer, drag the appropriate action to the correct computer. Each action 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.

Select and Place:



Correct Answer:

Section: Manage remote access
Explanation

Explanation/Reference:
Explanation:
You can connect to your work computer by using Remote Desktop. You first need to enable Remote Desktop on the work computer. You then run the Remote Desktop Client on the home computer to connect to the work computer.

With Remote Desktop Connection, you can connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet. For example, you can use all of your work computer's programs, files, and network resources from your home computer, and it's just like you're sitting in front of your computer at work.
To connect to a remote computer, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have permission to connect. For permission to connect, you must be on the list of users. Before you start a connection, it's a good idea to look up the name of the computer you're connecting to and to make

sure Remote Desktop connections are allowed through its firewall.

Incorrect Answers:
Remote assistance is not required. This enables remote users to connect to a computer for 'assistance'.
APP-V is not required. The App-V client is already running on the work computer and the App-V packages have already been deployed to the work computer.

QUESTION 28
A company has Windows 10 Enterprise client computers. The client computers are connected to a corporate private network. Users are currently unable to connect from their home computers to their work computers by using Remote Desktop.

You need to ensure that users can remotely connect to their office computers by using Remote Desktop. Users must not be able to access any other corporate network resource by using the local Windows installation from their home computers.

Which setting should you configure on the home computers?

A. Virtual Private Network connection
B. Remote Desktop local resources
C. DirectAccess connection
D. Remote Desktop Gateway IP address

Correct Answer: D
Section: Manage remote access
Explanation

Explanation/Reference:
Explanation:
The solution is to deploy Remote Desktop Gateway in the office. Remote users can then connect to their computers on the office network by using Remote Desktop client on their home computers configured with the IP address of the Remote Desktop Gateway.
Remote Desktop Gateway (RD Gateway) is a role service that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be Remote Desktop Session Host (RD Session Host) servers, RD Session Host servers running RemoteApp programs, or computers with Remote Desktop enabled.
RD Gateway uses the Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users on the Internet and the internal network resources on which their productivity applications run.
RD Gateway provides a comprehensive security configuration model that enables you to control access to specific internal network resources. RD Gateway provides a point-to-point RDP connection, rather than allowing remote users access to all internal network resources.

Incorrect Answers:
A: Virtual Private Network connections would enable remote access to the office network but this solution would not prevent users accessing other corporate network resources.
B: Remote Desktop local resources determine which local resources (printers, drives etc.) are available in a Remote Desktop connection. However, this solution makes no provision for actually connecting to the office network.

C: DirectAccess connections would enable remote access to the office network but this solution would not prevent users accessing other corporate network resources.

References:
https://technet.microsoft.com/en-gb/library/cc731150.aspx

QUESTION 29
You manage a network that includes Windows 10 Enterprise computers. All of the computers on the network are members of an Active Directory domain.

The company recently proposed a new security policy that prevents users from synchronizing applications settings, browsing history, favorites, and passwords from the computers with their Microsoft accounts.

You need to enforce these security policy requirements on the computers.

What should you do?

A. On the Group Policy Object, configure the **Accounts: Block Microsoft accounts** Group Policy setting to **Users can't add Microsoft accounts**.
B. On the Group Policy Object, configure the **Accounts: Block Microsoft accounts** Group Policy setting to **Users can't add or log on with Microsoft accounts**.
C. From each computer, navigate to Change Sync Settings and set the **Sync Your Settings** options for Apps, Browser, and Passwords to **Off.**
D. From each computer, navigate to Change Sync Settings and set the **Sync Your Setting**s option to **Off**.

Correct Answer: B
Section: Manage remote access
Explanation

Explanation/Reference:
Explanation:
The computers are members of a domain so the users should be using domain user accounts. We need to block the use of Microsoft accounts.
We could use the **Users can't add Microsoft accounts** setting which would mean that users will not be able to create new Microsoft accounts on a computer, switch a local account to a Microsoft account, or connect a domain account to a Microsoft account.
Alternatively, we can also deny the ability to log on to a domain computer with a Microsoft account (and sync computer settings) by using the**Users can't add or log on with Microsoft accounts.** This will ensure that the company policy is enforced.

Incorrect Answers:
A: If we only applied the **Users can't add Microsoft accounts** setting, users would still be able to log on with existing Microsoft accounts and sync their settings.
C: It is not necessary to change the sync settings on every client computer. Furthermore, this would not prevent the users from simply changing the sync settings back again. This solution does not 'enforce' the company policy.
D: It is not necessary to change the sync settings on every client computer. Furthermore, this would not prevent the users from simply changing the sync settings back again. This solution does not 'enforce' the company policy.

References:
https://technet.microsoft.com/en-us/library/jj966262.aspx

QUESTION 30
DRAG DROP
You manage 50 computers that run Windows 10 Enterprise. You have a Microsoft Azure RemoteApp deployment. The deployment consists of a hybrid collection named Collection1.

All computers have the Hyper-V feature installed and have a virtual machine that runs Windows 7.

You plan to install applications named App1 and App2 and make them available to all users. App1 is a 32-bit application. App2 is a 64-bit application.

You need to identify the installation method for each application. The solution needs to minimize the number of installations.

Which deployment method should you identify for each application? To answer, drag the appropriate deployment methods to the correct applications. Each deployment method 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.

NOTE: Each correct selection is worth one point.

Select and Place:

Correct Answer:

Section: Manage apps
Explanation

Explanation/Reference:
Explanation:
Azure RemoteApp supports streaming 32-bit or 64-bit Windows-based applications. Therefore, we can minimize the number of installations by installing the applications on Azure and making them available as Azure RemoteApps. This would mean one installation for App1 and one installation for App2.

Incorrect Answers:
The two other installation options (client Hyper-V and Local installation) would involve installing the application once for each computer: 50 installations for each app.

References:
https://azure.microsoft.com/en-gb/documentation/articles/remoteapp-appreqs/

QUESTION 31
You plan to deploy a Microsoft Azure RemoteApp collection by using a custom template image. The image will contain Microsoft Office 365 ProPlus apps.

You need to ensure that multiple users can run Office 365 ProPlus from the custom template image simultaneously.

What should you include in the configuration file?

A. <Property Name = “FORCEAPPSHUTDOWN” Value = “FALSE” />
B. <Product ID = “0365ProPlusRetail” />
C. <Property Name = “SharedComputerLicensing” Value = “1” />
D. <Property Name = “AUTOACTIVATE” Value = “1” />

Correct Answer: C
Section: Manage apps
Explanation

Explanation/Reference:
Explanation:
To make Microsoft Office 365 ProPlus apps available as RemoteApps, you need to enable Shared computer activation. You do this by including the following text in the configuration file:
<Property Name = “SharedComputerLicensing” Value = “1” />

Shared computer activation lets you to deploy Office 365 ProPlus to a computer in your organization that is accessed by multiple users. For example, several nurses at a hospital connect to the same remote server to use their applications or a group of workers share a computer at a factory.
The most common shared computer activation scenario is to deploy Office 365 ProPlus to shared computers by using Remote Desktop Services (RDS). By using RDS, multiple users can connect to the same remote computer at the same time. The users can each run Office 365 ProPlus programs, such as Word or Excel, at the same time on the remote computer.

Incorrect Answers:
A: This setting determines how click-to-run apps are shutdown when an app is open. This setting is not required to ensure that multiple users can run Office 365 ProPlus using RemoteApp.
B: This setting is used for the installation of Office 365. This setting is not required to ensure that multiple users can run Office 365 ProPlus using RemoteApp.
D: This setting determines how Office 365 is activated. This setting is not required to ensure that multiple users can run Office 365 ProPlus using RemoteApp.

References:
https://technet.microsoft.com/en-us/library/dn782858.aspx

QUESTION 32
HOTSPOT
You have a server that runs Windows Server 2012 R2 server named Server1. Server1 has Remote Desktop Services (RDS) installed. You create a session collection named Session1 and publish a RemoteApp in Session1.

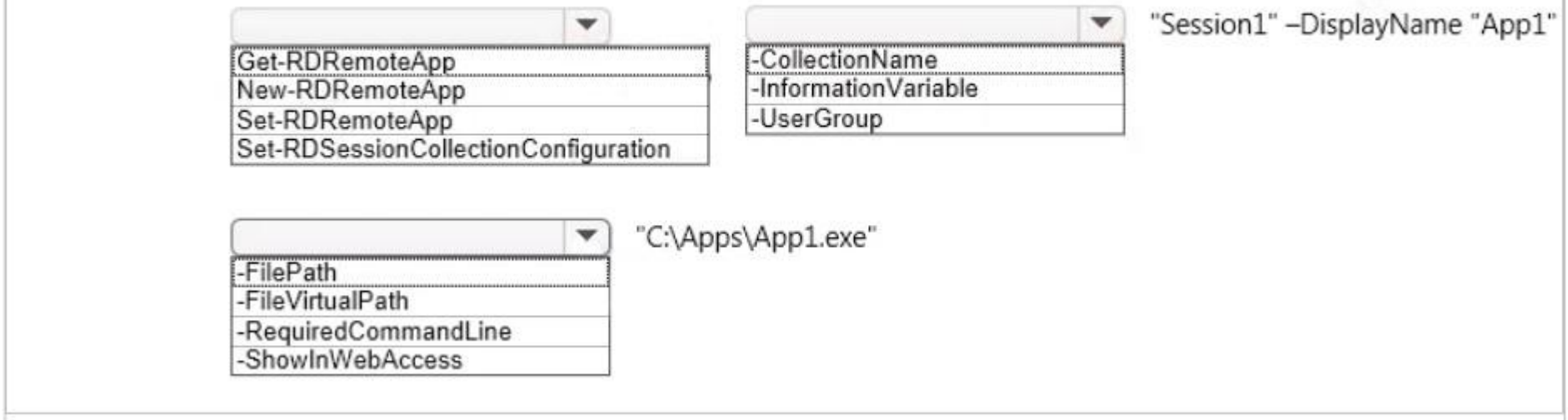
Server1 has an application named App1. The executable for App1 is C:\Apps\App1.exe.

You need to ensure that App1 is available as a RemoteApp in Session1.

What command should you run? To answer, select the appropriate options in the answer area.

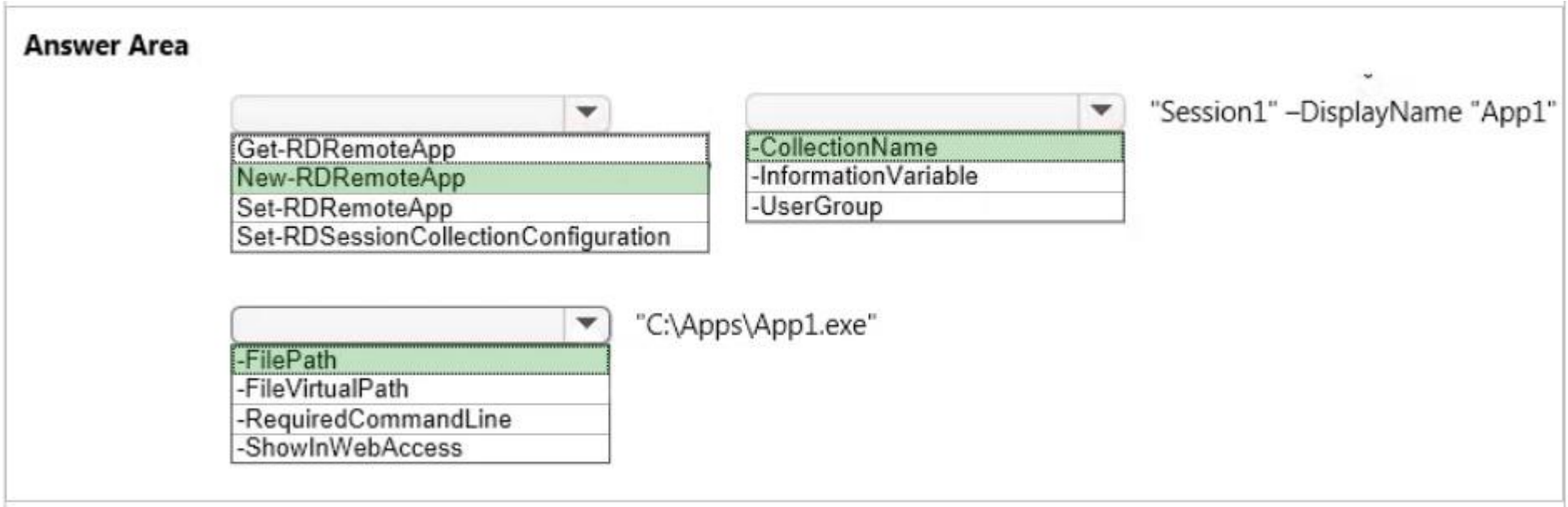
Hot Area:

Answer Area



Correct Answer:

Answer Area



Section: Manage apps
Explanation

Explanation/Reference:
Explanation:
We need to publish App1 as a RemoteApp. We do this with the New-RDRemoteApp cmdlet.
The –CollectionName parameter allows us to specify the session as “Session1”. The display name for the App1 will be “App1”.
The –FilePath parameter allows us to specify the path to the executable for App1.

Incorrect Answers:
Get-RDRemoteApp just retrieves information about existing RemoteApps.
Set-RDRemoteApp is used to reconfigure an existing RemoteApp. This question does not ask us to reconfigure the existing RemoteApp; it asks us to make App1 available as (another) RemoteApp.
Set-RDSessionCollectionConfiguration is used to modify a session collection. It is not used to deploy a RemoteApp to a session collection.

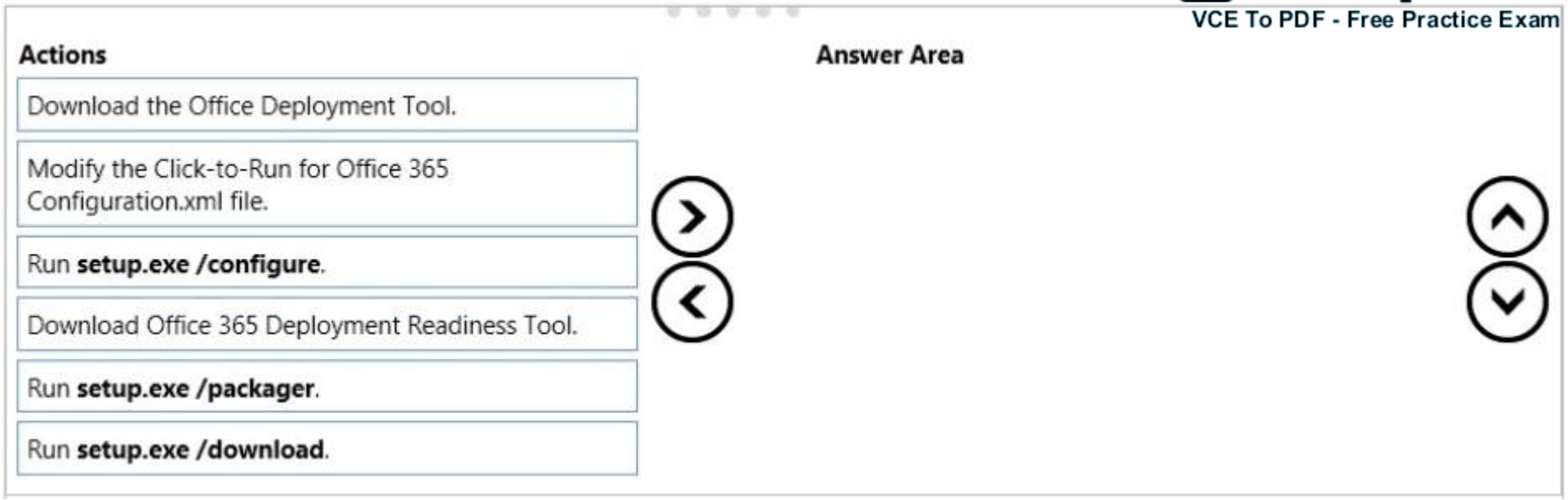
References:
https://technet.microsoft.com/en-us/library/jj215450.aspx

QUESTION 33
DRAG DROP
You plan to deploy a Microsoft Azure RemoteApp collection by using a custom template image. The image will contain Microsoft Word and Excel Office 365 ProPlus programs.

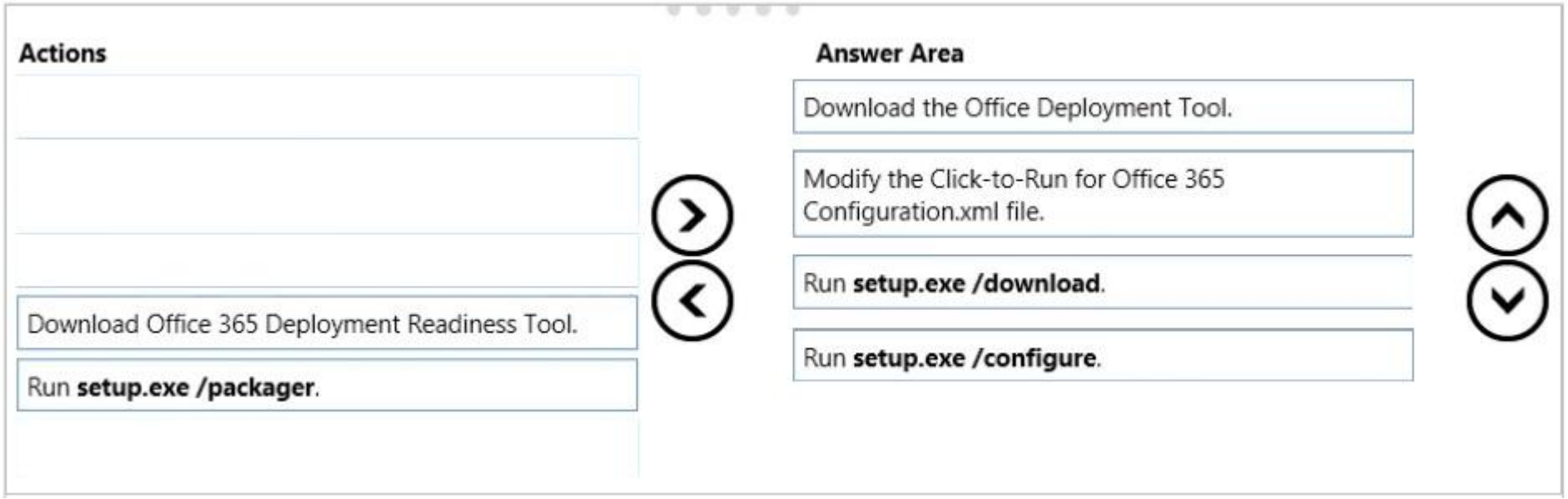
You need to install the Word and Excel programs. The solution must minimize the amount of Internet traffic used during installation.

Which four 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.

Select and Place:



Correct Answer:



Section: Manage apps
Explanation

Explanation/Reference:
Explanation:
The first step is to download the Office Deployment Tool.
You then need to modify the configuration file. This will be used to specify the installation options for Word and Excel.
You then run Setup.exe from the Office Deployment Tool with the /download option to download the required software based on the options in the configuration file.
The final step is to install Word and Excel by running Setup.exe from the Office Deployment Tool with the /configure option to install the required software based on the options in the configuration file.

Incorrect Answers:
You do not need the Office 365 Deployment Readiness Tool. This is used to check if your environment can support Office 365.
Setup.exe with the /packager option is used to create App-V packages. We are not using App-V in this question.

References:
http://blogs.technet.com/b/odsupport/archive/2014/07/11/using-the-office-deployment-tool.aspx
https://technet.microsoft.com/library/Dn782858.aspx

QUESTION 34
You are a system administrator for a department that has Windows 10 Enterprise computers in a domain configuration.

You deploy an application to all computers in the domain.

You need to use group policy to restrict certain groups from running the application.

What should you do?

A. Set up DirectAccess.
B. Configure AppLocker.
C. Disable BitLocker.
D. Run the User State Management Tool.

Correct Answer: B
Section: Manage apps
Explanation

Explanation/Reference:
Explanation:
AppLocker is a feature in Windows Server 2012, Windows Server 2008 R2, Windows 8, and Windows 7 that advances the functionality of the Software Restriction Policies feature. AppLocker contains new capabilities and extensions that reduce administrative overhead and help administrators control

how users can access and use files, such as executable files, scripts, Windows Installer files, and DLLs.
AppLocker rules can be applied to security groups. We can use a group policy to apply AppLocker rules to the security groups to prevent them from running the application.

Incorrect Answers:
A: DirectAccess is a remote access solution that enables remote access to company resources. It cannot be used to prevent members of security groups from running an application.
C: BitLocker is used to encrypt data. It cannot be used to prevent members of security groups from running an application.
D: The User State Management Tool is used for managing user profiles. It cannot be used to prevent members of security groups from running an application.

References:
https://technet.microsoft.com/en-us/library/ee619725(v=ws.10).aspx#BKMK_WhatRruleConditions

QUESTION 35
You support desktop computers and tablets that run Windows 8 Enterprise. All of the computers are able to connect to your company network from the Internet by using DirectAccess.

Your company wants to deploy a new application to the tablets. The deployment solution must meet the following requirements:

- The application is able to access files stored on an internal solid-state drive (SSD) on the tablets.
- The application is isolated from other applications.
- The application uses the least amount of disk space on the tablet.

You need to deploy the new application to the tablets.

What should you do?

A. Deploy the application as an Application Virtualization (App-V) package. Install the App-V 4.6 client on the tablets.
B. Deploy the application as a published application on the Remote Desktop server. Create a Remote Desktop connection on the tablets.
C. Install the application on a local drive on the tablets.
D. Install the application in a Windows To Go workspace.
E. Install Hyper-V on tablets. Install the application on a virtual machine.
F. Publish the application to Windows Store.
G. Install the application within a separate Windows 8 installation in a virtual hard disk (VHD) file. Configure the tablets with dual boot.
H. Install the application within a separate Windows 8 installation in a VHDX file. Configure tablets with dual boot.

Correct Answer: B
Section: Manage apps
Explanation

Explanation/Reference:

Explanation:
Deploying the application as a published application on the Remote Desktop server will use no disk space on the tablets. Users will be able to access the application by using Remote Desktop Connections. This will also ensure that the application is isolated from other applications on the tablets.
We can use Remote Desktop Connection 'redirection' to ensure that the application is able to access files stored on an internal solid-state drive (SSD) on the tablets. Redirection enables access to local resources such as drives, printers etc. in a Remote Desktop Connection.

Incorrect Answers:
A: This solution does not minimize the disk space used on the tablets as the application will be downloaded to the tablets.
C: This solution does not minimize the disk space used on the tablets as the application will be installed on the tablets. This solution also does not provide the required isolation from other applications.
D: This solution does not provide the required access to files stored on the internal solid-state drive (SSD) on the tablets.
E: This solution does not minimize the disk space used on the tablets as disk space will be required for the virtual machine. This solution also does not provide the required access to files stored on the internal solid-state drive (SSD) on the tablets.
F: This solution does not minimize the disk space used on the tablets as the application will need to be downloaded and installed on the tablets.
G: This solution does not minimize the disk space used on the tablets as disk space will be required for the VHD.
H: This solution does not minimize the disk space used on the tablets as disk space will be required for the VHDX.

References:
https://azure.microsoft.com/en-gb/documentation/articles/remoteapp-redirection/