

## 70-697 Configuring windows Devices Aug 2016 Drake

Number: 70-697  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1.0



### **Manage identity (13%)**

#### **Support Windows Store and cloud apps**

Install and manage software by using Microsoft Office 365 and Windows Store apps, sideload apps by using Microsoft Intune, sideload apps into online and offline images, deeplink apps by using Microsoft Intune, integrate Microsoft account including personalization settings

#### **Support authentication and authorization**

Identifying and resolving issues related to the following: Multi-factor authentication including certificates, Microsoft Passport, virtual smart cards, picture passwords, and biometrics; workgroup vs. domain, Homegroup, computer and user authentication including secure channel, account policies, credential caching, and Credential Manager; local account vs. Microsoft account; Workplace Join; Configuring Windows Hello

### **Plan desktop and device deployment (13%)**

#### **Migrate and configure user data**

Migrate user profiles; configure folder location; configure profiles including profile version, local, roaming, and mandatory

#### **Configure Hyper-V**

Create and configure virtual machines including integration services, create and manage checkpoints, create and configure virtual switches, create and configure virtual disks, move a virtual machine's storage

#### **Configure mobility options**

Configure offline file policies, configure power policies, configure Windows To Go, configure sync options, configure Wi-Fi direct, files, powercfg, Sync Center

#### **Configure security for mobile devices**

Configure BitLocker, configure startup key storage

### **Plan and implement a Microsoft Intune device management solution (11%)**

#### **Support mobile devices**

Support mobile device policies including security policies, remote access, and remote wipe; support mobile access and data synchronization including Work Folders and Sync Center; support broadband connectivity including broadband tethering and metered networks; support Mobile Device Management by using Microsoft Intune, including Windows Phone, iOS, and Android

#### **Deploy software updates by using Microsoft Intune**

Use reports and In-Console Monitoring to identify required updates, approve or decline updates, configure automatic approval settings, configure deadlines for update installations, deploy thirdparty updates

#### **Manage devices with Microsoft Intune**

Provision user accounts, enroll devices, view and manage all managed devices, configure the Microsoft Intune subscriptions, configure the Microsoft

Intune connector site system role, manage user and computer groups, configure monitoring and alerts, manage policies, manage remote computers

### **Configure networking (11%)**

#### **Configure IP settings**

Configure name resolution, connect to a network, configure network locations

#### **Configure networking settings**

Connect to a wireless network, manage preferred wireless networks, configure network adapters, configure location-aware printing

#### **Configure and maintain network security**

Configure Windows Firewall, configure Windows Firewall with Advanced Security, configure connection security rules (IPsec), configure authenticated exceptions, configure network discovery

### **Configure storage (10%)**

#### **\* Support data storage**

Identifying and resolving issues related to the following: DFS client including caching settings, storage spaces including capacity and fault tolerance, OneDrive

#### **Support data security**

Identifying and resolving issues related to the following: Permissions including share, NTFS, and Dynamic Access Control (DAC); Encrypting File System (EFS) including Data Recovery Agent; access to removable media; BitLocker and BitLocker To Go including Data Recovery Agent and Microsoft BitLocker Administration and Monitoring (MBAM)

### **Manage data access and protection (11%)**

#### **\* Configure shared resources**

Configure shared folder permissions, configure HomeGroup settings, configure libraries, configure shared printers, configure OneDrive \* **Configure file and folder access**

Encrypt files and folders by using EFS, configure NTFS permissions, configure disk quotas, configure file access auditing Configure authentication and authorization

### **Manage remote access (10%)**

#### **Configure remote connections**

Configure remote authentication, configure Remote Desktop settings, configure VPN connections and authentication, enable VPN reconnect, configure broadband tethering

#### **Configure mobility options**

Configure offline file policies, configure power policies, configure Windows To Go, configure sync options, configure Wi-Fi direct

### **Manage apps (11%)**

#### **Deploy and manage Azure RemoteApp**

Configure RemoteApp and Desktop Connections settings, configure Group Policy Objects (GPOs) for signed packages, subscribe to the Azure RemoteApp and Desktop Connections feeds, export and import Azure RemoteApp configurations, support iOS and Android, configure remote desktop web access for Azure RemoteApp distribution

#### **Support desktop apps**

The following support considerations including: Desktop app compatibility using Application Compatibility Toolkit (ACT) including shims and compatibility database; desktop application coexistence using Hyper-V, Azure RemoteApp, and App-V; installation and configuration of User Experience Virtualization (UE-V); deploy desktop apps by using Microsoft Intune

**Manage updates and recovery (10%)****Configure system recovery**

Configure a recovery drive, configure system restore, perform a refresh or recycle, perform a driver rollback, configure restore points

**Configure file recovery**

Restore previous versions of files and folders, configure File History, recover files from OneDrive

**Configure and manage updates**

## Exam A

### QUESTION 1

You administer a Windows 10 Enterprise computer that runs Hyper-V. The computer hosts a virtual machine with multiple snapshots. The virtual machine uses one virtual CPU and 512 MB of RAM.

You discover that the virtual machine pauses automatically and displays the state as paused-critical. You need to identify the component that is causing the error. Which component should you identify?

- A. no virtual switch defined
- B. insufficient memory
- C. insufficient hard disk space
- D. insufficient number of virtual processors

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

In this question, the VM has "multiple snapshots" which would use up a lot of disk space. Virtual machines will go into the "Paused-Critical" state in Hyper-V if the free space on the drive that contains the snapshots goes below 200MB.

One thing that often trips people up is if they have their virtual hard disks configured on one drive - but have left their snapshot files stored on the system drive. Once a virtual machine snapshot has been taken - the base virtual hard disk stops expanding and the snapshot file stores new data that is written to the disk - so it is critical that there is enough space in the snapshot storage location.

Incorrect Answers:

A: No virtual switch being defined would not cause the Pause-Critical state.

B: Insufficient memory would not cause the Pause-Critical state.

D: An insufficient number of virtual processors would not cause the Pause-Critical state.

[http://blogs.msdn.com/b/virtual\\_pc\\_guy/archive/2009/04/22/why-is-my-virtual-machine-pausedcritical-hyper-v.aspx](http://blogs.msdn.com/b/virtual_pc_guy/archive/2009/04/22/why-is-my-virtual-machine-pausedcritical-hyper-v.aspx)

### QUESTION 2

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: (none)**

**Explanation**

**Explanation/Reference:**

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.

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

**QUESTION 3**

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: (none)**

**Explanation**

**Explanation/Reference:**

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 4

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.



```
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.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

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.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\>
```

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]

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

Correct Answer:

**Answer Area**

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

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

Section: (none)  
Explanation

**Explanation/Reference:**

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.
```

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

#### QUESTION 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 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:** (none)

**Explanation**

#### Explanation/Reference:

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.

<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 6

Drag and Drop Question

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:

Permissions	Answer Area
Full Control	Folder2: <input type="text" value="Permission"/>
List Folder Contents	Folder3: <input type="text" value="Permission"/>
Modify	Folder5: <input type="text" value="Permission"/>
Read	
Read & Execute	
Write	

**Correct Answer:**

Permissions	Answer Area
<input type="text"/>	Folder2: <input type="text" value="Write"/>
<input type="button" value="List Folder Contents"/>	Folder3: <input type="text" value="Modify"/>
<input type="text"/>	Folder5: <input type="text" value="Full Control"/>
<input type="text" value="Read"/>	
<input type="text" value="Read &amp; Execute"/>	

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

<http://windows.microsoft.com/en-gb/windows/before-applying-permissions-filefolder#1TC=windows-7>

**QUESTION 7**

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:** (none)

**Explanation**

**Explanation/Reference:**

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 8**

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:** (none)

**Explanation**

**Explanation/Reference:**

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.

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

## QUESTION 9

Drag and Drop Question

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:**

Actions	Answer Area
Enable Remote Desktop.	desktop computer
Enable Remote Assistance.	tablet
Install Client Hyper-V.	
Install the Application Virtualization (App-V) Client.	
Deploy Application Virtualization (App-V) packages.	
Run the Remote Desktop Client.	

**Correct Answer:**

Actions	Answer Area
	desktop computer
Enable Remote Assistance.	tablet
Install Client Hyper-V.	
Install the Application Virtualization (App-V) Client.	
Deploy Application Virtualization (App-V) packages.	

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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 10

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 Settings option to Off.

**Correct Answer: B**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

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

**QUESTION 11**

Drag and Drop Question

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: (none)

Explanation

**Explanation/Reference:**

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.

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



**QUESTION 12**

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: (none)**

**Explanation**

**Explanation/Reference:**

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

**QUESTION 13**

Hotspot Question

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**

Get-RDRemoteApp	-CollectionName	"Session1" -DisplayName "App1"
New-RDRemoteApp	-InformationVariable	
Set-RDRemoteApp	-UserGroup	
Set-RDSessionCollectionConfiguration		

-FilePath	"C:\Apps\App1.exe"
-FileVirtualPath	
-RequiredCommandLine	
-ShowInWebAccess	

**Correct Answer:**

**Answer Area**

Get-RDRemoteApp	-CollectionName	"Session1" -DisplayName "App1"
New-RDRemoteApp	-InformationVariable	
Set-RDRemoteApp	-UserGroup	
Set-RDSessionCollectionConfiguration		

-FilePath	"C:\Apps\App1.exe"
-FileVirtualPath	
-RequiredCommandLine	
-ShowInWebAccess	

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

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.

SetRDSessionCollectionConfiguration is used to modify a session collection. It is not used to deploy a RemoteApp to a session collection. <https://technet.microsoft.com/en-us/library/jj215450.aspx>

**QUESTION 14**

Drag and Drop Question

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:**

Actions		Answer Area
Download the Office Deployment Tool.		
Modify the Click-to-Run for Office 365 Configuration.xml file.		
Run <code>setup.exe /configure</code> .		
Download Office 365 Deployment Readiness Tool.		
Run <code>setup.exe /packager</code> .		
Run <code>setup.exe /download</code> .		

**Correct Answer:**

Actions		Answer Area
		Download the Office Deployment Tool.
		Modify the Click-to-Run for Office 365 Configuration.xml file.
		Run <code>setup.exe /download</code> .
Download Office 365 Deployment Readiness Tool.		Run <code>setup.exe /configure</code> .
Run <code>setup.exe /packager</code> .		

**Section: (none)**

**Explanation**

**Explanation/Reference:**

The first step is to download the Office Deployment Tool.

You then need to download 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.

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

#### QUESTION 15

You have a computer named Computer1 that runs Windows 10 Enterprise.

You need to identify the locations that you can select as a File History drive.

What are two possible locations? Each correct answer presents a complete solution?

- A. The operating system volume
- B. An unformatted partition
- C. a non-system volume
- D. a network share

**Correct Answer:** CD

**Section:** (none)

**Explanation**

#### Explanation/Reference:

You can use a non-system volume as a File History drive. This can be a volume on a hard drive in a computer, a Virtual Hard Drive (VHD) or an external USB drive.

You can also use a network share as a File History drive.

In the File History Control Panel item, you can click the "Select Drive" option. This will display a list of all detected drives that are suitable for use as the File History drive. Under the list of drives, there is a link "Add Network Location". You can click the link and browse to or enter the path to the network share.

Incorrect Answers:

A: You cannot use the operating system volume (usually the C: drive) as the File History drive.

B: The volume used for the File History drive must be a formatted volume.

<http://computerbeginnersguides.com/blog/2015/08/23/enable-file-history-backups-in-windows-10/>

#### QUESTION 16

You have a computer named Computer1 that runs Windows 10 Enterprise.

Computer1 is configured to receive Windows updates from the Internet.

If a user is logged on to Computer1, you need to prevent Computer1 from automatically restarting without the logged on user's consent after the installation of the Windows updates. What should you do?

- A. Enable the Defer upgrades setting.
- B. Edit the Automatic App Update scheduled task.
- C. Configure the Choose how updates are delivered setting.

D. Configure the Choose how updates are installed setting.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In the Choose how updates are installed setting, you can use the drop-down menu to choose an option:

Schedule a restart

Automatically restart

The Schedule a restart option will allow the user to choose when the computer is restarted. Of the answers given, this is the only way to prevent Computer1 from automatically restarting without the logged on user's consent after the installation of the Windows updates.

Incorrect Answers:

A: The Defer Upgrades setting delays feature upgrades for several months while allowing security updates through. It does not prevent a computer from automatically restarting without the logged on user's consent after the installation of the Windows updates.

B: The Automatic App Update scheduled task is for updating Windows Store Apps, not the operating system. Furthermore, there is no setting in the Automatic App Update scheduled task that can prevent a computer from automatically restarting without the logged on user's consent after the installation of updates.

C: The Choose how updates are delivered setting can be used to enable or disable peer-to-peer updates.

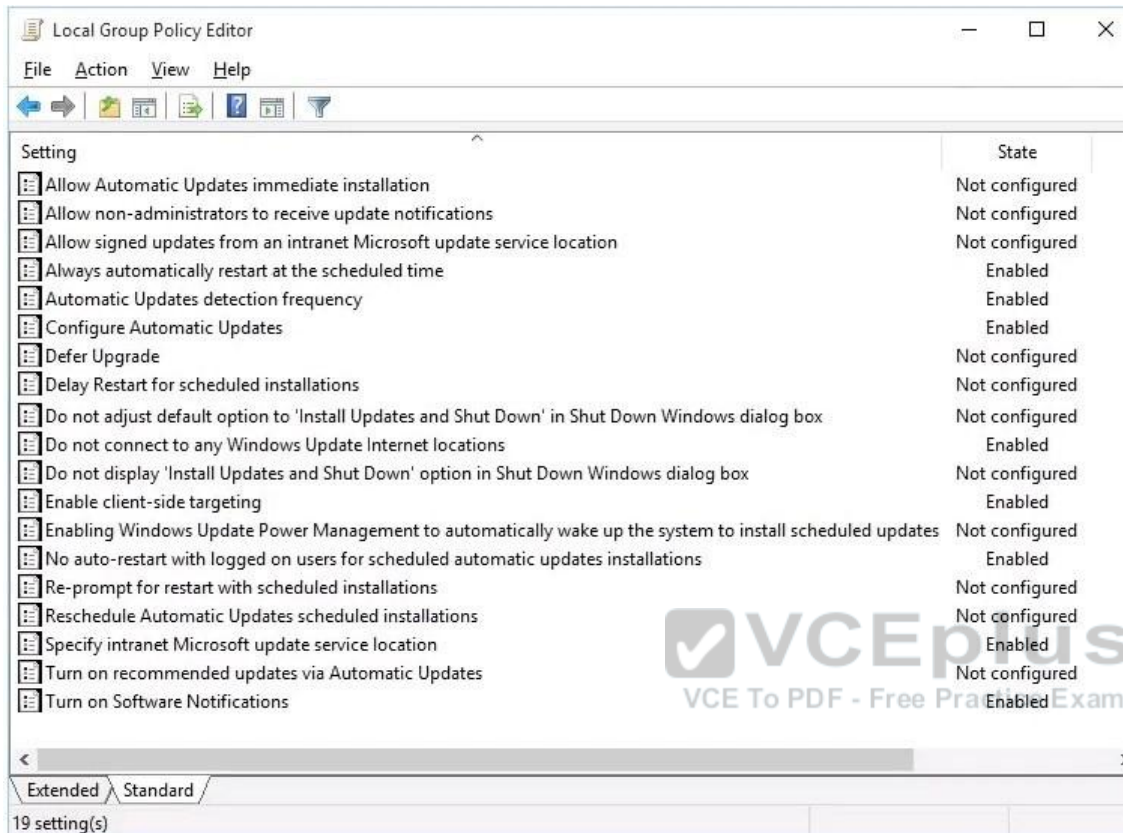
This is where one computer on the network downloads the updates from Microsoft and other computers on the network download the updates from that computer. This setting cannot prevent a computer from automatically restarting without the logged on user's consent after the installation of the Windows updates.

<http://windows.microsoft.com/en-gb/windows-10/getstarted-choose-how-updates-are-installed>

**QUESTION 17**

Hotspot Question

You have a computer that runs Windows 10 Enterprise that has a local group policy as shown in the following graphic.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

### Hot Area:

**Answer Area**

Windows updates will be downloaded from  
[answer choice].

If a user is logged into the computer and an update requires a restart, the computer will  
[answer choice].

Windows Server Update Services only  
Microsoft Windows Update servers only  
Windows Server Updates Services and Microsoft Windows Update servers

restart when the user signs out  
restart within a maximum delay of 3 hours  
restart within a maximum delay of 3 days

**Correct Answer:**

**Answer Area**

Windows updates will be downloaded from [answer choice].

If a user is logged into the computer and an update requires a restart, the computer will [answer choice].

Windows Server Update Services only
Microsoft Windows Update servers only
Windows Server Updates Services and Microsoft Windows Update servers

restart when the user signs out
restart within a maximum delay of 3 hours
restart within a maximum delay of 3 days

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Windows Updates will be downloaded from Windows Server Update Services only. This is determined by the "Specify Intranet Microsoft Update Service Location" setting and the "Do not connect to any Windows Update Internet locations" setting both being 'Enabled'.

In the "Specify Intranet Microsoft Update Service Location" setting, you can specify the name of the Windows Server Updates Services server.

If a user is logged into the computer and an update requires a restart, the computer will restart when the user signs out. This is determined by the "No auto-restart with logged on users for schedule automatic updates" setting being enabled. This group policy setting creates a registry key named NoAutoRebootWithLoggedOnUsers and sets the value of the key to 1 (enabled). With this setting enabled, you should be aware that the computer should be restarted at the earliest opportunity in order to complete the installation of the Windows Updates.

Incorrect Answers:

The "restart with a maximum delay of 3 hours or 3 days" answers are incorrect. The computer will never restart for as long as a user is logged in. The user could be logged in indefinitely and the computer will not restart.

### QUESTION 18

You use a Windows 8.1 tablet. The tablet receives Windows Update updates automatically from the Internet.

The tablet has Wi-Fi and is connected to a 3G mobile broadband Wi-Fi hot spot.

You need to minimize data usage while connected to this hot spot. What should you do?

- A. Turn on Airplane Mode.
- B. Disable File and Print Sharing for mobile broadband connections.
- C. Configure the interface metric of IP settings for Wi-Fi connection as 1.
- D. Edit the Inbound Rule of Windows Firewall, and then disable Internet Control Message Protocol (ICMP) traffic.
- E. Configure the broadband connection as a metered network.

**Correct Answer: E**

**Section: (none)**

**Explanation**



**Explanation/Reference:**

You can limit the bandwidth used by the broadband connection by configuring it as a metered network. A metered network is a network where data downloaded is 'metered' (measured) and you are charged for the amount of data downloaded.

Setting a connection as metered prevents Windows from automatically using bandwidth in a number of ways including the following:

Disables automatic downloading of Windows updates: Windows won't automatically download updates from Windows Update on metered Internet connections. You'll get a "Download" button you can click whenever you want to install updates.

Disables automatic downloading of app updates: The Windows Store won't automatically download updates for your installed "Store apps" on metered connections, either. Desktop apps like Chrome, Firefox, and others will continue updating themselves normally.

Tiles may not update: Microsoft says that the live tiles on your Start menu or Start screen "may" stop updating on a metered connection:

Incorrect Answers:

A: Turning on Airplane Mode would disable the Wi-Fi connection which would prevent you from connecting to the Internet. It would 'minimize data usage' but you would lose your connection to the Wi-Fi hotspot.

B: Disabling File and Print Sharing for mobile broadband connections is not best way to minimize data usage. It is very unlikely that data usage while connected to a 3G mobile broadband Wi-Fi hot spot is network sharing traffic.

C: Modifying the metric of the Wi-Fi connection will have no effect on the amount of data used. An interface metric is used to determine which interface will be used when there are multiple active connections.

D: Disabling Internet Control Message Protocol (ICMP) traffic on the firewall is not best way to minimize data usage. The data usage will not be caused by ICMP traffic. <http://www.howtogeek.com/226722/how-when-and-why-to-set-a-connection-as-metered-on-windows-10/>

**QUESTION 19**

You support Windows 10 Enterprise computers that are members of an Active Directory domain. Your company policy defines the list of approved Windows Store apps that are allowed for download and installation.

You have created a new AppLocker Packaged Apps policy to help enforce the company policy. You need to test the new AppLocker Packaged Apps policy before you implement it for the entire company.

What should you do?

- A. From Group Policy, enforce the new AppLocker policy in Audit Only mode.
- B. From Group Policy, run the Group Policy Results Wizard.
- C. From Group Policy, run the Group Policy Modeling Wizard.
- D. From PowerShell, run the Get-AppLockerPolicy -effective command to retrieve the AppLocker effective policy.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

You can test an AppLocker Packaged Apps policy by running it in audit mode.

After AppLocker rules are created within the rule collection, you can configure the enforcement setting to Enforce rules or Audit only.

When AppLocker policy enforcement is set to Enforce rules, rules are enforced for the rule collection and all events are audited. When AppLocker policy enforcement is set to Audit only, rules are only evaluated but all events generated from that evaluation are written to the AppLocker log.

Incorrect Answers:

B: The Group Policy Results Wizard is used to determine which group policy settings are applied to a user or computer object and the net results when multiple group policies are applied.

The Group Policy Results Wizard is not used to test an AppLocker Packaged Apps policy.

C: The Group Policy Modeling Wizard calculates the simulated net effect of group policies. Group Policy Modeling can also simulate such things as security group membership, WMI filter evaluation, and the effects of moving user or computer objects to a different Active Directory container. The Group Policy Modeling Wizard is not used to test an AppLocker Packaged Apps policy.

D: The Get-AppLockerPolicy -Effective command returns the effective AppLocker policy on the local computer. The effective policy is the merge of the local AppLocker policy and any applied domain policies on the local computer. The Get-AppLockerPolicy -effective command is not used to test an AppLocker Packaged Apps policy.

[https://technet.microsoft.com/en-us/library/ee791796\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee791796(v=ws.10).aspx)

### QUESTION 20

You support Windows 10 Enterprise computers.

Your company has started testing Application Virtualization (App-V) applications on several laptops. You discover that the App-V applications are available to users even when the laptops are offline. You need to ensure that the App-V applications are available to users only when they are connected to the company network.

What should you do?

- A. Change user permissions to the App-V applications.
- B. Disable the Disconnected operation mode.
- C. Configure mandatory profiles for laptop users.
- D. Reset the App-V client FileSystem cache.

**Correct Answer: B**

**Section: (none)**

**Explanation**



### Explanation/Reference:

Disconnected operation mode is enabled by default and allows App-V applications to be available to users even when the laptops are offline. We need to disable Disconnected operation mode to prevent offline access.

The disconnected operation mode settings --accessible by right-clicking the Application Virtualization node, selecting Properties, and clicking the Connectivity tab--enables the Application Virtualization Desktop Client or Client for Remote Desktop Services (formerly Terminal Services) to run applications that are stored in the file system cache of the client when the client is unable to connect to the Application Virtualization Management Server.

Incorrect Answers:

A: The ability to run an App-V application while the computer is offline is not determined by user permissions.

C: Mandatory profiles prevent users from making changes to their user profile. They do not prevent offline access to App-V applications.

D: When an App-V application is downloaded, it is stored in the App-V client FileSystem cache. Resetting the App-V client FileSystem cache will clear the contents of the cache and prevent the users from running the App-V application while their computers are offline. However, next time they connect to the network, they will download the App-V application again and will be able to run it offline again.

<https://technet.microsoft.com/en-gb/library/cc843712.aspx>

### QUESTION 21

Hotspot Question

You have an image of Windows 10 Enterprise named Image1. Image1 has version number 1.0.0.0 of a custom, line-of-business universal app named

App1.  
You deploy Image1 to Computer1 for a user named User1.  
You need to update App1 to version 1.0.0.1 on Computer1 for User1 only.  
What command should you run? To answer, select the appropriate options in the answer area.

**Hot Area:**

**Answer Area**

		App1_1.0.0.1
Add-AppxPackage	-dependancypath	
Add-AppxProvisionedPackage	-MainPackage	
Set-AppxProvisionedDataFile	-path	

**Correct Answer:**

**Answer Area**

		App1_1.0.0.1
Add-AppxPackage	-dependancypath	
Add-AppxProvisionedPackage	-MainPackage	
Set-AppxProvisionedDataFile	-path	

**Section: (none)**  
**Explanation**

**Explanation/Reference:**

In this question, we need to update App1 to version 1.0.0.1 on Computer1 "for User1 only". The Add-AppxPackage cmdlet adds a signed app package (.appx) to a user account. To update the application, we need to use the -path parameter to specify the path to the upgraded application.

Incorrect Answers:

add-provisionedappxpackage would make the app available to all users, not just User1 only. SetAppXProvisionedDataFile adds custom data into an app. It does not update it to a later version.

<https://technet.microsoft.com/en-us/library/hh856048.aspx> <http://blogs.technet.com/b/sunshine/archive/2014/03/22/updating-a-modern-app-in-windows-8.aspx>

**QUESTION 22**

Drag and Drop Question

You manage Microsoft Intune for a company named Contoso.

You have an administrative computer named Computer1 that runs Windows 10 Enterprise. You need to add a Windows Store universal app named App1 to the Company Portal Apps list for all users.

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:**

Actions	Answer Area
From the Microsoft Intune administration console, manage the deployment settings of App1.	
Log on to Computer1 by using your domain account.	
On Computer1, run the Add Software - Microsoft Intune Software Publisher wizard.	
From Windows Store, install App1 on Computer1.	
Log on to Computer1 by using the built-in Administrator account.	

**Correct Answer:**

Actions	Answer Area
	Log on to Computer1 by using your domain account.
	On Computer1, run the Add Software - Microsoft Intune Software Publisher wizard.
	From the Microsoft Intune administration console, manage the deployment settings of App1.
From Windows Store, install App1 on Computer1.	
Log on to Computer1 by using the built-in Administrator account.	

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Log into your computer using a domain account.

Run the Microsoft Intune Software Publisher wizard app.

Configure the deployment settings of the app. Incorrect Answers:

You do not need to install App1 on Computer1.

You need to log in with a domain account, not a local administrator account. <https://technet.microsoft.com/en-gb/library/dn646961.aspx>

[https://technet.microsoft.com/en-gb/library/dn646955.aspx#BKMK\\_SoftwareDistProcess](https://technet.microsoft.com/en-gb/library/dn646955.aspx#BKMK_SoftwareDistProcess)

### QUESTION 23

Your network contains an Active Directory domain named contoso.com.

The domain contains Windows 10 Enterprise client computers.

Your company has a subscription to Microsoft Office 365. Each user has a mailbox that is stored in Office 365 and a user account in the contoso.com domain. Each mailbox has two email addresses.

You need to add a third email address for each user.  
What should you do?

- A. From Active Directory Users and Computers, modify the E-mail attribute for each user.
- B. From Microsoft Azure Active Directory Module for Windows PowerShell, run the Set-Mailbox cmdlet.
- C. From Active Directory Domains and Trust, add a UPN suffix for each user.
- D. From the Office 365 portal, modify the Users settings of each user.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

We can use the Set-Mailbox cmdlet to modify the settings of existing mailboxes.

The EmailAddresses parameter specifies all the email addresses (proxy addresses) for the recipient, including the primary SMTP address. In on-premises Exchange organizations, the primary SMTP address and other proxy addresses are typically set by email address policies. However, you can use this parameter to configure other proxy addresses for the recipient. To add or remove specify proxy addresses without affecting other existing values, use the following syntax:

@{Add=" [<Type>]:<emailaddress1>" , "[<Type>]:<emailaddress2>" ...; Remove=" [<Type>]:<emailaddress2>" , "[<Type>]:<emailaddress2>" ...}.

Incorrect Answers:

A: You cannot use the E-mail attribute in Active Directory Users and Computers to add email addresses.

C: A UPN (User Principal Name) is used for authentication when you enter your credentials as username@domainname.com instead of: domainname\username. A UPN suffix is not an email address.

D: Users' email addresses are not configured in the User settings in the Office 365 portal.

[https://technet.microsoft.com/en-us/library/bb123981\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/bb123981(v=exchg.160).aspx)

**QUESTION 24**

Hotspot Question

You manage a Microsoft Azure RemoteApp deployment. The deployment consists of a cloud collection named CloudCollection1 and a hybrid collection named HybridCollection1. Both collections reside in a subscription named Subscription1. Subscription1 contains two Active Directory instances named AzureAD1 and AzureAD2. AzureAD1 is the associated directory of Subcsription1.

AzureAD1 is synchronized to an on-premises Active Directory forest named constoso.com.

Passwords are synchronized between AzureAD1 and the on-premises Active Directory. You have the following user accounts:

User Name	Account Type
User1	Microsoft account
User2	AzureAD1 account
User3	Contoso.com account

You need to identify to which collections each user can be assigned access.

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

Hot Area:

User1:  ▼

None
CloudCollection1 only
HybridCollection1 only
CloudCollection1 and HybridCollection1

User2:  ▼


None
CloudCollection1 only
HybridCollection1 only
CloudCollection1 and HybridCollection1

User3:  ▼


None
CloudCollection1 only
HybridCollection1 only
CloudCollection1 and HybridCollection1

Correct Answer:




User1:  

None
CloudCollection1 only
HybridCollection1 only
CloudCollection1 and HybridCollection1

User2:  

None
CloudCollection1 only
HybridCollection1 only
CloudCollection1 and HybridCollection1

User3:  

None
CloudCollection1 only
HybridCollection1 only
CloudCollection1 and HybridCollection1

**Section: (none)**

**Explanation**

**Explanation/Reference:**

A Microsoft account can only access a cloud collection.

An Azure Active Directory (Azure AD) account can access a cloud collection and it can access a hybrid collection if directory synchronization with password sync is deployed. An on-premise domain account that does not exist in any Azure Active Directory cannot access Azure cloud resources.  
<https://azure.microsoft.com/en-gb/documentation/articles/remoteapp-collections/>

**QUESTION 25**

Your Windows 10 Enterprise work computer is a member of an Active Directory domain.

You use your domain account to log on to the computer.

You use your Microsoft account to log on to a home laptop.

You want to access Windows 10 Enterprise apps from your work computer by using your Microsoft account.

You need to ensure that you are able to access the Windows 10 Enterprise apps on your work computer by logging on only once.

What should you do?



- A. Add the Microsoft account as a user on your work computer.
- B. Enable Remote Assistance on your home laptop.
- C. Connect your Microsoft account to your domain account on your work computer.
- D. Install SkyDrive for Windows on both your home laptop and your work computer.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

You can connect your Microsoft account to your domain account on your work computer. This will enable you to sign in to your work computer with your Microsoft account and access the same resources that you would access if you were logged in with your domain account.

When you connect your Microsoft account to your domain account, you can sync your settings and preferences between them. For example, if you use a domain account in the workplace, you can connect your Microsoft account to it and see the same desktop background, app settings, browser history and favorites, and other Microsoft account settings that you see on your home PC.

Incorrect Answers:

A: If you add the Microsoft account as a user on your work computer, this would be a separate account with no domain access. The account would not have access to the resources that you access with your domain account.

B: Enabling Remote Assistance on your home laptop would just enable you to send remote assistance invitations from your home laptop. It would have no effect on your work computer or your ability to log on to it.

D: SkyDrive is a cloud storage solution. You can save your files on SkyDrive and access them from any device. Installing SkyDrive will not enable you to log on to your work computer with your Microsoft account.

<http://windows.microsoft.com/en-gb/windows-8/connect-microsoft-domain-account>

**QUESTION 26**

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:** (none)

**Explanation**

**Explanation/Reference:**

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 ReceivePSSession cmdlet with the same parameter will not work.

[https://msdn.microsoft.com/en-us/virtualization/hyperv\\_on\\_windows/about/whats\\_new](https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/about/whats_new)

### QUESTION 27

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: (none)**

**Explanation**



### Explanation/Reference:

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

### QUESTION 28

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. 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:** (none)

**Explanation**

**Explanation/Reference:**

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.

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

**QUESTION 29**

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:** (none)

**Explanation**

**Explanation/Reference:**

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.

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

**QUESTION 30**

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:** (none)

**Explanation**

**Explanation/Reference:**

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.

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

### QUESTION 31

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: (none)**

**Explanation**



#### Explanation/Reference:

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

### QUESTION 32

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:** (none)

**Explanation**

**Explanation/Reference:**

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.

<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 33**

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:** (none)

**Explanation**

**Explanation/Reference:**

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.

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

### QUESTION 34

Drag and Drop Question

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: (none)**

**Explanation**

**Explanation/Reference:**

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

**QUESTION 35**

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: (none)**

**Explanation**

**Explanation/Reference:**

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 <http://blogs.technet.com/b/configmgrteam/archive/2013/03/20/configuring-configuration-managersp1-to-manage-mobile-devices-using-windows-intune.aspx>

### QUESTION 36

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.
- C. Set resiliency type to Parity.
- D. From Disk Management, create a new spanned volume.
- E. From Disk Management, create a new striped volume.

**Correct Answer: B**

**Section: (none)**

**Explanation**

### Explanation/Reference:

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

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

### QUESTION 37

Drag and Drop Question

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:**

Actions	Answer Area
Restore your data from the backup.	
From Storage Spaces, create a new storage pool. Set the Resiliency Type to <b>two-way mirror</b> .	
From Storage Spaces, create a new storage pool. Set the Resiliency Type to <b>parity</b> .	
From Storage Spaces, create a new storage pool. Set the Resiliency Type to <b>three-way mirror</b> .	
Back up the existing data on your original external hard drive.	
From Disk Management, create and format a new volume on the second external drive.	
From Disk Management, create a mirrored volume containing the two external drives.	

**Correct Answer:**

Actions	Answer Area
	Back up the existing data on your original external hard drive.
	From Storage Spaces, create a new storage pool. Set the Resiliency Type to <b>two-way mirror</b> .
From Storage Spaces, create a new storage pool. Set the Resiliency Type to <b>parity</b> .	Restore your data from the backup.
From Storage Spaces, create a new storage pool. Set the Resiliency Type to <b>three-way mirror</b> .	
From Disk Management, create and format a new volume on the second external drive.	
From Disk Management, create a mirrored volume containing the two external drives.	

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.  
<http://www.howtogeek.com/109380/how-to-use-windows-8s-storage-spaces-to-mirror-combinedrives/>

**QUESTION 38**

Hotspot Question

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 <b>san policy</b> option.	<input type="checkbox"/>	<input type="checkbox"/>
From DiskPart, configure the <b>attributes volume</b> option.	<input type="checkbox"/>	<input type="checkbox"/>
From DiskPart, configure the <b>attributes disk</b> option.	<input type="checkbox"/>	<input type="checkbox"/>
From fsutil, configure the <b>volume</b> option.	<input type="checkbox"/>	<input type="checkbox"/>
From fsutil, configure the <b>behavior</b> option.	<input type="checkbox"/>	<input type="checkbox"/>

**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 <b>san policy</b> option.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
From DiskPart, configure the <b>attributes volume</b> option.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From DiskPart, configure the <b>attributes disk</b> option.	<input type="checkbox"/>	<input type="checkbox"/>
From fsutil, configure the <b>volume</b> option.	<input type="checkbox"/>	<input type="checkbox"/>
From fsutil, configure the <b>behavior</b> option.	<input type="checkbox"/>	<input type="checkbox"/>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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. <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 39**

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: (none)**

## Explanation

### Explanation/Reference:

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.

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

## QUESTION 40

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: (none)**

## Explanation

### Explanation/Reference:

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

<http://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/> <https://technet.microsoft.com/en-us/library/>

jj679890.aspx#BKMK\_depot4

#### QUESTION 41

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: (none)**

**Explanation**

#### Explanation/Reference:

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.

<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](https://technet.microsoft.com/en-us/library/cc779180(v=ws.10).aspx)

#### QUESTION 42

Hotspot Question

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.

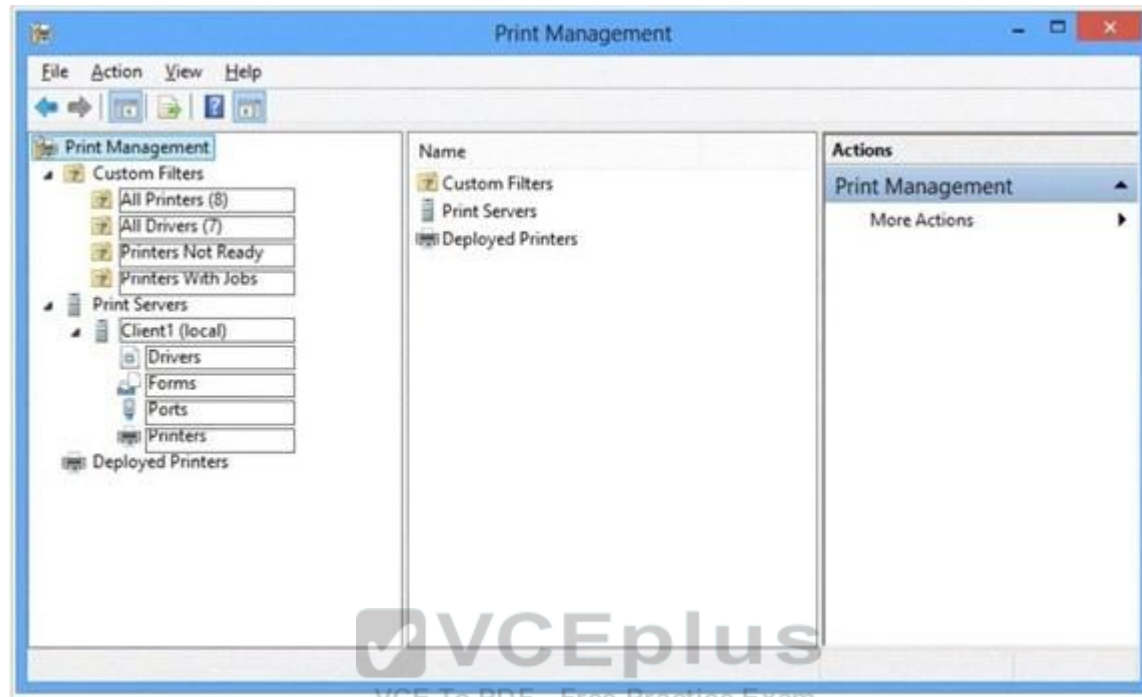
You export the printers on Wst1 to a file.

You need to import printers from the file to Client1.

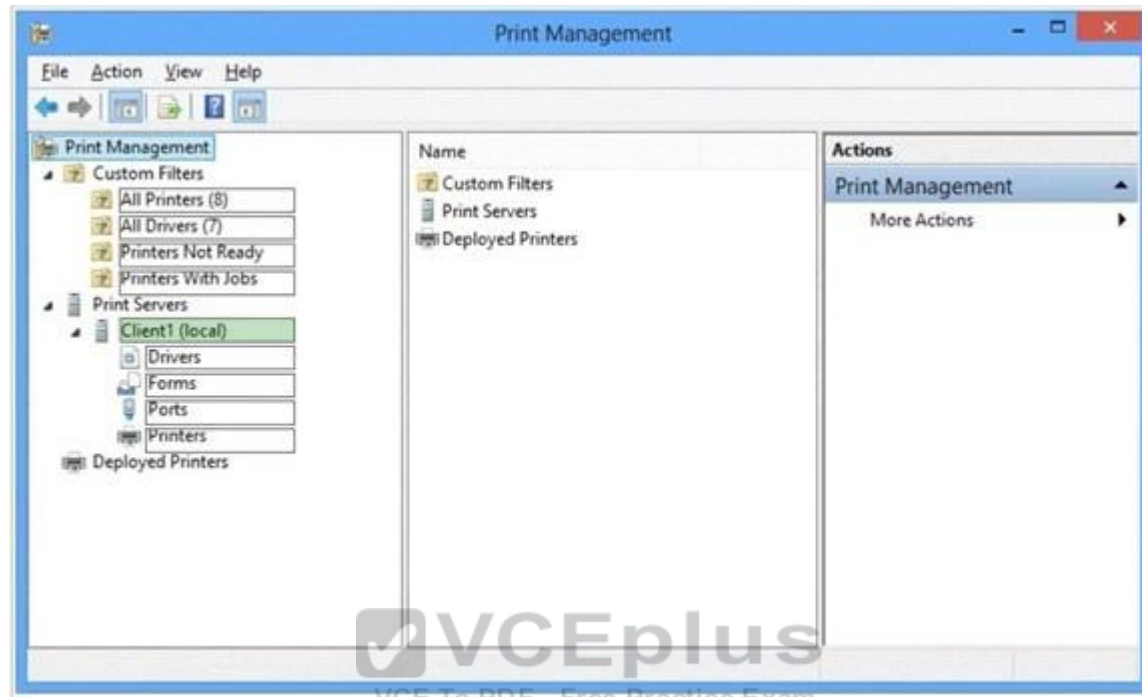
From the Print Management console, which Print Management node should you select? To answer, select the appropriate node in the answer area.

**Hot Area:**





**Correct Answer:**



**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

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: (none)**

## Explanation

### Explanation/Reference:

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. [https://technet.microsoft.com/en-us/library/ee619725\(v=ws.10\).aspx#BKMK\\_WhatRuleConditions](https://technet.microsoft.com/en-us/library/ee619725(v=ws.10).aspx#BKMK_WhatRuleConditions)

### QUESTION 44

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 solidstate 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: (none)**

**Explanation**

### Explanation/Reference:

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.

<https://azure.microsoft.com/en-gb/documentation/articles/remotepapp-redirection/>

#### QUESTION 45

You have a computer named Computer1 that runs Windows 10 Enterprise.

Computer1 is a member of an Active Directory domain named contoso.com.

You have a line-of-business universal app named App1.

App1 is developed internally.

You need to ensure that you can run App1 on Computer1.

The solution must meet the following requirements:

Minimize costs to deploy the app.

Minimize the attack surface on Computer1.

What should you do?



A. Have App1 certified by the Windows Store.

B. Sign App1 with a certificate issued by a third-party certificate authority.

C. From the Update & Security setting on Computer1, enable the Sideload apps setting.

D. Run the Add-AppxProvisionedPackage cmdlet.

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

To install the application, you need to 'Sideload' it. First you need to enable the Sideload apps setting.

LOB Windows Store apps that are not signed by the Windows Store can be sideloaded or added to a PC in the enterprise through scripts at runtime on a per-user basis. They can also be provisioned in an image by the enterprise so that the app is registered to each new user profile that's created on the PC. The requirements to sideload the app per-user or in the image are the same, but the Windows PowerShell cmdlets you use to add, get, and remove the apps are different. Before you can sideload LOB Windows Store apps that are not signed by the Windows Store, you will need to configure the PC.

Incorrect Answers:

A: We only need to install the app on one computer so it is not necessary to have App1 certified by the Windows Store. This solution does not minimize costs.

B: This solution does not minimize costs as you would have to pay for a third party certificate. D: The Add-AppxProvisionedPackage cmdlet adds an app package (.appx) that will install for each new user to a Windows image. However, to install an unsigned app, we need to enable sideloading first. Furthermore, the question states that 'you' need to ensure that you can run App1 on Computer1. The Add-AppxProvisionedPackage cmdlet would make the app available to all users, not just you.  
<https://msdn.microsoft.com/en-us/library/hh454036.aspx>

#### QUESTION 46

You have a computer named Computer1 that runs Windows 10 Enterprise.

You plan to install the most recent updates to Computer1.

You need to ensure that you can revert to the current state of Computer1 in the event that the computer becomes unresponsive after the update.

What should you include in your solution?

- A. The Reset this PC option from the Recovery section of the Settings app
- B. The Sync your settings options from the Accounts section of the Settings app
- C. The Backup and Restore (Windows 7) control panel item
- D. The Refresh your PC option from the PC Settings

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

The question states that you need to ensure that you can revert to the current state of Computer1.

The question does not specify what exactly the current state is in terms of software configuration but it would be safe to assume that Computer1 has Windows Store Apps installed, desktop applications installed and some previous Windows Updates installed.

The only way to recover the computer to its 'current' state is to perform a full backup of the computer before updating it. Then if the computer becomes unresponsive after the update, we can simply restore the backup to return the computer to its state at the time of the backup.

Incorrect Answers:

A: When you Reset your PC, all your applications and data will be removed. It is like doing a complete Windows reinstall and formatting your hard drive.

B: The Sync your settings options are used for syncing settings with a Microsoft account.

This does not return the computer to its current state.

D: When you Refresh your PC, your data, Windows Store Apps and application settings will be preserved.

However, all your desktops applications and any existing Windows Updates will be removed.

This does not return the computer to its current state.

<http://www.howtogeek.com/220986/how-to-use-all-of-windows-10%E2%80%99s-backup-and-recovery-tools/>

#### QUESTION 47

You administer a Windows 10 Enterprise computer.

The computer has File History turned on, and system protection turned on for drive C.

You accidentally delete a folder named Libraries\Customers by using the Shift+Delete keyboard shortcut.

You need to restore the most recent version of the folder to its original location. Which approach should you use to restore the folder?

- A. Recycle Bin
- B. the latest restore point
- C. File History
- D. a manually selected restore point

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

File History is similar to Previous Versions in previous versions of Windows. It takes regular backups of your data and saves them to a separate disk volume or external drive. When File History is enabled, it backs up all the system libraries and your custom libraries by default.

To restore a deleted folder, you can browse to the parent folder or library and select Restore Previous Versions. The Previous Versions tab will list the previous versions that can be restored to its original location or restored to an alternative location.

Incorrect Answers:

A: The question states that you deleted the folder by using the Shift+Delete keyboard shortcut. The Shift +Delete keyboard shortcut bypasses the Recycle Bin; the file or folder is permanently deleted without moving it to the Recycle Bin.

B: System Restore points do not back up user data. They are used for restoring the system and applications to a previous state.

You cannot use a System Restore point to recover a deleted folder.

D: System Restore points do not back up user data. They are used for restoring the system and applications to a previous state.

You cannot use a System Restore point to recover a deleted folder.

<https://www.winhelp.us/file-history-in-windows-8.html>

**QUESTION 48**

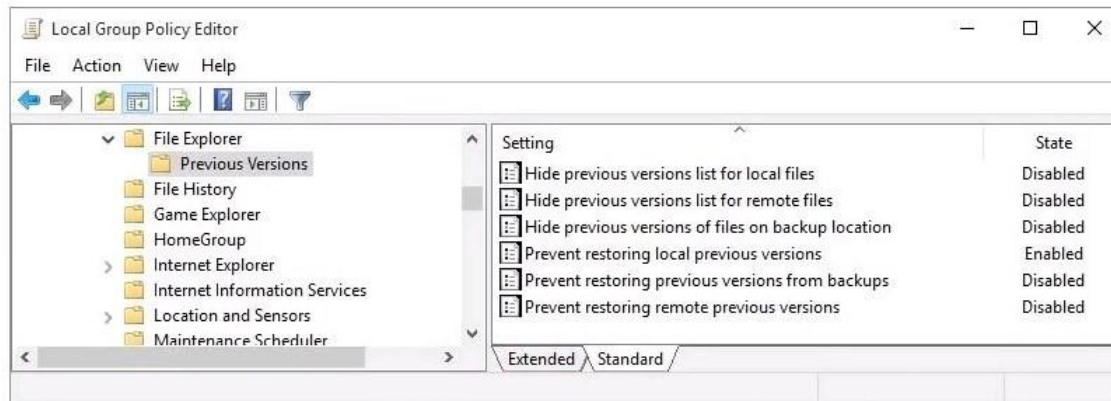
Hotspot Question

You have a standalone computer that runs Windows 10 Enterprise.

The computer is configured to automatically back up files by using File History.

The user of the computer uses the OneDrive desktop app to sync files.

The Previous Versions settings from the local group policy of the computer are shown in the following graphic.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

**Hot Area:**

**Answer Area**

If a user deletes a file from OneDrive by using File Explorer, the file [answer choice].

If a user deletes a file from a local drive by using File Explorer, the file [answer choice].

**Correct Answer:**

**Answer Area**

If a user deletes a file from OneDrive by using File Explorer, the file [answer choice].

If a user deletes a file from a local drive by using File Explorer, the file [answer choice].

**Section: (none)**



## Explanation

### Explanation/Reference:

When a file is deleted from the local OneDrive folder with File Explorer, the deletion is replicated to Onedrive.com and the file is moved to the OneDrive recycle bin. The deleted file can therefore be recovered from the Recycle Bin on Onedrive.com.

If a user deletes a file from a local drive by using File Explorer, the file cannot be restored. If the file is not in the OneDrive folder, it will not be a file that is synced to onedrive.com. We could use Previous Versions to restore the file but this is prevented by the Group Policy settings.

The "Prevent restoring local previous versions" -Enabled group policy setting would prevent the previous version from being restored.

<http://www.groovypost.com/howto/restore-deleted-files-local-onedrive-folder/>

### QUESTION 49

You have a Windows 10 Enterprise computer named Computer1.

Computer1 has File History enabled.

You create a folder named Folder1 in the root of the C: drive.

You need to ensure that Folder1 is protected by File History.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

- A. From File Explorer, include Folder1 in an existing library
- B. Modify the Advanced settings from the File History Control Panel item.
- C. From the Settings app, modify the Backup options.
- D. From File Explorer, modify the system attribute of Folder1.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

### Explanation/Reference:

By default, File History backs up all libraries. We can therefore ensure that Folder1 is protected by File History by adding the folder to a library.

The second method of ensuring that Folder1 is protected by File History is to add the folder location to File History. You do this by modifying the Backup options, not the File History Control Panel item as you might expect. In the Settings app, select Update & Security then Backup. Under the Back up using File History heading, select the Add a drive option.

Incorrect Answers:

B: The Advanced settings from the File History Control Panel item are for configuring settings such as backup frequency, the size of the offline cache and the amount of time that previous versions should be kept for. This is not where you can configure Folder1 to be protected by File History. D: You cannot configure Folder1 to be protected by File History by modifying the system attribute of the folder. System files are not automatically protected by File History.

<https://www.winhelp.us/file-history-in-windows-8.html>

### QUESTION 50

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:** (none)

**Explanation**

**Explanation/Reference:**

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.

[https://technet.microsoft.com/en-gb/library/cc740203\(v=ws.10\).aspx#BKMK\\_3](https://technet.microsoft.com/en-gb/library/cc740203(v=ws.10).aspx#BKMK_3)

**QUESTION 51**

Hotspot Question

You have a network that contains Window 10 Enterprise computers. The network configuration of one of the computers is shown in the following output.

iverter - VCE Exam Simulator - VCE Online - IT Certifications

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:**

**Answer Area**

The computer has obtained [answer choice] from a DHCP server.

The computer [answer choice] access the Internet.

only the IPv4 configuration
only the IPv6 configuration
the IPv4 and IPv6 configurations

will be unable to
will use 10.1.1.1 to
will use fe80::224:1ff:fedf:699f to

**Correct Answer:**

**Answer Area**

The computer has obtained [answer choice] from a DHCP server.

The computer [answer choice] access the Internet.

only the IPv4 configuration
only the IPv6 configuration
the IPv4 and IPv6 configurations

will be unable to
will use 10.1.1.1 to
will use fe80::224:1ff:fedf:699f to

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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.

```

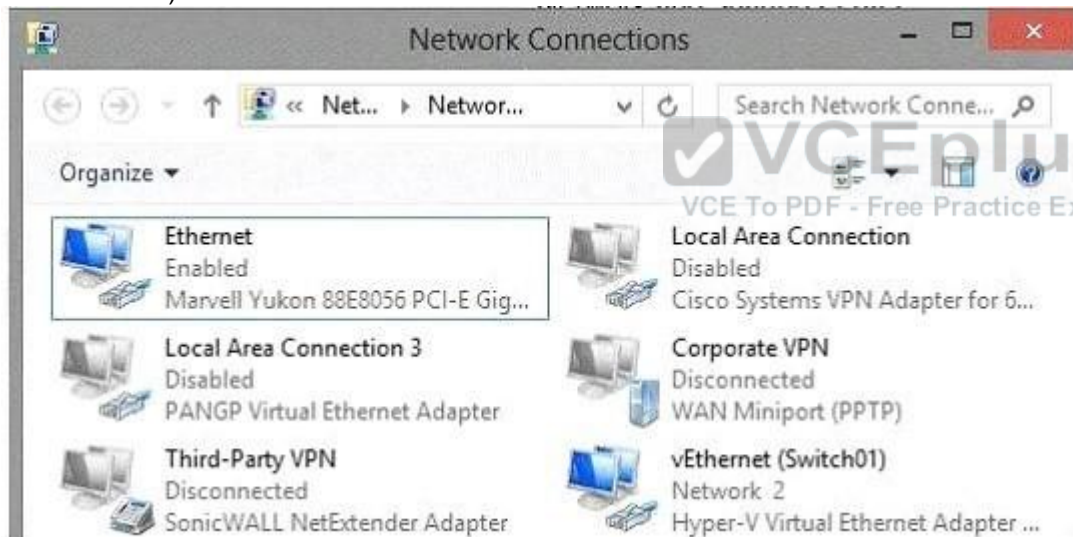
Link-local IPv6 Address . . . . . : fe80::c4e9:416b:3ebe:a6cb%13(Preferred)
  
```

The IP address of the Default Gateway is 10.1.1.1

## QUESTION 52

### Hotspot Question

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.)

**Advanced TCP/IP Settings**

IP Settings | DNS | WINS

**IP addresses**

IP address	Subnet mask
192.168.1.55	255.255.255.0

Add... Edit... Remove

**Default gateways:**

Gateway	Metric
192.168.1.1	Automatic

Add... Edit... Remove

☒ Automatic metric

Interface metric:

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.	<input type="radio"/>	<input type="radio"/>
The computer has a static IP address.	<input type="radio"/>	<input type="radio"/>
The computer is a Microsoft Hyper-V virtual machine.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area		
	Yes	No
The computer is a Microsoft Hyper-V host.	<input checked="" type="radio"/>	<input type="radio"/>
The computer has a static IP address.	<input checked="" type="radio"/>	<input type="radio"/>
The computer is a Microsoft Hyper-V virtual machine.	<input type="radio"/>	<input checked="" type="radio"/>

Section: (none)

Explanation

Explanation/Reference:

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 53

A company has client computers that run Windows 10. The client computer systems frequently use IPSec tunnels to securely transmit data. You need to configure the IPSec tunnels to use 256-bit encryption keys. Which encryption type should you use?

- A. 3DES
- B. DES
- C. RSA
- D. AES



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 54

You administer a group of 10 client computers that run Windows 10. The client computers are members of a local workgroup. Employees log on to the client computers by using their Microsoft accounts. The company plans to use Windows BitLocker Drive Encryption. You need to back up the BitLocker recovery key. Which two options can you use? (Each correct answer presents a complete solution. Choose two.)

- A. Save the recovery key to a file on the BitLocker-encrypted drive.
- B. Save the recovery key in the Credential Store.
- C. Save the recovery key to SkyDrive.

D. Print the recovery key.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

It's not possible to save a Bitlocker file into the same disk. Moreover, what would be the point to save recovery key on the drive, which is locked and you cannot access it without the key anyway.

#### QUESTION 55

You are using sysprep to prepare a system for imaging. You want to reset the security ID (SID) and clear the event logs. Which option should you use?

- A. /generalize
- B. /oobe
- C. /audit
- D. /unattend

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

Generalize prepares the Windows installation to be imaged.

If this option is specified, all unique system information is removed from the Windows installation. The security ID (SID) resets, any system restore points are cleared, and event logs are deleted. The next time the computer starts, the specialize configuration pass runs. A new security ID (SID) is created, and the clock for Windows activation resets, if the clock has not already been reset three times.

#### QUESTION 56

Group Policy is a set of rules which control the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications and users' settings in an Active Directory environment. In other words, Group Policy in part controls what users can and can't do on a computer system. Which one of these policies requires a reboot?

- A. Turn off Windows Defender
- B. Turn off Autoplay for non-volume devices
- C. Disable Active Desktop
- D. Turn off Data Execution Prevention for Explorer

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:**

You can Turn Off Windows Defender anytime (Uninstalling it is another thing!) without rebooting. A reboot is REQUIRED when turning off DEP for Explorer.

**QUESTION 57**

Which term is used to refer to installing apps directly to a device without going through the Windows Store?

- A. SQL Injection
- B. BranchCache
- C. DLL Hijack
- D. Sideload

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 58**

IPv6 has a vastly larger address space than IPv4. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT). Do you know how many more bits there are in an IPv4 address compared to an IPv6 address?

- A. 4 times more
- B. 6 times more
- C. Twice as many
- D. 8 times more

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:**

IPv4 addresses are 32 bit, IPv6 addresses are 128 bit.

**QUESTION 59**

You are using sysprep to prepare a system for imaging. You want to enable end users to customize their Windows operating system, create user accounts, name the computer, and other tasks. Which sysprep setting should you use?

- A. /oobe
- B. /audit
- C. /generalize
- D. /unattend

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 60

You have set up a new wireless network for one of your prestigious clients. The director wants to ensure that only certain designated wireless laptops can connect to the new network to prevent misuse. What do you need to do?

- A. Use MAC address control
- B. Use IPv4 address control
- C. Use WEP
- D. Use WPA



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification, and used in the Media Access Control protocol sub-layer. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number. It may also be known as an Ethernet Hardware Address (EHA), hardware address, adapter address, or physical address.

#### QUESTION 61

Drag and Drop Questions

You support desktop computers for a company named Fabrikam, Inc.

The computers are members of the Active Directory domain named fabrikam.com.

Fabrikam works with a supplier named Contoso, Ltd.

Each company has a public key infrastructure (PKI), and no public certificate authorities (CAs) are used. Fabrikam employees regularly use a Contoso website that is hosted on a server in the contoso.com domain.

The website requires SSL and mutual authentication.

You need to configure the computers to allow Fabrikam users to access the Contoso website without any warning prompts.

You also need to use the fewest certificates possible.

Which certificate or certificates should you use? (To answer, drag the appropriate certificate to the correct certificate store. Each certificate 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:**

Certificate	Certificate Store
contoso.com root certificate	trusted root authorities certificate store for the local computer account
Fabrikam root certificate	untrusted certificates store for the user's account
client (user) certificate issued by Contoso	personal certificate store for the local computer account
client (user) certificate issued by Fabrikam	personal certificate store for the user's account
no certificate required	

**Correct Answer:**

Certificate	Certificate Store
contoso.com root certificate	trusted root authorities certificate store for the local computer account
Fabrikam root certificate	untrusted certificates store for the user's account
client (user) certificate issued by Contoso	personal certificate store for the local computer account
client (user) certificate issued by Fabrikam	personal certificate store for the user's account
no certificate required	

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Note:

contoso.com provided the resources. contoso.com be the trusted root authorities store - No untrusted certificates

Not allow access to local computer account (just to user account)

user account access through client (user) certificate issued by Contoso

**QUESTION 62**

You administer computers that run Windows 8 Pro and are members of an Active Directory domain. The computers are encrypted with BitLocker and are configured to store BitLocker encryption passwords in Active Directory. A user reports that he has forgotten the BitLocker encryption password for volume E on his computer.

You need to provide the user a BitLocker recovery key to unlock the protected volume.

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

- A. Ask the user for his computer name.
- B. Ask the user to run the manage-bde-unlock E:-pw command.
- C. Ask the user for his logon name.
- D. Ask the user for a recovery key ID for the protected volume.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

(1) Saying a name does not verify you at all. You can easily find out the name of the owner if you have the access to the PC. For example, open Outlook or simply press Start to verify username. In such cases mobile phone call verification would be preferred, but it is not mentioned in the answers. (2) It is mentioned in the conditions, that some (NOT ONE) volumes on the computers are encrypted. This means you will have to find out which is locked. So you need recovery key ID. <http://www.concurrency.com/blog/enable-bitlocker-automatically-save-keys-to-active-directory/>

**QUESTION 63**

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### Create a Spanned Volume

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.

<http://technet.microsoft.com/en-us/library/cc772180.aspx> To create a spanned volume using the Windows interface

In Disk Management, right click the unallocated space on one of the dynamic disks where you want to create the spanned volume.

Click New Spanned Volume.

Follow the instructions on your screen. Using GPT Drives <http://msdn.microsoft.com/en-us/library/windows/hardware/gg463524.aspx> A GPT disk uses the GUID partition table (GPT) disk partitioning system.

A GPT disk offers these benefits:

Allows up to 128 primary partitions.

Master Boot Record (MBR) disks can support up to four primary partitions and an additional 124 partitions inside extended partitions.

Allows a much larger partition size-greater than 2 terabytes (TB), which is the limit for MBR disks. Provides greater reliability because of replication and cyclical redundancy check (CRC) protection of the partition table. Can be used as a storage volume on all x64-based platforms, including platforms running Windows XP Professional x64 Edition.

Starting with Windows Server 2003 SP1, GPT disks can also be used as a storage volume on x86based Windows platforms. Can be used as a boot volume on x64-based editions of Windows 7, Windows Vista, and Windows Server 2008.

Starting with Windows Server 2003 SP1, GPT disks can also be used as a boot volume on Itaniumbased systems.

Note: Windows only supports booting from a GPT disk on systems that contain Unified Extensible Firmware Interface (UEFI) boot firmware.

### QUESTION 64

A company has a main office located in Miami, and brach offices in Boston, Los Angeles and Portland.

The Office Networks are configured as described in the following table.

City	Network
Boston	10.30.0.0/24
Los Angeles	10.40.0.0/24
Miami	10.10.0.0/16
Portland	10.20.0.0/16

A management computer in the main office, named COMPUTER1, runs windows 8 and several third-party management applications.

Ensure that only users in the Boston office can connect to COMPUTER1 by using http.

Ensure that only users in the Los Angeles office can connect COMPUTER1 by using https

Ensure that only users in th Portland office can connect to COMPUTER1 by using FTP.

You are configuring access to COMPUTER1.

How should you configure windows firewall? (To answer, drag the appropriate elements to the correct location or locations in the answer area. Elements may be used once, more than once, or not at all. You ma need to drag the split bar between panes or scroll.)

**Select and Place:**



Source network		Answer Area		
10.10.0.0/16				
10.20.0.0/16				
10.30.0.0/24				
10.40.0.0/24				
Port number				
21				
22				
80				
443				
IP type				
TCP				
UDP				

**Correct Answer:**

Source network		Answer Area	
10.10.0.0/16			
10.20.0.0/16			
10.30.0.0/24			
10.40.0.0/24			
<b>Port number</b>			
21			
22			
80			
443			
<b>IP type</b>			
TCP			
UDP			

Protocol	Source Network	Port Number	IP Type
FTP	10.20.0.0/16	21	TCP
HTTP	10.30.0.0/24	80	TCP
HTTPS	10.40.0.0/24	443	TCP

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Seems to be TCP on every answer.

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)