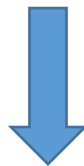


Microsoft MCSA Certification 70-697 Exam



- Vendor: Microsoft
- Exam Code: 70-697
- Exam Name: Configuring Windows Devices

Get Complete Version Exam 70-697 Dumps with VCE and PDF Here



<https://www.passleader.com/70-697.html>

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

Answer: C

Explanation:

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-paused-critical-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.

Answer: C

Explanation:

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

Incorrect Answers:

A: You cannot change the parent of a group by modifying the properties of the parent group.

B: You cannot change the parent of a group by modifying the properties of the group.

D: Deleting a group does not delete the users that belong to that group. Therefore, you do not need to remove the users from the group; you can just delete the group and recreate it.

<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.

Answer: C

Explanation:

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

Incorrect Answers:

A: This solution would enable network discovery for the CorpWifi network, but not the CorpWired network.

B: This solution would enable network discovery for the CorpWifi and HotSpot networks, but not the CorpWired network.

D: This solution would enable network discovery for the CorpWired network, but not the CorpWifi network.

E: This solution would enable network discovery for the CorpWired network, but not the CorpWifi network.

QUESTION 4

Hotspot Question

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 directory(ies)] within 2 directory(ies) 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 directory(ies)] within 2 directory(ies) 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.

Answer Area

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

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

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

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

Answer:

Answer Area

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

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

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

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

Explanation:

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

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

Setting the directory ProtectedFiles to encrypt new files [OK]

Encrypting files in C:\ProtectedFiles\

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

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

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

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

Setting the directory Backups to encrypt new files [OK]

Encrypting files in C:\Backups\

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

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

<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.

Answer: BCD

Explanation:

To limit the amount of space that each user can consume, you should enable the Enable Quota Management setting, and then enter the appropriate values in the Limit Disk Space To text box and the Set Warning Level To text box, and then select the Deny Disk Space To Users Exceeding Quota Limit check box to enforce identical quota limits for all users.

Incorrect Answers:

A: The fsutil quota violations D: command will search the system and application logs and display a message to indicate that quota violations have been detected or that a user has reached a quota threshold or quota limit. It will not, however, set the quota limit.

E: The convert D: /FS:NTFS command will convert the volume to NTFS. It will not set the quota limit.

F: A default quota entry exists for administrators so answer F is not required.

<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

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

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.

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	

Answer:

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

Explanation:

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

<http://windows.microsoft.com/en-gb/windows/before-applying-permissions-file-folder#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

Answer: D

Explanation:

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

Incorrect Answers:

A: The effective permission is Modify, not Full Control.

B: The effective permission is Modify, not Read and Execute.

C: The effective permission is Modify, not Read.

QUESTION 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

Answer: D

Explanation:

The solution is to deploy Remote Desktop Gateway in the office. Remote users can then connect

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

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.

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

Answer:

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

Explanation:

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

Incorrect Answers:

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

QUESTION 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.

Answer: B

Explanation:

The computers are members of a domain so the users should be using domain user accounts. We need to block the use of Microsoft accounts. We could use the Users can't add Microsoft accounts

setting which would mean that users will not be able to create new Microsoft accounts on a computer, switch a local account to a Microsoft account, or connect a domain account to a Microsoft account. Alternatively, we can also deny the ability to log on to a domain computer with a Microsoft account (and sync computer settings) by using the Users can't add or log on with Microsoft accounts. This will ensure that the company policy is enforced.

Incorrect Answers:

A: If we only applied the Users can't add Microsoft accounts setting, users would still be able to log on with existing Microsoft accounts and sync their settings.

C: It is not necessary to change the sync settings on every client computer. Furthermore, this would not prevent the users from simply changing the sync settings back again. This solution does not 'enforce' the company policy.

D: It is not necessary to change the sync settings on every client computer. Furthermore, this would not prevent the users from simply changing the sync settings back again. This solution does not 'enforce' the company policy.

<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.

Deployment Methods	Answer Area
Azure RemoteApp	App1: <input type="text" value="Deployment method"/>
Client Hyper-V	App2: <input type="text" value="Deployment method"/>
Local installation	

Answer:

Deployment Methods	Answer Area
Azure RemoteApp	App1: <input type="text" value="Azure RemoteApp"/>
Client Hyper-V	App2: <input type="text" value="Azure RemoteApp"/>
Local installation	

Explanation:

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

Incorrect Answers:

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

<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" />

Answer: C

Explanation:

To make Microsoft Office 365 ProPlus apps available as RemoteApps, you need to enable Shared computer activation. You do this by including the following text in the configuration file:

```
<Property Name = "SharedComputerLicensing" Value = "1" />
```

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

Incorrect Answers:

A: This setting determines how click-to-run apps are shutdown when an app is open. This setting is not required to ensure that multiple users can run Office 365 ProPlus using RemoteApp.

B: This setting is used for the installation of Office 365. This setting is not required to ensure that multiple users can run Office 365 ProPlus using RemoteApp.

D: This setting determines how Office 365 is activated. This setting is not required to ensure that multiple users can run Office 365 ProPlus using RemoteApp.

<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.

Answer Area

<div>Get-RDRemoteApp</div> <div>New-RDRemoteApp</div> <div>Set-RDRemoteApp</div> <div>Set-RDSessionCollectionConfiguration</div>	<div>"Session1" -DisplayName "App1"</div> <div><div>-CollectionName</div><div>-InformationVariable</div><div>-UserGroup</div></div>
<div>"C:\Apps\App1.exe"</div> <div><div>-FilePath</div><div>-FileVirtualPath</div><div>-RequiredCommandLine</div><div>-ShowInWebAccess</div></div>	

Answer:

Answer Area

Get-RDRemoteApp
New-RDRemoteApp
 Set-RDRemoteApp
 Set-RDSessionCollectionConfiguration

"Session1" -DisplayName "App1"

-CollectionName
 -InformationVariable
 -UserGroup

"C:\Apps\App1.exe"

-FilePath
 -FileVirtualPath
 -RequiredCommandLine
 -ShowInWebAccess

Explanation:

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

Incorrect Answers:

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

<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.

Actions

Download the Office Deployment Tool.

Modify the Click-to-Run for Office 365 Configuration.xml file.

Run **setup.exe /configure**.

Download Office 365 Deployment Readiness Tool.

Run **setup.exe /packager**.

Run **setup.exe /download**.

>

<

Answer Area

>

<

Answer:

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

Explanation:

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

Incorrect Answers:

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

<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

Answer: CD

Explanation:

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.

Answer: D

Explanation:

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.

Local Group Policy Editor	
File Action View Help	
Setting	State
Allow Automatic Updates immediate installation	Not configured
Allow non-administrators to receive update notifications	Not configured
Allow signed updates from an intranet Microsoft update service location	Not configured
Always automatically restart at the scheduled time	Enabled
Automatic Updates detection frequency	Enabled
Configure Automatic Updates	Enabled
Defer Upgrade	Not configured
Delay Restart for scheduled installations	Not configured
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Not configured
Do not connect to any Windows Update Internet locations	Enabled
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Not configured
Enable client-side targeting	Enabled
Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates	Not configured
No auto-restart with logged on users for scheduled automatic updates installations	Enabled
Re-prompt for restart with scheduled installations	Not configured
Reschedule Automatic Updates scheduled installations	Not configured
Specify intranet Microsoft update service location	Enabled
Turn on recommended updates via Automatic Updates	Not configured
Turn on Software Notifications	Enabled
<div> <div>Extended</div> <div>Standard</div> </div>	
19 setting(s)	

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.

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].

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].

Explanation:

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.

Answer: E

Explanation:

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.

Answer: A

Explanation:

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.

Answer: B

Explanation:

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.

Answer Area

.....

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

Answer:

Answer Area

.....

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

Explanation:

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. Set-AppxProvisionedDataFile 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.

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.	

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 Windows Store, install App1 on Computer1.	
Log on to Computer1 by using the built-in Administrator account.	From the Microsoft Intune administration console, manage the deployment settings of App1.

Explanation:

1. Log into your computer using a domain account.
2. Run the Microsoft Intune Software Publisher wizard app.
3. 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

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 Trusts, add a UPN suffix for each user.
- D. From the Office 365 portal, modify the Users settings of each user.

Answer: B

Explanation:

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 Subscription1. 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.


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

Answer:

User1:	<div>None CloudCollection1 only HybridCollection1 only CloudCollection1 and HybridCollection1</div>
User2:	<div>None CloudCollection1 only HybridCollection1 only CloudCollection1 and HybridCollection1</div>
User3:	<div>None CloudCollection1 only HybridCollection1 only CloudCollection1 and HybridCollection1</div>

Explanation:

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.

Answer: C

Explanation:

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.

Answer: D

Explanation:

We can use Windows PowerShell Direct to run PowerShell cmdlets on a virtual machine from the Hyper-V host. Because Windows PowerShell Direct runs between the host and virtual machine, there is no need for a network connection or to enable remote management. There are no network or firewall requirements or special configuration. It works regardless of your remote management configuration. To use it, you must run Windows 10 or Windows Server Technical Preview on the host and the virtual machine guest operating system. To create a PowerShell Direct session, use one of the following commands:

Enter-PSSession -VMName VMName

Invoke-Command -VMName VMName -ScriptBlock { commands }

Incorrect Answers:

A: WinRM is Windows Remote Management. This is not required when using Windows PowerShell Direct.

B: Running PowerShell.exe with a PowerShell cmdlet will execute the PowerShell cmdlet on the local machine. It will not remotely execute the PowerShell cmdlet on the VM.

C: You could run the Enter-PSSession cmdlet with the -VMName parameter but the Receive-PSSession cmdlet with the -Name parameter will not work.

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.

Answer: B

Explanation:

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

Incorrect Answers:

A: Sleep is a power-saving state that allows a computer to quickly resume full-power operation. A sleeping computer draws a small amount of power whereas a hibernating computer uses no power.

C: A passive cooling policy slows down the processor before speeding up the processor's cooling fan to conserve power. However, this will still use more power than a hibernating tablet.

D: C-States are different modes of CPU clock speed used to conserve power when processors are idle. Disabling C-State control disables the ability to reduce the power consumption of the computer.
<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. 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.

Answer: AB

Explanation:

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

Incorrect Answers:

C: You need to use the /X switch to modify the power scheme, not the /S switch.

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

[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.

Answer: AC

Explanation:

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

Incorrect Answers:

B: Enabling the 'Enforce drive encryption type on operating system drives' policy setting allows you to configure whether the entire drive or used space only is encrypted when BitLocker is enabled. However, it does not enable the use of BitLocker on computers without a TPM chip.

D: The Platform Configuration Register indices (PCRs) 0, 2, 4, and 11 are enabled by default for computers that use an Extensible Firmware Interface (EFI). Configuring the TPM validation profile does not enable the use of BitLocker on computers without a TPM chip.

<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.

Answer: BD

Explanation:

The personally owned portable Windows 10 Enterprise computers being managed by the management infrastructure agent enables the use of remote wipe. By initiating a remote wipe, we can erase all company data including email from the stolen device. Microsoft Intune provides selective wipe, full wipe, remote lock, and passcode reset capabilities. Because mobile devices can store sensitive corporate data and provide access to many corporate resources, you can issue a remote device wipe command from the Microsoft Intune administrator console to wipe a lost or stolen device. Changing the user's password should be the first step. If the stolen computer is accessed before the remote wipe happens, the malicious user could be able to access company resources if the laptop has saved passwords.

Incorrect Answers:

A: Preventing the computer from connecting to the corporate wireless network will not offer much protection. The person in possession of the laptop would still be able to access all the data on the laptop and download emails. Furthermore, it is likely that the corporate applications can access corporate servers over any Internet connection.

C: Disconnecting the computer from the management infrastructure will not help. The person in possession of the laptop would still be able to access all the data on the laptop and download emails. This step would also remove the ability to perform a remote wipe. The computer will be disconnected from the management infrastructure when the remote wipe happens.

<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.

Answer: A

Explanation:

A Trusted Platform Module (TPM) chip of version 1.2 or greater is required to support Virtual Smart Cards. Virtual smart card technology from Microsoft offers comparable security benefits to physical smart cards by using two-factor authentication. Virtual smart cards emulate the functionality of physical smart cards, but they use the Trusted Platform Module (TPM) chip that is available on computers in many organizations, rather than requiring the use of a separate physical smart card and reader. Virtual smart cards are created in the TPM, where the keys that are used for authentication are stored in cryptographically secured hardware.

Incorrect Answers:

B: BitLocker Drive Encryption does not need to be enabled on a system drive of the laptops and tablets to support Virtual Smart Cards.

C: The ability to read a physical smart card does not ensure support for Virtual Smart Cards.

D: Windows 10 Enterprise edition is not a requirement for Virtual Smart Cards; other versions of Windows 10 (and Windows 8) can use Virtual Smart Cards.

<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.

Answer: E

Explanation:

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

Incorrect Answers:

A: Users can only install the Company Portal app after they have been added as Intune users, which require the Apple Push Notification (APN) certificate to be in place.

B: The device enrollment manager account is a special Intune account that has permission to enroll more than five corporate-owned devices. It is not used for BYOD.

C: The Set a DNS alias for the enrollment server address setting is an optional setting for enrolling Windows devices.

D: The Configure Intune service to service connector for hosted Exchange setting is used to connect Microsoft Intune and hosted Exchange without an on-premises infrastructure.

<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)

Answer: A

Explanation:

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

Incorrect Answers:

B: You make use of the Microsoft Intune Windows general configuration policy to configure settings for enrolled devices, but not the policy setting in question.

C: The Microsoft Intune Center allows users to get applications from the company portal, check for updates, manage Microsoft Intune Endpoint Protection, and request remote assistance. It does not allow users to configure settings to prevent users from receiving prompts to restart Windows following the installation of mandatory updates.

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

<http://blogs.technet.com/b/windowsintune/archive/2013/01/09/policy-settings-for-mandatory-updates.aspx>

<https://technet.microsoft.com/en-us/library/dn646989.aspx>

QUESTION 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.

Policy Templates	Answer Area
Microsoft Intune Agent Settings	Require automatic updates: Policy template
Windows Configuration Policy	Minimum classification of updates to install automatically: Policy template
Windows Custom Policy (Windows 10 and Windows 10 Mobile)	Allow immediate installation of updates that do not interrupt Windows: Policy template

Answer:

Policy Templates	Answer Area
Microsoft Intune Agent Settings	Require automatic updates: Windows Configuration Policy
Windows Configuration Policy	Minimum classification of updates to install automatically: Windows Configuration Policy
Windows Custom Policy (Windows 10 and Windows 10 Mobile)	Allow immediate installation of updates that do not interrupt Windows: Microsoft Intune Agent Settings

Explanation:

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

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

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

Incorrect Answers:

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

<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.

Answer: DE

Explanation:

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

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

<http://blogs.technet.com/b/configmgrteam/archive/2013/03/20/configuring-configuration-manager-sp1-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. Set resiliency type to Parity.
- C. From Disk Management, create a new spanned volume.
- D. From Disk Management, create a new striped volume.

Answer: B

Explanation:

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

Incorrect Answers:

A: The Three-way mirror resiliency type allows Windows to store three copies of your data. Mirroring uses drive space less efficiently than parity.

C: Spanned volumes are not fault tolerant

D: Striped volumes are not fault tolerant

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

<https://technet.microsoft.com/en-us/library/cc772180.aspx>

<https://technet.microsoft.com/en-us/library/cc732422.aspx>

QUESTION 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.

Actions	Answer Area
Restore your data from the backup.	
From Storage Spaces, create a new storage pool. Set the Resiliency Type to two-way mirror .	
From Storage Spaces, create a new storage pool. Set the Resiliency Type to parity .	
From Storage Spaces, create a new storage pool. Set the Resiliency Type to three-way mirror .	
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.	

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 parity .	From Storage Spaces, create a new storage pool. Set the Resiliency Type to two-way mirror .
From Storage Spaces, create a new storage pool. Set the Resiliency Type to three-way mirror .	Restore your data from the backup.
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.	

Explanation:

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

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

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.

• • • • •

Answer Area

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

Answer:

• • • • •

Answer Area

Actions	When you run Windows To Go from USB1, you can see the contents of the computer's internal drives from File Explorer.	When you connect USB1 to a computer that runs Windows 10, you can automatically view the content of USB1 from File Explorer
From DiskPart, configure the san policy option.	<input checked="" type="radio"/>	<input type="radio"/>
From DiskPart, configure the attributes volume option.	<input type="radio"/>	<input checked="" type="radio"/>
From DiskPart, configure the attributes disk option.	<input type="radio"/>	<input type="radio"/>
From fsutil, configure the volume option.	<input type="radio"/>	<input type="radio"/>
From fsutil, configure the behavior option.	<input type="radio"/>	<input type="radio"/>

Explanation:

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

Incorrect Answers:

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

<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.

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

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.

Answer: B

Explanation:

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

Incorrect Answers:

A: A super mandatory profile is a roaming profile in which the profile path ends in .man. Removing the .man extension will create a roaming profile, which will not solve the problem.

C: A super mandatory profile prevents users from saving any changes to their profile, which includes the user's documents library.

D: A super mandatory profile is a roaming profile in which the profile path ends in .man. Adding the .dat extension will result in an error.

<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.

Answer: B

Explanation:

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

Incorrect Answers:

A: The Allow access to BitLocker-protected fixed data drives from earlier version of Windows policy setting is used to control whether access to drives is allowed via the BitLocker To Go Reader, and if the application is installed on the drive.

C: The Allow network unlock at startup policy allows clients running BitLocker to create the necessary network key protector during encryption.

D: The Configure use of hardware-based encryption for operating system drives policy controls how BitLocker reacts when encrypted drives are used as operating system drives.

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

https://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_depopt4

QUESTION 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.

Answer: B

Explanation:

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

Incorrect Answers:

A: The Remote Management Users group is normally used to allow users to manage servers via the Server Manager console.

C: Members of the Domain Backup Operators group will be able to back up all files and folders on all computers in the domain, not just the Windows 10 Enterprise desktop computers.

D: Setting the backup task account as NTFS owner on all the profiles will allow the backup task account to control how permissions are set on the NTFS volumes for those user profiles and to whom permissions are granted. You only need to grant the backup task user account access to the user profiles, not control over its permissions.

<https://technet.microsoft.com/en-us/library/cc771990.aspx>

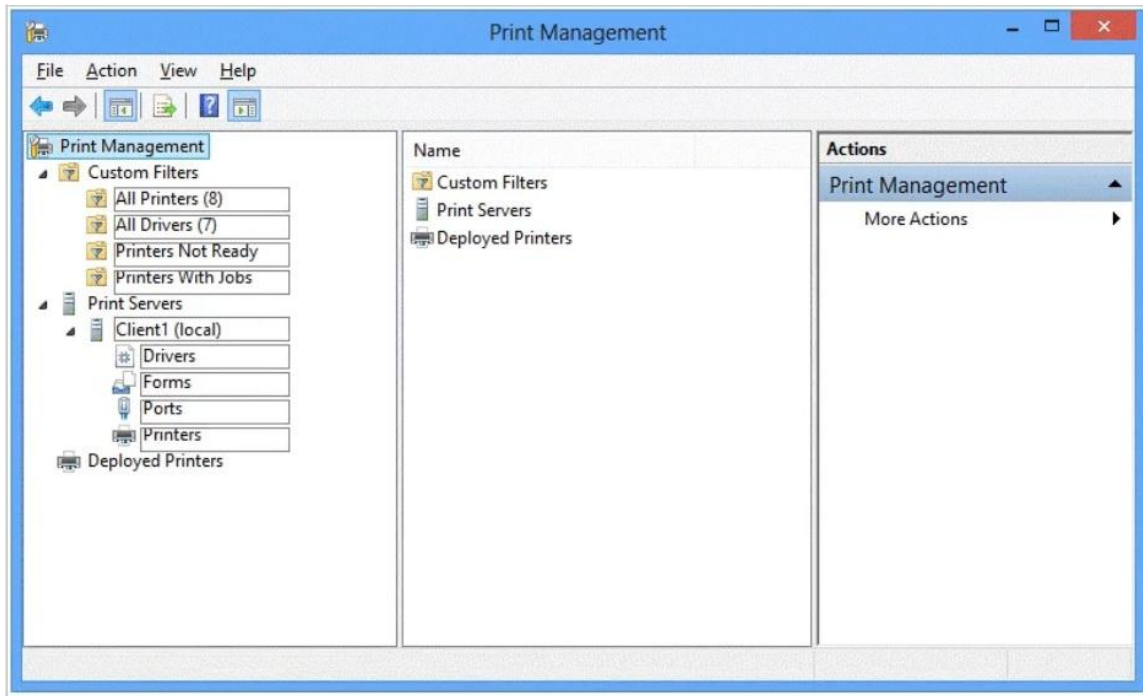
<https://technet.microsoft.com/en-us/library/dn579255.aspx>

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

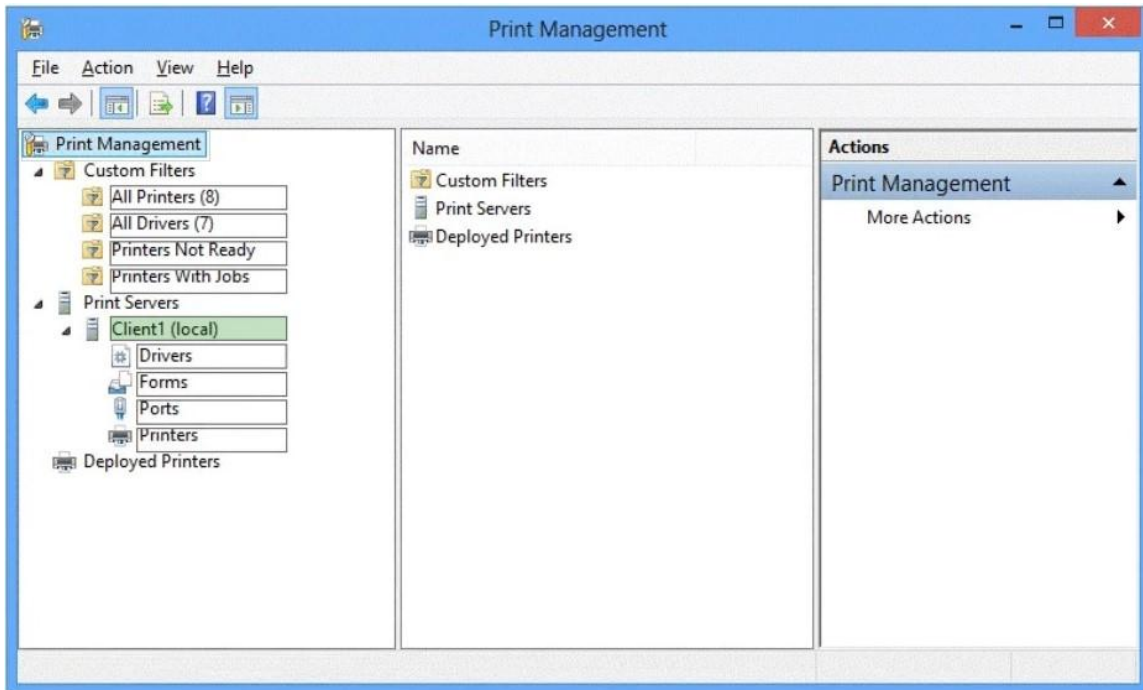
QUESTION 42

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.



Answer:



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.

Answer: B

Explanation:

AppLocker is a feature in Windows Server 2012, Windows Server 2008 R2, Windows 8, and Windows 7 that advances the functionality of the Software Restriction Policies feature. AppLocker contains new capabilities and extensions that reduce administrative overhead and help administrators control how users can access and use files, such as executable files, scripts, Windows Installer files, and DLLs. AppLocker rules can be applied to security groups. We can use a group policy to apply AppLocker rules to the security groups to prevent them from running the application.

Incorrect Answers:

A: DirectAccess is a remote access solution that enables remote access to company resources. It cannot be used to prevent members of security groups from running an application.

C: BitLocker is used to encrypt data. It cannot be used to prevent members of security groups from running an application.

D: The User State Management Tool is used for managing user profiles. It cannot be used to prevent members of security groups from running an application.

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

[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 solid-state drive (SSD) on the tablets.
- The application is isolated from other applications.
- The application uses the least amount of disk space on the tablet.

You need to deploy the new application to the tablets. What should you do?

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

Answer: B

Explanation:

Deploying the application as a published application on the Remote Desktop server will use no disk space on the tablets. Users will be able to access the application by using Remote Desktop Connections. This will also ensure that the application is isolated from other applications on the tablets. We can use Remote Desktop Connection `redirection' to ensure that the application is able

to access files stored on an internal solid-state drive (SSD) on the tablets. Redirection enables access to local resources such as drives, printers etc. in a Remote Desktop Connection.

Incorrect Answers:

A: This solution does not minimize the disk space used on the tablets as the application will be downloaded to the tablets.

C: This solution does not minimize the disk space used on the tablets as the application will be installed on the tablets. This solution also does not provide the required isolation from other applications.

D: This solution does not provide the required access to files stored on the internal solid-state drive (SSD) on the tablets.

E: This solution does not minimize the disk space used on the tablets as disk space will be required for the virtual machine. This solution also does not provide the required access to files stored on the internal solid-state drive (SSD) on the tablets.

F: This solution does not minimize the disk space used on the tablets as the application will need to be downloaded and installed on the tablets.

G: This solution does not minimize the disk space used on the tablets as disk space will be required for the VHD.

H: This solution does not minimize the disk space used on the tablets as disk space will be required for the VHDX.

<https://azure.microsoft.com/en-gb/documentation/articles/remotetapp-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.

Answer: C

Explanation:

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

Answer: C

Explanation:

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

Answer: C

Explanation:

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.

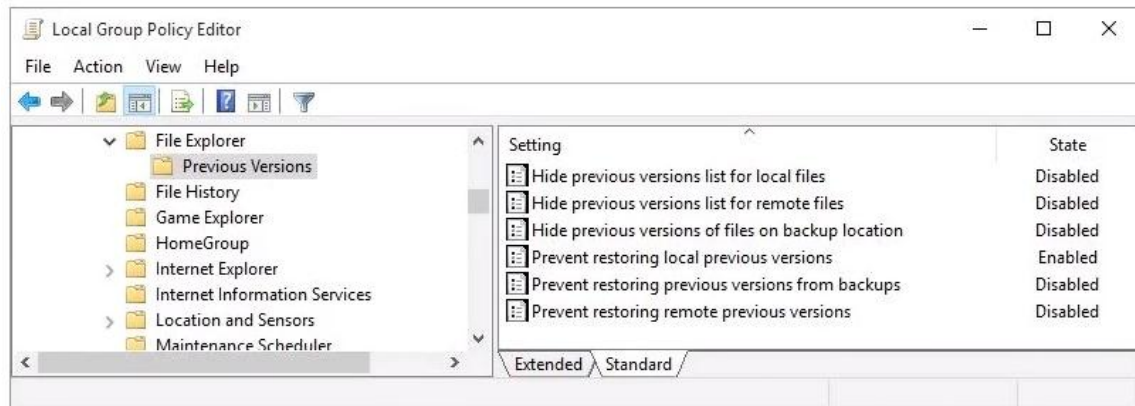
B: System Restore points do not back up user data. They are used for restoring the system and applications to a previous state. You cannot use a System Restore point to recover a deleted folder.

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.

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].

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].

Explanation:

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.

Answer: AC

Explanation:

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

Answer: A

Explanation:

The add address Network Shell (netsh) command adds an IPv6 address to a specified interface.

Incorrect Answers:

B: The set interface Network Shell (netsh) command modifies interface configuration parameters.

C: The set global Network Shell (netsh) command modifies global configuration parameters.

D: The set address Network Shell (netsh) command modifies an IPv6 address on a specified interface.

[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.

```

Connection-specific DNS Suffix  : 
Description . . . . . : Intel(R) Dual Band Wireless-AC 7260 #2
Physical Address. . . . . : E8-B1-FC-29-7D-F0
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
Default Gateway . . . . . : 10.1.1.1
DHCP Server . . . . . : 10.1.1.1
DNS Servers . . . . . : 10.1.1.1
NetBIOS over Tcpip. . . . . : Enabled

```

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.

Answer Area

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

The computer [answer choice] access the Internet.

Answer:

Answer Area

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

The computer [answer choice] access the Internet.

Explanation:

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

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

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

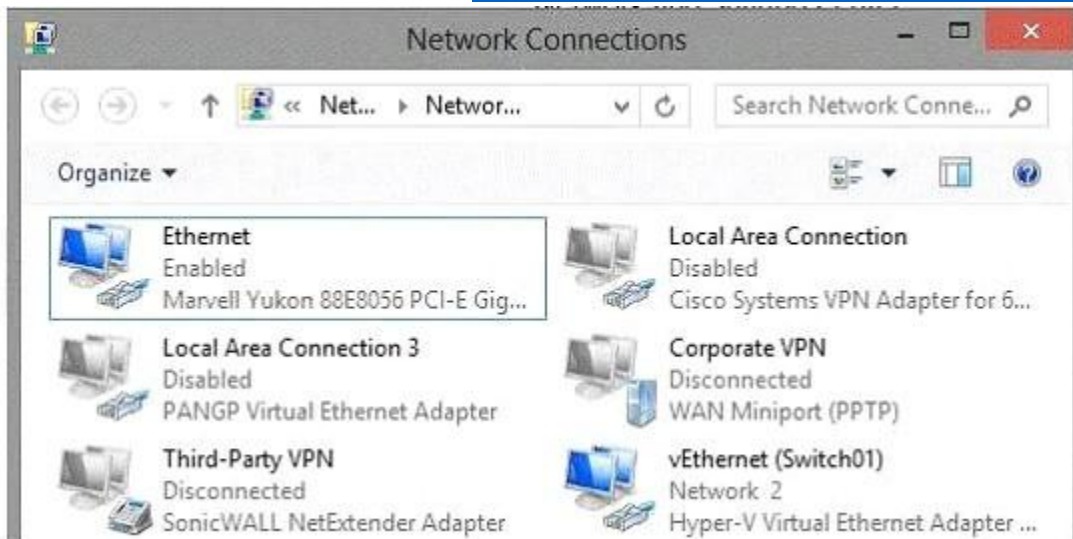
```
Link-local IPv6 Address . . . . . : fe80::c4e9:416b:3ebe:a6cb%13(Preferred)
```

The IP address of the Default Gateway is 10.1.1.1

QUESTION 52

Hotspot Question

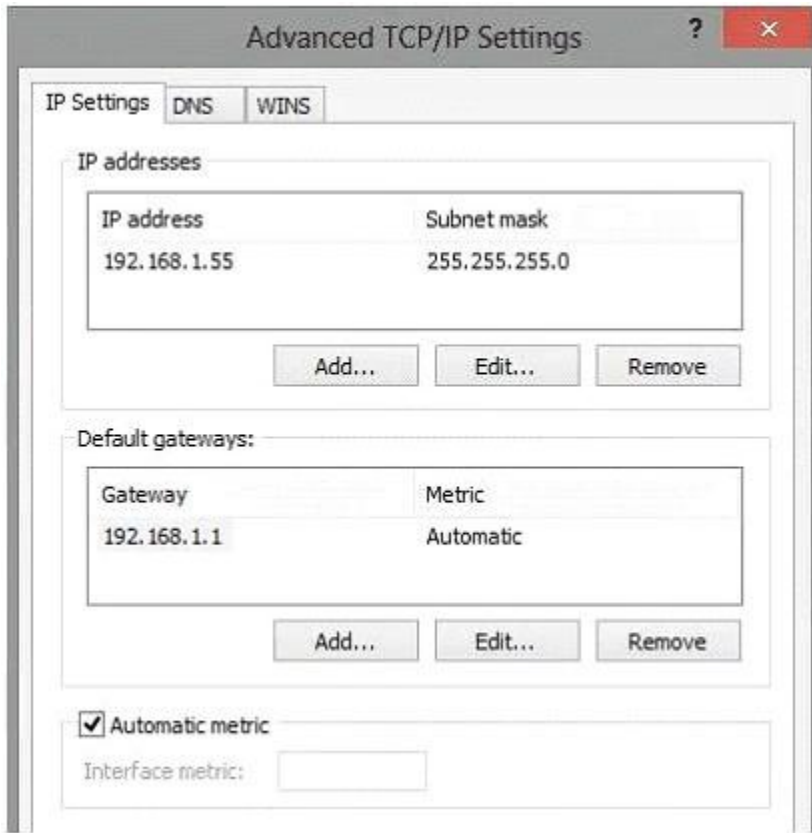
You are setting up a Windows 10 Enterprise computer. The computer's network connections are shown in the Network connections exhibit. (Click the Exhibit button.)



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.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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"/>

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"/>

Explanation:

The computer has a physical network adapter.



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



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



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

QUESTION 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

Answer: D

Explanation:

IPSec tunnels can be encrypted by 256-bit AES. L2TP/IPsec allows multiprotocol traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery, such as IP or Asynchronous Transfer Mode (ATM). The L2TP message is encrypted with one of the following protocols by using encryption keys generated from the IKE negotiation process: Advanced Encryption Standard (AES) 256, AES 192, AES 128, and 3DES encryption algorithms.

QUESTION 54

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

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.

Answer: CD

Explanation:

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

Answer: A

Explanation:

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

Answer: D

Explanation:

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

Answer: D

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

Answer: A

Explanation:

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

Answer: A

Explanation:

The /oobe option restarts the computer into Windows Welcome mode. Windows Welcome enables end users to customize their Windows operating system, create user accounts, name the computer, and other tasks. Any settings in the /oobe System configuration pass in an answer file are processed immediately before Windows Welcome starts.

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

Answer: A

Explanation:

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.)

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	

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	

Explanation:

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.

Answer: AD

Explanation:

(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.

Answer: AB

Explanation:

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:

1. In Disk Management, right click the unallocated space on one of the dynamic disks where you want to create the spanned volume.
2. Click New Spanned Volume.
3. 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 x86-based 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 Itanium-based 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.)

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			

Answer:

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

Explanation:

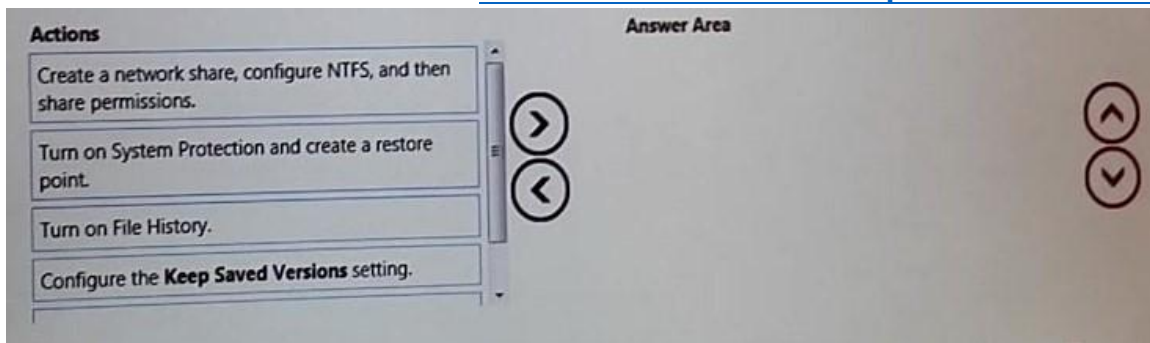
Seems to be TCP on every answer.

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

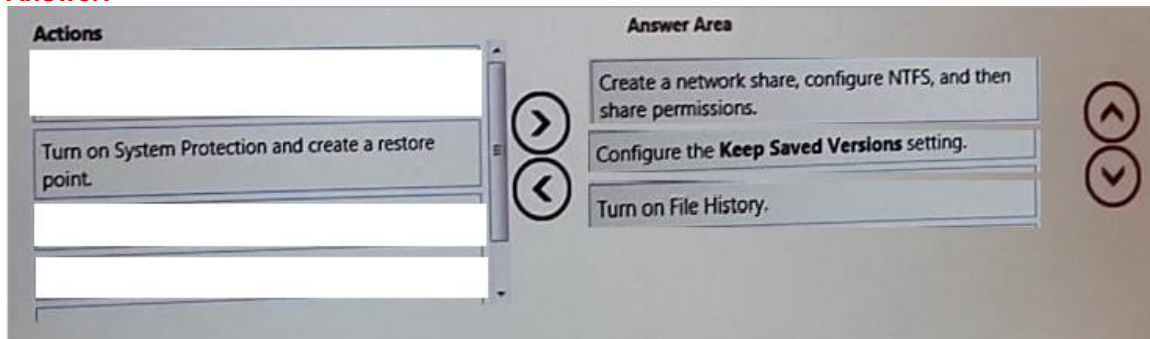
QUESTION 65

Drag and Drop Question

You administer Windows 8.1 Enterprise computers. Your company has a team of technical writers that is preparing technical manuals and help files. The team manager wants to ensure that the technical writers are able to restore any documents that been modified within the last year. You need to ensure that the technical writers can restore Microsoft Word files to any previous versions for up to one year. 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.)



Answer:



Explanation:

We need a NTFS folder. In the Advanced settings we can configure the Keep Saved Versions settings. Finally we turn on File History.

Incorrect Answers:

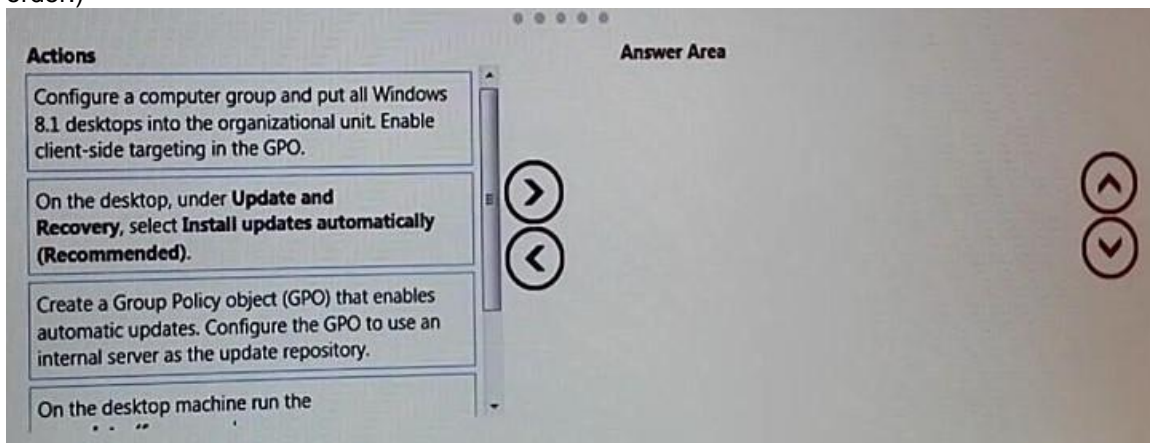
File History does not use restore points.

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

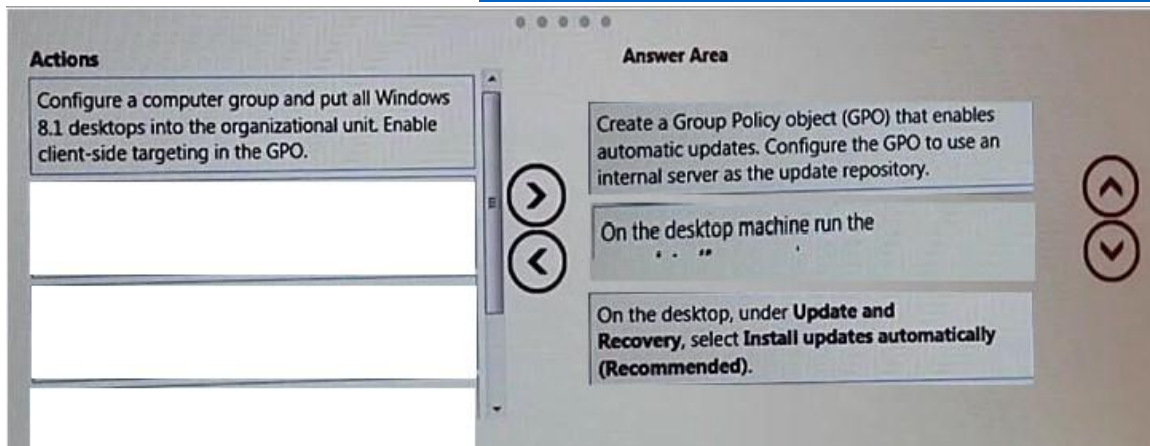
QUESTION 66

Drag and Drop Question

You manage update compliance for Windows 8.1 desktop computers that are part of a domain. You need to configure new desktops to automatically receive updates from an intranet resource that you manage. Which three actions should you perform in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:



Explanation:

Box 1: Create a GPO that enables automatic updates through the intranet source.

Box 2: gpupdate /force

The Gpupdate command refreshes local and Active Directory-based Group Policy settings, including security settings. The /force ignores all processing optimizations and reapplies all settings.

Box 3: Configure the clients to install updates automatically.

Incorrect Answers:

* Client side targeting

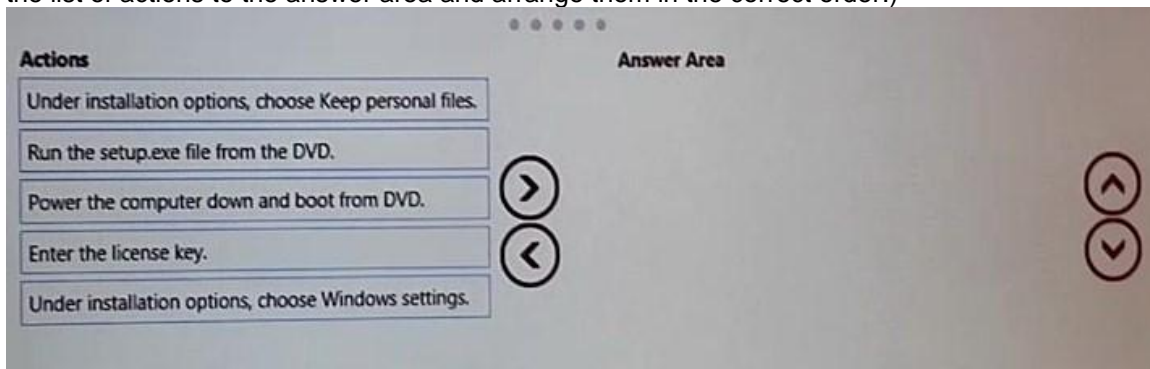
With client-side targeting, you enable client-computers to add themselves to the computer groups you create in the WSUS console.

<https://technet.microsoft.com/en-us/library/bb490983.aspx>

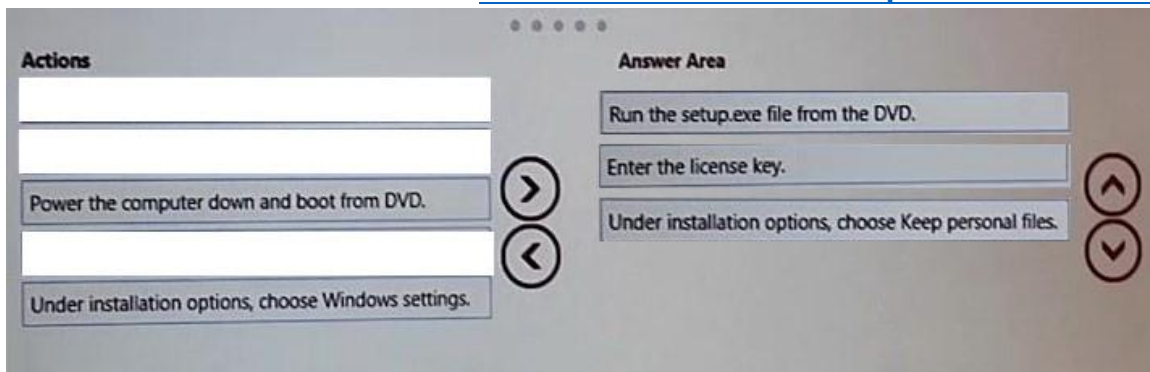
QUESTION 67

Drag and Drop Question

You have a Windows 8 computer. You need to migrate from Windows 8 to Windows 8.1 while retaining as much data as possible. You load the Windows 8 media into the DVD drive. Which three actions should you perform next in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:

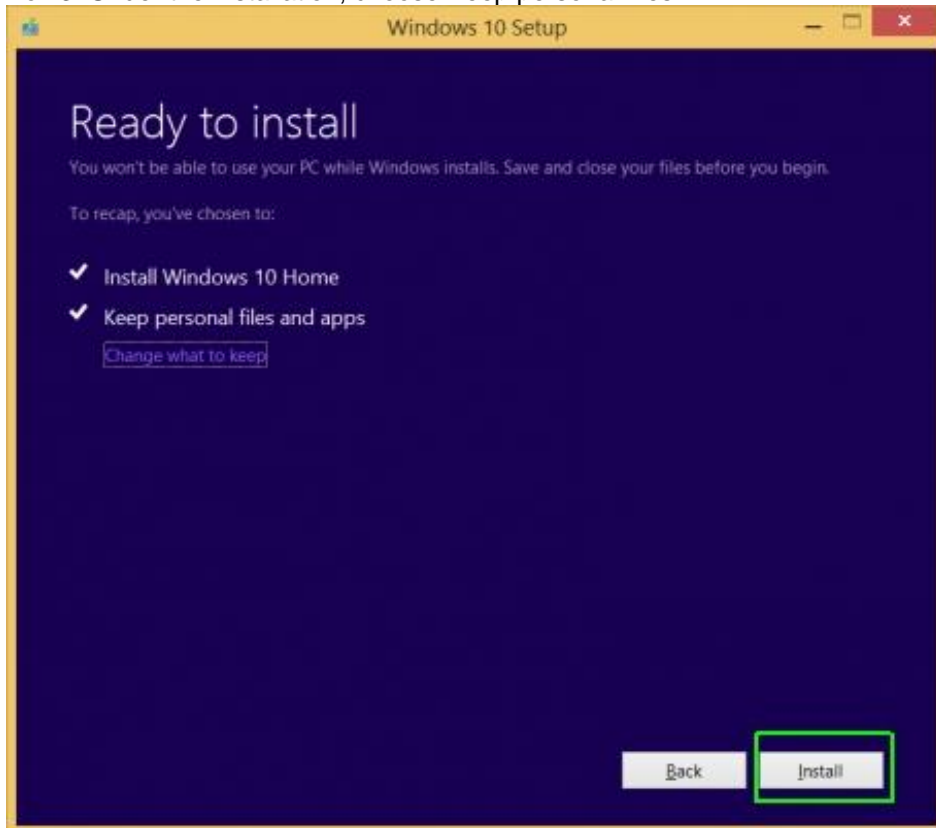


Explanation:

Box 1: Run the Setup.exe file from the DVD. Launch setup.exe on the DVD drive to start the upgrade process.

Box 2: Enter the license key. You will be prompted for the license key.

Box 3: Under the installation, choose Keep personal files.



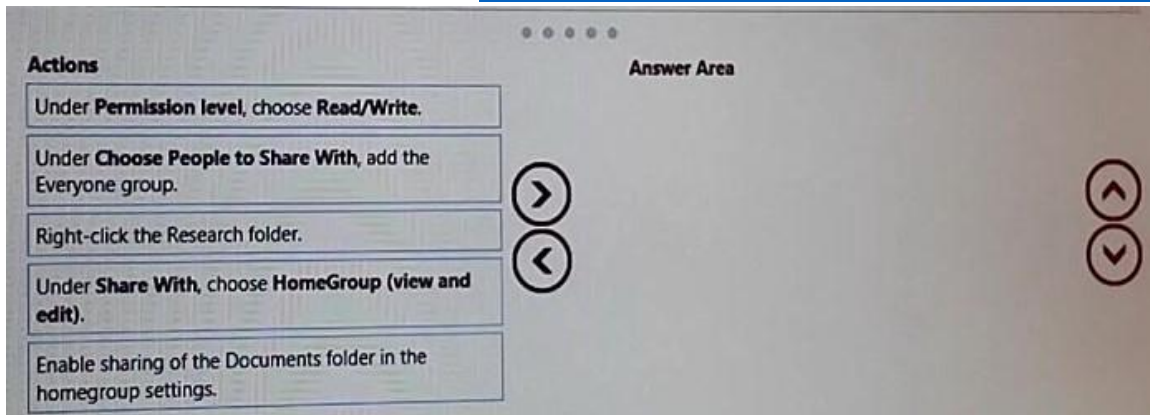
References:

<http://www.laptopmag.com/articles/how-to-upgrade-windows-10>

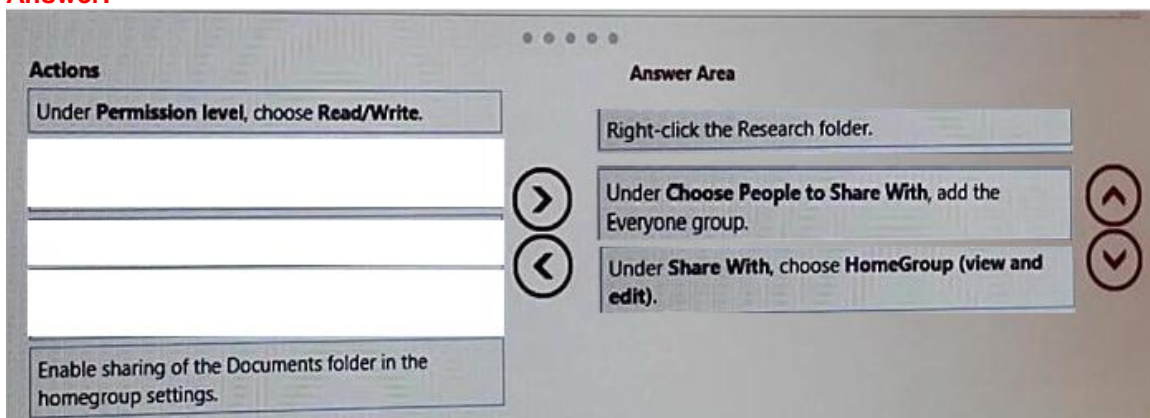
QUESTION 68

Drag and Drop Question

You work for a small company that uses Windows 8.1 computers. The computers are joined to a homegroup. You want to share an existing folder named Research. It is located in the Documents folder. You need to give users the ability to change the files in this folder. Which three actions should you perform in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:



Explanation:

Box 1: Right-click on the Research folder. Select the folder.

Box 2: Share it with the home group. Finally we need to change the level of access, which by default is view.

Box 3: Under Share With, choose HomeGroup (View and edit).

Incorrect Answers:

* Not read/write

There is no option read/write for Homegroup. The two options are view and view and edit.

Note:

To share individual files or folders:

- Open File Explorer by typing file explorer in the search box in the taskbar, and then selecting File Explorer.

- Select the item, and then select the Share tab.

- Choose an option in the Share with group. There are different Share with options depending on whether your PC is connected to a network and what kind of network it is. To share items with a particular person, choose that person's account. To share with all the members of your homegroup, choose one of the Homegroup options.(Select libraries to share with all the members of your homegroup by opening HomeGroup.)To prevent a file or folder from being shared with anyone, select the Share tab, and then select Stop sharing. To change the level of access to a file or folder, select the Share tab, and then select either Homegroup (view) or Homegroup (view and edit).If you need to share a location such as a drive or system folder, select the Advanced sharing option.

<https://support.microsoft.com/en-us/help/17145/windows-homegroup-from-start-to-finish>

QUESTION 69

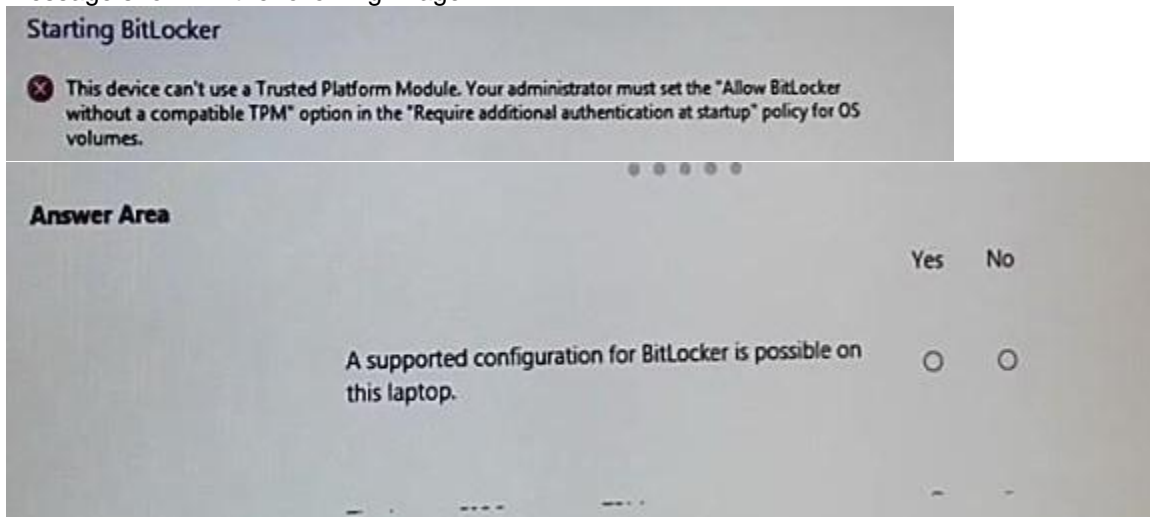
Hotspot Question

You provide support for a small company. The company purchases a Windows 8.1 laptop for an

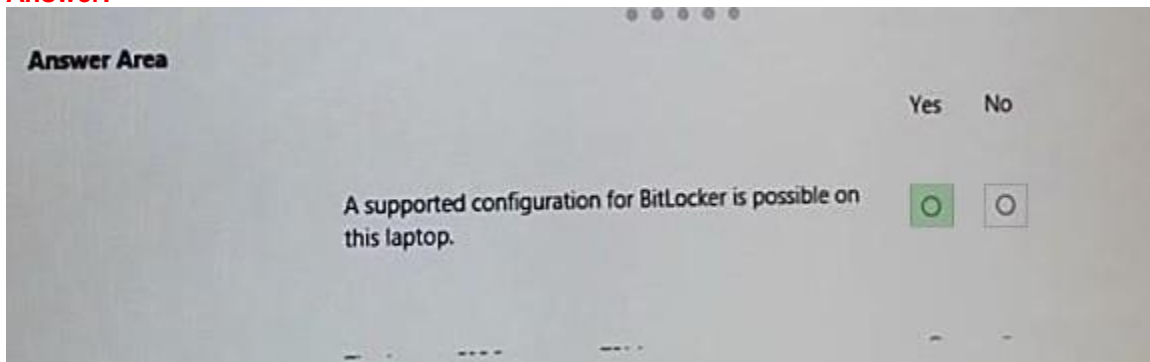
[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

employee who travels often. The company wants to use BitLocker to secure the hard drive for the laptop in case it is lost or stolen. While attempting to enable BitLocker, you receive the error message shown in the following image.



Answer:



Explanation:

How to Configure Computer to Enable BitLocker without Compatible TPM:

- Administrators must follow the steps below to configure their Windows 8 computers to allow enabling Bit Locker Drive Encryption without compatible TPM.
- Log on to Windows 8 computer with the account that has administrative privileges.
- Assuming that the computer has been configured to display classic start menu, click Start and at the bottom of the menu in search box type GPEDIT.MSC command and press enter key.
- On the opened Local Group Policy Editor snap-in from the left pane expand Computer Configuration > Administrative Templates > Windows Components > Bit Locker Drive Encryption and from the expanded list click to select Operating System Devices.
- From the right pane double-click "Require additional authentication" at startup.
- On the opened box click to select Enabled radio button and ensure that under Options section Allow Bit Locker without a compatible TPM checkbox is checked.
- Once done, click Ok button to allow the changes to take effect and close Local Group Policy Editor snap-in.

https://answers.microsoft.com/en-us/windows/forum/windows_8-security/allow-bitlocker-without-compatible-tpm-module/4c0623b5-70f4-4953-bde4-34ef18045e4f?auth=1

QUESTION 70

You have 100 client Windows 8.1 computers. Users are NOT configured as local administrators. You need to prevent the users from running applications that they downloaded from the Internet,

unless the applications are signed by a trusted publisher. What should you configure in the Security settings from the Action Center?

- A. Virus protection
- B. User Account Control
- C. Windows SmartScreen settings
- D. Network Access Protection

Answer: C

Explanation:

<http://windows.microsoft.com/en-ZA/internet-explorer/products/ie-9/features/smartscreen-filter>
<http://windows.microsoft.com/en-US/windows7/SmartScreen-Filter-frequently-asked-questions-IE9>
<http://technet.microsoft.com/en-us/network/bb545879.aspx>
<http://technet.microsoft.com/en-us/library/cc709691%28v=WS.10%29.aspx>

QUESTION 71

At home, you use a Windows 8.1 desktop computer. At work, you use a Windows 8.1 laptop that is connected to a corporate network. You use the same Microsoft account to log on to both computers. You have a folder with some personal documents on your desktop computer. The folder must be available and synced between both computers. You need to ensure that the latest version of these files is available. What should you do?

- A. Create a folder by using SkyDrive for Windows.
Move all of the personal documents to the new folder.
- B. Move the folder to the Libraries folder.
Go to PC Settings.
Under Sync your settings, enable App settings.
- C. Right-click the folder and click Properties.
Under Security, provide Full Control for the Microsoft account.
- D. Right-click the folder and select Share With, and then select Homegroup (view and edit).

Answer: A

Explanation:

http://answers.microsoft.com/en-us/windows/forum/windows8_1-files/some-solutions-for-skydrive-syncing-problems-in/f69180ad-e9b5-47cd-a3f3-24a4d67e0093
http://answers.microsoft.com/en-us/windows/forum/windows8_1-files/skydrive-in-windows-81-is-not-syncing/1627111e-2ccb-4e6d-ae5f-ee325829191f

QUESTION 72

Drag and Drop Questions

You administer 50 laptops that run Windows 7 Professional 32-bit. You want to install Windows 8 Pro 64-bit on every laptop. Users will keep their own laptops. You need to ensure that user application settings, Windows settings, and user files are maintained after Windows 8 Pro is installed. 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.)

	Answer Area
Run the Scanstate.exe c:\store / i:migdocs.xml /i:migapp.xml /v:13 /c / hardlink /nocompress command.	
Copy the User State Migration Tool (USMT) files and tools to the source computer.	
Run the Scanstate.exe c:\store / i:migdocs.xml /i:migapp.xml /v:13 / c command.	
Install Windows 8 Pro on the existing Windows partition with no formatting or repartitioning. Install standard operating environment applications.	
Run the Loadstate.exe c:\store / i:migdocs.xml /i:migapp.xml /v:13 /c / hardlink /nocompress command.	
Install Windows 8 Pro by deleting all existing partitions and creating a new one. Install standard operating environment applications.	

Answer:

	Answer Area
	Copy the User State Migration Tool (USMT) files and tools to the source computer.
	Run the Scanstate.exe c:\store / i:migdocs.xml /i:migapp.xml /v:13 /c / hardlink /nocompress command.
Run the Scanstate.exe c:\store / i:migdocs.xml /i:migapp.xml /v:13 / c command.	Install Windows 8 Pro by deleting all existing partitions and creating a new one. Install standard operating environment applications.
Install Windows 8 Pro on the existing Windows partition with no formatting or repartitioning. Install standard operating environment applications.	Run the Loadstate.exe c:\store / i:migdocs.xml /i:migapp.xml /v:13 /c / hardlink /nocompress command.

Explanation:

User State Migration Toolkit (USMT) Reference.

<http://technet.microsoft.com/en-us/library/hh825171.aspx>

How to Use Hard Links for User State Migration

<http://technet.microsoft.com/en-us/library/ee344267.aspx>

32-bit and 64-bit Windows: frequently asked questions

<http://windows.microsoft.com/en-us/windows7/32-bit-and-64-bit-windows-frequently-asked-questions>

If you want to move from a 32-bit version of Windows to a 64-bit version of Windows 7 or vice versa, you'll need to back up your files and choose the Custom option during Windows 7 installation. Then, you'll need to restore your files and reinstall your programs.

QUESTION 73

You are a systems administrator for your company. The company has employees who work remotely by using a virtual private network (VPN) connection from their computers, which run Windows 8 Pro. These employees use an application to access the company intranet database servers. The company recently decided to distribute the latest version of the application through using a public cloud. Some users report that every time they try to download the application by using Internet Explorer, they receive a warning message that indicates the application could harm their computer. You need to recommend a solution that prevents this warning message from appearing, without compromising the security protection of the computers. What should you do?

- A. Publish the application through a public file transfer protocol (FTP) site.
- B. Publish the application through an intranet web site.
- C. Instruct employees to disable the SmartScreen Filter from within the Internet Explorer settings.
- D. Publish the application to Windows Store.

Answer: B

Explanation:

Intranet is the generic term for a collection of private computer networks within an organization. An intranet uses network technologies as a tool to facilitate communication between people or work groups to improve the data sharing capability and overall knowledge base of an organization's employees. Intranets utilize standard network hardware and software technologies like Ethernet, Wi-Fi, TCP/IP, Web browsers and Web servers. An organization's intranet typically includes Internet access but is firewalled so that its computers cannot be reached directly from the outside.

http://compnetworking.about.com/cs/intranets/g/bldef_intranet.htm

<http://www.dynamicwebs.com.au/tutorials/ftp.htm>

<http://msdn.microsoft.com/en-us/library/windows/apps/xaml/hh974576.aspx>

QUESTION 74

You administer computers that run Windows 8 Enterprise and are members of an Active Directory domain. Some volumes on the computers are encrypted with BitLocker. The BitLocker recovery passwords are stored in Active Directory. A user forgets the BitLocker password to local drive E: and is unable to access the protected volume. You need to provide 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 to run the manage-bde-protectors-disable e: command.
- B. Ask the user for his or her logon name.
- C. Ask the user to run the manage-bde-unlock E:-pw command.
- D. Ask the user for his or her computer name.
- E. Ask the user for a recovery key ID for the protected drive.

Answer: DE

Explanation:

Asking user their logon name is a very lame way to verify their identity. Answers D & E seem to be the best solution, because:

- You need to know computer name in order to find computer object in AD, where bitlocker passwords are store
- Without recovery key ID you will not know which bitlocker recovery password to use

QUESTION 75

Hotspot Questions

Your company has a main office and two branch offices named Branch1 and Branch2. The main

office contains a file server named Server1 that has BranchCache enabled. Branch1 contains a server named Server2 that is configured as a hosted cache server. All client computers run Windows 8 Enterprise. All of the computers are joined to an Active Directory domain. The BranchCache settings of all the computers are configured as shown in the following exhibit. (Click the Exhibit button.)

BranchCache GPO
Data collected on: 5/17/2013 7:30:30 AM

Computer Configuration (Enabled)

Policies

Administrative Templates
Policy definitions (ADMX files) retrieved from the local computer.

Network/BranchCache

Policy	Setting	Comment
Configure BranchCache for network files	Enabled	
Type the maximum round trip network latency (milliseconds) after which caching begins		
	80	
Enable Automatic Hosted Cache	Enabled	
Discovery by Service Connection Point	Enabled	
Set BranchCache Distributed Cache mode	Enabled	
Set percentage of disk space used for client computer cache	Enabled	
Specify the percentage of total disk space allocated for the cache		
	5	
Turn on BranchCache	Enabled	

User Configuration (Enabled)
No settings defined.

In the table below, identify the effective setting for the client computers in each branch office. Make one selection in each column. Each correct selection is worth one point.

Effective setting	Branch1 Computers	Branch2 Computers
Will not use BranchCache.	<input type="radio"/>	<input type="radio"/>
Will retrieve cached content from peers.	<input type="radio"/>	<input type="radio"/>
Will retrieve cached content from Server1.	<input type="radio"/>	<input type="radio"/>
Will retrieve cached content from Server2.	<input type="radio"/>	<input type="radio"/>

Answer:

Effective setting	Branch1 Computers	Branch2 Computers
Will not use BranchCache.	<input type="radio"/>	<input type="radio"/>
Will retrieve cached content from peers.	<input type="radio"/>	<input checked="" type="radio"/>
Will retrieve cached content from Server1.	<input type="radio"/>	<input type="radio"/>
Will retrieve cached content from Server2.	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 76

Your network contains an Active Directory domain and 100 Windows 8.1 client computers. All software is deployed by using Microsoft Application Virtualization (App-V) 5.0. Users are NOT configured as local administrators. Your company purchases a subscription to Microsoft Office 365 that includes Office 365 ProPlus. You need to create an App-V package for Office 365 ProPlus. What should you do?

- A. Run the Office Customization Tool (OCT), run the App-V Sequencer and then run Setup /Packager.
- B. Download the Office Deployment Tool for Click-to-Run, run the App-V Sequencer and then run Setup /Ad mm.
- C. Download the Office Deployment Tool for Click-to-Run, run Setup /Download and then run Setup /Packager.
- D. Run the Office Customization Tool (OCT), run Setup /Download and then run the App-V Sequencer.

Answer: C

Explanation:

<http://blogs.technet.com/b/pauljones/archive/2013/08/28/office-2013-click-to-run-with-configuration-manager-2012.aspx>

<http://technet.microsoft.com/en-us/library/cc179097%28v=office.15%29.aspx>

<http://technet.microsoft.com/en-us/library/hh825212.aspx>

<http://technet.microsoft.com/en-us/library/jj713463.aspx>

<http://technet.microsoft.com/en-us/library/dn144768.aspx>

QUESTION 77

You administer laptop and desktop computers that run Windows 8 Pro. Your company uses Active Directory Domain Services (AD DS) and Active Directory Certificate Services (AD CS). Your

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

company decides that access to the company network for all users must be controlled by two-factor authentication. You need to configure the computers to meet this requirement. What should you do?

- A. Install smart card readers on all computers.
Issue smart cards to all users.
- B. Enable the Password must meet complexity requirements policy setting.
Instruct users to log on by using the domain \username format for their username and their strong password.
- C. Create an Internet Protocol security (IPsec) policy that requires the use of Kerberos to authenticate all traffic.
Apply the IPsec policy to the domain.
- D. Issue photo identification to all users.
Instruct all users to set up and use PIN Logon.

Answer: A

Explanation:

Smart cards contain a microcomputer and a small amount of memory, and they provide secure, tamper-proof storage for private keys and X.509 security certificates. A smart card is a form of two-factor authentication that requires the user to have a smart card and know the PIN to gain access to network resources. Registry certificates cannot be used for two factor authentication. Although certificates are ideal candidates for two-factor authentication, registry certificates-which are protected by a strong private key and are the most appropriate certificates for two-factor authentication-cannot be used. The reason for this is that Windows does not support registry certificates and completely ignores them. As a result, organizations must deploy and manage complex and expensive smart card solutions rather than using registry based certificates.

<http://technet.microsoft.com/en-us/library/cc770519.aspx>

<http://technet.microsoft.com/en-us/library/jj200227.aspx>

QUESTION 78

You support computers that run Windows 8 and 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. Configure the user's documents library to include folders from network shares.
- B. Remove the .man extension from the user profile name.
- C. Add the .dat extension to the user profile name.
- D. Configure Folder Redirection by using the domain group policy.

Answer: D

Explanation:

A mandatory user profile is a special type of pre-configured roaming user profile that administrators can use to specify settings for users. With mandatory user profiles, a user can modify his or her desktop, but the changes are not saved when the user logs off. The next time the user logs on, the mandatory user profile created by the administrator is downloaded. There are two types of mandatory profiles: normal mandatory profiles and super-mandatory profiles. User profiles become mandatory profiles when the administrator renames the NTuser.dat file (the registry hive) on the server to NTuser.man. The .man extension causes the user profile to be a read-only profile. User profiles become super-mandatory when the folder name of the profile path ends in .man; for example, \\server\share\mandatoryprofile.man\. Super-mandatory user profiles are similar to normal mandatory profiles, with the exception that users who have super-mandatory profiles cannot log on when the server that stores the mandatory profile is unavailable. Users with normal mandatory profiles can log on with the locally cached copy of the mandatory profile. Only system administrators can make changes to mandatory user profiles.

Reference:

[http://msdn.microsoft.com/en-us/library/windows/desktop/bb776895\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb776895(v=vs.85).aspx)

<http://technet.microsoft.com/en-us/windows/hh868022.aspx>

QUESTION 79

Drag and Drop Questions

You administer desktop computers that run Windows 8 Enterprise and are members of an Active Directory domain. A new security policy states that all traffic between computers in the research department must be encrypted and authenticated by using Kerberos V5. You need to configure the requested traffic authentication settings by using Windows Firewall with Advanced Settings. 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.)

	Answer Area
Select Require authentication for inbound and outbound connection , and then for authentication method, select Computer (Kerberos V5) .	
Select Allow on app or feature through Windows Firewall .	
Click to expand Inbound Rule , and then select New Rule .	
Select the rule type Isolation , and then add the IP addresses of the research department computers.	
Click to expand Outbound Rule , and then select New Rule .	
Click to expand Connection Security Rule , and then select New Rule .	
Select the rule type Server-to-Server , and then add the IP addresses of the research department computers.	

Answer:

	Answer Area
Select Require authentication for inbound and outbound connection , and then for authentication method, select Computer (Kerberos V5) .	Click to expand Connection Security Rule , and then select New Rule .
Select Allow on app or feature through Windows Firewall .	Select the rule type Isolation , and then add the IP addresses of the research department computers.
Click to expand Inbound Rule , and then select New Rule .	Select Require authentication for inbound and outbound connection , and then for authentication method, select Computer (Kerberos V5) .
Select the rule type Isolation , and then add the IP addresses of the research department computers.	
Click to expand Outbound Rule , and then select New Rule .	
Click to expand Connection Security Rule , and then select New Rule .	
Select the rule type Server-to-Server , and then add the IP addresses of the research department computers.	

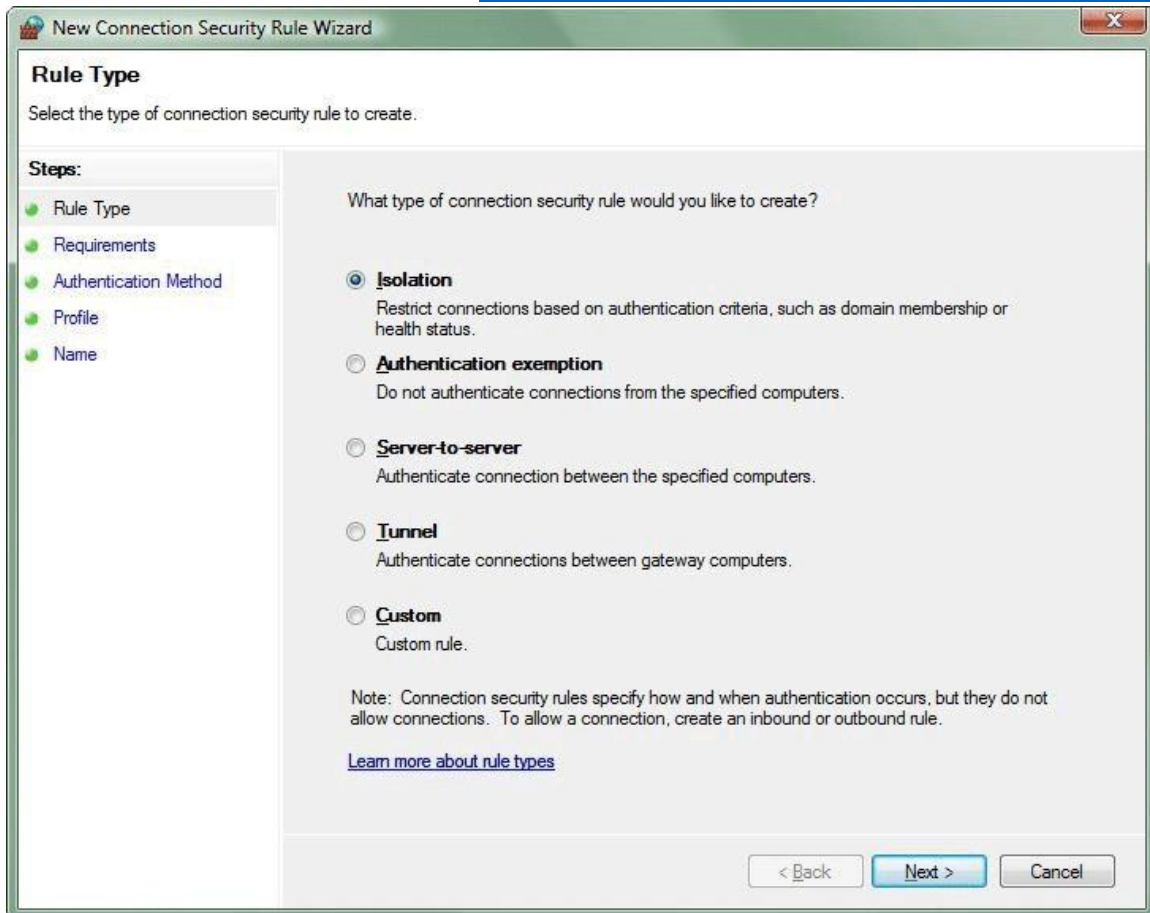
Explanation:

Note:

A connection security rule forces two peer computers to authenticate before they can establish a connection and to secure information transmitted between the two computers. Windows Firewall with Advanced Security uses IPsec to enforce these rules. To create a connection security rule:

1. In Windows Firewall with Advanced Security, in the console tree, click Connection Security Rules.
2. In the Actions list, click New Rule.

The Rule Type page, shown in the Figure below, allows you to select the type of rule you want to create. Select a type, and use the wizard to configure the new rule according to the information in the following sections.



Isolation. An isolation rule isolates computers by restricting inbound connections based on credentials, such as domain membership or compliance with policies that define the required software and system configurations. Isolation rules allow you to implement a server or domain isolation strategy. When you create an isolation rule, you will see the following wizard pages:

- Requirements. You can choose when authentication is required:
 - Request authentication for inbound and outbound connections.
 - Require authentication for inbound connections and request authentication for outbound connections.
 - Require authentication for inbound and outbound connections
- *Authentication Method.

You can select from the following authentication methods:

- Default. This selection uses the current computer default selections specified on the IPsec Settings tab of the Windows Firewall Properties page.
- Computer and user (Kerberos V5). This method uses both computer-and user-based Kerberos V5 authentication to restrict connections to domain-joined users and computers. User authentication, and therefore this method, is compatible only with computers running Windows Vista and later.
- Computer (Kerberos V5). This method uses Kerberos V5 authentication to restrict connections to domain-joined computers. This method is compatible with computers running Windows 2000 or later.
- Advanced. This setting allows you to designate multiple authentication methods, such as computer certificate, NTLMv2, and preshared key.
- Profile. Choose the profiles (Domain, Public, and Private) to which the rule applies.
- Name. Name the rule and type an optional description.

Reference: Creating Connection Security Rules

QUESTION 80

Your network contains an Active Directory domain. The domain contains 100 Windows 8.1 client computers. All of the computers secure all connections to computers on the internal network by using IPSec. The network contains a server that runs a legacy application. The server does NOT support IPSec. You need to ensure that some of the Windows 8 computers can connect to the legacy server. The solution must ensure that all other connections are secured by using IPSec. What should you do?

- A. Modify the settings of the Domain Profile.
- B. Create a connection security rule.
- C. Create an inbound firewall rule.
- D. Modify the settings of the Private Profile,

Answer: B

QUESTION 81

You are a systems administrator of a small branch office. Computers in the office are joined to a Windows 8 HomeGroup. The HomeGroup includes one shared printer and several shared folders. You join a new computer to the HomeGroup and try to access the HomeGroup shared folders. You discover that the shared folders are unavailable, and you receive an error message that indicates the password is incorrect. You need to reconfigure the new computer in order to access the HomeGroup resources. What should you do?

- A. Adjust the time settings on the new computer to match the time settings of the HomeGroup computers.
- B. Change the HomeGroup password and re-enter it on the computers of all members of the HomeGroup.
- C. Change the default sharing configuration for the shared folders on the HomeGroup computers.
- D. Reset your account password to match the HomeGroup password.

Answer: A

Explanation:

You may receive a misleading error message when trying to join a Windows 7 Homegroup, when the computer's date and time does not match the date/time of system that owns the homegroup. Symptoms When joining a system to a homegroup, you may receive the following error message "The password is incorrect", even though you have typed the password correctly. This can be caused by a difference in the Date and Time settings on the computer trying to join the homegroup, and not an invalid password. If the date/time of the computer joining a homegroup is greater than 24 hours apart from the date/time of the system that owns the homegroup, this will cause the error. Resolution:

Adjust the date/time settings on the system joining the homegroup, to match the system that owns the homegroup, and then try to join again.

<http://support.microsoft.com/kb/2002121>

QUESTION 82

Drag and Drop Question

Your network contains an Active Directory domain and 100 Windows 8.1 Enterprise client computers. All software is deployed by using Microsoft Application Virtualization (App-V) 5.0. Users are NOT configured as local administrators. Your company purchases a subscription to Microsoft Office 365 that includes Office 365 ProPlus. You need to create an App-V package for Office 365 ProPlus. Which three actions should you perform in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)

Actions	Answer Area
Run the App-V Sequencer.	
Download the Office Deployment Tool for Click-to-Run.	
Run Setup /Download.	
Run the Office Customization Tool (OCT).	
Run Setup /Packager.	
Run Setup /Admin.	

Answer:

Actions	Answer Area
Run the App-V Sequencer.	
	Download the Office Deployment Tool for Click-to-Run.
	Run Setup /Download.
Run the Office Customization Tool (OCT).	Run Setup /Packager.
Run Setup /Admin.	

Explanation:

<http://blogs.technet.com/b/pauljones/archive/2013/08/28/office-2013-click-to-run-with-configuration-manager-2012.aspx>

QUESTION 83

Drag and Drop Questions

You administer computers that run Windows 8. The computers on your network are produced by various manufacturers and often require custom drivers. You need to design a recovery solution that allows the repair of any of the computers by using a Windows Recovery Environment (WinRE). In which order should you perform the actions? (To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.)

	Answer Area
Create a bootable WinRE Recovery media.	
Extract WinRE files from the Windows Assessment and Deployment Kit (ADK).	
Unmount the image file.	
Add additional drivers.	
Mount the WinRE image file.	
Commit the changes.	

Answer:

	Answer Area
Create a bootable WinRE Recovery media.	Extract WinRE files from the Windows Assessment and Deployment Kit (ADK).
Extract WinRE files from the Windows Assessment and Deployment Kit (ADK).	Mount the WinRE image file.
Unmount the image file.	Add additional drivers.
Add additional drivers.	Unmount the image file.
Mount the WinRE image file.	Commit the changes.
Commit the changes.	Create a bootable WinRE Recovery media.

Explanation:

Note:

- The Windows Assessment and Deployment Kit (Windows ADK) is a collection of tools and documentation that you can use to customize, assess, and deploy Windows operating systems to new computers.

- Walkthrough: Create a Custom Windows PE Image.

Step 1: Set Up a Windows PE Build Environment

Step 2: Mount the Base Windows PE Image

Step 3: Add Boot-Critical Drivers

Step 4: Add Optional Components

Step 5: Add Language Support (Optional)

Step 6: Add More Customization (Optional)

Step 7: Commit Changes

- Walkthrough: Create a Windows RE Recovery Media.

Step 1: Create a Windows RE Image

Step 2: Create a bootable media

QUESTION 84

You administer computers that run Windows 8 Enterprise in an Active Directory domain in a single Active Directory Site. All user account objects in Active Directory have the Manager attribute populated. The company has purchased a subscription to Windows Intune. The domain security groups are synchronized with the Microsoft Online directory. You create a Windows Intune group that specifies a manager as a membership criterion. You notice that the group has no members. You need to ensure that users that meet the membership criteria are added to the Windows Intune group. What should you do?

- A. Force Active Directory replication within the domain.
- B. Ensure that all user accounts are identified as synchronized users.
- C. Ensure that the user who is performing the search has been synchronized with the Microsoft Online directory.
- D. Synchronize the Active Directory Domain Service (AD DS) with the Microsoft Online directory.

Answer: B

Explanation:

Add Computers, Users, and Mobile Devices.

<http://technet.microsoft.com/library/hh441723.aspx>

<http://technet.microsoft.com/en-us/windows/intune.aspx>

QUESTION 85

You support laptops that run Windows 8 Pro and are part of a workgroup. An employee is unable to start Windows Mobility Center on his laptop. You need to make it possible for the employee to use Windows Mobility Center on the laptop. What should you do?

- A. Use Add features to Windows 8 to add Windows Mobility Center.

- B. Use Programs and Features to repair the installation of Windows Mobility Center.
- C. Use Local Group Policy Editor to set Turn off Windows Mobility Center to Not Configured.
- D. Use Turn Windows features on or off in Programs and Features to enable Windows Mobility Center.

Answer: C

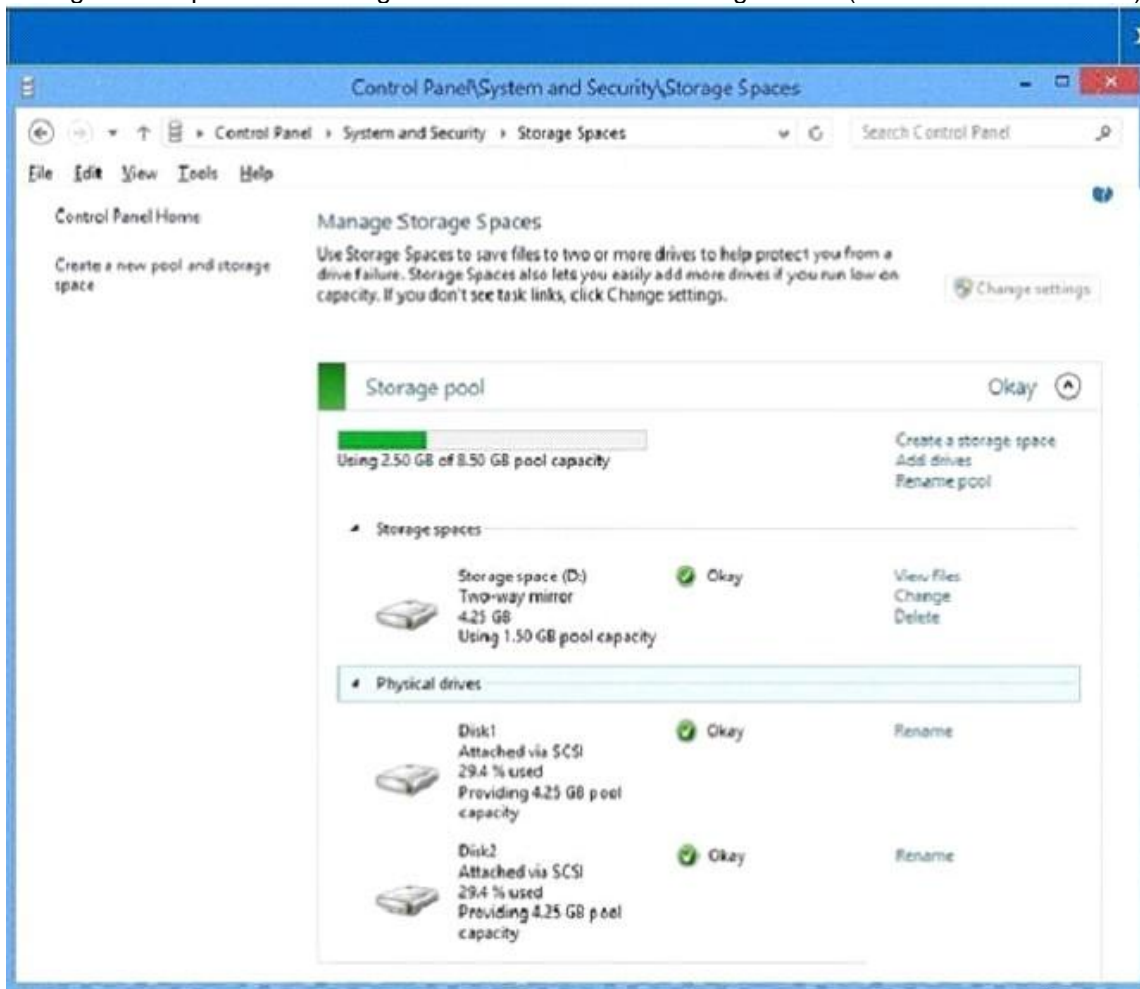
Explanation:

To Enable or Disable Windows Mobility Center using Group Policy Open the all users, specific users or groups, or all users except administrators Local Group Policy Editor for how you want this policy applied. In the left pane, click/tap on to expand User Configuration, Administrative Templates, Windows Components, and Windows Mobility Center. In the right pane of Windows Mobility Center, double click/tap on Turn off Windows Mobility Center to edit it. To Enable Windows Mobility Center:

- Select either Not Configured or Disabled.
- Click OK.

QUESTION 86

You have a Windows 8.1 Enterprise client computer named Computer1. The Storage Spaces settings of Computer1 are configured as shown in the following exhibit. (Click the Exhibit button.)



You plan to create a three-way mirror storage space in the storage pool and to set the size of the storage space to 50 GB. You need to identify the minimum number of disks that must be added to the storage pool for the planned mirror. How many disks should you identify?

- A. 1
- B. 3
- C. 4
- D. 5

Answer: D

Explanation:

In Windows Server 2012 Storage Spaces and Windows 8 Storage Spaces, a 2-way mirror requires at least 2 physical disks.

However, a 3-way mirror requires at least 5 physical disks.

The reason is that a 3-way mirror uses a quorum. In order to keep running, the mirror space must keep over 50% of the disks functioning.

So a 3-way mirror must have at least 5 physical disks to be able to survive the loss of up to 2 physical disks.

QUESTION 87

Your company has Windows 10 client computers. All of the computers are managed by using Windows Intune. You need to provide a user with the ability to deploy software to the computers by using Windows Intune. The solution must minimize the number of permissions assigned to the user. Which role should you use?

- A. User management administrator from the Windows Intune account portal
- B. Global administrator from the Windows Intune account portal
- C. Service administrator from the Windows Intune administrator console
- D. Service administrator from the Windows Intune account portal

Answer: C

Explanation:

As a service administrator, you use the Microsoft Intune administrator console to manage day-to-day tasks, such as deploying applications, for Intune.

QUESTION 88

Your company has a main office that has a connection to the Internet. The company has 100 Windows 10 Pro client computers that run Microsoft Office 2010. You purchase a subscription to Office 365 for each user. You download the Office Deployment Tool for Click-to-Run. You need to deploy Office 365 Pro Plus to the computers. The solution must minimize the amount of traffic over the Internet connection. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. On a file server, run setup.exe and specify the /download parameter.
- B. On each client computer, run setup.exe and specify the /configure parameter.
- C. On a file server, run setup.exe and specify the /configure parameter.
- D. On each client computer, run setup.exe and specify the /download parameter.

Answer: AB

Explanation:

[https://technet.microsoft.com/en-us/windows/jj219423\(v=office.14\)](https://technet.microsoft.com/en-us/windows/jj219423(v=office.14))

QUESTION 89

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 10. A local printer is shared from a client computer. The client computer user is a member of the Sales AD security group. You need to ensure that members of the Sales security group can modify the order of documents in the print queue, but not delete the printer share. Which permission

should you grant to the Sales group?

- A. Manage queue
- B. Manage this printer
- C. Print
- D. Manage documents
- E. Manage spooler

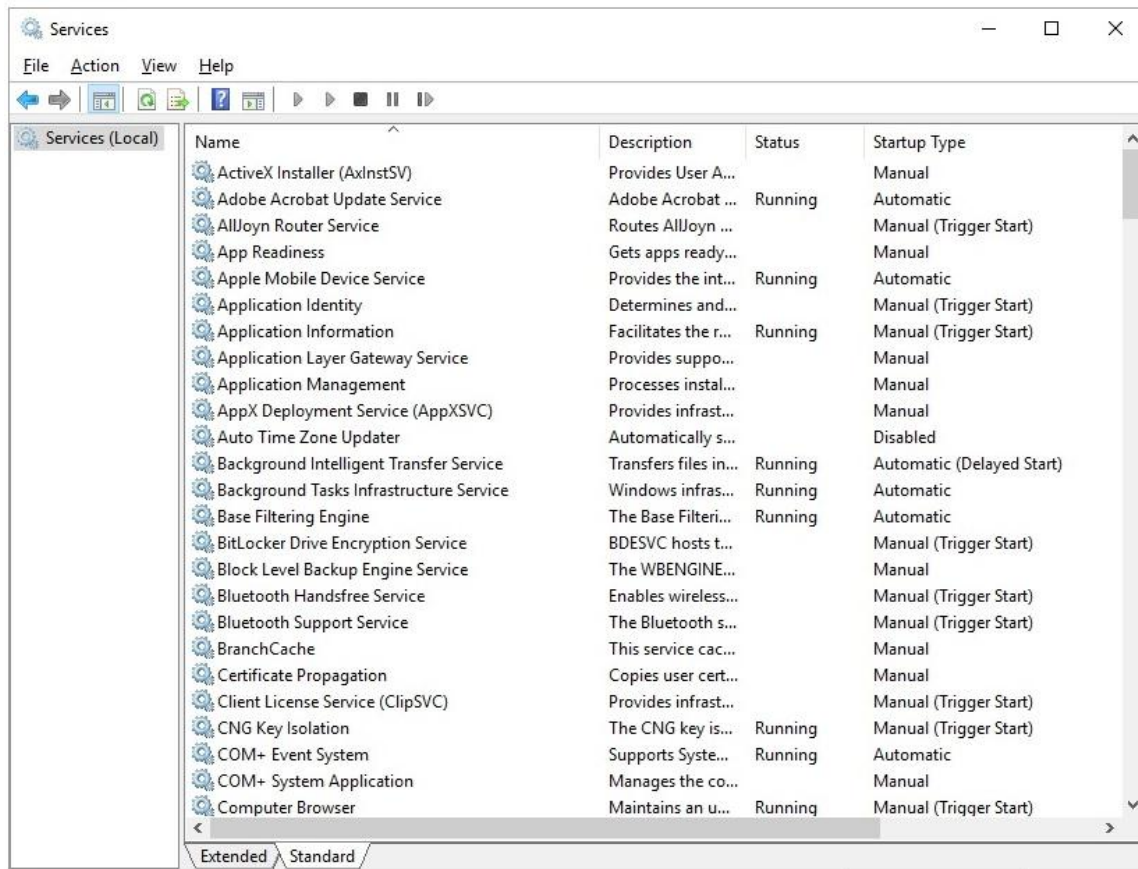
Answer: D

Explanation:

With the Manage Documents permission the user can pause, resume, restart, cancel, and rearrange the order of documents submitted by all other users. The user cannot, however, send documents to the printer or control the status of the printer.

QUESTION 90

You have a computer that runs Windows 10. You have an application control policy on the computer. You discover that the policy is not enforced on the computer. You open the Services snap-in as shown in the exhibit. (Click the Exhibit button.)



You need to enforce the application control policy on the computer. What should you do?

- A. Set the Application Identity service Startup Type to Automatic and start the service.
- B. Set the Application Information service Startup Type to Automatic and start the service.
- C. Set the Application Management service Startup Type to Automatic and start the service.
- D. Set the Application Experience service Startup Type to Automatic and start the service.

Answer: A

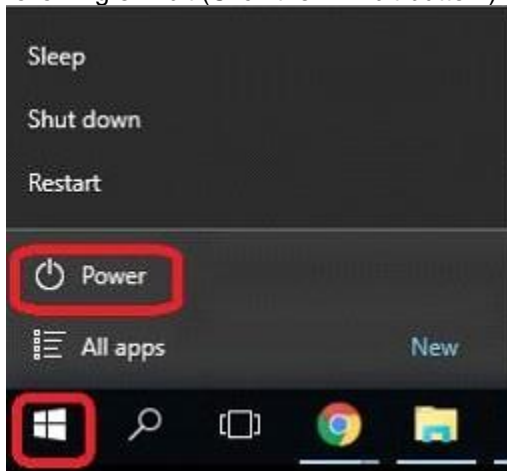
Explanation:

AppLocker, and its applications control policies, relies upon the Application Identity Service being active. Note: When you install Windows 7, the startup type of the Application Identity Service is set to Manual. When testing AppLocker, you should keep the startup type as Manual in case you configure rules incorrectly. In that event, you can just reboot the computer and the AppLocker rules will no longer be in effect. Only when you are sure that your policies are applied correctly should you set the startup type of the Application Identity Service to Automatic.

QUESTION 91

Drag and Drop Question

You administer Windows 8 Pro computers in your company network. You discover that Sleep, Shut down and Restart are the only options available when you select the Power button as shown in the following exhibit (Click the Exhibit button.)



You need to enable hibernation on the computer. Which three steps should you perform in sequence?

Actions	Answers
Change the When I press the power button menu settings.	
From the Charm Bar, open Change PC settings .	
Select Don't require a password	
Select What the power button does .	

Answer:

Actions	Answers
	From the Charm Bar, open Change PC settings .
	Select What the power button does .
Select Don't require a password	Change the When I press the power button menu settings.

Explanation:

<http://www.addictivetips.com/windows-tips/how-to-enable-windows-8-hibernate-option/>

QUESTION 92

Drag and Drop Question

A local printer named PRINTER1 is shared from a client computer named COMPUTER1 that run a 32-bit version of Windows 10. A workgroup contains client computers that run a 64-bit version of Windows 10. Computers in the workgroup can't currently print to PRINTER1. You need to ensure that the workgroup computers can print to PRINTER1. Which three actions should you perform in sequence?

Connect the workgroup computers to PRINTER1.
Add the driver on COMPUTER1.
Obtain the 32-bit driver for PRINTER1.
Obtain the 64-bit driver for PRINTER1.
Install the driver on one computer in the workgroup.

Answer:

	Obtain the 64-bit driver for PRINTER1.
	Add the driver on COMPUTER1.
Obtain the 32-bit driver for PRINTER1.	Connect the workgroup computers to PRINTER1.
Install the driver on one computer in the workgroup.	

Explanation:

You can very well add a 64-bit printer driver to a local printer on a 32-bit Windows operating system. After the 64-bit driver has been added connect the 64-bit Windows 10 computers to the printer.

Incorrect Answers:

- * There is no need for a 32-bit driver. We need a 64-bit driver.
- * We should add, not install, the driver on the computer which is attached to the printer.
<https://support.microsoft.com/en-us/kb/3041911>

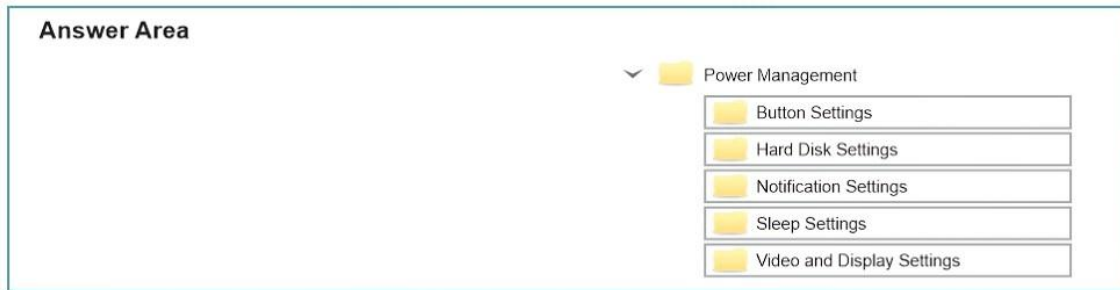
QUESTION 93

Hotspot Question

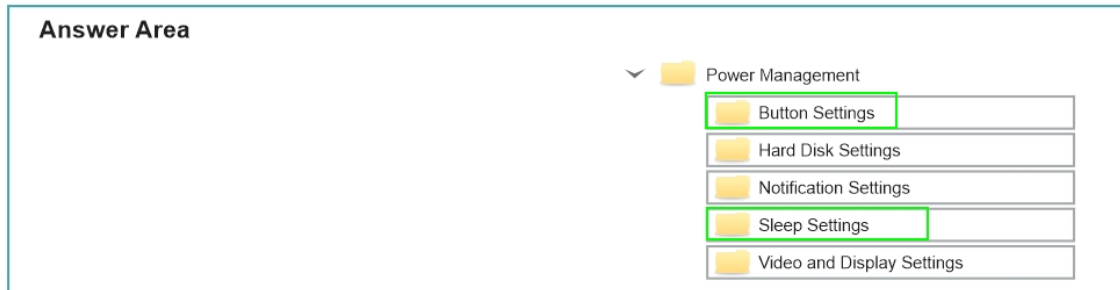
You plan to use a Group Policy to configure the power settings of several laptops. You need to ensure that the laptops meet the following requirements:

- Enter hibernation mode when the lid is closed.
- Enter sleep mode when the battery level is critical.

Which two Power Management Group Policy settings should you modify? To answer, select the appropriate settings in the answer area.



Answer:



QUESTION 94

You administer Windows 10 Enterprise client computers in your company network. You change settings on a reference computer by using the Windows Firewall with Advanced Security tool. You want to apply the same settings to other computers. You need to save the windows Firewall with Advanced Security configuration settings from the reference computer. You also need to be able to import the configuration settings into a Group Policy object later. What should you do?

- A. Open Local Group Policy Editor, select the Windows Firewall with Advanced Security node, and then select the Export Policy action.
- B. Run the netsh advfirewall export c:\settings.wfw command.
- C. Run the netsh firewall export c:\settings.xml command.
- D. Run the netsh advfirewall export c:\settings.xml command.

Answer: A

QUESTION 95

A company has Windows 10 Enterprise computers in an Active Directory Domain Services (AD DS) domain. A computer named COMPUTER1 has a shared printer named PRINTER1 installed and has Remote Desktop enabled. A user named Intern is a member of a security group named Sales. The Sales group is a member of the Remote Desktop Users group on COMPUTER1. Only the Sales group has access to PRINTER1. You need to configure COMPUTER1 to meet the following requirements:

- Allow only Intern to establish Remote Desktop connections to COMPUTER1.
- Allow Intern to print to PRINTER1.

What should you do?

- A. Assign Intern the Deny log on user right by using the Remote Desktop Services user right.
- B. Assign Intern the Deny access to this computer from the network user right.
Assign the Sales group the Allow log on locally user right.
- C. Remove Intern from the sales group.
- D. Remove the Sales group from the Remote Desktop Users group and add Intern to the Remote Desktop Users

group.

Answer: D

QUESTION 96

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question. You have an application named app1 installed on computer named Computer1. Computer1 runs Windows10. App1 saves data to %UserProfile% \App1\Data. You need to ensure that you can recover the App1 data if Computer1 fails. What should you configure?

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

Answer: F

QUESTION 97

You are the network administrator for Contoso, Ltd. Many users have Windows 10 Enterprise laptops, and your IT department configures all of the to use BitLocker on all fixed drives. Many users carry sensitive corporate data on their USB drives. You need to enable BitLocker for these USB drives. Which key protector option should you use?

- A. a smartcard
- B. a startup key
- C. TPM+PIN
- D. TPM+Password

Answer: D

Explanation:

<https://www.groovypost.com/howto/use-bitlocker-encryption-windows-10/>

QUESTION 98

You administer Windows 10 Enterprise client computers in your company network. A user reports that her Internet connection is slower than usual. You need to identify the Process Identifiers (PIDs) of applications that are making connections to the Internet. Which command should you run?

- A. netstat -an
- B. jpconfig /showclassid
- C. netstat -o
- D. netsh set audit-logging
- E. netsh show netdls

Answer: C

Explanation:

<http://technet.microsoft.com/en-us/library/bb490947.aspx>

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

Netstat

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

Syntax

netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Parameters

-a : Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

-n : Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

-o : Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.

Further Information: netstat -an - there is no "an" parameter.

<http://technet.microsoft.com/en-us/library/cc940124.aspx>

QUESTION 99

Your network contains an Active Directory domain. The domain contains 100 computers that run Windows 10. You plan to develop a line-of-business application and to deploy the application by using Windows Store for Business. You need to ensure that users can see the private store of your company when they sign in to the Windows Store for Business. What should you do first?

- A. Provision a Windows Dev Center dev account for each user.
- B. Assign the Windows Store Purchaser role to each user.
- C. Assign the Windows Store Admin role to each user.
- D. Provision a Microsoft Azure Active Directory (Azure AD) account for each user.
- E. Provision a Microsoft account for each user.

Answer: D

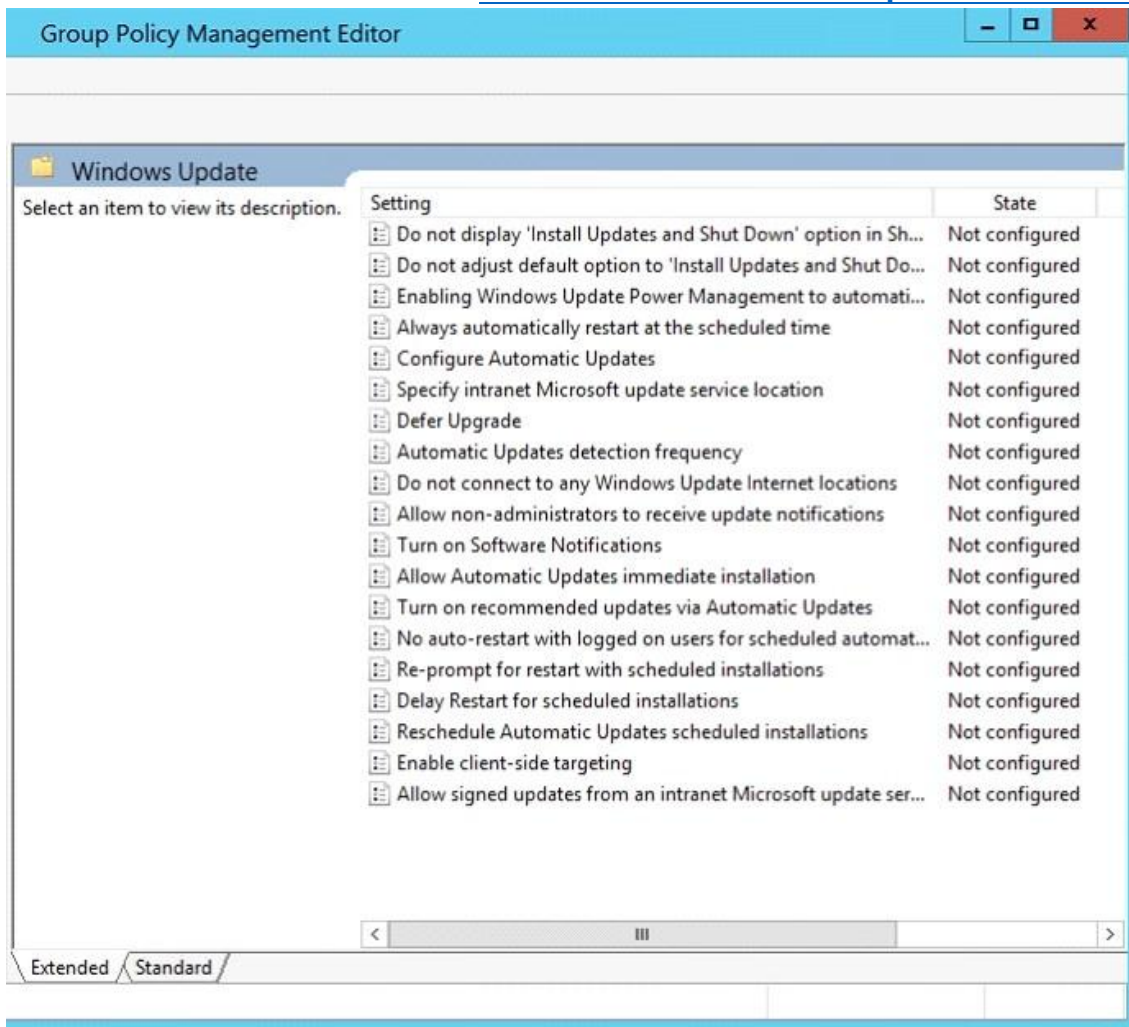
Explanation:

<https://www.sepago.de/blog/2016/02/18/windows-10-enterprise-serie-windows-business-store>

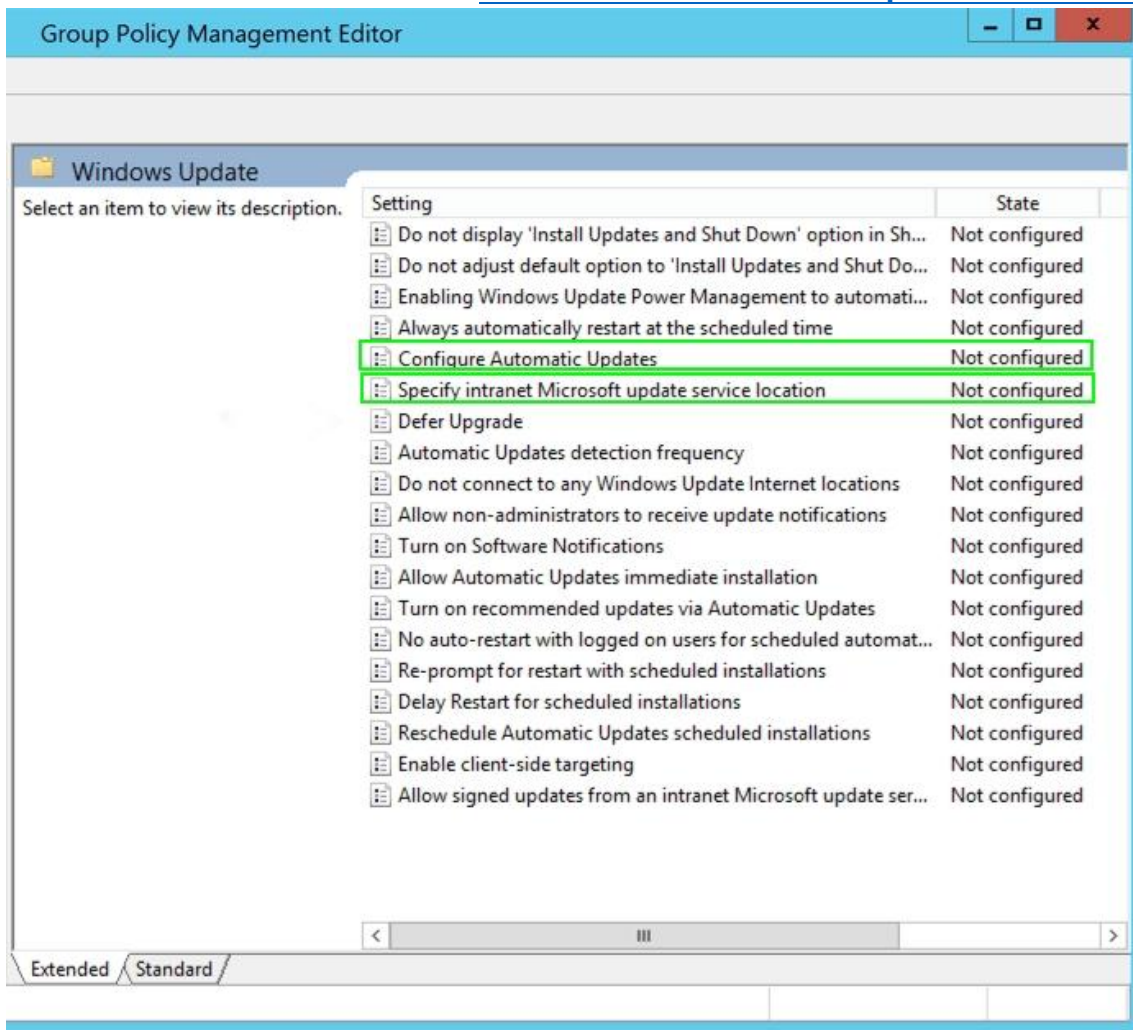
QUESTION 100

Hotspot Question

You have an Active Directory domain. All of the client computers in the domain run Windows 10 Enterprise. You need to configure the client computers to download updates from a Windows Server Update Service server. Which two settings should you configure? To answer, select the appropriate settings in the answer area.



Answer:



QUESTION 101

Your company has a standard power scheme for the sales team. You are replacing a laptop for a sale associate. You import the power scheme onto the new laptop. You need to apply the power scheme. What should you do?

- A. Modify the power scheme under Power and Sleep settings.
- B. Run the gpupdate /F command.
- C. Run the powercfg /S command.
- D. Modify the advanced power settings.

Answer: C

Explanation:

To Import a Power Plan

1. Open an elevated command prompt.
2. Type the command below into the command prompt, and press Enter to export the power plan.
3. Substitute Full path of .pow file in the command above with the actual full path of the .pow file of the power plan you exported in Option One. For example: powercfg -import "%UserProfile%\Desktop\PowerPlanBackup.pow".
4. When finished, you can close the command prompt if you like.
5. Users on the PC will now be able to select the imported power plan as their active power plan.

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

QUESTION 102

All client computers in a company's network environment run Windows 10 Enterprise. A client computer has drives that are configured as shown in the following table.

Drive	Location	Type
C:	Internal	Dynamic
D:	Internal	Dynamic
E:	Internal	Optical
F:	External	Basic
Z:	Network	Mapped

You are choosing a backup destination for drive C. You have the following requirements:

- Ensure that the backup file is available if drive C: fails.
- Ensure that the backup file can be accessed by other computers on the network.
- Support the storage of multiple versions of system image backups.

You need to select a backup destination that meets the requirements. Which destination should you select?

- A. drive D:
- B. drive F:
- C. drive E:
- D. drive Z:

Answer: B

QUESTION 103

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question. A user successfully accesses \\server1\Sources\App1\. The user cannot access \\server1\Sources\App2\. You need to ensure that the user can access \\server1\Sources\App2\. What should you configure?

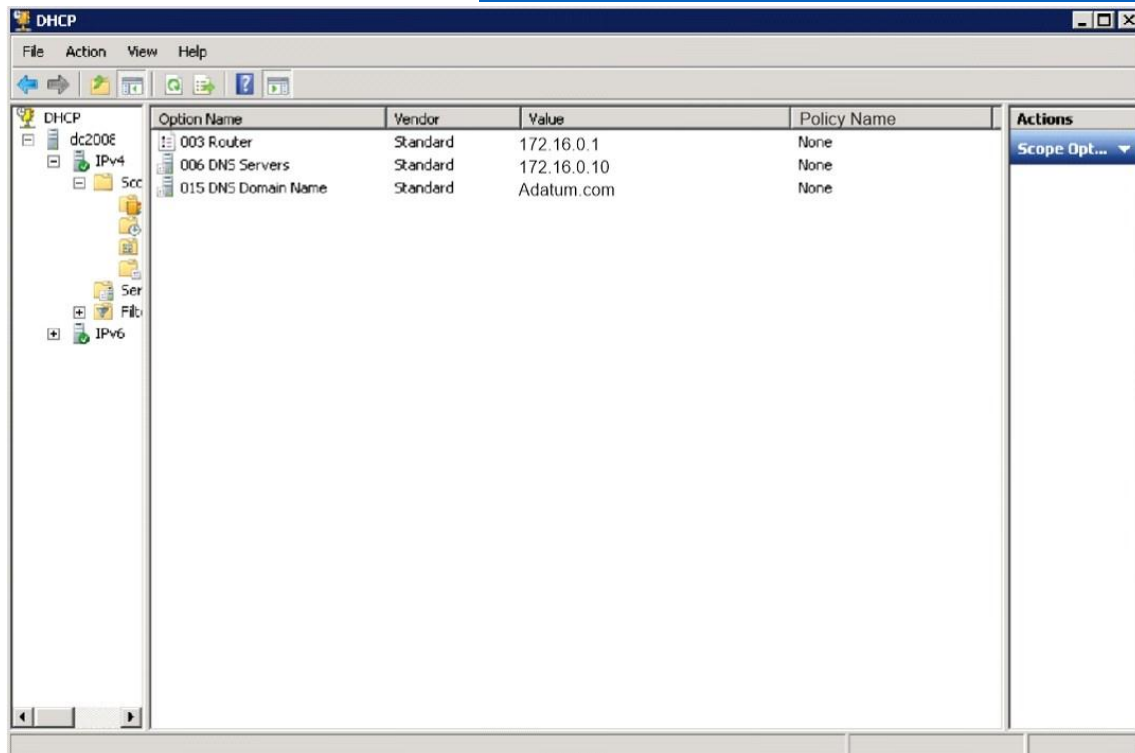
- A. Microsoft OneDrive
- B. share permission
- C. account policies
- D. software restriction policies
- E. HomeGroup settings
- F. application control policies
- G. NTFS permissions
- H. Encrypting File System (EFS) settings

Answer: G

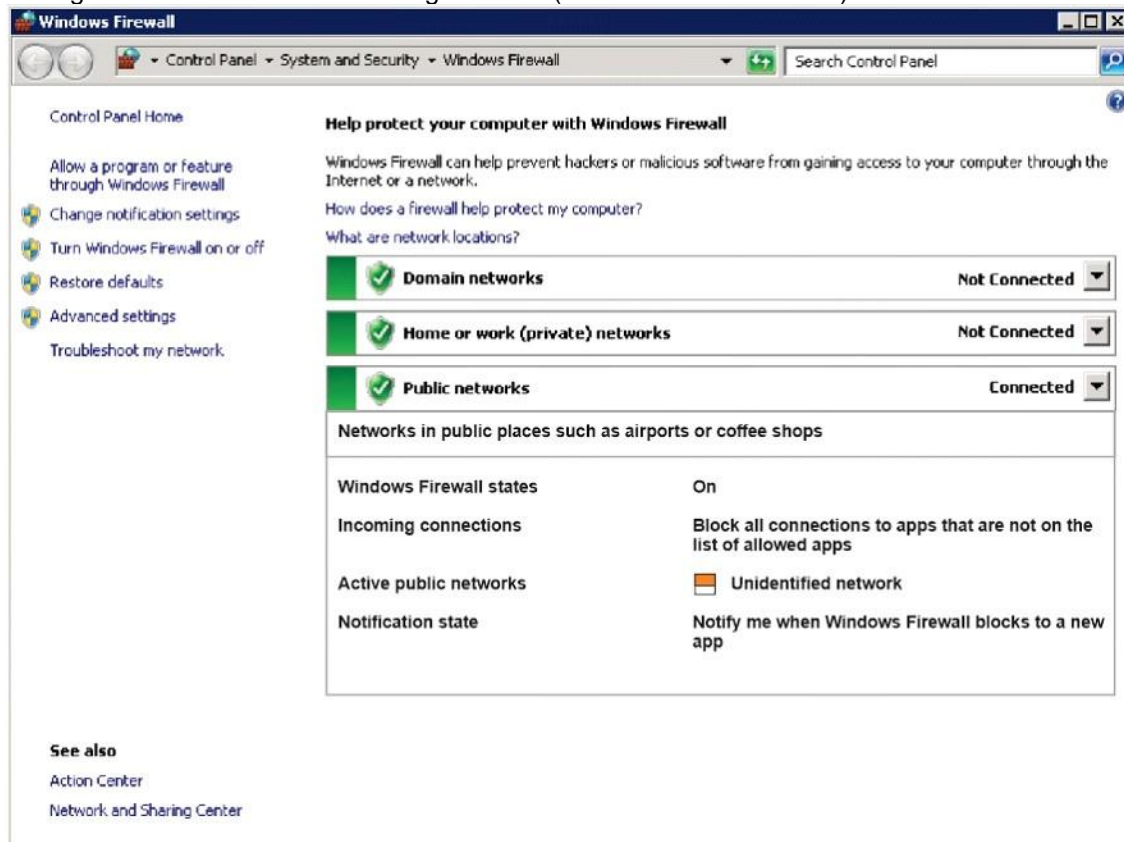
QUESTION 104

Hotspot Question

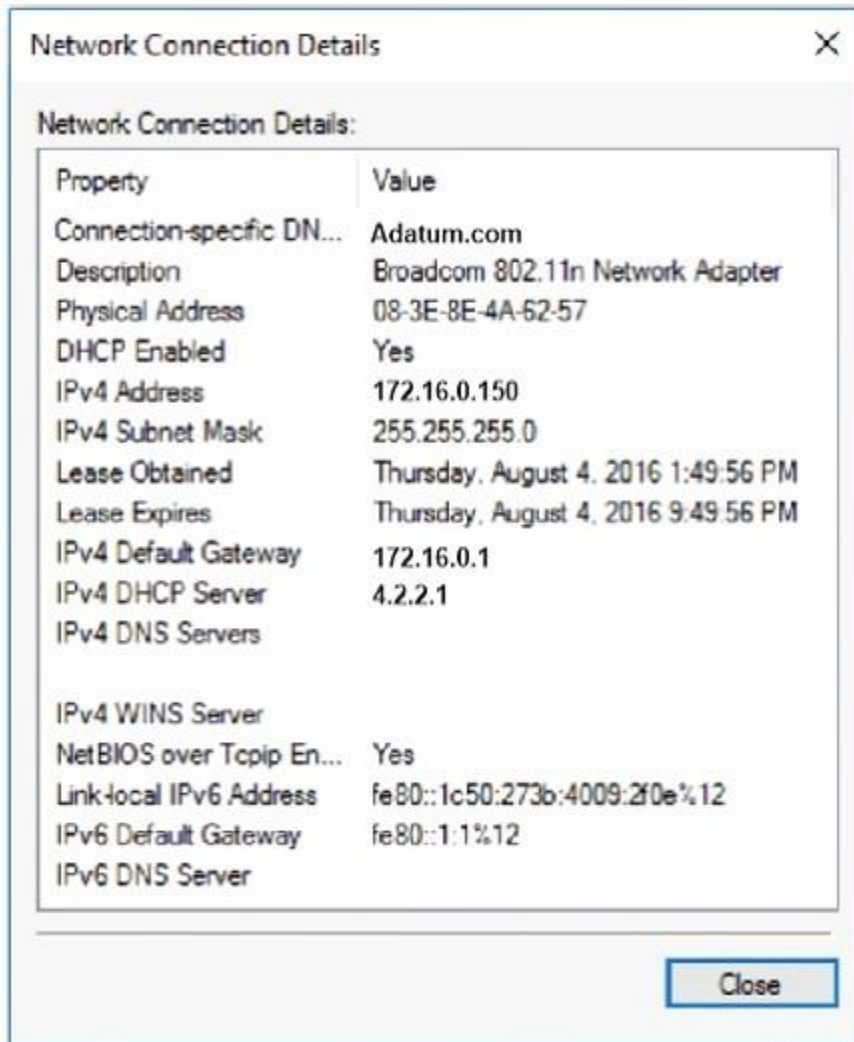
You have DHCP server. The server has a scope that is configured as shown in the DHCP scope exhibit. (Click the Exhibit button.)



A user fails to access internal websites and resources. The computer of the user has the firewall settings shown in the Firewall settings exhibit. (Click the Exhibit button.)



The computer also has the network settings shown in the Network Settings exhibit. (Click the Exhibit button.)



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

Answer Area			
Statements	Yes	No	
The computer has a valid DHCP lease.	<input type="radio"/>	<input type="radio"/>	
The computer is configured to use the correct DNS server.	<input type="radio"/>	<input type="radio"/>	
The Windows Firewall service runs on the computer.	<input type="radio"/>	<input type="radio"/>	

Answer:

Statements	Yes	No
The computer has a valid DHCP lease.	<input checked="" type="radio"/>	<input type="radio"/>
The computer is configured to use the correct DNS server.	<input type="radio"/>	<input checked="" type="radio"/>
The Windows Firewall service runs on the computer.	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 105

You purchase a new Windows 10 Enterprise desktop computer. You have six external USB hard drives. You want to create a single volume by using the six USB drives. You want the volume to be expandable, portable, and resilient in the event of simultaneous failure of two USB hard drives. You need to create the required volume. What should you do?

- A. From Control Panel, create a new Storage Space across 6 USB hard drives. Set resiliency type to Parity.
- B. From Disk Management create a new striped volume.
- C. From Disk Management, create a new spanned volume.
- D. From control Panel, create a new Storage Space across 6 USB hard drives. Set resiliency type to Three-way mirror.

Answer: D

Explanation:

Resiliency

Storage Spaces supports four types of resiliency:

Simple: A simple storage space writes one copy of your data and does not protect you from driver failures. This option requires, at least, one drive, and each new additional drive adds another point of failure.

Two-way mirror: This option writes two copies of your data on the drives, which can protect your data from a single driver failure. Two-way mirror requires a least two drives.

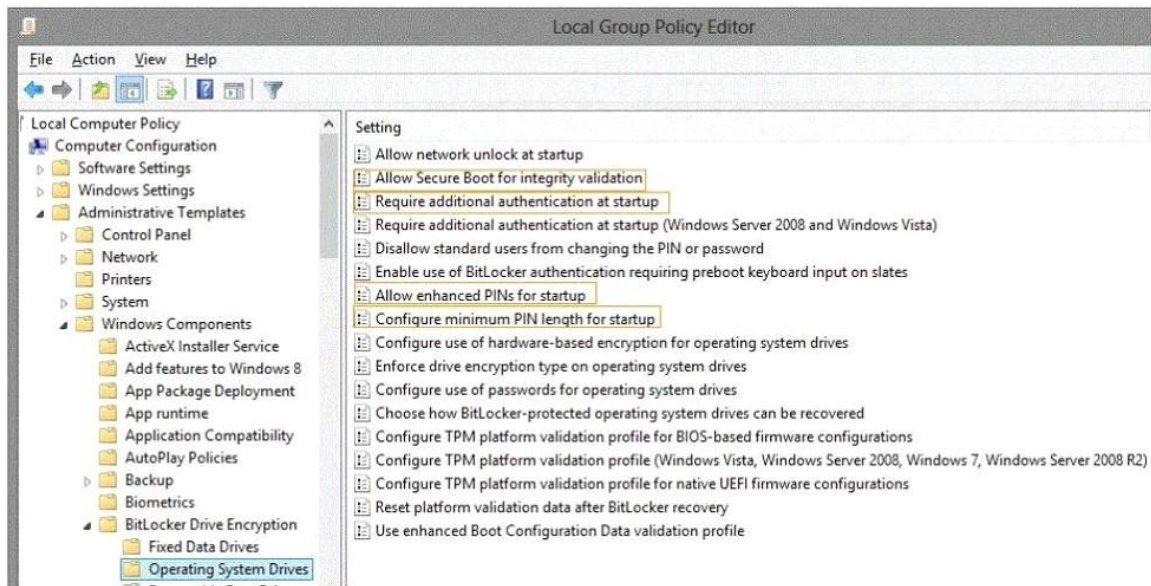
Three-way mirror: This option works similar to the two-way mirror, but it writes three copies of your data on the drives, which will help you to protect your data from two simultaneous drive failures. Three-way mirror requires, at least, three drives.

Parity: Similar to the standard RAID 5 technology, Parity for a storage space writes your data with parity information on the available driver to help you protect your data from a single driver failure. This option requires a least three drivers.

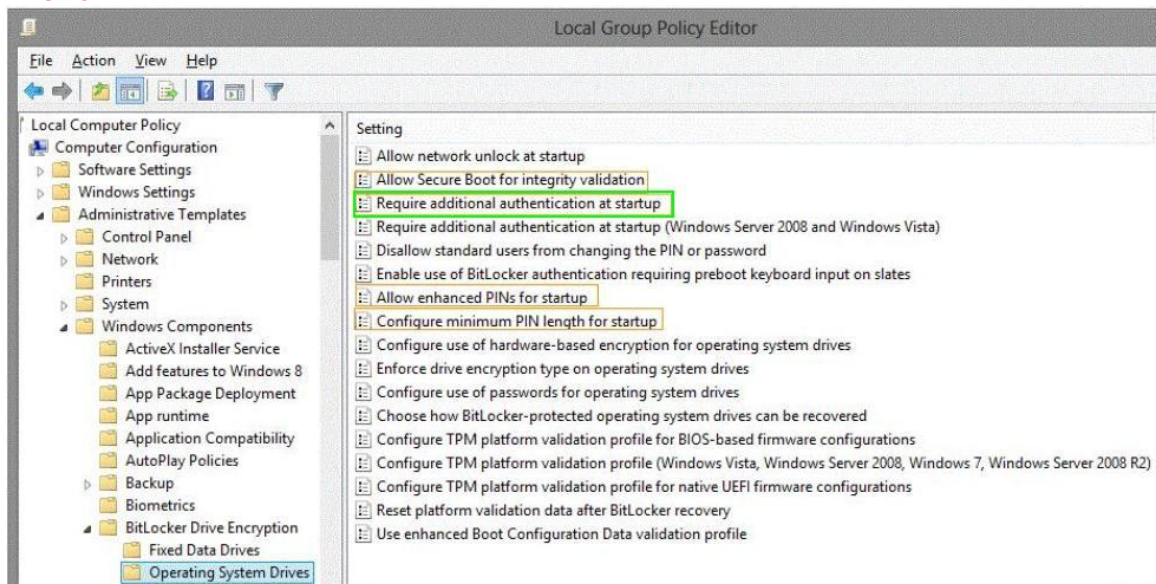
QUESTION 106

Hotspot Question

You administer Windows 10 Enterprise computers in your company network. All computers include Windows 10 Enterprise compatible Trusted Platform Module (TPM). You configure a computer that will run a credit card processing application. You need to ensure that the computer requires a user to enter a PIN code when starting the computer. Which policy should you configure? (To answer, select the appropriate policy in the answer area.)



Answer:



QUESTION 107

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question. You have a computer that runs Windows 10 and is used by 10 users. The computer is joined to an Active Directory domain. All of the users are members of the Administrators group. Each user has an Active Directory account. You have a Microsoft Word document that contains confidential information. You need to ensure that you are the only user who can open the document. What should you configure?

- A. account policies
- B. application control policies
- C. HomeGroup settings

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

Answer: H

QUESTION 108

Hotspot Question

You plan to deploy a Microsoft Azure RemoteApp hybrid collection. You plan to use a custom template image named Image1 to deploy the hybrid collection. You need to identify the role and feature that must be enabled in the image to support the deployment of the hybrid collection. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Role:

- Remote Desktop Connection Broker
- Remote Desktop Licensing Server
- Remote Desktop Session Host
- Remote Desktop Virtualization Hosts

Feature:

- Desktop Experience
- Quality Windows Audio Video Experience
- Windows Internal Database

Answer:

Answer Area

Role:

- Remote Desktop Connection Broker
- Remote Desktop Licensing Server
- Remote Desktop Session Host
- Remote Desktop Virtualization Hosts

Feature:

- Desktop Experience
- Quality Windows Audio Video Experience
- Windows Internal Database

Explanation:

Link a template image. Azure RemoteApp uses a Windows Server 2012 R2 template image to host all the programs that you want to share with your users. To create a custom RemoteApp template image, you can start with an existing image or create a new one. I created a new one. The requirements for the image that can be uploaded for use with Azure RemoteApp are:

- It must be on a VHD file (VHDX files are not currently supported). The VHD can be either fixed-size or dynamically expanding. A dynamically expanding VHD is recommended because it takes less time to upload to Azure than a fixed-size VHD file.
- The disk must be initialized using the Master Boot Record (MBR) partitioning style. The GUID partition table (GPT) partition style is not supported. The VHD must contain a single installation of Windows Server 2012 R2. It can contain multiple volumes, but only one that contains an installation

of Windows. The Remote Desktop Session Host (RDSH) role and the Desktop Experience feature must be installed.

- The Encrypting File System (EFS) must be disabled. The image must be SYSPREPED using the parameters /oobe /generalize /shutdown (DO NOT use the /mode:vm parameter).

QUESTION 109

Drag and Drop Question

You have a line-of-business universal app named Appl. You have an image of Windows 10 Enterprise named Image1. Image1 is mounted to the C:\Folder1 folder on a Windows 10 Enterprise computer named Computer1. The source for App1 is in the C:\folder2 folder. You need to ensure that App1 is included in Image1. What command should you run on Computer1? To answer, drag the appropriate values to the correct locations. Each value 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.

Values

- Add-AppxPackage
- Add-AppxProvisionedPackage
- Online
- PackagePath
- Path
- SkipLicense

Answer Area

Value C:\Folder1

Value C:\Folder2\App1.appx Value

Answer:

Values

- Add-AppxPackage
- Add-AppxProvisionedPackage
- Online
- PackagePath
- Path
- SkipLicense

Answer Area

Add-AppxProvisionedPackage -Path C:\Folder1

-PackagePath C:\Folder2\App1.appx -SkipLicense

Explanation:

<https://technet.microsoft.com/en-us/library/dn376490.aspx>

QUESTION 110

You have a Microsoft Intune subscription. You need to uninstall the Intune agent from a computer. What should you do?

A. From the Groups node in the Microsoft Intune administration portal, click Delete.

- B. From the computer run the provisioningutil.exe command.
- C. From the computer, run the cltui.exe command.
- D. From the computer use Programs and Features in Control Panel.

Answer: B

QUESTION 111

A company has 100 client computers that run Windows 8.1. The client computers are members of a workgroup. A custom application requires a Windows Firewall exception on each client computer. You need to configure the exception on the client computers without affecting existing firewall settings. Which Windows PowerShell cmdlet should you run on each client computer?

- A. New-NetFirewallRule
- B. Set-NetFirewallSetting
- C. Set-NetFirewallRule
- D. Set-NetFirewallProfile
- E. New-NetIPSecMainModeRule

Answer: A

Explanation:

<http://technet.microsoft.com/en-us/library/jj554908.aspx>

New-NetFirewallRule. The New-NetFirewallRule cmdlet creates an inbound or outbound firewall rule and adds the rule to the target computer.

Further information:

- Set-NetFirewallSetting

The Set-NetFirewallSetting cmdlet configures properties that apply to the firewall and IPsec settings, regardless of which network profile is currently in use. This cmdlet allows the administrator to specify global firewall behavior.

- Set-NetFirewallRule

The Set-NetFirewallRule cmdlet modifies existing firewall rule properties.

- Set-NetFirewallProfile

The Set-NetFirewallProfile cmdlet configures options for the profiles, including domain, public, and private, that are global, or associated with the input rules.

- New-NetIPSecMainModeRule

The New-NetIPSecMainModeRule cmdlet creates an IPsec main mode rule. A main mode rule contains a set of local and remote end points to determine the peers to which it applies. When an application on the local computer attempts to communicate with one of these specified remote hosts, the computer attempts to establish a security association (SA) with the remote server.

QUESTION 112

You create a VPN connection that has the VPN type set to Automatic. When attempting to establish a VPN connection, which VPN protocol will be used first?

- A. PPTP
- B. L2TP
- C. SSTP
- D. IKEv2

Answer: D

Explanation:

<https://blogs.technet.microsoft.com/networking/2014/01/13/configuring-native-vpn-client-through-pc-settings/>

QUESTION 113

Drag and Drop Question

You have a Microsoft Intune subscription. You need to identify devices based on the following requirements:

- Devices that are jailbroken or rooted.
- Devices that are remote wiped or deleted.
- Devices that have blacklisted applications installed.

Which type of report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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.

● ● ● ● ●

Reports	Answer Area
Computer Inventory	Devices that are jailbroken or rooted: Report
Detected Software	Devices that have blacklisted applications installed: Report
Device History	Devices that are remote wiped or deleted: Report
Machine Device Inventory	
Noncompliant Apps	
Update	

Answer:

● ● ● ● ●

Reports	Answer Area
Computer Inventory	Devices that are jailbroken or rooted: Machine Device Inventory
Detected Software	Devices that have blacklisted applications installed: Noncompliant Apps
Device History	Devices that are remote wiped or deleted: Device History
Machine Device Inventory	
Noncompliant Apps	
Update	

Explanation:

<https://docs.microsoft.com/en-us/intune/deploy-use/understand-microsoft-intune-operations-by-using-reports>

QUESTION 114

You have a computer that runs Windows 10. You install a second hard disk drive on the computer and you create a new volume named E. You need to enable system protection for volume E. What should you use?

- A. the Wbadmin command
- B. the Settings app
- C. System Properties
- D. the Set-Volume cmdlet

Answer: C

Explanation:

System protection is a feature that regularly creates and saves information about your computer's system files and settings. System protection also saves previous versions of files that you've modified. It saves these files in restore points, which are created just before significant system events, such as the installation of a program or device driver. They're also created automatically once every seven days if no other restore points were created in the previous seven days, but you can create restore points manually at any time. When system protection is turned on, you can undo undesired system changes by doing a system restore to revert your computer (all drives that have system protection turned on) to a previous point in time. This tutorial will show you how to turn on or off system protection for drives of your choice to be able to create restore points and do a system restore in Windows 10. You must be signed in as an administrator to be able to turn on or off system protection.

QUESTION 115

You manage a client Windows 10 Enterprise computer named Computer1. You have an OneDrive synchronized folder that contains .pdf files. You need to ensure that you can restore previous versions of the .pdf files. What should you do?

- A. Enable File History.
- B. Configure System Restore.
- C. Configure Computer1 as a trusted PC.
- D. Enable Sync your settings on Computer1.

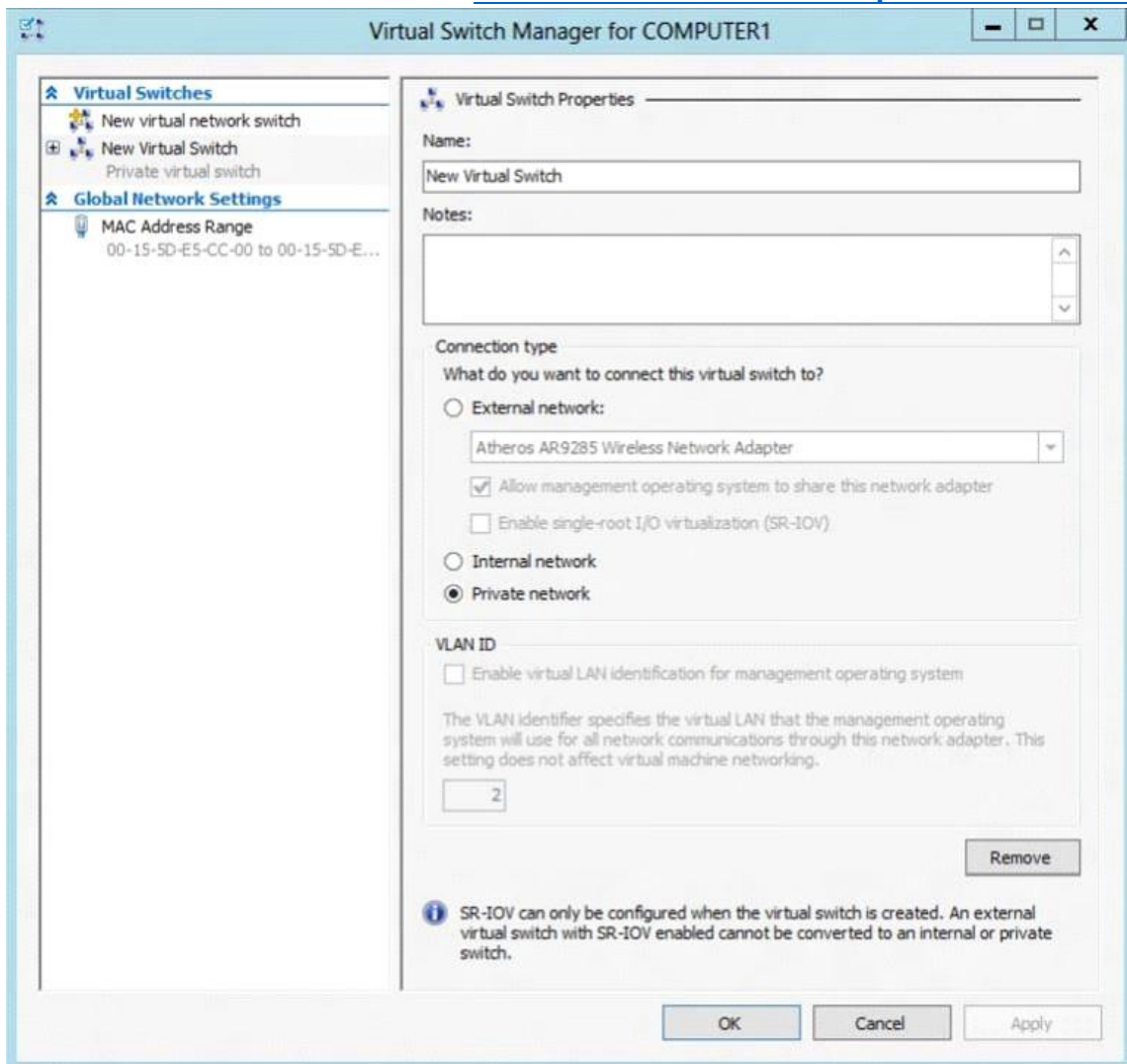
Answer: A

Explanation:

File History regularly backs up versions of your files in the Documents, Music, Pictures, Videos, and Desktop folders and the OneDrive files available offline on your PC. Over time, you'll have a complete history of your files. If the originals are lost, damaged, or deleted, you can restore them. You can also browse and restore different versions of your files. For example, if you want to restore an older version of a file (even if it wasn't deleted or lost), you can browse through a timeline, select the version you want, and restore it.

QUESTION 116

A company has an Active Directory Domain Services (AD DS) domain with one physical domain controller. All client computers run Windows 10 Enterprise. A client computer hosts a Windows 10 Enterprise virtual machine (VM) test environment. The VMs are connected to a private virtual switch that is configured as shown in the Virtual Switch Manager exhibit. (Click the Exhibit button.)



You have the following requirements:

- Configure the test environment to allow VMs to communicate with the host machine.
- Minimize impact on the host machine.

You need to meet the requirements. What should you do?

- A. Create a new virtual switch with a Private Network [CP1] connection type.
- B. Create a new virtual switch with an ExternalNetwork connection type.
- C. Change the VLAN ID of the private virtual switch to Enable Virtual LAN identification.
- D. Create a new virtual switch with an Internal Network connection type.

Answer: D

Explanation:

<http://john.bryntze.net/jbkb-v2/certification-exam-70-687-configuring-windows-8-part-2-configure-hardware-and-applications-16/>

Virtual switches/ Hyper-V VLAN - you can create 3 different types of virtual switches depending the needs of your virtual machines and one single machine can use multiple virtual NICs that is member of different Virtual Switches.

External - This virtual switch binds to the physical network adapter and create a new adapter you

can see in Control Panel\Network and Internet\Network Connections so if a virtual machine needs contact outside the host machine this one is a must.

Internal - This virtual switch can be used to connect all virtual machines and the host machine but cannot go outside that.

Private - This virtual switch can only be used by the virtual host.

Further information:

<http://technet.microsoft.com/en-us/library/cc816585%28v=ws.10%29.aspx>

Configuring Virtual Networks

Hyper-V Networking: Three types of Virtual Networks:

Type	Parent OS	VMs on Same HV	VMs on Remote HV	LAN	Remark
External	x	x	x	x	Conn. Lost Temporarily
Internal	x	x			
Private		x			
Dedicated		x		x	

Private will not allow communication with the host machine. External will allow communication with the host machine but also allow access to other machines on the host machine's network which is not a requirement.

QUESTION 117

Your network contains an Active Directory domain named contoso.local. All users have email addresses in the @contoso.com domain. You need to ensure that users can register Windows Phone 8.1 devices for mobile device management (MDM). Which DNS record should you create?

- A. Enterprisedevice.contoso.com
- B. Deviceregistration.contoso.local
- C. Deviceregistration.contoso.com
- D. Enterpriseregistration.contoso.com
- E. Enterpriseregistration.contoso.local

Answer: D

Explanation:

<https://technet.microsoft.com/en-us/windows/dn771709.aspx>

QUESTION 118

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 10 Enterprise and are joined to the domain. You have the following requirements:

- Ensure that files in shared network folders are available offline.
- Maximize efficiency for users who connect to shared network folders from a mobile device.

You need to configure Group Policy settings to meet the requirements. What should you do first?

- A. Enable the Enable file synchronization on costed networks policy setting.
- B. Enable the Synchronize all offline files when logging on policy setting.
- C. Enable and configure the Configure slow-link mode policy setting.
- D. Enable and configure the Specify administratively assigned Offline Files policy setting.

Answer: A

Explanation:

<https://technet.microsoft.com/en-us/library/hh968298.aspx>

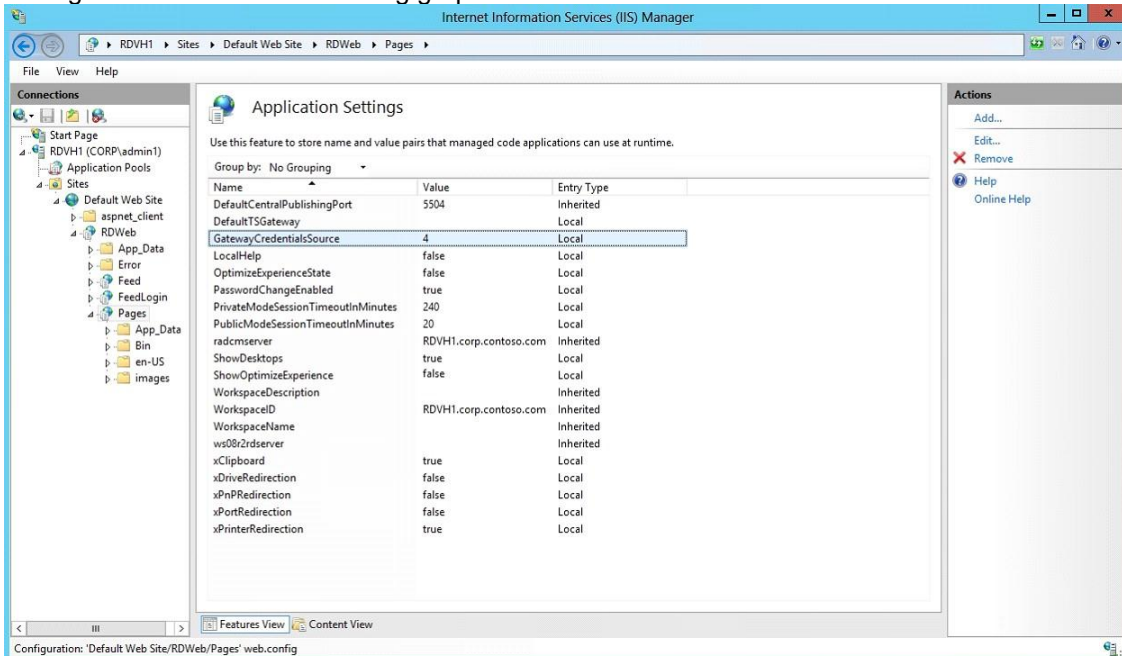
QUESTION 119

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

Hotspot Question

You have an Active Directory domain named contoso.com. You have a server that runs Windows Server 2012 R2 and that is a Remote Desktop server. The RD Web Access Web application settings 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.

Answer Area

When a user connected to the RDWeb site, [answer choice] will appear.

Users that have Android devices can [answer choice] from the RDWeb site.

Answer:

Answer Area

When a user connected to the RDWeb site, [answer choice] will appear.

Users that have Andriod devices can [answer choice] from the RDWeb site.

only RemoteApps
only Remote Desktop Connections
both RemoteApps and Remote Desktop Connections

never change their passwords
only change expired passwords
only change unexpired passwords

QUESTION 120

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question. You have a computer that runs Windows 10 and is used by 10 users. The computer is joined to an Active Directory domain. Each user has an Active Directory account. You need to ensure that all of the users can access the files located in one another's libraries. What should you configure?

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

Answer: D

QUESTION 121

You are configuring two Windows 10 Enterprise client computers: A desktop computer named COMPUTER1 and a portable computer named COMPUTER2. You have the following requirements:

- Store all personal data in a folder named data on COMPUTER1.
- Ensure that you can access all personal data from Computer2, even when a network connection is unavailable.
- Synchronize personal data between the computers twice a day.

You need to configure the computers to meet the requirements. Which two actions should you perform? Each correct answer presents part of the solution.

- A. From COMPUTER2, connect to COMPUTER1 and configure the Data folder to always be available offline.
- B. From COMPUTER1, connect to COMPUTER2 and configure the Data folder to always be available offline.
- C. In Sync Center, configure a schedule for offline files.
- D. From COMPUTER2, map a network drive to the DATA folder on COMPUTER1.
- E. In Sync Center, set up a new sync partnership.

Answer: AC

QUESTION 122

Drag and Drop Question

You have a computer that runs Windows 10. You need to meet the following requirements:

- Users must use complex passwords.
- Users must change their password every 180 days.
- Users must be prompted to change their password seven days before the password expires.

Which policy setting should you configure for each requirement? To answer, drag the appropriate policy settings to the correct requirements. Each policy setting 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.

Values

- Account Lockout Policy
- Audit Policy
- Password Policy
- Security Options
- User Rights Assignment

Answer Area

Users must change their password every 180 days: Policy setting

Users must use complex passwords: Policy setting

Users must be prompted to change their password seven days before the password expires: Policy setting

Answer:

Values

- Account Lockout Policy
- Audit Policy
- Password Policy
- Security Options
- User Rights Assignment

Answer Area

Users must change their password every 180 days: Password Policy

Users must use complex passwords: Password Policy

Users must be prompted to change their password seven days before the password expires: Security Options

Explanation:

[https://technet.microsoft.com/en-us/library/jj852243\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj852243(v=ws.11).aspx)

QUESTION 123

You support Windows 10 Enterprise laptops. Microsoft BitLocker Administration and Monitoring (MBAM) is deployed on your network on a server named SERVER1. Company policy requires that laptops with MBAM client installed prompt users to enable BitLocker within 2 hours of being started. You need to make changes to the Configure MBAM Services Group Policy settings. Which two actions should you perform? Each correct answer presents part of the solution.

- A. Set Select BitLocker Recovery Information to store to Recovery password only.

- B. Set Select Bitlocker Recovery Information to store to Recovery password and key package.
- C. Set Enter status reporting frequency (in minutes) to 120.
- D. Set MBAM Status reporting endpoint to SERVER1.
- E. Set MBAM Recovery and Hardware service endpoint to SERVER1.
- F. Set Enter client checking status frequency (in minutes) to 120.

Answer: EF

Explanation:

http://www.projectleadership.net/blogs_details.php?id=3519

QUESTION 124

You administer Windows 10 Enterprise computers in your company network. The computers are configured to allow remote connections. You attempt to create a Remote Desktop Connection to a computer named Computer1. You receive the following message:

"Remote Desktop can't connect to the remote computer."

You are able to ping Computer1. You discover that Remote Desktop Firewall rules are not present on Computer1. You need to connect to Computer1 by using Remote Desktop. Which PowerShell commands should you run on Computer1?

- A. Set-NetFirewallRule -Name RemoteSvcAdmin-in-TCP -Enable True
- B. Set -NetFirewallRule -Name RemoteFwAdmin-In-TCP -Enable True
- C. New-NetFirewallRule -DisplayName RdpTCPIn -localPort 3389 - Protocol TCP
- D. New-NetFirewallRule -DisplayName RdpTCPout -localPort 3389 - Protocol TCP -Direction Out -Action Allow

Answer: C

Explanation:

<http://technet.microsoft.com/en-us/library/jj554908.aspx>

New-NetFirewallRule

Creates a new inbound or outbound firewall rule and adds the rule to the target computer.

Syntax

New-NetFirewallRule -DisplayName <String> [-Action <Action>] [-AsJob] [-Authentication <Authentication>] [- CimSession <CimSession[]>] [-Description <String>] [-Direction <Direction>] [-DynamicTarget <DynamicTransport>] [-EdgeTraversalPolicy <EdgeTraversal>] [-Enabled <Enabled>] [-Encryption <Encryption>] [-GPOSession <String>] [-Group <String>] [-IcmpType <String[]>] [-InterfaceAlias <WildcardPattern[]>] [-InterfaceType <InterfaceType>] [-LocalAddress <String[]>] [-LocalOnlyMapping <Boolean>] [-LocalPort <String[]>] [-LocalUser <String>] [-LooseSourceMapping <Boolean>] [-Name <String>] [-OverrideBlockRules <Boolean>] [-Owner <String>] [- Package <String>] [-Platform <String[]>] [-PolicyStore <String>] [-Profile <Profile>] [-Program <String>] [-Protocol <String>] [-RemoteAddress <String[]>] [- RemoteMachine <String>] [-RemotePort <String[]>] [-RemoteUser <String>] [-Service <String>] [- ThrottleLimit <Int32>] [-Confirm] [-WhatIf] [<CommonParameters>] The New-NetFirewallRule cmdlet creates an inbound or outbound firewall rule and adds the rule to the target computer.

http://en.wikipedia.org/wiki/Remote_Desktop_Protocol

Remote Desktop Protocol

By default, the server listens on TCP port 3389 and UDP port 3389.

QUESTION 125

A company has Windows 10 Enterprise client computers that use DirectAccess. You need to ensure that the client computers can communicate to IPv4 resources by name. What should you implement on the client computers?

- A. AAA (Quad A) resource records
- B. Teredo tunnels

- C. NAT64/DNS64
- D. Teredo relays
- E. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Answer: C

QUESTION 126

You administer Windows 10 Enterprise laptops. The laptops are configured to connect to an unsecured wireless access point. You plan to configure the wireless access point to encrypt wireless traffic and turn off SSID broadcast. You need to ensure the laptops will join the secured wireless network automatically after the configuration changes. What should you do?

- A. Create an ad hoc network
- B. Set Network Discovery to Enabled for the Public profile
- C. Create a network profile
- D. Set the Unidentified Networks Properties User permissions to User can change location

Answer: D

QUESTION 127

You have a new computer that runs Windows 10. The computer is a member of a workgroup and is connected to a WiFi network. You discover that the active network is a public network. You need to change the network location to a private network. Which Control Panel application should you use?

- A. Network and Sharing Center
- B. System
- C. Windows Firewall
- D. HomeGroup

Answer: A

Explanation:

<https://tinkertry.com/how-to-change-windows-10-network-type-from-public-to-private>

QUESTION 128

You have a computers that runs Windows 10. You plan to configure Windows Hello. You need to configure the PIN complexity rules for the computer. Which policy setting should you modify?

- A. Credential User Interface
- B. Microsoft Passport for Work
- C. Smart Card
- D. Biometrics
- E. Windows Logon Options

Answer: B

Explanation:

<http://www.kapilarya.com/how-to-configure-pin-complexity-in-windows-10>

QUESTION 129

You have a computer that runs Windows 10 and has BitLocker Drive Encryption (BitLocker) configured. You need to change the BitLocker PIN for the drive. What should you do?

- A. the repair-bde.exe windows script file
- B. the manage-bde.exe command
- C. the bitsadmin.exe command
- D. the Enable-BitLocker cmdlet

Answer: B

QUESTION 130

Drag and Drop Question

You support Windows 10 Enterprise laptops. You need to configure the laptops to support offline file access. 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.

Actions	Answer Area
Select Enable offline files .	
Select Sync Setup .	
Select Set up new sync partnerships .	
Select Offline Files, and then select Set up .	
Select Manage offline files .	
On the laptop, right-click the network share folder and select Always available offline .	

Answer:

Actions	Answer Area
	Select Manage offline files .
Select Sync Setup .	Select Enable offline files
Select Set up new sync partnerships .	On the laptop, right-click the network share folder and select Always available offline .
Select Offline Files, and then select Set up .	

Explanation:

<http://www.thewindowsclub.com/windows-10-sync-center>

QUESTION 131

You have a laptop. Recently, you discovered that the battery life on the laptop is less than expected. You need to generate a report that lists the expected battery life after a full charge and that shows historical battery life. What should you use?

- A. the Power & sleep setting in the Settings app
- B. the Powercfg command
- C. Power Options in Control Panel
- D. Performance Monitor

Answer: B

Explanation:

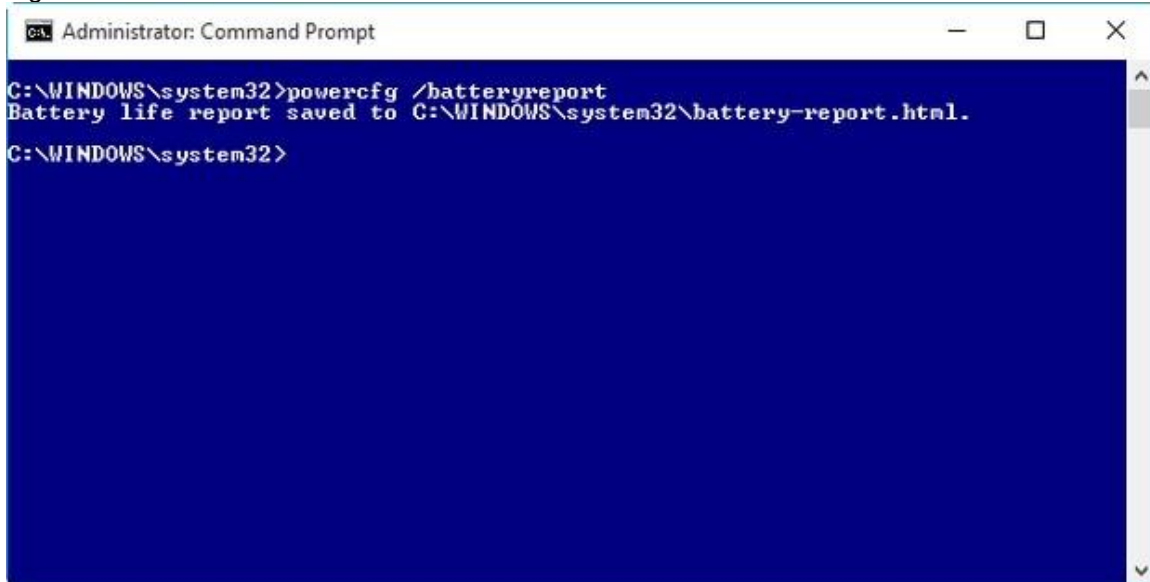
Launching the PowerCfg command and running the Battery Report is easy once you know how. To begin, you'll need to open an Administrator Command Prompt, which you can do by right-clicking on the Start button and selecting the Command Prompt (Admin) command. Then, type the command:

powercfg /batteryreport

and press [Enter]. The Power Configuration Utility will immediately compile the report and display

the message shown in Figure A.

Figure A



QUESTION 132

You have a Remote Desktop Session Host (RD Session Host) server. The server is accessible from the internal network. To access the server remotely, you must connect to a Remote Desktop Gateway (RD Gateway) server. On a laptop, you successfully configure a Remote Desktop connection that you use to access the RD Session Host server from the internal network. From your home, you attempt to connect to the RD Session Host server by using the Remote Desktop connection, but the connection fails. You need to connect to the RD Session Host server. What should you configure on the laptop?

- A. the Performance settings in Remote Desktop Connection
- B. the Connect from anywhere settings in Remote Desktop Connection
- C. the Remote Desktop settings in System Properties
- D. the Remote Assistance settings in System Properties

Answer: B

Explanation:

[https://technet.microsoft.com/en-us/library/cc770601\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc770601(v=ws.11).aspx)

QUESTION 133

Drag and Drop Question

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 8.1. The company has three departments named Accounting, Human Resources (HR), and Marketing. User account objects are stored in their respective departmental AD security groups and have full access to shared folders for each department. A new company policy requires that the following access rules are in place:

- Users must have complete access only to their department's shared folder.
- Accounting department users must be able to change files in the HR folder.
- HR department users must be able to change files in the Marketing folder.
- Marketing department users must be able to change files in the Accounting folder.

You need to comply with the company policy. Which permissions should you assign? (To answer,

drag the appropriate security group or groups to the correct location or locations in the answer area. Security groups 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.)

Security Groups	Answer Area																
Accounting	<table border="1"> <thead> <tr> <th rowspan="2">Shared folder</th> <th colspan="2">Access Control List</th> </tr> <tr> <th>Full Control</th> <th>Modify</th> </tr> </thead> <tbody> <tr> <td>Accounting</td> <td>Security Group</td> <td>Security Group</td> </tr> <tr> <td>HR</td> <td>Security Group</td> <td>Security Group</td> </tr> <tr> <td>Marketing</td> <td>Security Group</td> <td>Security Group</td> </tr> </tbody> </table>			Shared folder	Access Control List		Full Control	Modify	Accounting	Security Group	Security Group	HR	Security Group	Security Group	Marketing	Security Group	Security Group
Shared folder					Access Control List												
				Full Control	Modify												
Accounting				Security Group	Security Group												
HR	Security Group	Security Group															
Marketing	Security Group	Security Group															
Users																	
Everyone																	
HR																	
Marketing																	

Answer:

Security Groups	Answer Area																
Accounting	<table border="1"> <thead> <tr> <th rowspan="2">Shared folder</th> <th colspan="2">Access Control List</th> </tr> <tr> <th>Full Control</th> <th>Modify</th> </tr> </thead> <tbody> <tr> <td>Accounting</td> <td>Accounting</td> <td>Marketing</td> </tr> <tr> <td>HR</td> <td>HR</td> <td>Accounting</td> </tr> <tr> <td>Marketing</td> <td>Marketing</td> <td>HR</td> </tr> </tbody> </table>			Shared folder	Access Control List		Full Control	Modify	Accounting	Accounting	Marketing	HR	HR	Accounting	Marketing	Marketing	HR
Shared folder					Access Control List												
				Full Control	Modify												
Accounting				Accounting	Marketing												
HR	HR	Accounting															
Marketing	Marketing	HR															
Users																	
Everyone																	
HR																	
Marketing																	

QUESTION 134

Hotspot Question

You have Windows computers that are managed by using Microsoft Intune. You need to send an email notification to compliance@contoso.com when there is a critical Windows update that must be approved. The solution must minimize the number of email notifications sent. How should you configure the email notification rule? To answer, select the appropriate options in the answer are.

Category	Endpoint Protection
	Monitoring
	Notices
	Policy
	Remote Assistance
	System
	Updates
Alert Severity	Critical
	Information, Warning, and Critical
	Warning and Critical

Answer:

Category	Endpoint Protection
	Monitoring
	Notices
	Policy
	Remote Assistance
	System
	Updates
Alert Severity	Critical
	Information, Warning, and Critical
	Warning and Critical

QUESTION 135

You have a Microsoft Intune subscription. You create two compliance policies named Comp1 and Comp2. You create a configuration policy named ConfigPol1. The settings in each policy do not conflict with other policies. Comp1 has medium security settings. Comp2 has low security settings. ConfigPol1 has high security settings. You have a device named Device1. Device1 is a member of groups that have Comp1, Comp2 and ConfigPol1 applied. You need to identify which policies will be enforced on Device1. What should you identify?

- A. Comp1 and Comp2 only
- B. Comp1, Comp2 and ConfigPol1
- C. Comp2 only
- D. Comp1 only
- E. ConfigPol1 only

Answer: B

QUESTION 136

You have a computer that runs Windows 8.0. You create a system image backup on the computer and then you upgrade to Windows 10 Enterprise. You need to access a file from the backup. The solution must use the least amount of administrative effort. What should you do?

- A. From the Backup section of the Settings app, add a drive.
- B. From the File History section of the Settings app, add a drive.
- C. From the Computer Management console, attach a VHD.
- D. From the File History control panel item, restore the personal files.

Answer: C

QUESTION 137

You have a computer named Computer1 that runs Windows 10 Enterprise. You plan to implement File History on Computer1. You need to identify the interface that can be used to perform File History management actions. Which interface should you identify for each action? To answer, select the appropriate options in the answer area.

Add items to be included in the File History: Backup section from the Settings app
File history item from Control Panel
Storage Spaces item from Control Panel

Configure File History to use a network location: Backup section from the Settings app
File history item from Control Panel
Storage Spaces item from Control Panel

Answer:

Add items to be included in the File History: Backup section from the Settings app
File history item from Control Panel
Storage Spaces item from Control Panel

Configure File History to use a network location: Backup section from the Settings app
File history item from Control Panel
Storage Spaces item from Control Panel

QUESTION 138

Hotspot Question

You plan to deploy two Microsoft Azure RemoteApp cloud collections named Collection1 and Collection2. Each user of Collection1 will store up to 20 GB of data. Each user of Collection2 will store up to 60 GB of data. You need to identify the valid locations to store data for the users of each collection. The solution must ensure that the stored data persists between Azure RemoteApp sessions. What storage locations should users use for each collection? To answer, drag the appropriate locations to the correct collection. Each location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll content. NOTE: Each correct selection is worth one point.

Collection1:

Documents folder only
OneDrive only
OneDrive for Business only
OneDrive and OneDrive for Business
Documents folder and OneDrive for Business

Collection2:

Documents folder only
OneDrive only
OneDrive for Business only
OneDrive and OneDrive for Business
Documents folder and OneDrive for Business

Answer:

Collection1:

Documents folder only
OneDrive only
OneDrive for Business only
OneDrive and OneDrive for Business
Documents folder and OneDrive for Business

Collection2:

Documents folder only
OneDrive only
OneDrive for Business only
OneDrive and OneDrive for Business
Documents folder and OneDrive for Business

Explanation:

<https://docs.microsoft.com/en-us/azure/remoteapp/remoteapp-upd>

QUESTION 139

You have a computer named C1 that runs win10 enterprise. C1 is member of a home-group. You plan to join C1 to MS Azure AD tenant named T1. You need to ensure that an Azure AD user named User1 is a member of the local Administrators group on C1, when C1 is joined to Azure AD. What should you do?

- A. From azure classic portal modify the membership of T1 global admin group
- B. From the settings app on C1, set up assigned access
- C. From settings app on C1, modify the Work access settings
- D. From settings all on C1, modify the Family & other user settings

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-join-windows-vm>

<http://www.tomsitpro.com/articles/windows-10-azure-active-directory-domain,2-27.html>

QUESTION 140

All computers are connected to homgroup. User wants to share a printer. The printer function for the computer it is attached to. You verify that printers are enabled under homegroup settings, but the printer does not appear on the network. The user is able to share documents and access other shared printers in the homegroup. you need to allow other users to use the printer. What should you do?

- A. Enable sharing under the printer properties
- B. map the printer on the client computers
- C. update the printer driver to a version that supports homegroup sharing
- D. disable and re enable the sharing of printers under homegroup on the computer

Answer: A

QUESTION 141

A company has client computer that run Win 10 enterprise. The corporate network is configured for IPv4 and IPv6. You need to disable IPv6 on the client computer without affecting IPv4 communicatins. What should you do on each computer?

- A. Run the Set-NetIPv4Protocol Windows PowerShell cmdlet
- B. Run the Set-NetIPv6Protocol Windows PowerShell cmdlet
- C. Run Disable-NetAdapter Windows PowerShell cmdlet
- D. Run the Disable-NetAdapterBinding Windows PowerShell cmdlet

Answer: D

QUESTION 142

A company has a client that run Windows 10 enterprise. File history is on. An employee downloads data to a folder on D named Archives. You need to ensure that the user can restore files from the Archive folder by using File History. What should you do?

- A. Start the block level backup engine service
- B. Start windows backup service
- C. Create a library named History and add the Archives folder to the library
- D. Turn on volume Shadow Copy service

Answer: C

QUESTION 143

You manage a branch office of a company named Contose. The branch office contains 20 computers that run Win 10 enterprise. The main office of Contose hosts a Win Server Update Service server. (WSUS). Branch office computers are configured to download updates from the internet. You need to prevent computers in the branch office from sharing updates with other computers. What should you do?

- A. Modify the branch cache hosted mode settings
- B. Modify branch cache distributed cache mode settings
- C. Modify the Chose how updates are delivered settings
- D. Deploy a downstream WSUS server to the branch office

Answer: C

QUESTION 144

Your network contains an Active Directory domain. Roaming profiles are stored in \\server1\profiles. The content of the profiles share is shown in the following graphic.

Name	Date modified	Type	Size
User1	2016/09/30 11:51 AM	File folder	
User1.v2	2016/09/30 11:51 AM	File folder	
User1.v3	2016/09/30 11:51 AM	File folder	
User1.v5	2016/09/30 11:51 AM	File folder	
User2	2016/09/30 11:51 AM	File folder	
User2.v2	2016/09/30 11:51 AM	File folder	
User2.v3	2016/09/30 11:51 AM	File folder	
User2.v5	2016/09/30 11:51 AM	File folder	
User3	2016/09/30 11:51 AM	File folder	
User3.v2	2016/09/30 11:51 AM	File folder	
User3.v5	2016/09/30 11:51 AM	File folder	

A user named User2 works from a computer that runs Windows 8. User2 reports an issue with a user profile. You need to view the contents of the user profile. Which folder should you open?

- A. User1
- B. User2.v5
- C. User2.v2
- D. User2.v3

Answer: D

QUESTION 145

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 four Actions should you perform in sequence?

Actions:	Answer Area:
Run the powercfg /d command	1 Run the powercfg /import command
Run the powercfg /import command	2 Run the powercfg /s command
Run the powercfg /setacvalueindex command	3 Run the powercfg /x command
Run the powercfg /export command	4 Run the powercfg /export command
Run the powercfg /s command	
Run the powercfg /x command	

Answer:

QUESTION 146

Note: this question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question. You need to change the password used for an L2TP VPN connection. Which Control Panel application should you use?

- A. System
- B. Credential Manager
- C. Work Folders
- D. Phone and Modem

- E. Power Options
- F. RemoteApp and Desktop Connections
- G. Sync Center
- H. Network and Sharing Center

Answer: H

QUESTION 147

You need to create a new connection to the Internet that uses PPOE. Which Control Panel application should you use?

- A. System
- B. Credential Manager
- C. Work Folders
- D. Network and Sharing Center
- E. Power Options
- F. RemoteApp and Desktop Connections
- G. Sync Center
- H. Phone and Modem

Answer: D

QUESTION 148

Note: this question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question. You have a mobile device that connects to a 4G network and a laptop. You work from a remote location that does not have Internet access. You plan to use the mobile device as a mobile hotspot for the laptop, so that you can access files from the corporate office. Which Control Panel application should you use on the laptop to connect to the mobile hotspot?

- A. System
- B. Work Folders
- C. Network and Sharing Center
- D. Power Options
- E. RemoteApp and Desktop Connections
- F. Sync Center

Answer: C

QUESTION 149

You have a Windows To Go workspace on a USB memory drive. When you attempt to start a computer from the drive, you receive the following error message.

"Your PC/Device needs to be repaired. The application or operating system couldn't be loaded because a required file is missing or contains errors."

You need to repair the Windows To Go workspace. What should you do?

- A. Reapply the Windows To Go image to the USB memory drive.
- B. Restart the computer by using a recovery disk, and then perform a system restore.
- C. Restart the computer, and then select the Last Known Good Configuration.
- D. Restart the computer in safe mode, and then perform a system restore.

Answer: A

QUESTION 150

You have a computer that has the disk configuration shown in the following table.

Disk controller	Size	Purpose
0	128 GB	System and boot
1	256 GB	Not applicable
2	256 GB	Not applicable
3	256 GB	Not applicable

You need to configure a storage space that will provide data redundancy if a disk fails. The solution must minimize impact if a disk fails. Which resiliency type should you choose?

- A. three-way mirror
- B. two-way mirror
- C. simple
- D. parity

Answer: B

Explanation:

https://social.technet.microsoft.com/wiki/contents/articles/11382.storage-spaces-frequently-asked-questions-faq.aspx#What_types_of_drives_can_I_use_with_Storage_Spaces

QUESTION 151

You have an Active Directory domain named contoso.com. You use RemoteApp to make applications available to Android and iOS users. The external DNS zone for contoso.com is shown in the exhibit. (Click the Exhibit button.) You need to provide a user with the connection URL for the Remote Desktop app on an Android device. Which connection URL should you provide?

- A. Server1.contoso.com
- B. <https://server1.contoso.com/RDWeb?feed>
- C. _msradc.contoso.com
- D. <https://server1.contoso.com/RDWeb/feed/webfeed.aspx>

Answer: D

QUESTION 152

Drag and Drop Question

You administer Windows 10 Enterprise tablets and virtual desktop computers that are joined to an Active Directory domain. Your company provides virtual desktop computers to all users. Employees in the sales department also use tablets, sometimes connected to the company network and sometimes disconnected from the company network. You want sales department employees to have the same personal data, whether they are using their virtual desktop or their tablets. You need to configure the network environment to meet the requirements. 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. More than one order to answer choices may be correct. You will receive credit for any of the correct orders you select.

Actions

- Enable slow-link mode for the tablets.
- Create a network share.
- Configure offline files for the tablets.
- Disable offline files on the network share.
- Configure folder redirection for the employees' domain accounts to the network share.
- Specify the file share for which you want to enable Always Offline mode and set the value to 1.
- Set the primary computer for all employees from the sales department.

Answer Area



Answer:

Actions

-
-
- Configure offline files for the tablets.
- Disable offline files on the network share.
- Configure folder redirection for the employees' domain accounts to the network share.
-
- Set the primary computer for all employees from the sales department.

Answer Area



- Create a network share.
- Enable slow-link mode for the tablets.
- Specify the file share for which you want to enable Always Offline mode and set the value to 1.

Explanation:

[https://technet.microsoft.com/en-us/library/cc732275\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732275(v=ws.11).aspx)

QUESTION 153

You have a laptop that is a member of a workgroup. The laptop does not have a Trusted Platform Module (TPM) chip. You plan to enable BitLocker Drive Encryption (BitLocker) for the operating system drive. What are two methods that you can use to unlock the drive when the laptop restarts? Each correct answer presents a complete solution.

- A. a password
- B. a Near Field Communication (NFC)-enabled portable device
- C. a USB drive
- D. a user account
- E. Network Unlock

Answer: A

QUESTION 154

You administer Windows 10 Enterprise client computers that are members of an Active Directory

domain that includes Active Directory Certificate Services (AD CS). You restored a computer from a backup that was taken 45 days ago. Users are no longer able to log on to that computer by using their domain accounts. An error message states that the trust relationship between the computer and the primary domain has failed. What should you do?

- A. Renew the certificates issued to the client computer.
- B. Reset the passwords of all affected domain users.
- C. Logon as a local administrator and issue the `netdom resetpwd` command.
Log off and restart the computer.
- D. Restore the client computer from a known good backup that was taken two weeks earlier than the backup you previously restored.

Answer: C

Explanation:

<http://theitbros.com/fix-trust-relationship-failed-without-domain-rejoining/>

QUESTION 155

Drag and Drop Question

You have a computer named Client1 that runs Windows 10 Enterprise. Client1 is a member of an Active Directory domain. A domain administrator provisions a certificate template for a virtual smart card logon. In the BIOS of Client1, you enable the Trusted Platform Module (TPM). You need to enable the virtual smartcard logon on Client1. 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.

Actions

Run the `tpmvscmgr.exe` command.
Use the Certificate Enrollment wizard.
Run the `vaultcmd.exe` command.
Run the `tpmunit.exe` command.
Run the `certmgr.exe` command

Answer Area



Answer:

Actions

Run the `vaultcmd.exe` command.

Run the `certmgr.exe` command

Answer Area



Run the `tpmunit.exe` command.
Run the `tpmvscmgr.exe` command.
Use the Certificate Enrollment wizard.

Explanation:

[https://technet.microsoft.com/en-us/library/cc753140\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc753140(v=ws.11).aspx)

<http://ss64.com/nt/run.html>

[https://technet.microsoft.com/en-us/library/cc730689\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc730689(v=ws.11).aspx)

QUESTION 156

[70-697 Exam Dumps](#) [70-697 Exam Questions](#) [70-697 PDF Dumps](#) [70-697 VCE Dumps](#)

[Back to the Source of this PDF & Get More Free Braindumps -- www.microsoftbraindumps.com](#)

You have an unsecured wireless network for users to connect to from their personal Windows 10 devices. You need to prevent Wi-Fi Sense from sharing information about the unsecured wireless network. What should you do?

- A. Configure the SSIF of the unsecured wireless to contain_optout.
- B. Instruct the users to disable Internet Protocol Version 6 (TCP/IPv6) on their wireless network adapters.
- C. Configure the SSID of the guest wireless to be hidden.
- D. Instruct the users to turn off Network Discovery on their devices.

Answer: A

Explanation:

<http://www.pcworld.com/article/2951824/windows/how-to-disable-windows-10s-wi-fi-sense-password-sharing.html>

QUESTION 157

You have a computer that runs Windows 10. You need to block all outbound and inbound communications that occur over TCP 9997, TCP 9999, and TCP 4000. What is the minimum number of rules that you must create?

- A. 1
- B. 2
- C. 3
- D. 6

Answer: D

Explanation:

[https://technet.microsoft.com/en-us/library/dd421709\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd421709(v=ws.10).aspx)

QUESTION 158

You have a laptop that has connections for three Wi-Fi network named WiFi1, WiFi2, and Wi-Fi 3. You need to ensure that the laptop connects to WiFi1 when multiple WiFi1 networks are available. What should you do?

- A. From Netsh, configure the WLAN context.
- B. From NetworkConnections in Control Panel, modify the bindings for the WiFi.
- C. From the Windows Settings app, configure the Wi-Fi Sense settings.
- D. From Network Connections in Control Panel, modify the network provider order.

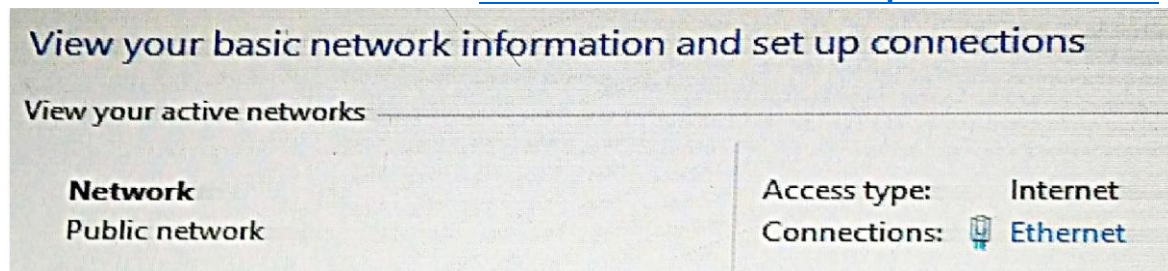
Answer: D

Explanation:

<http://www.quepublishing.com/articles/article.aspx?p=2455390&seqNum=3>

QUESTION 159

You administer Windows 10 Enterprise client computers in your company network. A guest at your company is connected to the Internet as shown in the following exhibit. (Click the exhibit button.)



You need to ensure that the guest user is able to share network resources over Wi-Fi without lowering the overall security of the computer. What should you do?

- A. Configure File and printer sharing settings for Public networks.
- B. Change the network location type to Private.
- C. Change the network location type to Work.
- D. Configure File sharing connections settings for All networks.

Answer: D

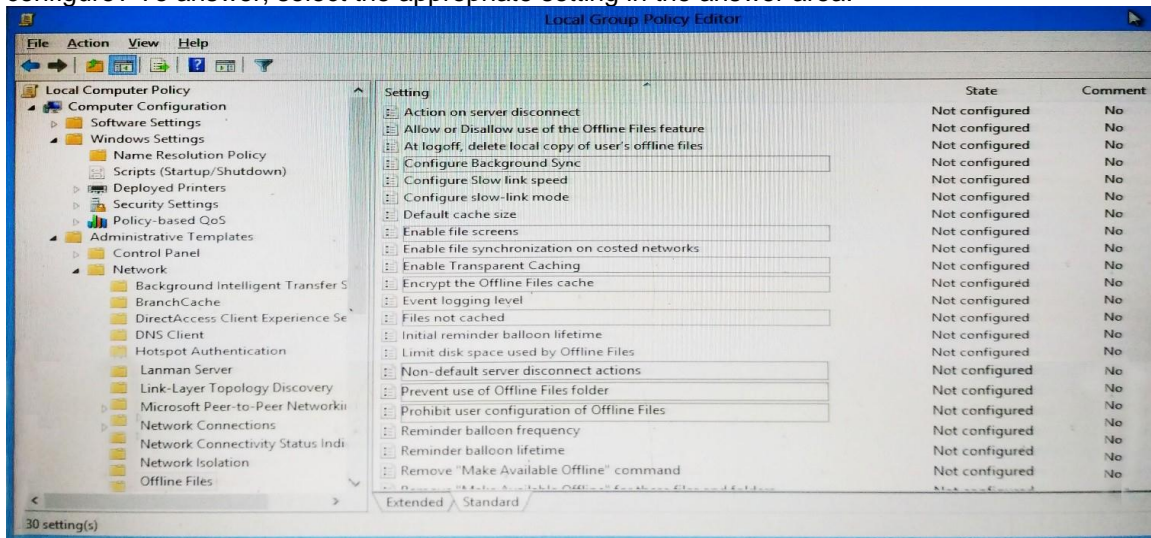
Explanation:

http://www.isunshare.com/windows-10/turn-off-or-on-password-protected-sharing-in-windows-10.html#_blank

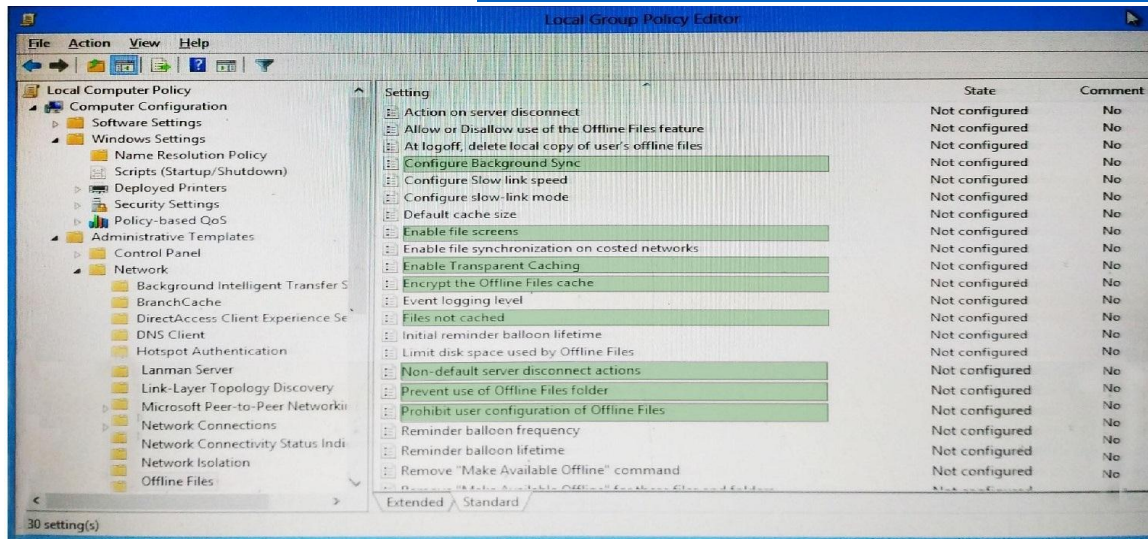
QUESTION 160

Hotspot Questions

You install Windows 10 Enterprise on a new laptop that will be shipped to a remote user. You logon to the laptop with the user credentials, map network drivers, and configure the network drivers to be always available offline. Company policy requires that files with a .db1 extension should be excluded from offline file synchronization. You need to prevent the user from creating files with a .db1 extension on the mapped drives. In the Local Group Policy Editor, which setting should you configure? To answer, select the appropriate setting in the answer area.



Answer:



Explanation:

<https://www.windows-security.org/1941654bad9040dfcb8ffaba2724b014/enable-file-screens>

QUESTION 161

You have a computer that runs Windows 10. You need to ensure that the next time the computer restarts, the computer starts in safe mode. What should you use?

- A. the System Configuration utility
- B. the Restore-Computer cmdlet
- C. the Bcdboot command
- D. System in Control Panel

Answer: A

Explanation:

<http://www.digitalcitizen.life/4-ways-boot-safe-mode-windows-10>

QUESTION 162

You have a computer named Computer1 that runs Windows 10 Enterprise. You install a Universal app named App1 on Computer1. You discover that an update for App1 is available. You need to install the update as soon as possible. What should you do?

- A. Log off and log on to the Computer1.
- B. From the Windows Update settings, modify the Choose how updates are delivered setting.
- C. From the Windows Update settings, modify the Choose how updates are installed setting.
- D. From the Windows Update settings, click Check for updates.

Answer: C

Explanation:

<http://www.howtogeek.com/223068/what-you-need-to-know-about-windows-update-on-windows-10/>

QUESTION 163

You have a Windows 10 Enterprise computer that has File History enabled. You create a folder named Data in the root of the C: drive. You need to ensure that Data 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 Data in an existing library.
- B. Modify the Advanced settings from the File History Control Panel item.
- C. From File Explorer, create a new library that contains Data
- D. From File Explorer, modify the system attribute of Data.

Answer: AC

Explanation:

<http://www.digitalcitizen.life/introducing-windows-8-how-backup-data-file-history>

QUESTION 164

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details in a question apply only to that question. You have a mobile device that connects to a 4G network and a laptop. You work from a remote location that does not have Internet access. You plan to use the mobile device as a mobile hotspot for the laptop, so that you can access files from the corporate office. Which Control Panel application should you use on the laptop to connect to the mobile hotspot?

- A. Phone and Modem
- B. RemoteApp and Desktop Connections
- C. System
- D. Credential Manager
- E. Work Folders
- F. Power Options
- G. Sync Center
- H. Network and Sharing Center

Answer: H

QUESTION 165

You have a standalone Windows 10 Enterprise computer that has a single hard drive installed and configured. You need to identify which storage devices can have content backed up by using File History. What should you identify?

- A. A writable Blu-ray disc
- B. A writable DVD disc
- C. An internal drive that is formatted NTFS
- D. An SD card that is formatted FAT32

Answer: D

Explanation:

<http://www.laptopmag.com/articles/back-files-file-history-windows-10>

QUESTION 166

You support Windows 10 Enterprise computers in a workgroup. You have configured a local AppLocker policy to prevent users from running versions of app.exe previous to v9.4. Users are still able to run app.exe. You need to block users from running app.exe by using the minimum administrative effort. What should you do?

- A. Change the Application Identity service startup mode to automatic and start the service.
- B. Configure enforcement for Windows Installed rules.
- C. Configure a Software Restriction Policy publisher rule.

D. Run the GPupdate /force command in an relevant command prompt.

Answer: A

Explanation:

[https://technet.microsoft.com/en-us/library/ee791779\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee791779(v=ws.10).aspx)

<https://technet.microsoft.com/en-us/itpro/windows/keep-secure/configure-the-application-identity-service>

QUESTION 167

Hotspot Question

You run the Get-AppvClientConfiguration cmdlet and you receive the following output.

Name	Value
-----	-----
PackageInstallationRoot	%programdata%\App-V
PackageSourceRoot	
LocationProvider	
AutoLoad	1
EnablePackageScripts	0
ReestablishmentInterval	5
ReestablishmentRetries	3
CertFilterForClientSsl	LOCAL_MACHINE\MY\1.3.6.1.5.5.7.3.2
VerifyCertificateRevocationList	1
SharedContentStoreMode	0
MigrationMode	0
RoamingFileExclusions	
RoamingRegistryExclusions	SOFTWARE\CLASSES
AllowHighCostLaunch	0
PackageStoreAccessControl	0
IntegrationRootUser	%LOCALAPPDATA%\Microsoft\AppV\Client\Integration
IntegrationRootGlobal	%ALLUSERSPROFILE%\Microsoft\AppV\Client\Integration
VirtualizableExtensions	exe,com,bat,cmd,vbs,ps1,cp1,jar,wsf,wsh,msc
IgnoreLocationProvider	0
ReportingEnabled	1
ReportingStartTime	1
ReportingRandomDelay	30
ReportingInterval	1
ReportingServerURL	http://SERVER10:8082
ReportingDataCacheLimit	
ReportingDataBlockSize	
ExperienceImprovementOptIn	0
EnablePublishingRefreshUI	0
ProcessesUsingVirtualComponents	{%SystemRoot%\explorer.exe, %ProgramFiles%\Internet Explore...
EnabledDynamicVirtualization	1

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

Answer Area

Microsoft Application Virtualization (App-V) packages launched by a user will [answer choice]

- not be cached
- be caught on the local disk
- be caught in the memory only

Background streaming is [answer choice]

- disabled for all applications
- enabled for all applications
- enabled for previously launched applications

Answer:

Answer Area

Microsoft Application Virtualization (App-V) packages launched by a user will [answer choice]

▼
not be cached
be caught on the local disk
be caught in the memory only

Background streaming is [answer choice]

▼
disabled for all applications
enabled for all applications
enabled for previously launched applications

QUESTION 168

You plan to deploy a Microsoft Azure Remote App collection by using a custom template image. The image will contain Microsoft Office 365 apps. The image will be used to deploy a collection that will be accessed by 50 users. You need to identify licensing requirements for the deployment. Which two requirements should you identify? Each correct answer presents part of the solution.

- A. An activated Office 365 ProPlus installation
- B. Windows client access licenses (CALs) assigned to the users
- C. Office 365 ProPlus licenses assigned to the users
- D. Remote Desktop client access licenses (CALs) assigned to the users
- E. Office 365 Enterprise E3 service plan

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/remoteapp/remoteapp-licensing>

QUESTION 169

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details in a question apply only to that question. You have a laptop that is joined to an Active Directory domain. You establish a Wi-Fi connection to a customer's Wi-Fi network. You need to identify whether the current network location of the Wi-Fi connection is private or public. Which Control Panel application should you use?

- A. Phone and Modem
- B. RemoteApp and Desktop Connections
- C. System
- D. Credential Manager
- E. Work Folders
- F. Power Options
- G. Sync Center
- H. Network and Sharing Center

Answer: H

QUESTION 170

.....

QUESTION 261

You work for a company that uses customized applications. The applications are published to 150 Windows 10 Enterprise laptops that are deployed in the field. All users must use the same version of the applications at the same time. You need to deploy and manage the applications updates centrally. What should you do?

- A. Deploy the applications as a Microsoft Application Virtualization.
- B. Use System Center Configuration Manager to deploy the application updates to the client.
- C. Deploy application updates as a shim through System Center Configuration.
- D. Use Intune to deploy the applications with the appropriate settings through the Windows Store.

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/management-tasks-applications#deploying-and-monitoring-apps>

<https://docs.microsoft.com/en-us/sccm/apps/deploy-use/revise-and-supersede-applications#application-supersedence>

QUESTION 262

Your network contains an Active Directory domain named contoso.com. A user receives the following error message when attempting to sign in to a computer: "The trust relationship between this workstation and the primary domain failed." You need to ensure that the user can sign in to the computer by using a domain user account. Which tool should you use?

- A. Netstat
- B. Netsh
- C. Netdom
- D. Netcfg

Answer: C

Explanation:

<https://www.petenetlive.com/KB/Article/0000504>

QUESTION 263

You support Windows 10 Enterprise computers that are members of an Active Directory domain. All of the computers have a dedicated recovery partition. A computer indicates that the domain is unavailable. The password of a local administrator account on the computer is unknown. You need to reset the password for the local administrator account on the computer. What should you do?

- A. Run Windows To Go workspace from a USB flash drive.
- B. Run the Windows 10 Enterprise installation wizard from a USB flash drive.
- C. Run Microsoft Diagnostic and Recovery Tool (DaRT) from a USB flash drive.
- D. Run Windows Recovery Environment (WinRE) from a recovery partition.

Answer: C

Explanation:

<https://www.top-password.com/knowledge/reset-windows-10-password.html>

QUESTION 264

You are the system administrator for a company. All devices run Windows 10 and use a variety of Microsoft Store for Business apps. All user reports issues updating a Windows Store app. You need to troubleshoot the issue. Which three actions should you perform? (Each correct answer presents a complete solution. Choose three.)

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

Answer: ADE

Explanation:

<https://windowsreport.com/windows-10-app-store-doesn-t-update/#6>

QUESTION 265

You administer a corporate network. Employees use docking stations for Windows 10 devices when the employees are working in their offices. The wireless adapters of the devices are connected to a specific network. The docking stations are connected to a separate network that uses twisted pair cabling. You need to ensure that the devices can access all resources from each network using either network adapter. What should you do?

- A. Configure a network bridge.
- B. Configure Internet Connection Sharing (ICS).
- C. Configure VPN Reconnect.
- D. Turn on Network Discovery.

Answer: C

Explanation:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd637803\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd637803(v=ws.10))

QUESTION 266

company installs a line-of-business (LOB) app on a server that runs Remote Desktop Services. You need to ensure that you can publish the application by using RemoteApp. What should you do first?

- A. Create a personal desktop session collection.
- B. Manually assign users to a session host.
- C. Create a pooled desktop collection.
- D. Automatically assign users to a session host.

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-create-collection#create-a-pooled-desktop-session-collection>

QUESTION 267

You have a Windows Server 2012 R2 server that runs Remote Desktop services. Users report that they cannot connect to RemoteApp programs. You observe that users do not know the proper connection details to access the Remote Desktop Web Access server. You need to simplify the process for connecting from Windows 10 devices to the Remote Desktop Web Access server. What should you create?

- A. Connection Manager Administration Kit connection profile
- B. Remote Desktop Connection configuration file
- C. Windows Remote Management script

D. Client configuration file

Answer: A

Explanation:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753977\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753977(v=ws.10))

QUESTION 268

A company has Windows 10 Enterprise client computers. File History is on. An employee downloads data to a folder on drive D named Archives. You need to ensure that the user can restore files from the Archives folder by using File History. What should you do?

- A. Configure the File History advanced settings to include the Archives folder.
- B. Create a library named History and add the Archives folder to the library.
- C. From the File History configuration options, change the drive and select the Archives folder.
- D. Move the Archives folder into the Windows system folder.

Answer: B

QUESTION 269

A company has Windows 10 Enterprise client computers. Users store data files in their user profile libraries. You need to ensure that users can restore data files to any date while minimizing system overhead. Which two actions should you perform? (Each answer presents part of the solution. Choose two.)

- A. Add each user to the local Backup Operations group.
- B. Turn on system protection.
- C. Configure settings to save copies of files daily.
- D. Turn on File History.

Answer: CD

Explanation:

<http://www.pcworld.com/article/2974385/windows/how-to-use-windows-10s-file-history-backup-feature.html>

QUESTION 270

You are the system administrator for a company. All employees have devices that run Windows 10. Employees store many files on network shares. You need to ensure that employees keep a copy of files from network shares on their devices, even when the devices are not connected to the company network. What should you first?

- A. Run the SettingSyncHost.exe command.
- B. Enable File History.
- C. Create a new pool and storage space.
- D. Run the Set-FileShare Windows PowerShell cmdlet.
- E. Enable Offline Files.

Answer: E

Explanation:

<https://www.howtogeek.com/98793/how-to-use-offline-files-in-windows-to-cache-your-networked-files-offline/>

QUESTION 271

You have a Microsoft Intune subscription. You need to uninstall the Intune agent from a computer. What should you do?

- A. From the Groups node in the Microsoft Intune administration portal, click Retire/Wipe.
- B. From the computer, use Programs and Features in Control Panel.
- C. From the Groups node in the Microsoft Intune administration portal, click Remote Lock on the Remote Tasks menu.
- D. From the computer, run the cltui.exe command.

Answer: A

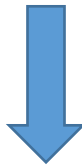
Explanation:

<https://www.petervanderwoude.nl/post/uninstall-the-microsoft-intune-client/>

QUESTION 272

.....

Get Complete Version Exam 70-697 Dumps with VCE and PDF Here



<https://www.passleader.com/70-697.html>