(70-697) Configuring Windows Devices

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 fregfe 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?

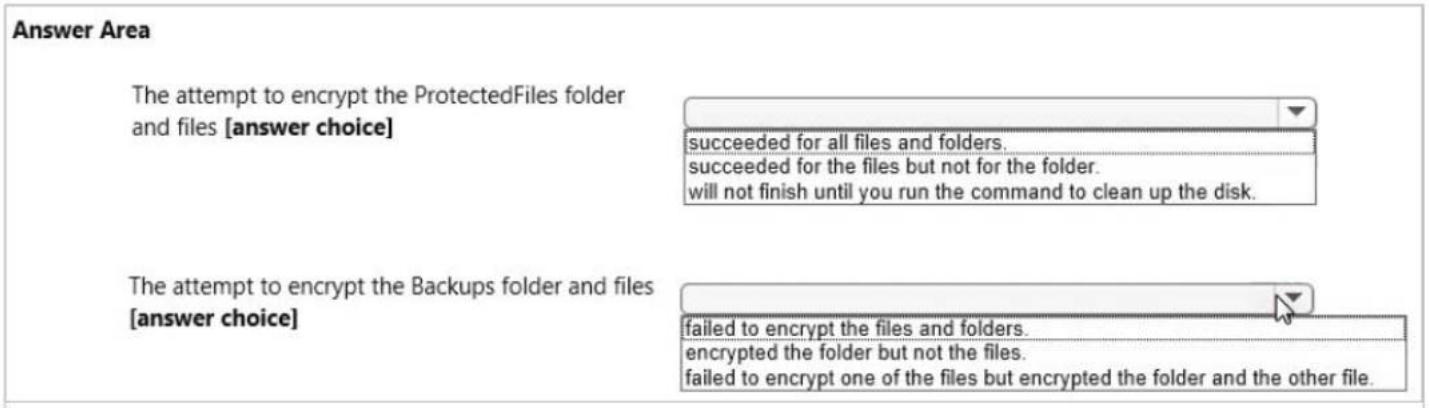
A. For the CorpWifi connection, select Yes, turn on sharing and connect to devices.
B. Turn on network discovery for the Public profile.
C. Change the CorpWired connection to public. Turn on network discovery for the Public profile. For the HotSpot connection, select No, don't turn on sharing or connect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

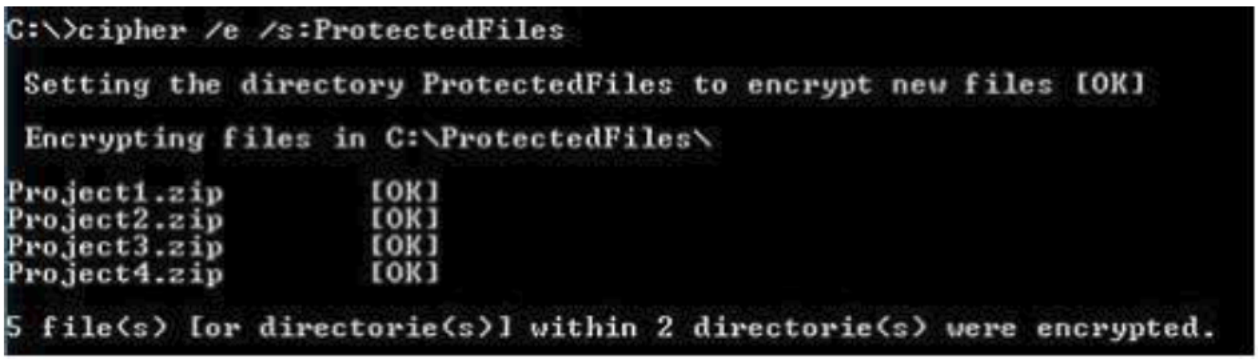
Use the drop-down menus to select the answer choice that completes each statement. NOTE: Each correct selection is worth one point.



Answer:

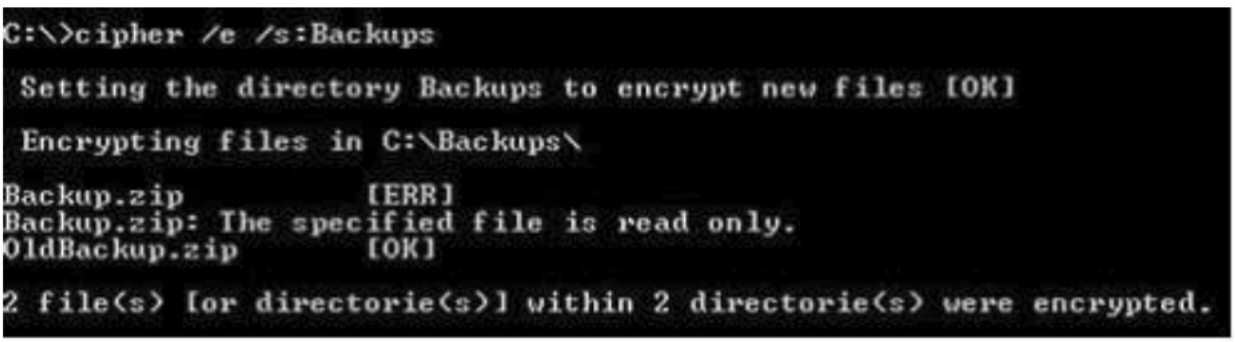
Explanation:

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).



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.



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

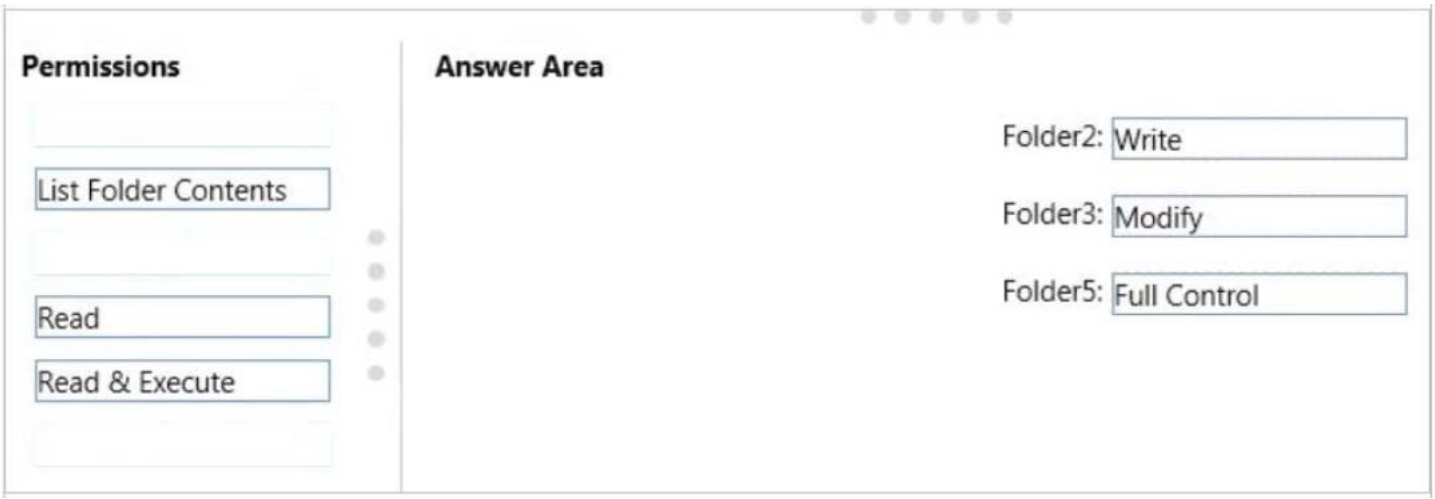
QUESTION 6
Drag and Drop Question
You have a computer that runs Windows 10 Enterprise that contains the following folders:

You have a local user named User1. User1 has read and execute permission to Folder1. You need to ensure that User1 can perform the following tasks.

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

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.

Answer:



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 I 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 Folders 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

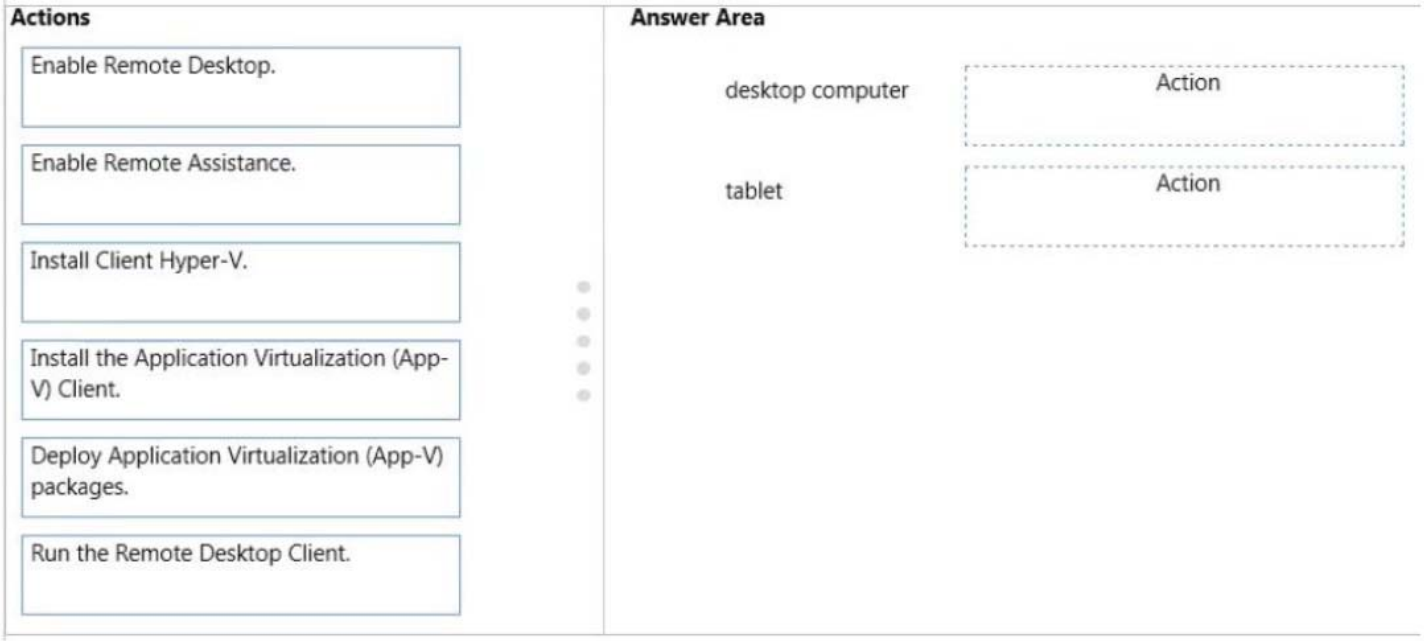
their home computers.
Which setting should you configure on the home computers?

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

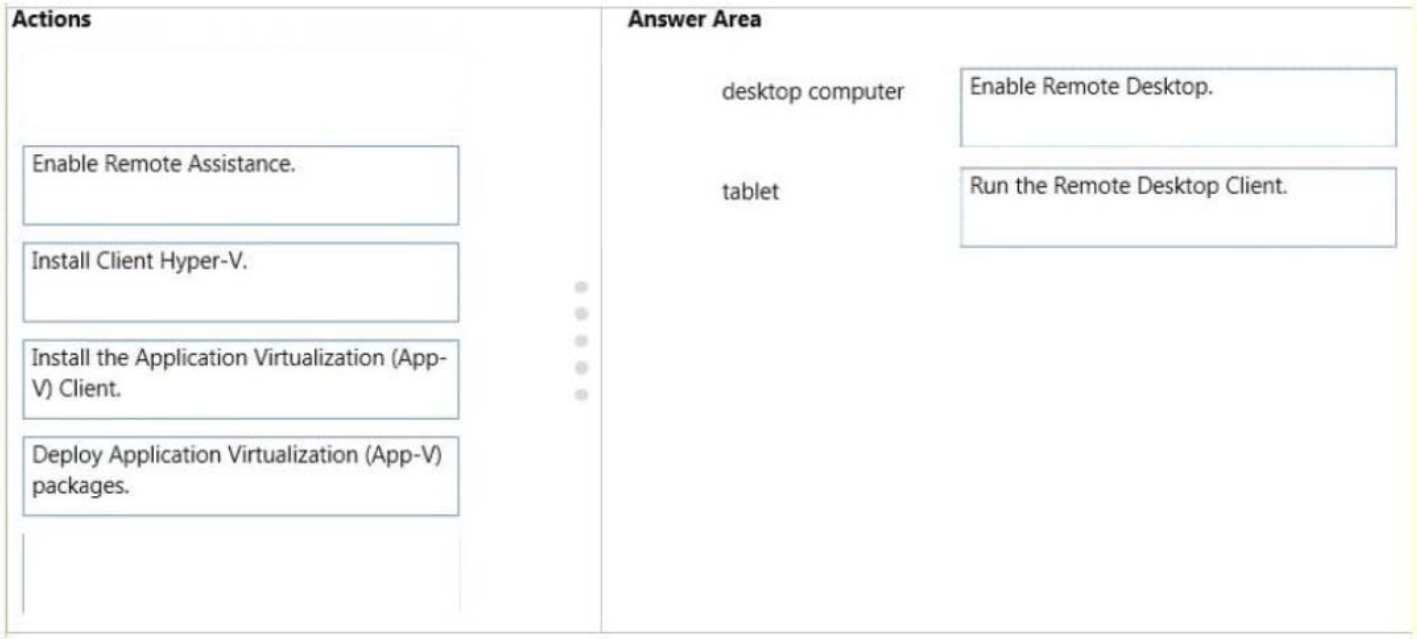
Answer: D
Explanation:
The solution is to deploy Remote Desktop Gateway in the office. Remote users can then connect to their computers on the office network by using Remote Desktop client on their home computers configured with the IP address of the Remote Desktop Gateway.
Remote Desktop Gateway (RD 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.



Answer:



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.