70-680 Q&As

Windows 7 Configuring

Pass Microsoft 70-680 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/70-680.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company has a server running Windows Server 2008 R2, with Windows Deployment Services (WDS), the Microsoft Deployment Toolkit (MDT), and the indows Automated Installation Kit (WAIK) set up. The company also has client computers running Windows 7 Enterprise.

You need to capture an image of a client computer.

What should you do on the server before performing actions on the client computer?

A. Use Sysprep with an answer file and set the UpdateInstalledDrivers option in the answer file to Mo.

B. Run the DiskPart command and the Attach command option.

C. Use Sysprep with an answer file and set the PersistAHDeviceInstalls option in the answer file to False.

D. Use Sysprep with an answer file and set the UpdateInstalledDrivers option in the answer file to Yes.

E. Add a boot image and create a capture image in WDS.

F. Run the BCDEdit /delete command.

G. Run the Dism command with the /Add-Driver option.

H. Run the ImageX command with the /Mount parameter.

I. Run the Dism command with the /Add-Package option.

J. Use Sysprep with an answer file and set the PersistAHDeviceInstalls option in the answer file to True.

K. Run the Start/w ocsetup command.

L. Run the Dism command with the /Mount-Wim option.

M. Run the PEImg /Prep command.

Correct Answer: E

QUESTION 2

Your company has a server named Server1 that runs Windows Server 2008. Server1 is a Windows Server Update Services (WSUS) server. You have a computer named Computer1 that runs Windows 7.

Computer1 is configured to obtain updates from Server1.

You open the WSUS snap-in on Server1 and discover that Computer1 does not appear.

You need to ensure that Computer1 appears in the WSUS snap-in.

What should you do?

A. On Server1, open Windows Update then select Check for updates.

B. On Server1, run Wsusutil.exe and specify the /import parameter.

C. On Computer1, open Windows Update and then select Change settings.

D. On Computer1, run Wuauclt.exe and specify the /detectnow parameter.

Correct Answer: D

wuauclt.exe

The wuauclt utility allows you some control over the functioning of the Windows Update Agent.

It is updated as part of Windows Update.

Detectnow Option

Because waiting for detection to start can be a time-consuming process, an option has been added to allow you to initiate detection right away. On one of the computers with the new Automatic Update client installed, run the following

command at the command prompt:

wuauclt.exe /detectnow

QUESTION 3

You have a Virtual Hard Disk (VHD) and a computer that runs Windows 7. The VHD has Windows 7 installed.

You need to start the computer from the VHD.

What should you do?

A. From Diskpart.exe, run Select vdisk.

B. From Disk Management, modify the active partition.

C. Run Bootcfg.exe and specify the /default parameter.

D. Run Bcdedit.exe and modify the Windows Boot Manager settings.

Correct Answer: D

When you have created a VHD and installed a system image on it, you can use the BCDEdit tool Bcdedit.exe to add a boot entry for the VHD file in your computer running Windows 7.

QUESTION 4

You have a computer that runs Windows 7. You create an Encrypting File System (EFS) recovery key and certificate.

You need to ensure that your user account can decrypt all EFS files on the computer.

What should you do?

A. From Credential Manager, add a Windows credential.

B. From Credential Manager, add a certificate-based credential.

C. From the local computer policy, add a data recovery agent.

D. From the local computer policy, modify the Restore files and directories setting.

Correct Answer: C

EFS Recovery Recovery Agents are certificates that allow the restoration of EFS encrypted files. When a recovery agent has been specified using local policies, all EFS encrypted files can be recovered using the recovery agent private key. You should specify a recovery agent before you allow users to encrypt files on a client running Windows 7. You can recover all files that users encrypt after the creation of a recovery agent using the recovery agent\\'s private key. You are not able to decrypt files that were encrypted before a recovery agent certificate was specified. You create an EFS recovery agent by performing the following steps:

1.

Log on to the client running Windows 7 using the first account created, which is the default administrator account.

2.

Open a command prompt and issue the command Cipher.exe /r:recoveryagent

3.

This creates two files: Recoveryagent.cer and Recoveryagent.pfx. Cipher.exe prompts you to specify a password when creating Recoveryagent.pfx.

4.

Open the Local Group Policy Editor and navigate to the \Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System node. Right-click this node and then click Add Data Recovery Agent. Specify the location of Recoveryagent.cer to specify this certificate as the recovery agent.

5.

To recover files, use the certificates console to import Recoveryagent.pfx. This is the recovery agent\\'s private key. Keep it safe because it can be used to open any encrypted file on the client running Windows 7.

QUESTION 5

Your company office network includes a file server that has Windows Server 2008 R2 installed and client computers that have Windows 7 Enterprise installed. The computers are members of an Active Directory domain. The file server has

the BranchCache feature installed.

The client computers have a third-party firewall application installed.

You configure BranchCache on all computers to run in Distributed Cache mode.

You need to ensure that the client computers can access all cached files.

What should you do?

A. Configure firewall exception rules for multicast traffic, inbound and outbound traffic for local UDP port 3702, and inbound and outbound traffic for local TCP port 80.

B. Check permissions.

C. Configure firewall exception rules for inbound and outbound traffic for local TCP port 80 and for inbound and outbound traffic for local TCP port 8443

D. Create a Group Policy object and enable the Set BranchCache Hosted Cache mode policy.

E. Run the Netsh branchcache set service mode=HOSTEDSERVER clientauthentication=NONE command.

F. Run the netsh branchcache set service mode=HOSTEDCLIENT command.

G. Run the netsh branchcache set service mode=DISTRIBUTED command

H. Create a Group policy object and configure the Set percetage of disk space used for client computer cache option.

I. Create a Group policy that sets Hash Publication for Branchcache as disabled.

Correct Answer: A

Configuring Windows 7 as a BranchCache client involves enabling BranchCache, selecting either Hosted Cache mode or Distributed Cache mode, and then configuring the client firewall to allow BranchCache traffic.

You can configure BranchCache either using Group Policy or by using the Netsh command-line utility. The firewall rules that you configure depend on whether you are using Hosted Cache or Distributed Cache mode.

You can use predefined firewall rules or manually create them based on protocol and port. The required firewall rules are as follows:

The BranchCache - Content Retrieval (Uses HTTP) predefined rule. If this rule is not available, create rules that allow inbound and outbound traffic on TCP port 80. This rule is required for both Hosted Cache and Distributed Cache mode.

You can create this rule using Windows Firewall With Advanced Security.

The BranchCache - Peer-Discovery (Uses WSD) predefined rule. If this rule is not available, create rules that allow inbound and outbound traffic on UDP port 3702. This rule is only required when using Distributed Cache mode. The

BranchCache - Hosted Cache Client (HTTPS-Out) predefined rule. It this rule is not available, configure a rule that allows outbound traffic on TCP port 443. This rule is required only when using Hosted Cache mode.

You need to configure the firewall rules only when you configure BranchCache using Group Policy. When you configure BranchCache using Netsh, the appropriate firewall rules are set up automatically.