70-646 Q&As

Pro: Windows Server 2008

Pass Microsoft 70-646 Exam with 100% Guarantee

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

https://www.lead4pass.com/70-646.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You are planning the deployment of Windows Server 2008 R2 to CHDATA03 and CHDATA04.

You have the following requirements:

-Do not impact settings for CHDATA01 and CHDATA02.

-Apply Windows Server 2008 R2-specific settings to CHDATA03 and CHDATA04 after migration.

-Ensure that the ServerSettings GPO does not apply to CHDATA03 and CHDATA04 after migration.

You need to plan a strategy that meets the requirements.

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

A. Create a GPO named MigratedServers that contains the Windows Server 2008 R2 settings. Create a WMI filter that targets Windows Server 2003 and link it to the MigratedServers GPO,

B. Block inheritance on the CH_FileServers OU.

C. Create a WMI filter that targets Windows Server 2003 and link it to the ServerSettings GPO.

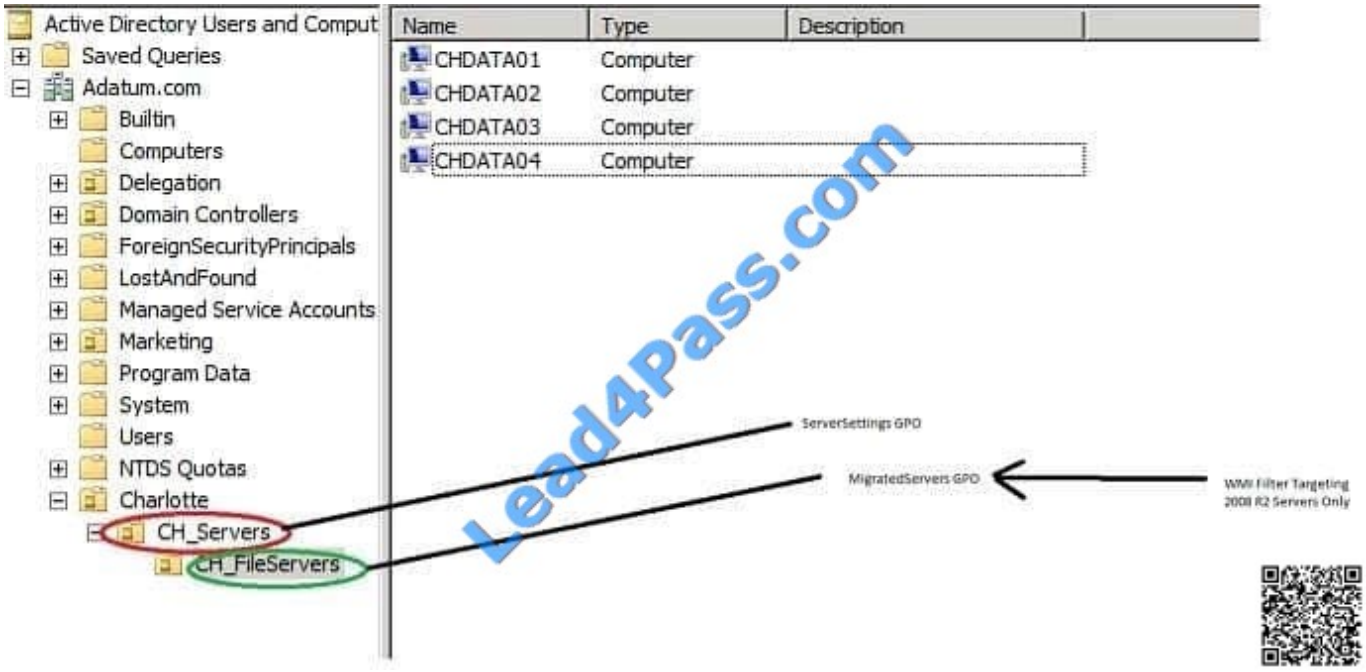
D. Enable loopback processing on the MigratedServers GPO.

E. Link the MigratedServers GPO to the CH_FileServers OU.

F. Create a GPO named MigratedServers that contains the Windows Server 2008 R2 settings. Create a WMI filter that targets Windows Server 2008 R2 and link it to the MigratedServers GPO.

Correct Answer: EF

A WMI filter enables you to specify criteria that must be matched before the linked GPO is applied to a computer. By letting you filter the computers to which the GPO applies, this reduces the need to further subdivide your OUs in Active Directory. This technique is dynamic, in that the filter is evaluated when the computer attempts to apply the policy. So if you are filtering based on the version of Windows then upgrading the computer from Windows XP to Windows 7 requires no changes to your GPO, because the filter will automatically recognize the change and filter the computer\\'s access to the GPO accordingly. I\\'ve just put the structure together in a DC and took a screen shot of it. this is how i interperate the information given



It on the second page of the exhibit it says that the ServerSettings GPO applies to all servers not all file servers. So that means one of two things, its linked to the CH_Servers OU OR its linked higher like at a domain level because then it applies to ALL servers in all regions. as the full AD structure is not clear I\\'ll assume its applied on all CH servers only, but either way if its applied at a domain level it shouldn\\'t matter.

If you first carry out step F you create the MigratedServers GPO, then you create the Server 2008 R2 WMI filter and apply that to the GPO you just created, then you carry out step E which links the MigratedServers GPO which has a Server 2008 R2 WMI filter to the CH_FileServers OU.

NOTE: possible issue Thanks to SoK for highlighting this. the question states what 2 steps But requirement 3 says Ensure that the ServerSettings GPO does not apply to CHDATA03 and CHDATA04 after migration. So ServerSettings GPO applies IE settings to servers in the CH_Servers ou and will also be applied to any Child OUs of that and on page 2 it says that CH_FileServers is a child of CH_servers so the ServerSettings GPO will be applied to all file servers by default regardless of their OS. the settings are IE settings and as its stands those settings would apply to CHDATA03 and CHDATA04 because of the ServerSettings GPO so unless you block that GPO somehow reaching the two 2008 file servers, answer B wont work because it then blocks them for CHDATA01 and CHDATA02 which you don\\'t want. A wont work at it is an incorrect "replacement" for F because its applying 2008 settings to 2003 servers which is as useful as tits on a bull. D is pointless in this specific case so it a[[ears that C may be required. I\\'m going to leave C out for the moment because the question clearly states 2 answers

QUESTION 2

You are designing a Windows Server 2008 R2 deployment strategy for the Minneapolis campus servers.

Which deployment strategy should you recommend?

A. install from media.

B. Use a discover image in WDS.

C. Deploy a VHD image.

D. Deploy a WIM image.

Correct Answer: D

Requirements - Bitlocker is needed on all disks in Minneapolis and installations must be done remotely

VHD Image

- according to the official MS courseware book 6433A - a VHD can not contain more than one partition. so if true that rules VHD Images out because you need bitlocker and bitlocker requires 2 partitions. so if this is true then answer C is wrong.also http://technet.microsoft.com/en-us/library/dd363560.aspx

A supported .vhd image. The only supported operating systems are Windows Server 2008 R2, Windows 7 Enterprise, and Windows 7 Ultimate. Fixed, dynamic, and differencing .vhd images are supported. However, note that a supported

image cannot contain the following:

More than one operating system.

More than one partition.

Applications or data (instead of an operating system).

A 64-bit operating system that is partitioned with a GUID partition table (GPT).

So again further evidence that C is not the right answer as Bit locker needs 2 partitions.

I\\'m leaning toward Answer B because

WDS Images

WDS uses two different types of images: install images and boot images. Install images are the operating system images that will be deployed to computers running Windows Server 2008 R2, Windows Server 2008, Windows 7, or Windows

Vista. A default installation image named Install.wim is located in the \Sources directory of the installation DVD. If you are using WDS to deploy Windows 7 to computers with different processor architectures, it will be necessary to add

separate installation images for each architecture to the WDS server.

Architecture-specific images can be found on the architecture-specific installation media; for example, the Itanium image is located on the Itanium installation media, and the x64 default installation image is located on the x64 installation

media. Although it is possible to create custom images, it is necessary to have only one image per processor architecture. For example, deploying Windows Server 2008 R2 Enterprise edition x64 to a computer with two x64 processors and to

a computer with eight x64 processors in SMP configuration only requires access to the default x64 installation image. Boot images are used to start a client computer prior to the installation of the operating system image. When a computer

starts off a boot image over the network, a menu is presented that displays the possible images that can be deployed to the computer from the WDS server. The Windows Server 2008 R2 Boot.wim file allows for advanced deployment options,

and this file should be used instead of the Boot.wim file that is available from other sources.

In addition to the basic boot image, there are two separate types of additional boot images that can be configured for use with WDS. The capture image is a boot image that starts the WDS capture utility. This utility is used with a

reference

computer, prepared with the Sysprep utility, as a method of capturing the reference computer\\'s image for deployment with WDS. The second type of additional boot image is the discover image. Discover images are used to deploy images to

computers that are not PXE-enabled or on networks that don\\'t allow PXE. These images are written to CD, DVD, or USB media and the computer is started off the media rather than off the PXE network card, which is the traditional method of

using WDS.

I\\'m gonna make a huge assumption that the Minneapolis servers are on a different subnet, which makes sense because they are all different campuses for a college. but if there is a DHCP Server or IP Helper is enabled then that wont be a

problem. So B may not be the answer

Media Install

It specifically says they use WDS for deployment. WDS is all about using images so would that not rule out media install? You can do media installs that are unattended but it requires sending a DVD and corresponding USB key with an

answer file to the site and it being inserted into the server. But GDI uses PXE enabled network cards so that would imply media is not used as images would be stored centrally.

QUESTION 3

Your network consists of a single Active Directory domain. The domain contains a server that runs Windows Server 2008 R2 and that has the Remote Desktop Services server role installed.

The server has six custom Applications installed. The custom Applications are configured as RemoteApps.

You notice that when a user runs one of the Applications, other users report that the server seems slow and that some Applications become unresponsive.

You need to ensure that active user sessions receive equal access to system resources.

What should you do?

A. Implement Remote Desktop Web Access.

B. Implement Remote Desktop Connection Broker.

C. Configure Performance Monitor.

D. Implement Windows System Resource Manager.

Correct Answer: D

http://technet.microsoft.com/en-us/library/cc771218%28WS.10%29.aspx http://technet.microsoft.com/en-us/library/cc732553%28WS.10%29.aspx Terminal Services and Windows System Resource Manager

Windows-System Resource Manager (WSRM) on Windows Server-2008 allows you to control how CPU and memory

resources are allocated to applications, services, and processes on the computer. Managing resources in this way improves system performance and reduces the chance that applications, services, or processes will take CPU or memory resources away from one another and slow down the performance of the computer. Managing resources also creates a more consistent and predictable experience for users of applications and services running on the computer.

You can use WSRM to manage multiple applications on a single computer or users on a computer on which Terminal Services is installed.

Resource-Allocation Policies WSRM uses resource-allocation policies to determine how computer resources, such as CPU and memory, are allocated to processes running on the computer. There are two resource-allocation policies that are specifically designed for computers running Terminal Services. The two Terminal Services-specific resource-allocation policies are:

Equal_Per_User Equal_Per_Session

Policy	Description
Equal per process	When the **Equal_Per_Process** resource allocation policy is managing the system, each running process is given equal treatment. For example, if a server that is running ten processes reaches 70% processor utilization, Windows System Resource Manager will limit each process to using 10% of the processor resources while they are in contention. Note that resources not used by low utilization processes will be allocated to other processes.
Equal per user	When the **Equal_Per_User** resource allocation policy is managing the system, processes are grouped according to the user account that is running them and each of these process groups is given equal treatment. For example, if four users are running processes on the server, each user will be allocated 25% of the system resources to complete those processes. A user running a single application is allocated the same resources as a user running several applications. This policy is especially useful for application servers.
Equal per session	When the **Equal_Per_Session** resource allocation policy is managing the system, resources are allocated on an equal basis for each session connected to the system. This policy is for use with terminal servers.
Equal per IIS application pool	When the **Equal_Per_IISAppPool** resource allocation policy is managing the system, each running IIS application pool is given equal treatment, applications that are not in an IIS application pool can only use resources that are not being consumed by IIS application pools.

QUESTION 4

Your network consists of a single Active Directory domain. The network contains two Windows Server 2008 R2 computers named Server1 and Server2. The company has two identical print devices. You plan to deploy print services. You need to plan a print services infrastructure to meet the following requirements:

-Manage the print queue from a central location.

-

Make the print services available, even if one of the print devices fails. What should you include in your plan?

A.

Install and share a printer on Server1. Enable printer pooling.

B.

Install the Remote Desktop Services server role on both servers. Configure Remote Desktop Connection Broker (RD Connection Broker).

C.

Install and share a printer on Server1. Install and share a printer on Server2. Use Print Management to install the printers on the client computers.

D.

Add Server1 and Server2 to a Network Load Balancing cluster. Install a printer on each node of the cluster.

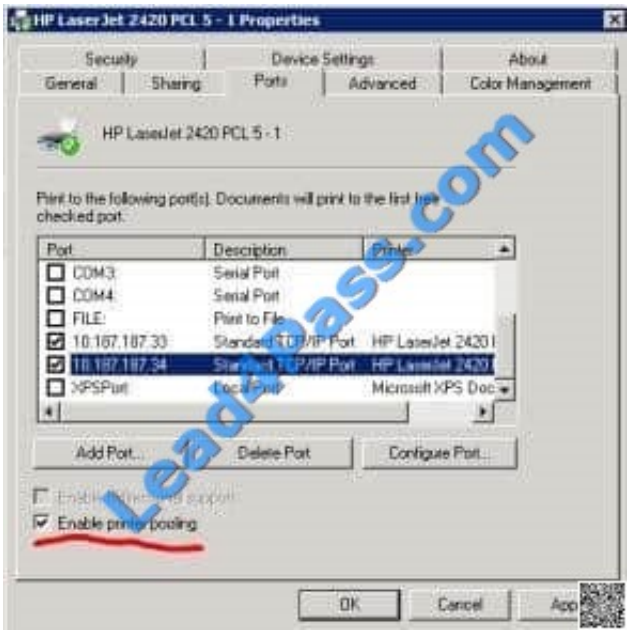
Correct Answer: A

http://www.techrepublic.com/blog/datacenter/configure-printer-pooling-in-windows-server-2008/964

Managing printers can be the bane of a Windows administrator. One feature that may assist you with this task is the Windows printer pooling feature. Windows Server 2008 offers functionality that permits a collection of multiple like-configured printers to distribute the print workload.

Printer pooling makes one share that clients print to, and the jobs are sent to the first available printer. Configuring print pooling is rather straightforward in the Windows printer configuration applet of the Control Panel. Figure A shows two like-modeled printers being pooled.

To use pooling, the printer models need to be the same so that the driver configuration is transparent to the end device; this can also help control costs of toner and other supplies. But plan accordingly -- you don\\'t want users essentially running track to look for their print jobs on every printer in the office.



QUESTION 5

You need to ensure that all servers meet the company\\'s security requirements. Which tool should you use?

A. Microsoft Baseline Security Analyzer (MBSA)

B. Microsoft Security Assessment Tool (MSAT)

C. Resultant Set of Policy (RSoP)

D. Security Configuration Wizard (SCW)

Correct Answer: A

http://technet.microsoft.com/en-us/security/cc184924

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in

accordance with Microsoft security recommendations and offers specific remediation guidance.

Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems.