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.geekcert.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

Your company has a main office and a branch office. Your network contains a single Active Directory domain.

The functional level of the domain is Windows Server 2008 R2. An Active Directory site exists for each office.

All servers run Windows Server 2008 R2. You plan to deploy file servers in each office.

You need to design a file sharing strategy to meet the following requirements:

-

Users in both offices must be able to access the same files.

-

Users in both offices must use the same Universal Naming Convention (UNC) path to access files.

-The design must reduce the amount of bandwidth used to access files.

-Users must be able to access files even if a server fails.

What should you include in your design?

A. A standalone DFS namespace that uses replication.

B. A domainbased DFS namespace that uses replication.

C. A multisite failover cluster that contains a server located in the main office and another server located in the branch office.

D. A Network Load Balancing cluster that contains a server located in the main office and another server located in the branch office.

Correct Answer: B

MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:

Domain-Based Namespaces

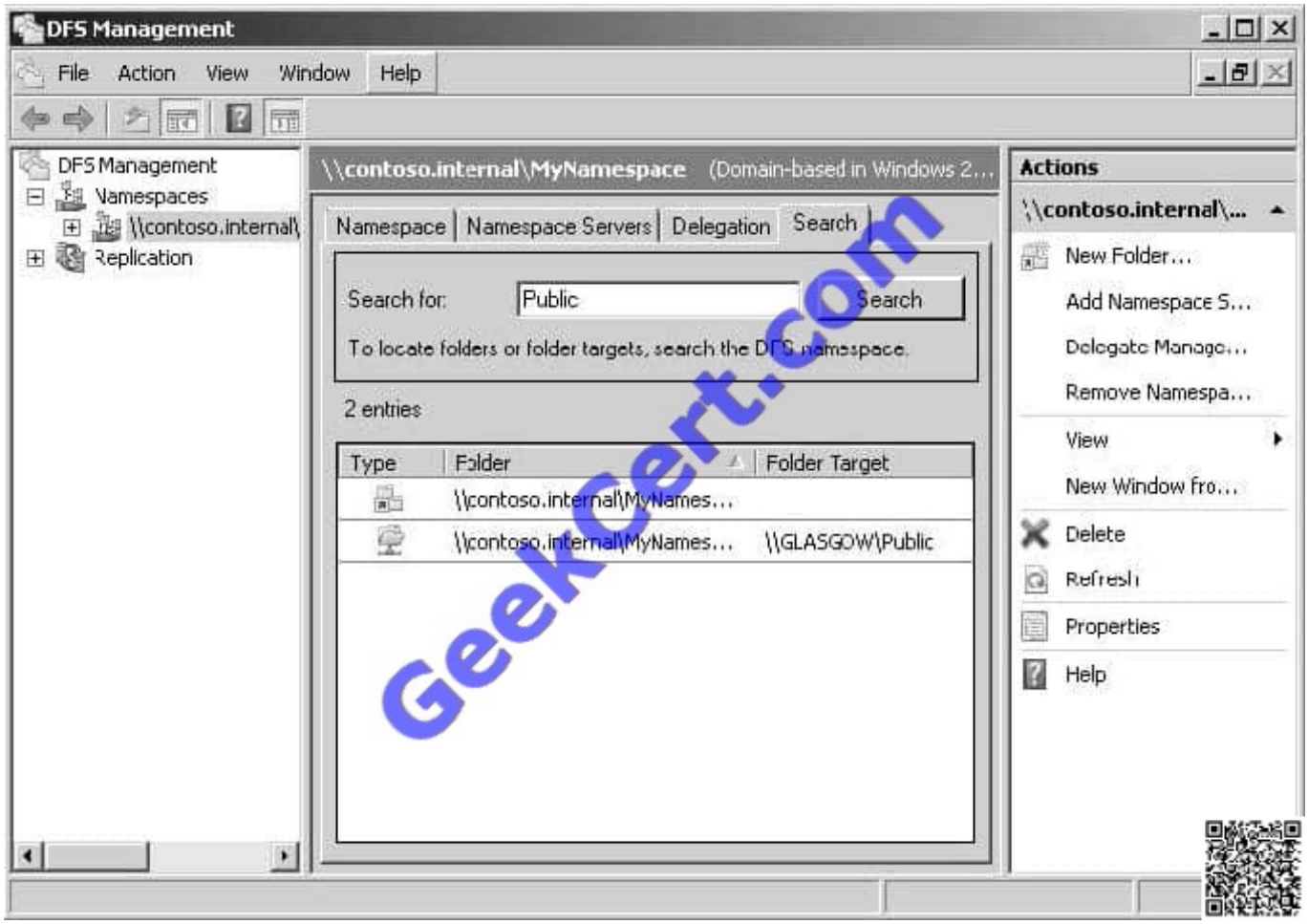
You can create domain-based namespaces on one or more member servers or DCs in the same domain.

Metadata for a domain-based namespaces is stored by AD DS. Each server must contain an NTFS volume to host the namespace. Multiple namespace servers increase the availability of the namespace and ensure failover protection. A domain-based namespace cannot be a clustered resource in a failover cluster. However, you can locate the namespace on a server that is also a node in a failover cluster provided that you configure the namespace to use only local resources on that server. A domain-based namespace in Windows Server 2008 mode supports access-based enumeration. Windows Server 2008 mode is discussed later in this lesson.

You choose a domain-based namespace if you want to use multiple namespace servers to ensure the availability of the namespace, or if you want to make the name of the namespace server invisible to users.

When users do not need to know the UNC path to a namespace folder it is easier to replace the namespace server or migrate the namespace to another server.

If, for example, a stand-alone namespace called \\Glasgow\Books needed to be transferred to a server called Brisbane, it would become \\Brisbane\Books. However, if it were a domain-based namespace (assuming Brisbane and Glasgow are both in the Contoso.internal domain), it would be \\Contoso.internal\Books no matter which server hosted it, and it could be transferred from one server to the other without this transfer being apparent to the user, who would continue to use \\Contoso.internal\Books to access it.



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

You plan to deploy a distributed database Application that runs on Windows Server 2008 R2.

You need to design a storage strategy that meets the following requirements:

-Allocates storage to servers as required

-Isolates storage traffic from the existing network

-

Ensures that data is available if a single disk fails

-

Ensures that data is available if a single storage controller fails

What should you include in your design?

A. An iSCSI disk storage subsystem that uses Microsoft Multipath I/O. Configure a RAID 0 array.

B. An iSCSI disk storage subsystem that uses Virtual Disk Service (VDS). Configure a RAID 5 array.

C. A Fibre Channel (FC) disk storage subsystem that uses Microsoft Multipath I/O. Configure a RAID 5 array.

D. A Fibre Channel (FC) disk storage subsystem that uses Virtual Disk Service (VDS). Configure a RAID 0 array.

Correct Answer: C

MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:

Fiber channel with isolate the network, Multipath I/O

Multipath I/O (MPIO) is a feature of Windows Server 2008 that allows a server to use multiple data paths to a storage device. This increases the availability of storage resources because it provides alternate paths from a server or cluster to a

storage subsystem in the event of path failure. MPIO uses redundant physical path components (adapters, switches, cabling) to create separate paths between the server or cluster and the storage device. If one of the devices in these

separate paths fails, an alternate path to the SAN device will be used, ensuring that the server is still able to access critical data. You configure failover times through the Microsoft iSCSI Software initiator driver or by modifying the Fibre

Channel HBA driver parameter settings, depending on the SAN technology deployed in your environment.

If the server will access a LUN through multiple Fibre Channel ports or multiple iSCSI initiator adapters, you must install MPIO on servers. You should verify that a server supports MPIO prior to enabling multiple iSCSI initiator adapters or

multiple Fibre Channel ports for LUN access. If you do not do this, data loss is likely to occur. In the event that you are unsure whether a server supports MPIO, only enable a single iSCSI initiator adapter or Fibre Channel port on the server.

Windows Server 2008 MPIO supports iSCSI, Fibre Channel, and Serially Attached Storage (SAS) SAN connectivity by establishing multiple connections or sessions to the storage device. The Windows Server 2008 MPIO implementation

includes a Device Specific Module (DSM) that works with storage devices that support the asymmetric logical unit access (ALUA) controller model as well as storage devices that use the Active/Active controller model. MPIO also supports the

following load-balancing policies:

Failover When this policy is implemented no load balancing is performed. The application specifies a primary path and a group of standby paths. The primary path is used for all device

requests. The standby paths are only used in the event that the primary path fails. Standby paths are listed from most preferred path to least preferred path.

Failback When this policy is configured, I/O is limited to a preferred path while that path is functioning. If the preferred path fails, I/O is directed to an alternate path. I/O will automatically switch back to the preferred path when that path returns

to full functionality.

Round-robin All available paths are used for I/O in a balanced fashion. If a path fails, I/O is redistributed among the remaining paths.

Round-robin with a subset of paths When this policy is configured, a set of preferred paths is specified for I/O and a set of standby paths is specified for failover. The set of preferred paths will be used until all paths fail, at which point failover

will occur to the standby path set. The preferred paths are used in a round-robin fashion.

Dynamic least queue depthI/O is directed to the path with the least number of outstanding requests.

Weighted path Each path is assigned a weight. The path with the least weight is chosen for I/O.

Load-balancing policies are dependent on the controller model (ALUA or true Active/ Active) of the storage array attached to the Windows Server 2008 computer. MPIO is added to a Windows Server 2008 computer by using the Add

Features

item in the Features area of Server Manager.

MORE INFO More on MPIO

To learn more about Multipath I/O, consult the following TechCenter article:http://www.microsoft.com/WindowsServer2003/technologies/storage/mpio/default.mspx.

Striped with Parity This LUN type, also known as RAID-5, offers fault tolerance and improved read performance, although write performance is hampered by parity calculation. This type

requires a minimum of three disks and the equivalent of one disk\\'s worth of storage is lost to the storage of parity information across the disk set. This LUN type will retain data if one disk is lost, but all data will be lost if two disks in the array

fail at the same time. In the event that one disk fails, it should be replaced as quickly as possible.

QUESTION 4

Which NAP enforcement method should you recommend?

A. 802.1x

B. DHCP

C. IPSec

D. VPN

Correct Answer: C

Requirements/information:

Implement Network Access Protection (NAP) for all of the client computers on the internal network and for all of the client computers that connect remotely

Some users work remotely. To access the company\\'s internal resources, the remote users use a VPN connection to NPAS1.

The network contains network switches and wireless access points (WAPs) from multiple vendors Some of the network devices are more than 10 years old and do not support portbased authentication.

Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer\\'s identity and compliance with corporate

governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance

policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAP Enforcement Methods

When a computer is found to be noncompliant with the enforced health policy, NAPenforces limited network access. This is done through an Enforcement Client (EC). Windows Vista,

Windows XP Service Pack 3, and Windows Server 2008 include NAPEC support for IPsec, IEEE 802.1X, Remote Access VPN, and DHCP enforcement methods. Windows Vista and Windows Server 2008 also support NAP enforcement for

Terminal Server Gateway connections.

NAP enforcement methods can either be used individually or can be used in conjunction with each other to limit the network access of computers that are found not to be in compliance with configured health policies. Hence you can apply the

remote access VPN and IPsec enforcement methods to ensure that internal clients and clients coming in from the Internet are only granted access to resources if they meet the appropriate client health benchmarks.

802.1X step-by-step guide.

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8a0925ee-ee06-4dfbbba2-07605eff0608anddisplaylang=en

802. 802.1X Enforcement

When 802.1X is used--over either wired or wireless networks--the client device\\'s access is restricted by network infrastructure devices such as wireless connection points and switches. Until the device has demonstrated its compliance, client

access is restricted.

Restriction is enforced on the network access device using an access control list (ACL) or by placing the client device on restricted virtual local area networks (VLANs). The 802.1X standard is more complex to deploy than DHCP, but it

provides a high degree of protection.

as a requirement of 802.1 is port authentication and some of the devices ate 10+ years old and do not support this then then this rules out this method

IPSEC ENFORCEMENT

IPsec enforcement works by applying IPsec rules. Only computers that meet health compliance requirements are able to communicate with each other. IPsec enforcement can be applied on a per-IP address, per-TCP port number, or per-

UDP port number basis. For example: You can use IPsec enforcement to block RDP access to a web server so that only computers that are healthy can connect to manage that server but allow clients that do not meet health requirements to

connect to view Web pages hosted by the same web server.

IPsec is the strongest method of limiting network access communication through NAP. Where it might be possible to subvert other methods by applying static addresses or switching ports, the IPsec certificate used for encryption can be

obtained by a host only when it passes the health check. No IPsec certificate means that communication with other hosts that encrypt their communications using a certificate issued from the same CA is impossible.

VPN Enforcemement

VPN enforcement is used on connecting VPN clients as a method of ensuring that clients granted access to the internal

network meet system health compliance requirements. VPN enforcement works by restricting network access to

noncompliant clients through the use of packet filters.

Rather than being able to access the entire network, incoming VPN clients that are noncompliant have access only to the remediation server group.

As is the case with 802.1X enforcement, the health status of a connected client is monitored continuously. If a client becomes noncompliant, packet filters restricting network access will be applied. If a noncompliant client becomes compliant,

packet filters restricting network access will be removed. VPN enforcement requires an existing remote access infrastructure and an NPS server. The enforcement method uses the VPN EC, which is included with Windows 7, Windows Vista,

Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

DHCP NAP Enforcement

DHCP NAP enforcement works by providing unlimited-access IPv4 address information to compliant computers and limited-access IPv4 address information to noncompliant computers.

Unlike VPN and 802.1X enforcement methods, DHCP NAP enforcement is applied only when a client lease is obtained or renewed. Organizations using this method of NAP enforcement should avoid configuring long DHCP leases because

this will reduce the frequency at which compliance checks are made.

To deploy DHCP NAP enforcement, you must use a DHCP server running Windows Server 2008 or Windows Server 2008 R2 because this includes the DHCP Enforcement Service (ES). The DHCP EC is included in the DHCP Client service

on Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

The drawback of DHCP NAP enforcement is that you can get around it by configuring a client\\'s IP address statically. Only users with local administrator access can configure a manual IP, but if your organization gives users local administrator

access, DHCP NAP enforcement may not be the most effective method of keeping these computers off the network until they are compliant.

QUESTION 5

You plan to deploy a distributed database Application that runs on multiple Windows Server 2008 R2 servers.

You need to design a storage strategy that meets the following requirements:

-Allocates storage to servers as required

-Uses the existing network infrastructure

-Uses standard Windows management tools

-Ensures that data is available if a single disk fails

What should you include in your design?

A. An iSCSI disk storage subsystem that supports Microsoft Multipath I/O. Configure the storage subsystem as a RAID?0 array.

B. An iSCSI disk storage subsystem that supports Virtual Disk Service (VDS). Configure the storage subsystem as a RAID?5 array.

C. A Fibre Channel (FC) disk storage subsystem that supports Microsoft Multipath I/O. Configure the storage subsystem as a RAID?0 array.

D. A Fibre Channel (FC) disk storage subsystem that supports the Virtual Disk Service (VDS). Configure the storage subsystem as a RAID?5 array.

Correct Answer: B

MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:

Virtual Disk Service (VDS)

Virtual Disk Service (VDS) provides a standard set of application programming interfaces (APIs) that provide a single interface through which disks can be managed. VDS provides a complete solution for managing storage hardware and

disks and enables you to create volumes on those disks. This means that you can use a single tool to manage devices in a mixed storage environment rather than tools provided by different hardware vendors. Before you can manage a LUN

using Storage Manager For SANs, you must install its VDS hardware provider. This will usually be provided by the hardware vendor. Prior to purchasing a storage device to be used on your organization\\'s SAN, you should verify that a

compatible VDS hardware provider exists.

VDS defines a software and a hardware provider interface. Each of these providers implements a different portion of the VDS API. The software provider is a program that runs on the host and is supported by a kernelmode driver. Software

providers operate on volumes, disks, and partitions.

The hardware provider manages the actual storage subsystem. Hardware providers are usually disk array or adapter cards that enable the creation of logical disks for each LUN type. The LUN type that can be configured will depend on the

options allowed by the VDS hardware provider. For example, some VDS hardware providers will allow the RAID-5 (Striped with Parity) LUN type to be implemented, while others might be limited to providing the Mirrored or Spanned LUN

types.

MORE INFO More on VDS

For more information on the functionality of VDS, consult the following TechNet article:http://technet2.microsoft.com/windowsserver/en/library/dc77e7c7-ae44-4483-878b-6bc3819e64dc1033.mspx?mfr=true

Storage Manager For SANs

You can use the Storage Manager For SANs console to create LUNs on Fibre Channel and iSCSI storage arrays. You install Storage Manager For SANs as a Windows Server 2008 feature. To use Storage Manager For SANs to manage

LUNs, the following criteria must be met:

The storage subsystems that you are going to manage must support VDS.

The VDS hardware provider for each subsystem must already be installed on the Windows Server 2008 computer. When you open Storage Manager For SANs from the Administrative Tools menu, you are presented with three main nodes,

which have the following functionality:

LUN ManagementThis node lists all of the LUNs created with Storage Manager For SANs. From this node you can create new LUNs, extend the size of existing LUNs, assign and unassign LUNs, and delete LUNs. You can also use this node

to configure the Fibre Channel and iSCSI connections that servers use to access LUNs.

SubsystemsThis node lists all of the storage subsystems currently discovered within the SAN environment. You can rename subsystems using this node.

DrivesThis node lists all of the drives in the storage subsystems discovered in the SAN. You can identify drives that you are working with by making the drive light blink from this node.

You can use any LUN type that is supported by the storage subsystem that you are deploying.

The different

LUN types are:

SimpleA simple LUN uses either an entire physical drive or a portion of that drive. The failure of a disk in a simple LUN means that all data stored on the LUN is lost.

SpannedA spanned LUN is a simple LUN that spans multiple physical drives. The failure of any one disk in a spanned LUN means that all data stored on the LUN is lost.

StripedData is written across multiple physical disks. This type of LUN, also known as RAID-0 has improved I/O performance because data can be read and written to multiple disks simultaneously, but like a spanned LUN, all data will be lost

in the event that one disk in the array fails.

MirroredThis LUN type, also known as RAID-1, is fault tolerant. Identical copies of the LUN are created on two physical drives. All read and write operations occur concurrently on both drives. If one disk fails, the LUN continues to be available

on the unaffected disk. Striped with ParityThis LUN type, also known as RAID-5, offers fault tolerance and improved read performance, although write performance is hampered by parity calculation. This type requires a minimum of three disks and the equivalent of one disk\\'s worth of storage is lost to the storage of parity information across the disk set. This LUN type will retain data if one disk is lost, but all data will be lost if two disks in the array fail at the same time. In the event that one disk fails, it should be replaced as quickly as possible.