# 70-646<sup>Q&As</sup>

70-646<sup>Q&As</sup>

**Pro: Windows Server 2008**

## Pass Microsoft 70-646 Exam with 100% Guarantee

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

*https://www.passapply.com/70-646.html*

### 100% Passing Guarantee
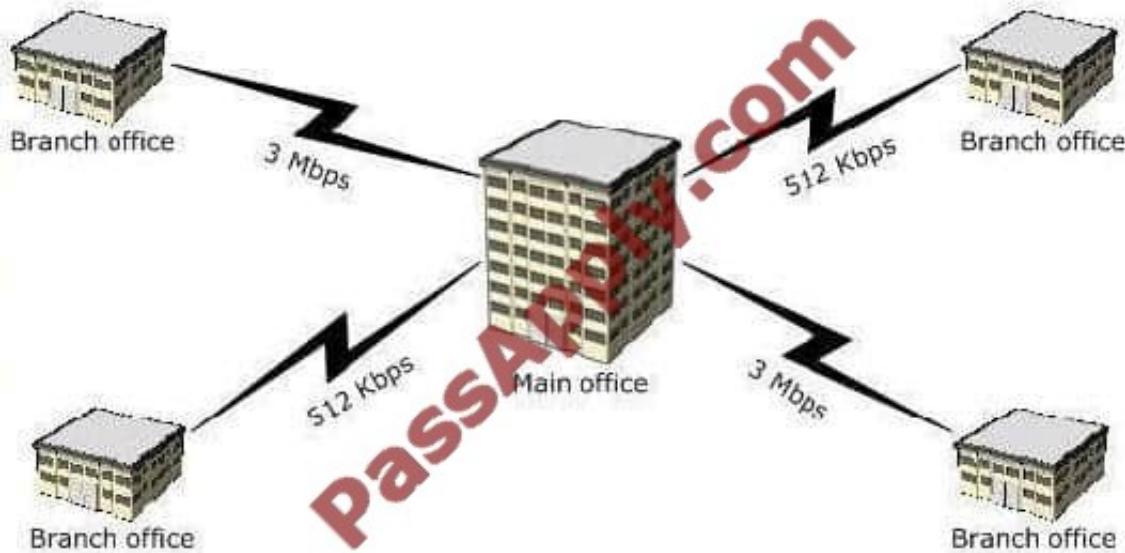### 100% Money Back Assurance

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**

Your network is configured as shown in the following diagram.



Each office contains a server that has the File Services server role installed. The servers have a shared folder named Resources. You need to plan the data availability of the Resources folder. Your plan must meet the following requirements:

-If a WAN link fails, the files in the Resources folder must be available in all of the offices.

- If a single server fails, the files in the Resources folder must be available in each of the branch offices, and the users must be able to use existing drive mappings.

-

Your plan must minimize network traffic over the WAN links. What should you include in your plan?

A.

a standalone DFS namespace that uses DFS Replication in a full mesh topology

B.

a domain-based DFS namespace that uses DFS Replication in a full mesh topology

C.

a standalone DFS namespace that uses DFS Replication in a hub and spoke topology

D.

a domain-based DFS namespace that uses DFS Replication in a hub and spoke topology

Correct Answer: D

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

Distributed File System (DFS) DFS is considerably enhanced in Windows Server 2008. It consists of two technologies, DFS Namespaces and DFS Replication, that you can use (together or independently) to provide fault-tolerant and flexible

file sharing and replication services.

DFS Namespaces lets you group shared folders on different servers (and in multiple sites) into one or more logically structured namespaces. Users view each namespace as a single shared folder with a series of subfolders. The underlying

shared folders structure is hidden from users, and this structure provides fault tolerance and the ability to automatically connect users to local shared folders, when available, instead of routing them over wide area network (WAN) connections.

DFS Replication provides a multimaster replication engine that lets you synchronize folders on multiple servers across local or WAN connections. It uses the Remote Differential Compression (RDC) protocol to update only those files that

have changed since the last replication. You can use DFS Replication in conjunction with DFS Namespaces or by itself.

Specifying the Replication Topology

The replication topology defines the logical connections that DFSR uses to replicate files among servers. When choosing or changing a topology, remember that that two one-way connections are created between the members you choose,

thus allowing data to flow in both directions. To create or change a replication topology in the DFS Management console, right-click the replication group for which you want to define a new topology and then click New Topology. The New

Topology Wizard lets you choose one of the following options:

Hub And Spoke This topology requires three or more members. For each spoke member, you should choose a required hub member and an optional second hub member for redundancy. This optional hub ensures that a spoke member can

still replicate if one of the hub members is unavailable. If you specify more than one hub member, the hub members will have a full-mesh topology between them.

Full Mesh In this topology, every member replicates with all the other members of the replication group. This topology works well when 10 or fewer members are in the replication group.

**QUESTION 2**

You need to recommend a VHD configuration for the virtual desktop pool VMs. What should you include in the recommendation?

A. differencing VHDs

B. dynamically expanding VHDs

C. fixed-size VHDs

D. passthrough disks

Correct Answer: B

http://technet.microsoft.com/en-us/library/dd440865%28WS.10%29.aspx#dynamic

When is it appropriate to use dynamically expanding VHDs?

Dynamically expanding VHDs are useful in nonproduction environments where flexible storage requirements and frequently changing the VHD image is more of an advantage than the reliability of the data within the VHD. In addition,

dynamically expanding VHDs are best for testing environments because there is less impact if you have to rebuild the VHD. For example, a test environment can use multiple dynamically expanding VHDs, each with a different Windows

image and set of applications to test. If the VHD files are modified during testing or accidentally become corrupt, you can replace the VHDs from a safe copy and restart testing.

Using dynamically expanding VHDs in a test environment provides the following benefits:

Flexible use of disk space. You can use free space for the VHD to expand during native VHD boot.

This space would have been unavailable if the volume hosted multiple VHDs in a fixed format.

Faster transfer time when copying VHDs between locations. The file size for a dynamically expanding VHD that is not using its maximum capacity, will transfer in less time between a

network share and a local disk than a fixed VHD of equivalent maximum size. Although rare, you may consider using dynamically expanding VHDs in production environments if

1) all of the content of the dynamically expanding VHD can be regenerated from other sources and ritical data is stored on volumes outside the dynamically expanding VHD.

---

**QUESTION 3**

Your company has several branch offices.

Your network consists of a single Active Directory domain. Each branch office contains domain controllers and member servers. The domain controllers run Windows Server 2003 SP2. The member servers run Windows Server 2008 R2.

Physical security of the servers at the branch offices is a concern.

You plan to implement Windows BitLocker Drive Encryption (BitLocker) on the member servers.

You need to ensure that you can access the BitLocker volume if the BitLocker keys are corrupted on the member servers. The recovery information must be stored in a central location.

What should you do?

A. Upgrade all domain controllers to Windows Server 2008 R2. Use Group Policy to configure Public Key Policies.

B. Upgrade all domain controllers to Windows Server 2008 R2. Use Group Policy to enable Trusted Platform Module (TPM) backups to Active Directory.

C. Upgrade the domain controller that has the schema master role to Windows Server 2008 R2. Use Group Policy to enable a Data Recovery Agent (DRA).

D. Upgrade the domain controller that has the primary domain controller (PDC) emulator role to Windows Server 2008 R2. Use Group Policy to enable a Data Recovery Agent (DRA).

---

Correct Answer: B

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

Planning BitLocker Deployment

Windows BitLocker and Drive Encryption (BitLocker) is a feature that debuted in Windows Vista Enterprise and Ultimate Editions and is available in all versions of Windows Server 2008.

BitLocker serves two purposes:

protecting server data through full volume encryption and providing an integrity-checking mechanism to ensure that the boot environment has not been tampered with.

Encrypting the entire operating system and data volumes means that not only are the operating system and data protected, but so are paging files, applications, and application configuration data. In the event that a server is stolen or a hard

disk drive removed from a server by third parties for their own nefarious purposes, BitLocker ensures that these third parties cannot recover any useful data. The drawback is that if the BitLocker keys for a server are lost and the boot

environment is compromised, the data stored on that server will be unrecoverable.

To support integrity checking, BitLocker requires a computer to have a chip capable of supporting the Trusted Platform Module (TPM) 1.2 or later standard. A computer must also have a BIOS that supports the TPM standard. When BitLocker

is implemented in these conditions and in the event that the condition of a startup component has changed, BitLocker-protected volumes are locked and cannot be unlocked unless the person doing the unlocking has the correct digital keys.

Protected startup components include the BIOS, Master Boot Record, Boot Sector, Boot Manager, and Windows Loader.

From a systems administration perspective, it is important to disable BitLocker during maintenance periods when any of these components are being altered. For example, you must disable BitLocker during a BIOS upgrade. If you do not, the

next time the computer starts, BitLocker will lock the volumes and you will need to initiate the recovery process. The recovery process involves entering a 48-character password that is generated and saved to a specified location when

running the BitLocker setup wizard. This password should be stored securely because without it the recovery process cannot occur. You can also configure BitLocker to save recovery data directly to Active Directory; this is the recommended

management method in enterprise environments.

You can also implement BitLocker without a TPM chip. When implemented in this manner there is no startup integrity check. A key is stored on a removable USB memory device, which must be present and supported by the computer\\'s BIOS

each time the computer starts up. After the computer has successfully started, the removable USB memory device can be removed and should then be stored in a secure location. Configuring a computer running Windows Server 2008 to use

a removable USB memory device as a BitLocker startup key is covered in the second practice at the end of this lesson.

BitLocker Group Policies

BitLocker group policies are located under the Computer Configuration\Policies\ Administrative Templates\Windows Components\BitLocker Drive Encryption node of a Windows Server 2008 Group Policy object. In the event that the

computers you want to deploy BitLocker on do not have TPM chips, you can use the Control Panel Setup: Enable Advanced Startup Options policy, which is shown in Figure 1-7. When this policy is enabled and configured, you can implement

BitLocker without a TPM being present. You can also configure this policy to require that a startup code be entered if a TPM chip is present, providing another layer of security.
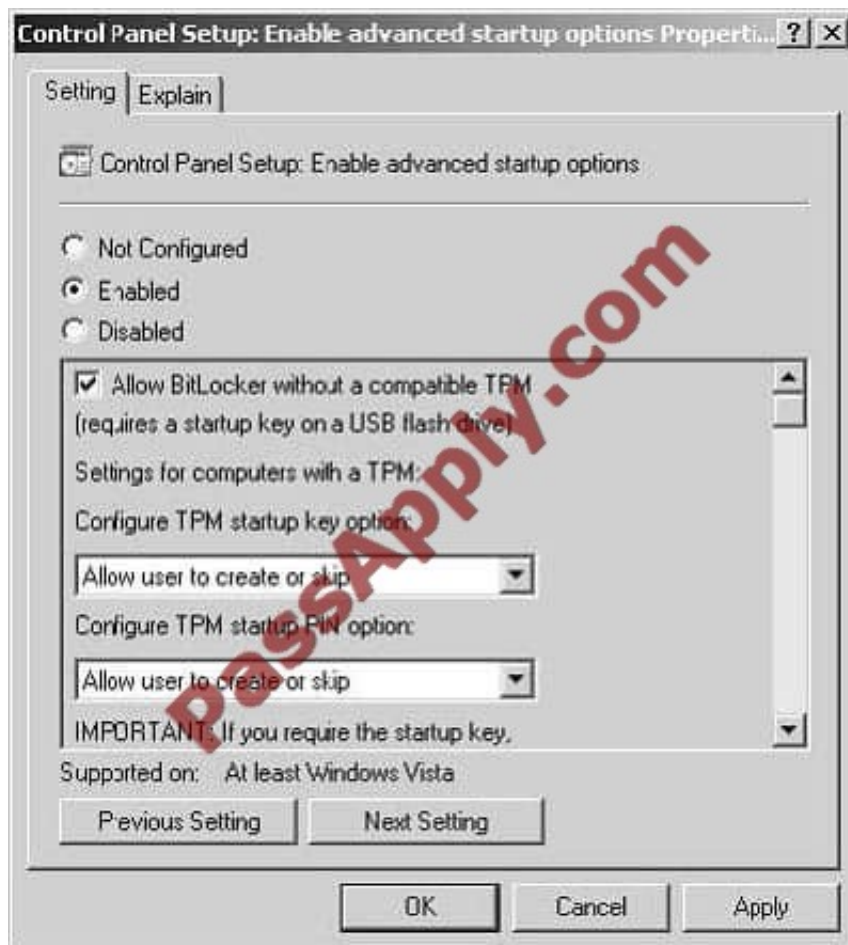


Figure 1-7Allowing BitLocker without the TPM chip Other BitLocker policies include:

Turn On BitLocker Backup To Active Directory Domain Services When this policy is enabled, a computer\\'s recovery key is stored in Active Directory and can be recovered by an authorized administrator.

Control Panel Setup: Configure Recovery Folder When enabled, this policy sets the default folder to which computer recovery keys can be stored.

**QUESTION 4**

You need to recommend changes to Web1 to ensure that server backups can be performed remotely from Backup1.

Which two changes should you include in the recommendation? (Each correct answer presents part of the solution. Choose two.)

A. Install Windows PowerShell.

B. Install Windows Server Backup.

C. Modify the Windows Firewall settings.

D. Enable the IIS Management Service feature.

Correct Answer: BC

**QUESTION 5**

You need to recommend a domain controller deployment strategy for Branch2 that meets the museum\\\'s technical requirements. What should you recommend for Branch2?

A. Deploy two writable domain controllers in ad.baldwinmuseumofscience. Configure both domain controllers as global catalog servers.

B. Deploy two read only domain controllers (RODCs) in ad.baldwin museum of science. Configure both RODCs as global catalog servers.

C. Deploy one writable domain controller in baldwinmuseumofscience.com and one writable domain controller in ad.baldwinmuseumofscience. Enable universal group membership caching.

D. Deploy one read only domain controller (RODC) in baldwinmuseumofscience.com and one writable domain controller in ad.baldwinmuseumofscience. Enable universal group membership caching.

Correct Answer: A

http://technet.microsoft.com/en-us/library/dd735489%28WS.10%29.aspx

Read-only domain controllers (RODCs) do not introduce any significant new considerations for determining whether to make a branch domain controller a global catalog server. Global catalog placement generally requires planning unless you have a single-domain forest. In a single-domain forest, you can configure all domain controllers as global catalog servers without causing any additional replication or an increase in disk size or CPU usage.

However, only domain controllers that are designated as global catalog servers can respond to global catalog queries on the global catalog Lightweight Directory Access Protocol (LDAP) port 3268. Designating all domain controllers as global catalog servers eliminates server or network capacity planning concerns about which domain controllers can respond to global catalog queries by applications or other domain controllers.

In a multiple-domain forest, deciding whether a domain controller should be a global catalog server takes extra planning. As a general rule, it is best to make branch-office domain controllers (including branch-office RODCs) be global catalog servers so that authentication--and, generally, any global catalog query--can be performed by using just the RODC. This comes, however, at the price of replicating the partial attribute set for objects from every domain in the forest to the branch office, which may be expensive in terms of network and disk usage if some domains have large amounts of users, computers, or groups with a high rate of updates.

If you determine that you cannot make the branch-office domain controller a global catalog server, you should enable universal group caching in that site. With universal group membership enabled, a domain controller must connect to a

global catalog server across a wide area network (WAN) link only for initial logons in the site.

Thereafter, universal group membership can be checked from a local cache.

**QUESTION 6**

You need to recommend a solution for managing the GPOs that supports the company\\'s planned changes. What should you include in the recommendation?

A. Group Policy Management Console (GPMC) and Authorization Manager

B. Group Policy Management Console (GPMC) and Microsoft SharePoint Foundation 2010

C. Microsoft Desktop Optimization Pack (MDOP)

D. Microsoft System Center Configuration Manager

Correct Answer: C

http://technet.microsoft.com/en-us/library/ee532079.aspx

Imagine a tool that could help you take control of Group Policy. What would this tool do? It could help you delegate who can review, edit, approve, and deploy Group Policy objects (GPOs). It might help prevent widespread failures that can result from editing GPOs in production environments. You could use it to track each version of each GPO, just as developers use version control to track source code. Any tool that provided these capabilities, cost little, and was easy to deploy would certainly be worth a closer look.

Such a tool indeed exists, and it is an integral part of the Microsoft?Desktop Optimization Pack (MDOP) for Software Assurance. MDOP can help organizations reduce the cost of deploying applications, deliver applications as services, and better manage desktop configurations.

Together, the MDOP applications shown in Figure 1 can give Software Assurance customers a highly cost-effective and flexible solution for managing desktop computers.

**QUESTION 7**

You need to recommend changes to the name resolution infrastructure that meet the company\\'s technical requirements.

What should you recommend?

A. Create a stub zone on all of the DNS servers in the branch offices.

B. Create a secondary zone on all of the DNS servers in the branch offices.

C. Move the DNS zone of the root domain to the ForestDnsZones Application directory partition.

D. Move the DNS zone of each branch office to the ForestDnsZones Application directory partition.

Correct Answer: C

To reduce replication traffic and the amount of data stored in the global catalog, you can use application directory partitions for Active Directory?ntegrated DNS zones. http://technet.microsoft.com/en-us/library/cc772101.aspx

All domain controllers in a specified application directory partition

Replicates zone data according to the replication scope of the specified application directory partition. For a zone to be stored in the specified application directory partition, the DNS server hosting the zone must be enlisted in the specified application directory partition. Use this scope when you want zone data to be replicated to domain controllers in multiple domains but you do not want the data to replicate to the entire forest.

**QUESTION 8**

Your network consists of a single Active Directory domain. Users access and share documents by using a DFS namespace. You need to recommend a solution to manage user access to documents. The solution must meet the following requirements:

-

Allow for document versioning

-

Allow for online collaboration What should you recommend?

A.

File Server Resource Manager (FSRM)

B.

Volume Shadow Copy Service (VSS)

C.

Microsoft SharePoint Foundation 2010

D.

Windows System Resource Manager (WSRM)

Correct Answer: C

sharepoint allows collaboration and versioning
http://www.plusconsulting.com/WhitePapers/SharePoint%202010%20Business%20Value%20Whit ePaper.pdf

**QUESTION 9**

You need to recommend a strategy for delegating administration to the consulting firm. What should you recommend?

A. Create local user accounts.

B. Create domain user accounts.

C. Create IIS Manager user accounts.

D. Implement Active Directory Lightweight Directory Services (AD LDS).

Correct Answer: C

http://technet.microsoft.com/en-us/library/cc732621%28WS.10%29.aspx

Add an IIS Manager user account in IIS Manager when you want to allow a user to connect to a site or an application on your server, but you do not want to create a Windows user account or add the user to a Windows group. IIS Manager

user credentials consist of a user name and password that are created in IIS Manager and are used exclusively for IIS Manager to access the IIS configuration files.

After you create an IIS Manager user account, you can allow the user to connect to sites and applications. The user can then configure delegated features in those sites and applications.

**QUESTION 10**

You need to apply a critical security update to all computers on the New Haven campus while ensuring that New Haven computers continue to receive scheduled updates from BODATA03. You must not apply the security update to any other computers.

What should you recommend?

A. Configure the New Haven campus client computers to synchronize hourly from Microsoft Update.

B. Change NEDATA01 to Autonomous mode, and deploy the security update from NEDATA01.

C. Change NEDATA01 to Autonomous mode, and deploy the security update from BODATA03.

D. Configure only NEDATA01 as an upstream server, and deploy the security update from NEDATA01.

Correct Answer: C

There are two ways to link WSUS servers together:

Autonomous mode: An upstream WSUS server shares updates with its downstream server or servers during synchronization, but not update approval status or computer group information. Downstream WSUS servers must be administered separately. Autonomous servers can also synchronize updates for a set of languages that is a subset of the set synchronized by their upstream server.

Replica mode: An upstream WSUS server shares updates, approval status, and computer groups with its downstream server or servers. Downstream replica servers inherit update approvals and cannot be administered apart from their upstream WSUS server.

**QUESTION 11**

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 12**

Your network contains two DHCP servers. The DHCP servers are named DHCP1 and DHCP2.

The internal network contains 1,000 DHCP client computers that are located on a single subnet. A router separates the internal network from the Internet. The router has a single IP address on the internal interface.

DHCP1 has the following scope information:

-Starting IP address: 172.16.0.1

-Ending IP address: 172.16.7.255

-

Subnet mask: 255.255.240.0

You need to provide a fault tolerant DHCP infrastructure that supports the client computers on the internal network. In the event that a DHCP server fails, all client computers must be able to obtain a valid IP address.

How should you configure DHCP2?

A.

Create a scope for the subnet 172.16.0.0/20. Configure the scope to use a starting IP address of 172.16.8.1 and an ending IP address of 172.16.15.254.

B.

Create a scope for the subnet 172.16.0.0/21. Configure the scope to use a starting IP address of 172.16.0.1 and an ending IP address of 172.16.15.254.

C.

Create a scope for the subnet 172.16.8.0/21. Configure the scope to use a starting IP address of 172.16.8.1 and an ending IP address of 172.16.10.254.

D.

Create a scope for the subnet 172.17.0.0/16. Configure the scope to use a starting IP address of 172.17.0.1 and an ending IP address of 172.17.255.254.

Correct Answer: A

Create a scope for the subnet 172.16.0.0/20.

Configure the scope to use a starting IP address of 172.16.8.1 and an ending IP address of 172.16.15.254.

Subnet 255.255.240.0 is a /20 subnet in CIDR notation, this allows for 4096 client IPs, ranging from 172.16.0.1 all the way to 172.16.15.254 as DHCP1 only used half of the available IPs then you should configure DHCP2 to use the other half.

http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing as an aside you could consider the 80/20 design rule for balancing scope distribution of addresses where multiple DHCP servers are deployed to service the same scope.

Using more than one DHCP server on the same subnet provides increased fault tolerance for servicing DHCP clients located on it. With two DHCP servers, if one server is unavailable, the other server can take its place and continue to lease

new addresses or renew existing clients.

A common practice when balancing a single network and scope range of addresses between two DHCP servers is to have 80 percent of the addresses distributed by one DHCP server and the remaining 20 percent provided by a second.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.passapply.com/allproducts

## Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

**One Year Free Update**
Free update is available within One
Year after your purchase. After One
Year, you will get 50% discounts for
updating. And we are proud to
boast a 24/7 efficient Customer
Support system via Email.

**Money Back Guarantee**
To ensure that you are spending on
quality products, we provide 100%
money back guarantee for 30 days
from the date of purchase.

**Security & Privacy**
We respect customer privacy. We
use McAfee's security service to
provide you with utmost security for
your personal information & peace
of mind.