# 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.pass4lead.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 need to recommend a solution for the research documents that meets the museum\\'s technical requirements.

What should you recommend?

A. On all client computers, enable shadow copies and configure the Previous Versions client settings.

B. On Server1, enable shadow copies. On all client computers, configure the Previous Versions client settings.

C. Deploy Microsoft SharePoint Foundation 2010, and then migrate Share1 to a new document library. Modify the blocked file types.

D. Deploy Microsoft SharePoint Foundation 2010, and then migrate Share1 to a new document library. Enable versioning for the library.

Correct Answer: B

Possible answers are B and D, the consensus is B as it doesn\\'t require the investment in other technology and one of your requirements is to minimize costs

Sharepoint versioning Versioning is the method by which successive iterations of a document are numbered and saved.

The default versioning control for a document library depends on the site collection template.

However, you can configure versioning control for a document library depending on your particular requirements. Each document library can have a different versioning control that best suits the kind of documents in the library. SharePoint

Foundation 2010 has three versioning options:

No versioning Specifies that no previous versions of documents are saved. When versioning is not being used, previous versions of documents are not retrievable, and document history is also not retained because comments that accompany

each iteration of a document are not saved. Use this option on document libraries that contain unimportant content or content that will never change.

Create major versions Specifies that numbered versions of documents are be retained by using a simple versioning scheme (such as 1, 2, 3). To control the effect on storage space, you can specify how many previous versions to keep,

counting back from the current version.

In major versioning, every time a new version of a document is saved, all users who have permissions to the document library will be able to view the content. Use this option when you do not want to differentiate between draft versions of

documents and published versions. For example, in a document library that is used by a workgroup in an organization, major versioning is a good choice if everyone on the team must be able to view all iterations of each document. Create

major and minor (draft) versions Specifies that numbered versions of documents are retained by using a major and minor versioning scheme (such as 1.0, 1.1, 1.2, 2.0, 2.1). Versions ending in .0 are major versions and versions ending with

non-zero extensions are minor versions.

Previous major and minor versions of documents are saved together with current versions. To control the effect on storage space, you can specify how many previous major versions to keep, counting back from the current version. You can

also specify how many major versions being kept should include their respective minor versions. For example, if you specify that minor versions should be kept for two major versions and the current major version is 4.0, then all minor

versions starting at 3.1 will be kept.

In major and minor versioning, any user who has read permissions can view major versions of documents. You can specify which users can also view minor versions. Typically, we recommend that you grant permissions to view and work with

minor versions to the users who can edit items, and restrict users who have read permissions to viewing only major versions.

Use major and minor versioning when you want to differentiate between published content that can be viewed by an audience and draft content that is not yet ready for publication. For example, on a human resources Web site that describes

organizational benefits, use major and minor versioning to restrict employees\\' access to benefits descriptions while the descriptions are being revised.

Configuring Volume Shadow Copy on Windows Server 2008

http://www.techotopia.com/index.php/Configuring_Volume_Shadow_Copy_on_Windows_Server_Once shadow copy has been configured for volumes on the server, the next step is to learn how to access the previous version of files from

client systems. This is achieved using a feature of Windows Server 2008 and Windows Vista called Previous Versions.

To access previous versions of a file on a client, navigate to the shared folder (or subfolder of a shared folder) or network drive using Start -> Network. Once the desired network drive or shared folder is visible, right click on it and select

Restore Previous Versions (or just Previous Versions on Windows Vista). Once selected, the Properties dialog box will appear with the Previous Versions tab pre-selected as illustrated in the following figure:

There are a number of issues that need to be considered when implementing shadow copy for shared folders. First and foremost the shared folders which are to be shadowed need to be identified. Secondly, a location for the shadow to be stored must be allocated. This can reside either on the same volume as the shared folders, or on a completely different volume or disk drive. Even before any data is shadowed, the shadow copy system requires 300MB of available space. The total amount of space required will depend on the size of the shared folder which is to be shadowed and the frequency and extent to which the files are likely to change (since shadow copy will only take new snapshots of files which have changed since the last snapshot). Finally, the time and frequency of the volume snapshots

needs to be defined. By default, Shadow Copy performs a snapshot twice a day at 7:00am and 12:00pm.

Once the Shadow Copy system has been configured the shadow copy client needs to be set up on the systems of any users that are likely to need to be able to restore files in shared folders.

Using Computer Management to Enable and Configure Volume Shadow Copies Shadow Copy is enabled on a per volume basis. Once configured on a volume, all shared folders residing on that volume will automatically be shadowed.

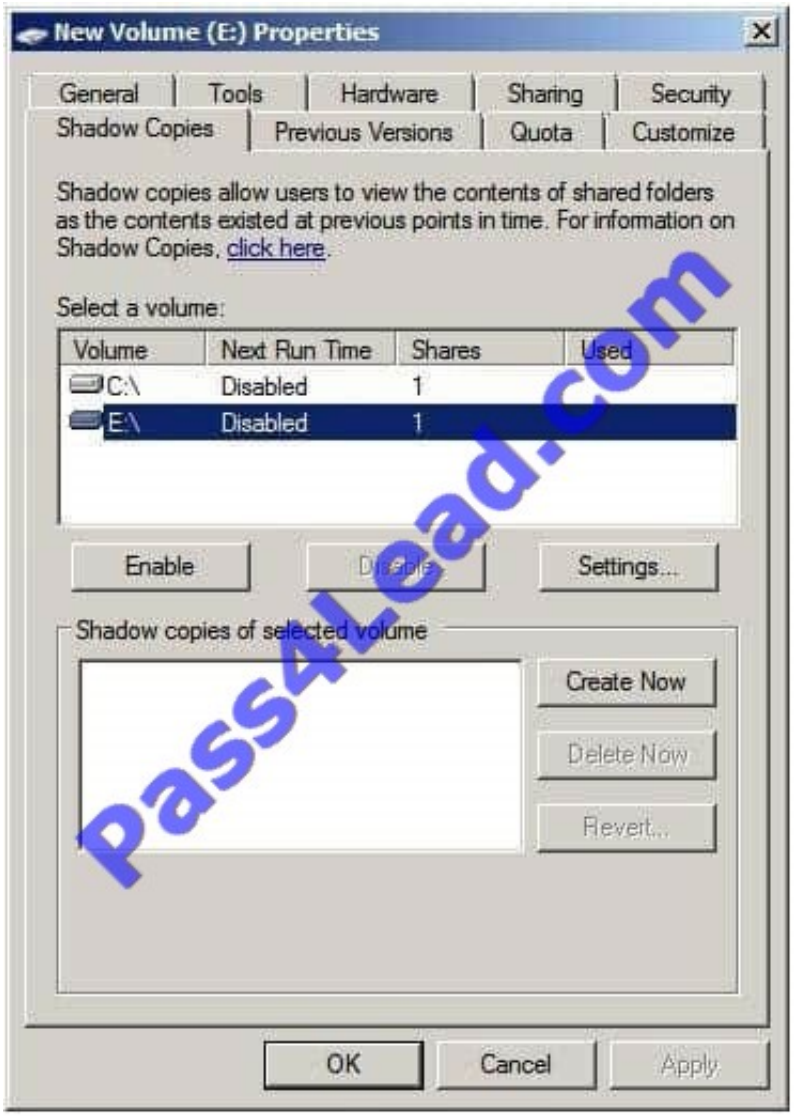
Shadow Copy can be configured either graphically using the Computer Management tool or via the command prompt. Command-line configuration of Shadow Copy will be covered in a later section of this chapter. This section will focus on

Computer Management configuration.

The first step is to launch the Computer Management configuration tool (Start -> All Programs ->Administrative Tools -> Computer Management). Once invoked, select Storage -> Disk

Management from the tree in the left panel to display the disk and volume information for the local system. In the graphical view, right click on a volume and select on Properties to launch the properties dialog. In the properties dialog, select

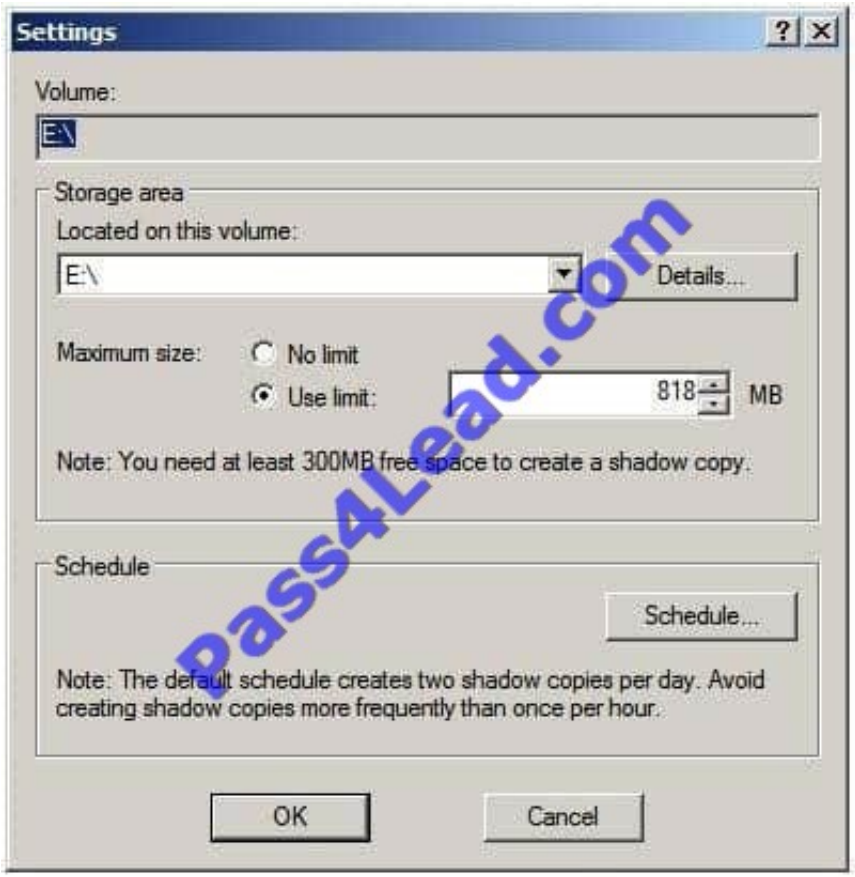
the Shadow Copy tab to display the Shadow Copy properties as illustrated in the following figure:




T

The Select a volume section of the properties dialog lists the volumes present on the local system.

Select the volume in this list for which Shadow Copy is to be enabled. With the volume selected click on the Settings button to display the following Shadow Copy Settings dialog box:






n the Located on this volume specify the volume on which the shadow copies are to be stored. This can be either the current volume or a different volume on the system. The Details button displays free and total disk space information for the currently specified volume. Once a suitable volume for the shadow copies has been selected the maximum size to be made available for the shadow copies may be defined. This can either be set to Maximum size which will use all available space on the specified volume, or capped to a specific size (keeping in mind that a minimum of 300MB is required for the shadow storage volume even before any snapshots are taken). Shadow Copy uses a differential approach to backing up files in that only files that have changed since the last snapshot are copied. For certain files, Shadow Copy also only copies the part of the file that has changed, rather than the entire file. As such, it is not necessary to reserve 64 times the size of the volume to be copied since only parts of the volume will be copied with each snapshot.

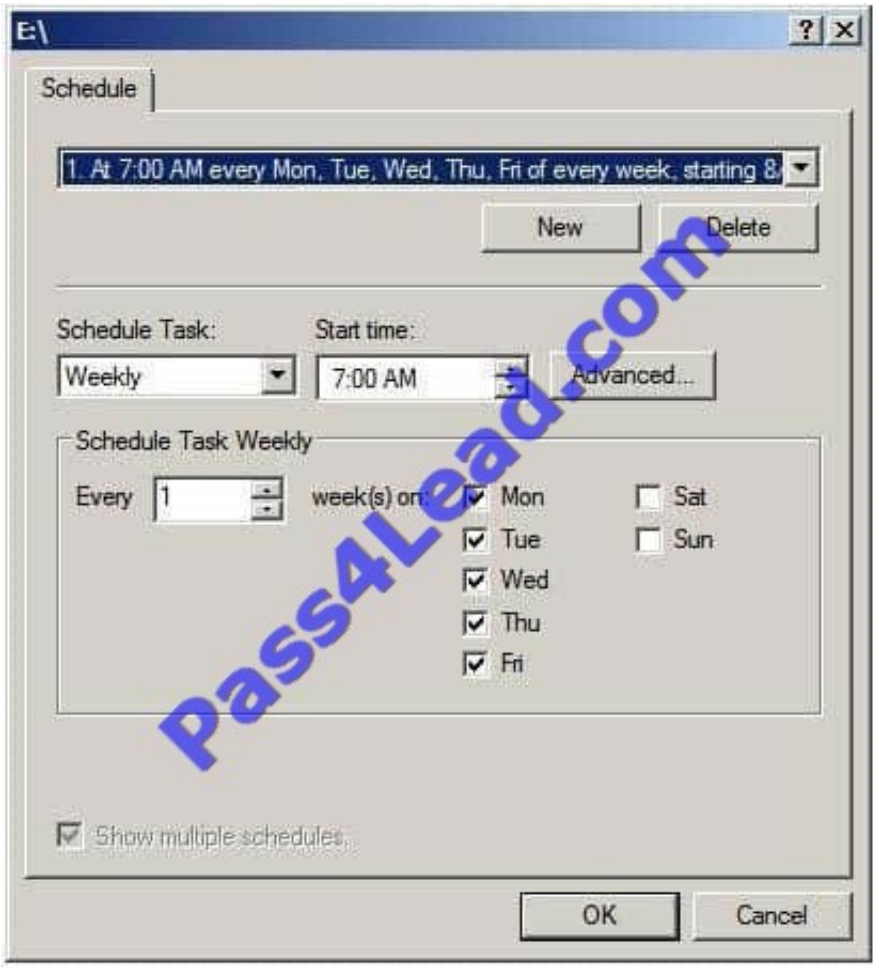
Schedule the shadow copy snapshots by clicking on the Schedule... button. By default, Windows configures two snapshots each day (at 7:00am and 12:00pm respectively). To remove a currently defined snapshot, select it from the drop down list and click on Delete. To modify a run, select it from the drop down list, modify the settings in the lower section of the dialog and click on OK.

To specify additional schedules, click on the New button and specify the days and time of the snapshot. Note that snapshots can also be configured to occur at user logon, system startup and even when the system is idle.

In fact, Windows Server 2008 provides considerable flexibility in terms of scheduling shadow copies. It is important to keep in mind, however, that there are disadvantages to running a shadow copy too frequently.

Firstly, shadow copies are resource intensive tasks, especially on large volumes where many files are subject to frequent changes. Repeated snapshots during periods when the server is heavily utilized may well degrade overall system performance. Secondly, it is important to keep in mind that Shadow Copy retains the last 64 versions of a file. Therefore, if a snapshot is run every hour, the oldest restore point available to a user will be approximately two and half days in the past. If, on the other hand, snapshots are taken twice a day, the user will have the luxury of restoring a file from a point as much as 32 days ago. It is important, therefore, to strike a balance between longevity and frequency.

The following screenshot illustrates the Shadow Copy scheduling dialog:

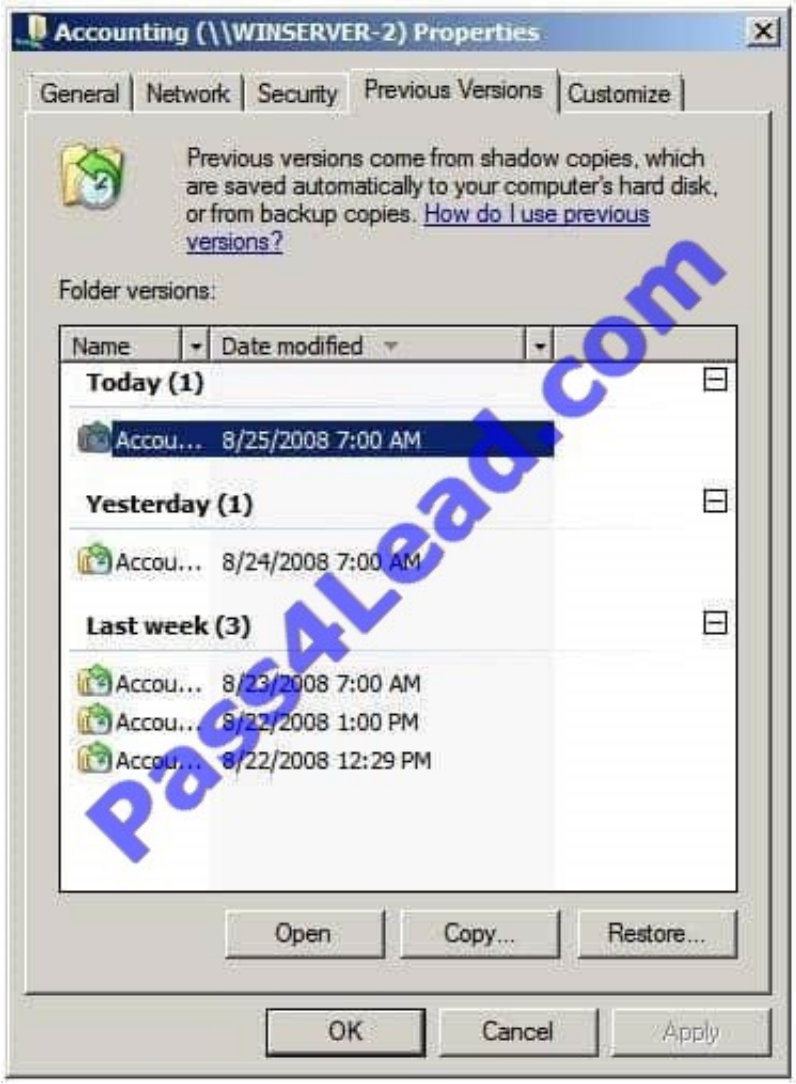



Once the schedules have been configured, click on OK to dismiss the scheduling dialog. Click OK once again in the Settings dialog to return to the Shadow Copy properties panel. At this point, the volume for which a schedule has been defined will have a small clock image superimposed over the volume icon and will indicate that 0 bytes of shadow copy storage have been used. The next step is to enable shadow copies on the volume by selecting the volume from the list and clicking on the Enable button. The volume in the list will update to display the date and time of the next scheduled copy and provide a summary of the current level of storage space used for the shadow copies.

To initiate a manual shadow copy now, or at any other time, simply select the volume to be copied from the list in the Shadow Copy properties panel and click on the Create Now button.

Restoring Shadow Copy Snapshots from Clients Once shadow copy has been configured for volumes on the server, the next step is to learn how to access the previous version of files from client systems. This is achieved using a feature of Windows Server 2008 and Windows Vista called Previous Versions.

To access previous versions of a file on a client, navigate to the shared folder (or subfolder of a shared folder) or network drive using Start -> Network. Once the desired network drive or shared folder is visible, right click on it and select Restore Previous Versions (or just Previous Versions on Windows Vista). Once selected, the Properties dialog box will appear with the Previous Versions tab pre-selected as illustrated in the following figure:




As shown in the previous figure, the Previous Versions property page lists the previous versions of the shared folder that are available for restoration. A number of options are available for each shadow copy snapshot listed in the properties dialog. Open will open the folder in Windows Explorer so that individual files and sub-folders can be viewed and copied. The Copy... button allows the snapshot of the folder and its contents to be copied to a different location. Finally, Restore... restores the folder and files to its state at the time of the currently selected shadow copy snapshot. As outlined in the warning dialog, this action cannot be undone once performed.

Topic 5, Woodgrove Bank Scenario: COMPANY OVERVIEW Overview Woodgrove Bank is an international financial organization. Physical Location The company has a main office and multiple branch offices. EXISTING ENVIRONMENT Active Directory Environment The network contains one Active Directory forest. A separate domain exists for each office. Network Infrastructure All offices have domain controllers that are configured as DNS servers. All client computers are configured to connect to the DNS servers in their respective office only. The main office has the following servers and client computers:

-One Windows Server Update Services (WSUS) server.

-Client computers that run either Windows XP Service Pack 3 (SP3) or Windows 7.

-

Ten file servers that host multiple shared folders. The file servers run either Windows Server 2003 or Windows Server 2008 R2.

-

One domain-based Distributed File System (DFS) namespace that has two replicas. The DFS servers run Windows Server 2008 R2. The DFS namespace is configured to use Windows 2000 Server mode.

Each branch office has a WAN link to the main office. The WAN links are highly saturated. Each office has a dedicated high-speed Internet connection.

All of the client computers in the branch offices run Windows 7.

User Problems

Users report that it is difficult to find the shared folders on the network.

REQUIREMENTS

Planned Changes

Woodgrove Bank plans to implement the following changes:

-

Deploy a new Application named App1 on each client computer. App1 has a Windows Installer package and is compatible with Windows XP, Windows Vista, and Windows 7.

-Designate a user in each office to manage the address information of the user accounts in that office.

-Deploy a new branch office named Branch22 that has the following servers:

Technical Requirements

Woodgrove Bank must meet the following technical requirements:

-Minimize hardware and software costs, whenever possible.

-Encrypt all DNS replication traffic between the DNS servers.

-

Ensure that users in the branch offices can access the DFS targets if a WAN link fails.

-

Ensure that users can only view the list of DFS targets to which they are assigned permissions.

-

Minimize the amount of network traffic between the main office and the branch offices, whenever possible.

-

Minimize the amount of name resolution traffic from the branch offices to the DNS servers in the main office.

-Ensure that the administrators in the main office manage all Windows update approvals and all computer groups.

-Manage all of the share permissions and the folder permissions for the file servers from a single management console.

-

Ensure that if a file on a file server is deleted accidentally, users can revert to a previous version of the file without administrator intervention.

-

Ensure that administrators are notified by e-mail each time a user successfully copies a file that has an .avi extension to one of the file servers.

Security Requirements

Woodgrove Bank must meet the following security requirements:

-Access rights and user rights must be minimized.

-The Guest account mustoe disabled on all servers.

-Internet Information Services (IIS) must only be installed on authorized servers.

**QUESTION 2**

A company\\'s file servers are running out of disk space. The company uses folder redirection policies to redirect user profile folders to 50 dedicated file servers.

The files stored on the file servers include the following types of files that should not be stored in user profile folders:

Audio and video files

Files created by a computer-aided drafting (CAD) Application

You decide to implement File Server Resource Manager (FSRM) on the dedicated file servers. You have the following requirements:

Prevent users from saving audio and video files to their user profile folders.

Prevent users from saving CAD files to their user profile folders.

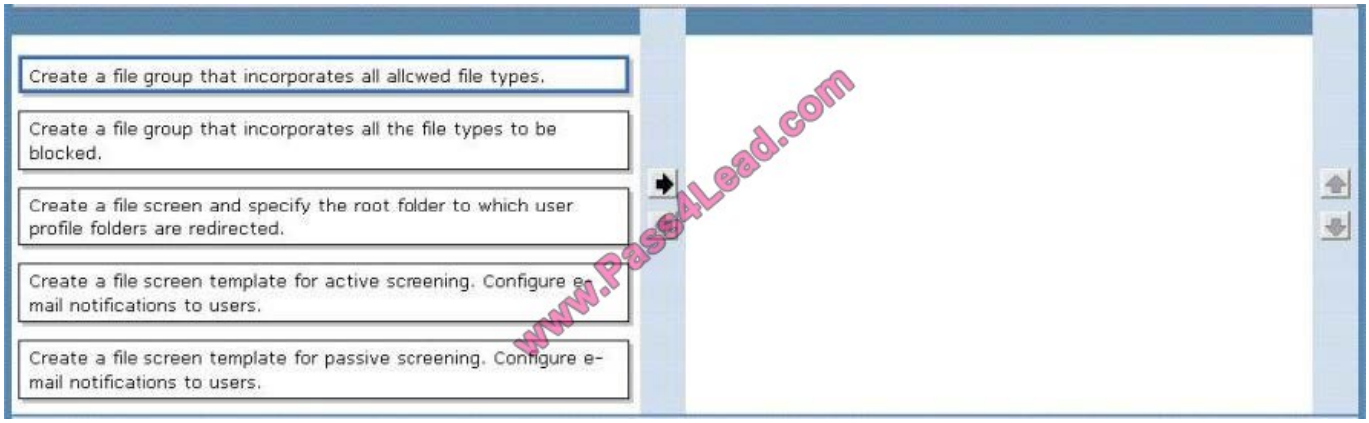
Notify users by e-mail if they attempt to save files of a blocked file type.

You need to configure FSRM with the least amount of administrative effort.

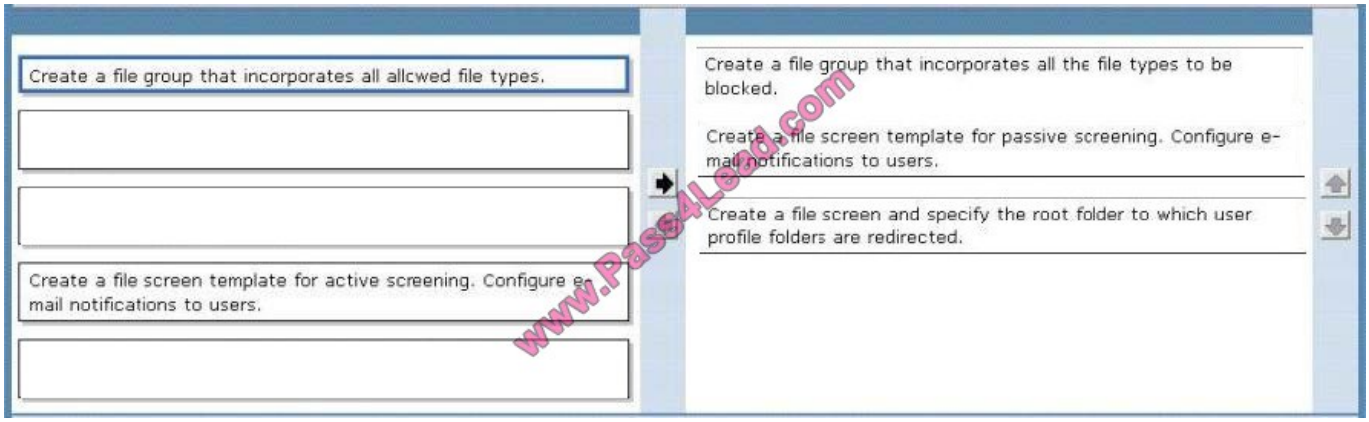
Which actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. (Use only actions that Apply.)

Select and Place:




Correct Answer:




FSRM File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. By using File Server Resource Manager, administrators can place quotas on folders and volumes, actively screen files, and generate comprehensive storage reports.

This set of advanced instruments not only helps the administrator to efficiently monitor existing storage resources but it also aids in the planning and implementation of future policy changes.

Also http://blogs.technet.com/b/josebda/archive/2008/08/20/the-basics-of-windows-server-2008-fsrmfile-serverresource-manager.aspx

**QUESTION 3**

A company has Remote Desktop Services (RDS) servers that run Windows Server 2008 R2 and client computers that run Windows 7.

You are designing a non-production remote desktop infrastructure that you will use for evaluation purposes for 180 days. The remote desktop infrastructure must meet the following requirements:

-Maximize the security of remote desktop connections.

-Minimize changes to the company\\'s firewall configuration.

-Provide external users with a secure connection from the Windows 7 Remote Desktop client to the RDS environment.

You need to design a temporary remote desktop infrastructure that meets the requirements.

Which services should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Remote Desktop Gateway, Remote Desktop Licensing, and Remote Desktop Session Host

B. Remote Desktop Licensing, Remote Desktop Session Host, and Remote Desktop Web Access

C. Only Remote Desktop Gateway and Remote Desktop Session Host

D. Only Remote Desktop Session Host and Remote Desktop Web Access

Correct Answer: C

Its true that the evaluation period for RD is only 120 days and your requirements are 180 days.

Maybe the question is inaccurate and it actually states 120 days?

But if you read http://technet.microsoft.com/en-us/library/cc738962%28WS.10%29.aspx it says To allow ample time for you to deploy a Terminal Server license server, Terminal Server provides a licensing grace period, during which no

license server is required. During this grace period, a terminal server can accept connections from unlicensed clients without contacting a license server. The grace period begins the first time the terminal server accepts a client connection. It

ends after you deploy a license server and that license server issues its first permanent client access license (CAL), or after 120 days, whichever comes first. In order for a license server to issue permanent CALs, you must activate the license

server and then purchase and install the appropriate number of permanent CALs. If a license server is not activated, it issues temporary licenses. These temporary licenses allow clients to connect to the terminal server for 90 days.

So is that the solution?

If you feel licensing is required then A is your answer, if you don\\'t then C is your answer.

Remote Desktop Gateway (RD Gateway), formerly Terminal Services Gateway (TS Gateway), is a role service in the Remote Desktop Services server role included with Windows Server?2008 R2 that enables authorized remote users to

connect to resources on an internal corporate or private network, from any Internetconnected 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 and virtual desktops 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 internal network resources

Why use Remote Desktop Gateway?

RD Gateway provides many benefits, including:

RD Gateway enables remote users to connect to internal network resources over the Internet, by using an encrypted connection, without needing to configure virtual private network (VPN) connections.

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.

RD Gateway enables most remote users to connect to internal network resources that are hosted behind firewalls in private networks and across network address translators (NATs). With RD Gateway, you do not need to perform additional

configuration for the RD Gateway server or clients for this scenario.

Prior to this release of Windows Server, security measures prevented remote users from connecting to internal network resources across firewalls and NATs. This is because port 3389, the port used for RDP connections, is typically blocked

for network security purposes. RD Gateway transmits RDP traffic to port 443 instead, by using an HTTP Secure Sockets

Layer/Transport Layer Security (SSL/TLS) tunnel. Because most corporations open port 443 to enable Internet connectivity, RD Gateway takes advantage of this network design to provide remote access connectivity across multiple firewalls.

The Remote Desktop Gateway Manager enables you to configure authorization policies to define conditions that must be met for remote users to connect to internal network resources. For example, you can specify:

Who can connect to internal network resources (in other words, the user groups who can connect).

What network resources (computer groups) users can connect to.

Whether client computers must be members of Active Directory security groups.

Whether device redirection is allowed.

Whether clients need to use smart card authentication or password authentication, or whether they can use either method.

You can configure RD Gateway servers and Remote Desktop Services clients to use Network Access Protection (NAP) to further enhance security. NAP is a health policy creation,

enforcement, and remediation technology that is included in Windows Server?2008 R2, Windows Server?2008, Windows?7, Windows Vista? and Windows?XP Service Pack 3. With NAP, system administrators can enforce health

requirements, which can include software requirements, security update requirements, required computer configurations, and other settings.

A Remote Desktop Session Host (RD Session Host) server is the server that hosts Windows-based programs or the full Windows desktop for Remote Desktop Services clients. Users can connect to an RD Session Host server to run

programs, to save files, and to use network resources on that server. Users can access an RD Session Host server by using Remote Desktop Connection or by using RemoteApp.

Remote Desktop Licensing

http://technet.microsoft.com/en-us/library/hh553157%28v=ws.10%29

Operating System Grace Period

Windows Server 2008 R2 120 days

Windows Server 2008 120 days

Windows Server 2003 R2 / Windows Server 2003 120 days

Windows 2000 Server 90 days

There has been some debate about licensing and some suggest you needed a license server.

however take a look here: http://support.microsoft.com/kb/948472

Evaluating Windows Server 2008 software does not require product activation. Any edition of Windows Server 2008 may be installed without activation, and it may be evaluated for 60 days.

Additionally, the 60-day evaluation period may be reset (re-armed) three times. This action extends the original 60-day evaluation period by up to 180 days for a total possible evaluation time of 240 days.

**QUESTION 4**

You need to recommend a Windows Server 2008 R2 server configuration that meets the following requirements:

-Supports the installation of Microsoft SQL Server 2008

-Provides redundancy for SQL services if a single server fails

What should you recommend?

A. Install a Server Core installation of Windows Server 2008 R2 Enterprise on two servers. Configure the servers in a failover cluster.

B. Install a full installation of Windows Server 2008 R2 Standard on two servers. Configure Network Load Balancing on the two servers.

C. Install a full installation of Windows Server 2008 R2 Enterprise on two servers. Configure Network Load Balancing on the two servers.

D. Install a full installation of Windows Server 2008 R2 Enterprise on two servers. Configure the servers in a failover cluster.

Correct Answer: D

Fail Over Clustering, which is available on the Enterprise edition (not on standard) will provide fail over as required.

Windows Server 2008 Enterprise Edition Windows Server 2008 Enterprise Edition is the version of the operating system targeted at large businesses. Plan to deploy this version of Windows 2008 on servers that will run applications such as SQL Server 2008 Enterprise Edition and Exchange Server 2007. These products require the extra processing power and RAM that Enterprise Edition supports. When planning deployments, consider Windows Server 2008 Enterprise Edition in situations that require the following technologies unavailable in Windows Server 2008 Standard Edition:

Failover Clustering I-ail over clustering is a technology that allows another server to continue to service client requests in the event that the original server fails. Clustering is covered in more detail in Chapter 11. "Clustering and High Availability." You deploy failover clustering on mission-critical servers to ensure that important resources are available even if a server hosting those resources fails.

**QUESTION 5**

You need to recommend a NAP enforcement method that meets the company\\'s security requirements. Which method should you recommend?

A. 802.1X

B. DHCP

C. IPSec

D. VPN

Correct Answer: A

Offices are both wired and wireless

Network Access Protection

You deploy Network Access Protection on your network as a method of ensuring that computers accessing important resources meet certain client health benchmarks. These benchmarks include (but are not limited to) having the most recent

updates applied, having antivirus and anti-spyware software up to date, and having important security technologies such as Windows Firewall configured and functional. In this lesson, you will learn how to plan and deploy an appropriate

network access protection infrastructure and enforcement method for your organization.

802.1X NAP Enforcement

802.1X enforcement makes use of authenticating Ethernet switches or IEEE 802.11 Wireless Access Points.

These compliant switches and access points only grant unlimited network access to computers that meet the compliance requirement. Computers that do not meet the compliance requirement are limited in their communication by a restricted

access profile. Restricted access profiles work by applying IP packet filters or VLAN (Virtual Local Area Network) identifiers. This means that hosts that have the restricted access profile are allowed only limited network communication. This

limited network communication generally allows access to remediation servers. You will learn more about remediation servers later in this lesson.

An advantage of 802.1X enforcement is that the health status of clients is constantly assessed.

Connected clients that become noncompliant will automatically be placed under the restricted access profile. Clients under the restricted access profile that become compliant will have that profile removed and will be able to communicate with

other hosts on the network in an unrestricted manner. For example, suppose that a new antivirus update comes out. Clients that have not installed the update are put under a restricted access profile until the new update is installed.

Once the new update is installed, the clients are returned to full network access.

A Windows Server 2008 computer with the Network Policy Server role is necessary to support 802.1X NAP enforcement. It is also necessary to have switch and/or wireless access point hardware that is 801.1xcompliant.

Client computers must be running Windows Vista, Windows Server 2008, or Windows XP Service Pack 3 because these operating systems include the EAPHost EC.

MORE INFO 802.1X enforcement step-by-step For more detailed information on implementing 802.1X NAP enforcement, consult the following Step-by-Step guide on TechNet: http://go.microsoft.com/fwlink/?LinkId=86036.

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.pass4lead.com/allproducts

## Need Help

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