



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.pass4itsure.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 consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2.

All client computers run Windows 7. All user accounts are stored in an organizational unit (OU) named Staff. All client computer accounts are stored in an OU named Clients. You plan to deploy a new Application.

You need to ensure that the Application deployment meets the following requirements:

- Users must access the Application from an icon on the Start menu.

-

The Application must be available to remote users when they are offline. What should you do?

A.

Publish the Application to users in the Staff OU.

B.

Publish the Application to users in the Clients OU.

C.

Assign the Application to computers in the Staff OU.

D.

Assign the Application to computers in the Clients OU.

Correct Answer: D

<http://www.youtube.com/watch?v=hQkRN96cKkM>

Group policy objects can be applied either to users or to computers. Deploying applications through the Active Directory is also done through the use of group policies, and therefore applications are deployed either on a per user basis or on a per computer basis. There are two different ways that you can deploy an application through the Active Directory. You can either publish the application or you can assign the application. You can only publish applications to users, but you can assign applications

to either users or to computers. The application is deployed in a different manner depending on which of these methods you use.

Publishing an application doesn't actually install the application, but rather makes it available to users. For example, suppose that you were to publish Microsoft Office. Publishing is a group policy setting, so it would not take effect until the

next time that the user logs in. When the user does log in though, they will not initially notice anything different. However, if the user were to open the Control Panel and click on the Add / Remove Programs option, they will find that Microsoft Office is now on the list. A user can then choose to install Microsoft office on their machine. One thing to keep in mind is that regardless of which deployment method you use, Windows does not perform any sort of software metering. Therefore, it will be up to you to make sure that you have enough licenses for the software that you

are installing.



Assigning an application to a user works differently than publishing an application. Again, assigning an application is a group policy action, so the assignment won't take effect until the next time that the user logs in.

When the user does log in, they will see that the new application has been added to the Start menu and / or to the desktop.

Although a menu option or an icon for the application exists, the software hasn't actually been installed though.

To avoid overwhelming the server containing the installation package, the software is not actually installed until the user attempts to use it for the first time.

This is also where the self healing feature comes in. When ever a user attempts to use the application, Windows always does a quick check to make sure that the application hasn't been damaged. If files or registry settings are missing, they

are automatically replaced.

Assigning an application to a computer works similarly to assigning an application to a user. The main difference is that the assignment is linked to the computer rather than to the user, so it takes effect the next time that the computer is

rebooted. Assigning an application to a computer also differs from user assignments in that the deployment process actually installs the application rather than just the application's icon. as assigning installs the application the next time a

computer reboots the app will be available when at next login regardless of which user logs in. also as its being assigned to a computer the GPO needs to be linked to the Clients OU as this is where the computer accounts are located.

Assigning Software to a group.

<http://support.microsoft.com/kb/324750>

Create a folder to hold the Windows Installer package on a server. Share the folder by applying permissions that let users and computers read and run these files. Then, copy the MSI package files into this location.

From a Windows Server 2003-based computer in the domain, log on as a domain administrator, and then start Active Directory Users and Computers.

In Active Directory Users and Computers, right-click the container to which you want to link the GPOs, and then click Properties.

Click the Group Policy tab, and then click New to create a new GPO for installing the Windows Installer package. Give the new GPO a descriptive name.

Click the new GPO, and then click Edit.

The Group Policy Object Editor starts.

Right-click the Software Settings folder under either Computer Configuration or User Configuration, point to New, and then click Package.

QUESTION 2

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



An Active Directory site exists for each office. All domain controllers run Windows Server 2008 R2.

You plan to modify the DNS infrastructure. You need to plan the new DNS infrastructure to meet the following requirements:

- Ensure that the DNS service is available even if a single server fails
- Encrypt the synchronization data that is sent between DNS servers
- Support dynamic updates to all DNS servers

What should you include in your plan?

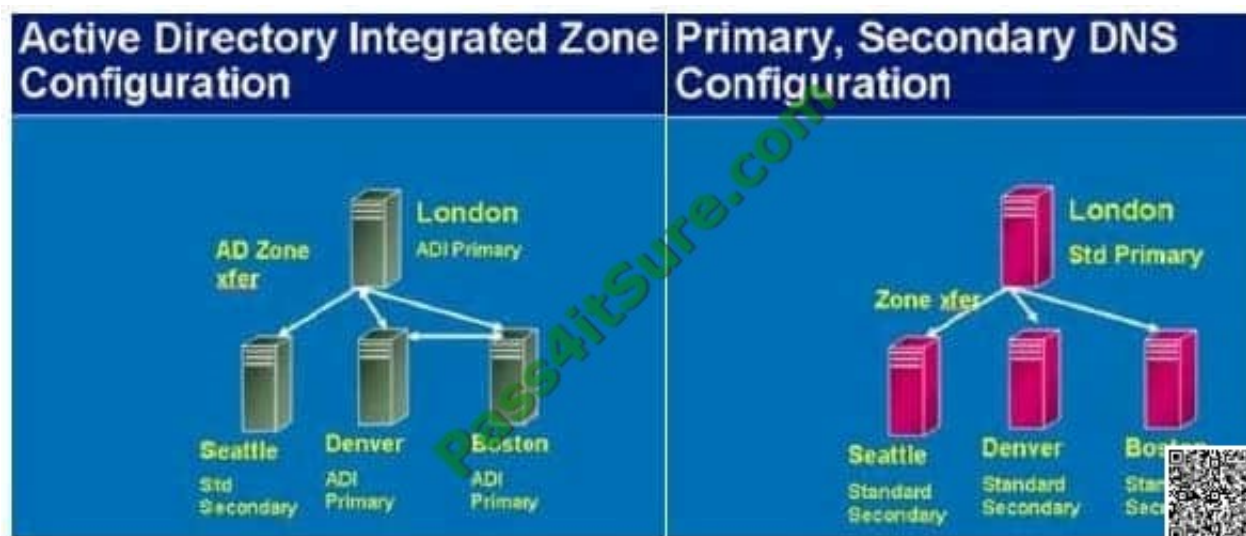
- A. Install the DNS Server server role on two servers. Create a primary zone on the DNS server in the main office. Create a secondary zone on the DNS server in the branch office.
- B. Install the DNS Server server role on a domain controller in the main office and on a domain controller in the branch office. Configure DNS to use Active Directory integrated zones.
- C. Install the DNS Server server role on a domain controller in the main office and on a Readonly Domain Controller (RODC) in the branch office. Configure DNS to use Active Directory integrated zones.
- D. Install the DNS Server server role on two servers. Create a primary zone and a GlobalNames zone on the DNS server in the main office. Create a GlobalNames zone on the DNS server in the branch office.

Correct Answer: B

<http://searchwindowsserver.techtarget.com/tip/DNS-Primer-Tips-for-understanding-Active-Directory-integratedzone-design-and-configuration> <http://technet.microsoft.com/en-us/library/cc772101.aspx>

In an ADI primary zone, rather than keeping the old zone file on a disk, the DNS records are stored in the AD, and Active Directory replication is used rather than the old problematic zone transfer. If all DNS servers were to die or become inaccessible, you could simply install DNS on any domain controller (DC) in the domain. The records would be automatically populated and your DNS server would be up without the messy import/export tasks of standard DNS zone files.

Windows 2000 and 2003 allow you to put a standard secondary zone (read only) on a member server and use one of the ADI primary servers as the master.





When you decide which replication scope to choose, consider that the broader the replication scope, the greater the network traffic caused by replication. For example, if you decide to have AD DS-integrated DNS zone data replicated to all DNS servers in the forest, this will produce greater network traffic than replicating the DNS zone data to all DNS servers in a single AD DS domain in that forest.

AD DS-integrated DNS zone data that is stored in an application directory partition is not replicated to the global catalog for the forest. The domain controller that contains the global catalog can also host application directory partitions, but it will not replicate this data to its global catalog.

AD DS-integrated DNS zone data that is stored in a domain partition is replicated to all domain controllers in its AD DS domain, and a portion of this data is stored in the global catalog. This setting is used to support Windows 2000. If an application directory partition's replication scope replicates across AD DS sites, replication will occur with the same intersite replication schedule as is used for domain partition data.

By default, the Net Logon service registers domain controller locator (Locator) DNS resource records for the application directory partitions that are hosted on a domain controller in the same manner as it registers domain controller locator (Locator) DNS resource records for the domain partition that is hosted on a domain controller.

Close integration with other Windows services, including AD DS, WINS (if enabled), and DHCP (including DHCPv6) ensures that Windows 2008 DNS is dynamic and requires little or no manual configuration. Windows 2008 DNS is fully compliant with the dynamic update protocol defined in RFC 2136. Computers running the DNS Client service register their host names and IPv4 and IPv6 addresses (although not link-local IPv6 addresses) dynamically. You can configure the DNS Server and DNS Client services to perform secure dynamic updates. This ensures that only authenticated users with the appropriate rights can update resource records on the DNS server.

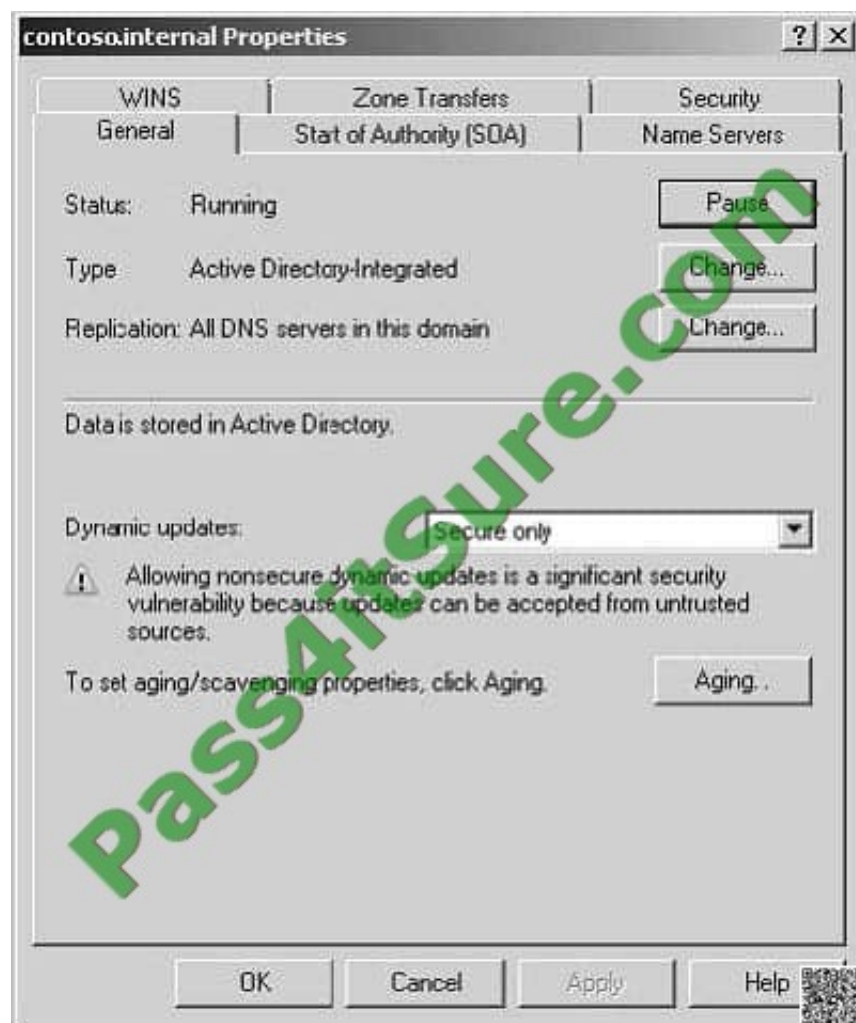




Figure 2-22 shows a zone being configured to allow only secure dynamic updates.

Figure 2-22 Allowing only secure dynamic updates MORE INFO Dynamic update protocol For more information about the dynamic update protocol, see <http://www.ietf.org/rfc/rfc2136.txt> and <http://www.ietf.org/rfc/rfc3007> NOTE Secure dynamic updates Secure dynamic updates are only available for zones that are integrated with AD DS.

QUESTION 3

Your network consists of a single Active Directory domain. The network contains 20 file servers that run Windows Server 2008 R2. Each file server contains two volumes. One volume contains the operating system.

The other volume contains all data files.

You need to plan a recovery strategy that meets the following requirements:

-

Allows the operating system to be restored

-

Allows the data files to be restored

-Ensures business continuity

-Minimizes the amount of time to restore the server

What should you include in your plan?

A. Windows Deployment Services (WDS)

B. Windows Automated Installation Kit (Windows AIK) and folder redirection

C. the Multipath I/O feature and Volume Shadow Copies

D. the Windows Server Backup feature and System Image Recovery

Correct Answer: D

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

Windows Server Backup Windows Server Backup provides a reliable method of backing up and recovering the operating system, certain applications, and files and folders stored on your server.

This feature replaces the previous backup feature that was available with earlier versions of Windows.

Windows Server Backup

The Windows Server Backup tool is significantly different from ntbackup.exe, the tool included in Windows Server 2000 and Windows Server 2003. Administrators familiar with the previous tool should study the capabilities and limitations of

the new Windows Server Backup utility because many aspects of the tool's functionality have changed.

Exam Tip: What the tool does



The Windows Server 2008 exams are likely to focus on the differences between NTBACKUP and Windows Server Backup.

The key points to remember about backup in Windows Server 2008 are:

Windows Server Backup cannot write to tape drives.

You cannot write to network locations or optical media during a scheduled backup.

The smallest object that you can back up using Windows Server Backup is a volume.

Only local NTFS-formatted volumes can be backed up.

Windows Server Backup files write their output as VHD (Virtual Hard Disk) files. VHD files can be mounted with the appropriate software and read, either directly or through virtual machine software such as Hyper-V.

MORE INFO Recovering NTbackup backups

You cannot recover backups written using ntbackup.exe. A special read-only version of ntbackup.exe that is compatible with Windows Server 2008 can be downloaded from

<http://go.microsoft.com/fwlink/?LinkId=82917>.

Windows Server Backup is not installed by default on Windows Server 2008 and must be installed as a feature using the Add Features item under the Features node of the Server Manager console.

When installed, the Windows Server Backup node becomes available under the Storage node of the Server Manager Console. You can also open the Windows Server Backup console from the Administrative Tools menu. The wbadmin.exe

command-line utility, also installed during this process, is covered in "The wbadmin Command-Line Tool" later in this lesson. To use Windows Server Backup or wbadmin to schedule backups, the computer requires an extra internal or

external disk. External disks will need to be either USB 2.0 or IEEE 1394 compatible. When planning the deployment of disks to host scheduled backup data, you should ensure that the volume is capable of holding at least 2.5 times the

amount of data that you want to back up. When planning deployment of disks for scheduled backup, you should monitor how well this size works and what sort of data retention it allows in a trial before deciding on a disk size for wider

deployment throughout your organization.

When you configure your first scheduled backup, the disk that will host backup data will be hidden from Windows Explorer. If the disk currently hosts volumes and data, these will be removed to store scheduled backup data. Note that this only

applies to scheduled backups and not to manual backups. You can use a network location or external disk for a manual backup without worrying that data already stored on the device will be lost. The format and repartition only happens when

a device is first used to host scheduled backup data.

It does not happen when subsequent backup data is written to the same location.

It is also important to remember that a volume can only store a maximum of 512 backups. If you need to store a greater number of backups, you will need to write these backups to a different volume. Of course given the amount of data on

most servers, you are unlikely to find a disk that has the capacity to store so many backups.



So that scheduled backups can always be executed, Windows Server Backup will automatically remove the oldest backup data on a volume that is the target of scheduled backups. You do not need to manually clean up or remove old backup

data.

Performing a Scheduled Backup

Scheduled backups allow you to automate the backup process. After you set the schedule, Windows Server Backup takes care of everything else. By default, scheduled backups are set to occur at 9:00 P.M. If your organization still has

people regularly working on documents at that time, you should reset this. When planning a backup schedule you should ensure that the backup occurs at a time when the most recent day\\'s changes to data are always captured.

Only

members of the local Administrators group can configure and manage scheduled backups.

To configure a scheduled backup, perform the following steps:

1.

Open Windows Server Backup. Click Backup Schedule in the Actions pane of Windows Server Backup. This will start the Backup Schedule Wizard. Click Next.

2.

The next page of the wizard asks whether you want to perform a full server backup or a custom backup.

Select Custom and click Next. As you can see in Figure 12-3, volumes that contain operating system components are always included in custom backups. Volume E is excluded in this case, because this is the location where backup data will be written.

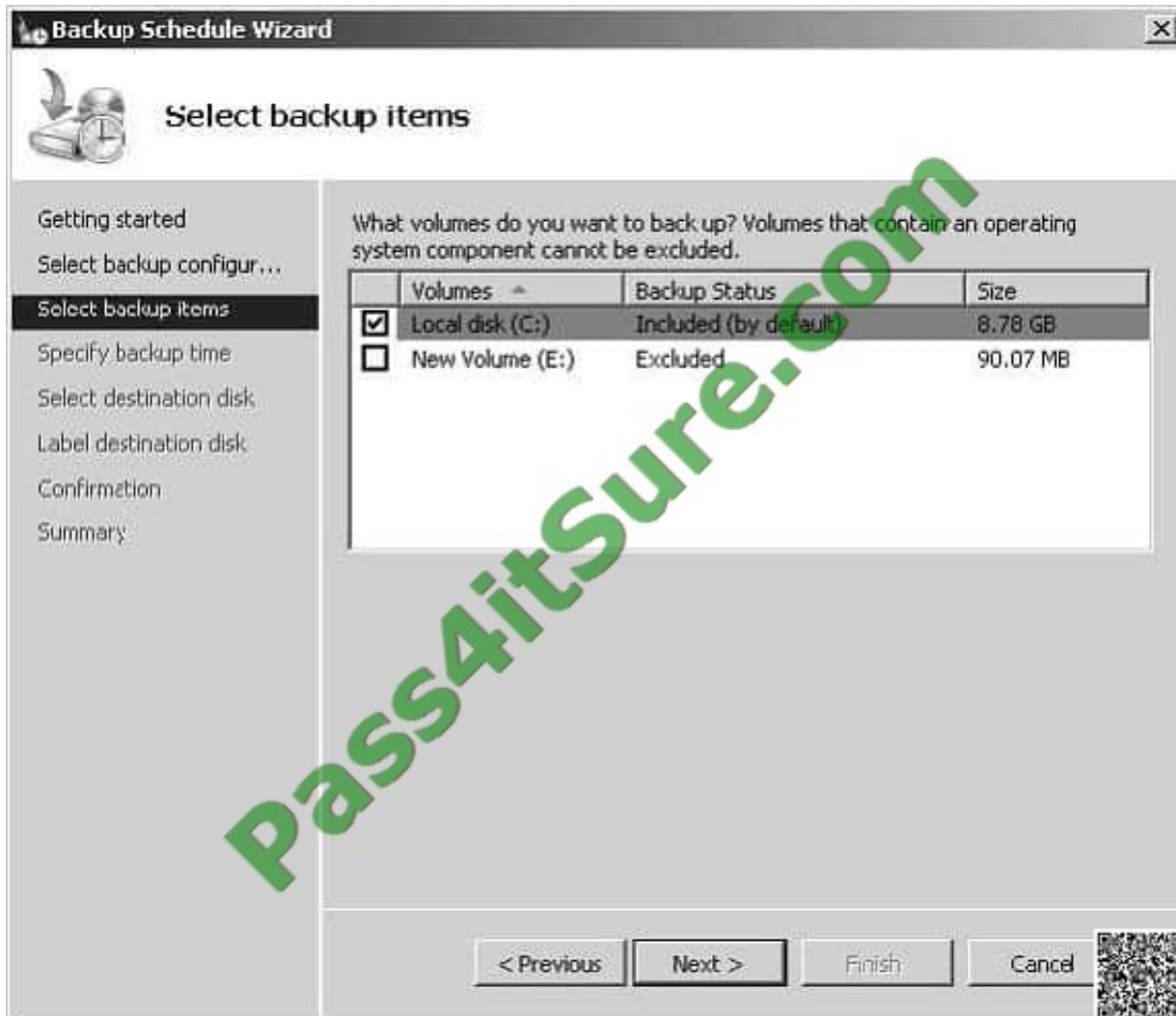


Figure 12-3 Selecting backup items

3. The default backup schedule is once a day at 9:00 P.M. You can configure multiple backups to be taken during the day. You are most likely to do this in the event that data on the server that you are backing up changes rapidly. On servers

where data changes a lot less often, such as on a Web server where pages are only updated once a week, you would configure a more infrequent schedule.

4. On the Select Destination Disk page, shown in Figure 12-4, you select the disk that backups are written to. If multiple disks are selected, multiple copies of the backup data are written. You should note that the entire disk will be used. All existing volumes and data will be removed and the backup utility will format and hide the disks prior to writing the first backup data.

5. On the Label Destination Disk page, note the label given to the disk you have selected to store backups. When you finish the wizard, the target destination is formatted and then the first backup will occur at the scheduled time.

An important limitation of Windows Server Backup is that you can only schedule one backup job.

In other words, you cannot use Windows Server Backup to schedule jobs that you might be used to scheduling in earlier versions of Windows, such as a full backup on Monday night with a series of incremental backups every other day of the



week. You can configure Windows Server Backup to perform incremental backups, but this process is different from what you might be used to with other backup applications.

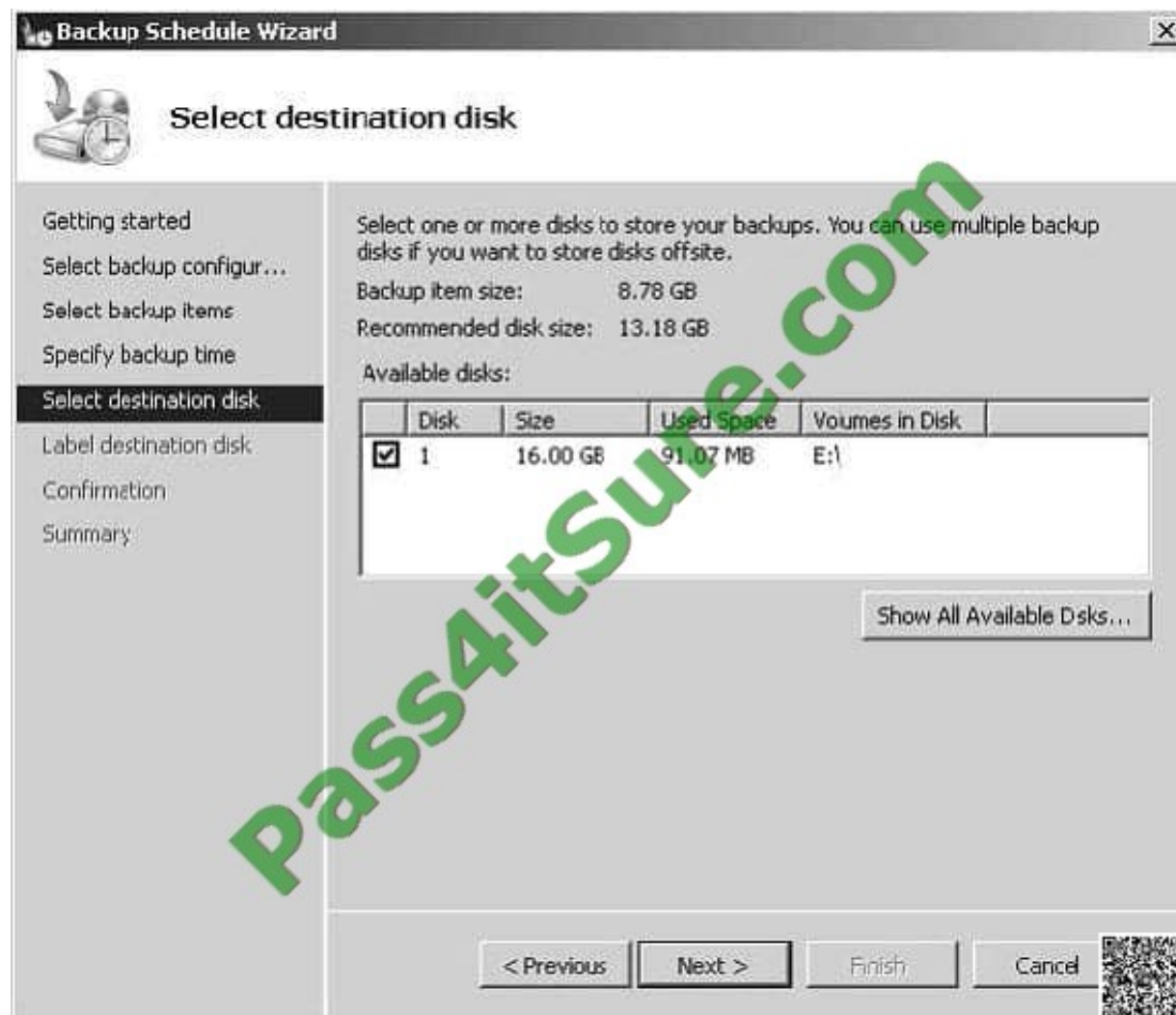


Figure 12-4 Selecting a destination disk

Performing an Unscheduled Single Backup

Unscheduled single backups, also known as manual backups, can be written to network locations, local and external volumes, and local DVD media. If a backup encompasses more than the space available on a single DVD media, you can

span the backup across multiple DVDs. Otherwise, if the calculated size of a backup exceeds the amount of free space available on the destination location, the backup will fail. You will perform a manual backup in a practice exercise at the end of this lesson.

When performing a manual backup, you must choose between using one of the following two types of Volume

Shadow Copy Service backup:

VSS Copy Backup Use this backup option when another backup product is also used to back up applications on volumes in the current backup. Application log files are retained when you perform this type of manual backup. This is the default



when taking a backup.

VSS Full Backup Use this backup option when no other backup products are used to back up the host computer. This option will update each file's backup attribute and clears application log files.

When performing a single backup, you can also back up a single volume without having to back up the system or boot volumes. This is done by clearing the Enable System Recovery option when selecting backup items.

You might use this option to back up a specific volume's data when you are going to perform maintenance on the volume or suspect that the disk hosting the volume might fail, but do not want to wait for a full server backup to complete.

Full Server and Operating System Recovery

Also known as Bare Metal Recovery, full server recovery allows you to completely restore the server by booting from the Windows Server 2008 installation media or Windows Recovery

Environment. See the note on building a recovery solution for more information on how to set up a local Windows Recovery Environment on a Windows Server 2008 computer. Full server recovery goes further than the Automated System

Recovery (ASR) feature that was available in Windows Server 2003 because full server recovery will restore all operating system, application, and other data stored on the server. ASR did not provide such a complete recovery and it was

necessary to further restore data from backup after the ASR process was complete.

An operating system recovery is similar to a full server recovery except that you only recover critical volumes and do not recover volumes that do not contain critical data. For example, if you have a file server where the disks that host critical

operating system volumes are separate from the disks that host shared folder volumes and the disks that host the critical operating system volumes fail, you should perform an operating system recovery.

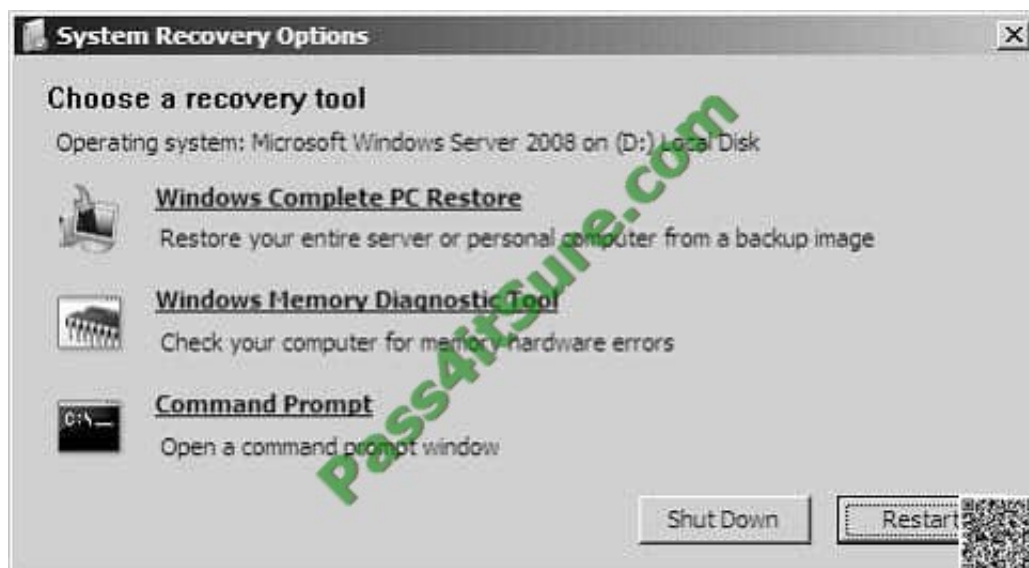


Figure 12-13 Select Windows Complete PC Restore

QUESTION 4



You need to recommend changes to the network that address the user problems statement. What should you recommend?

- A. Deploy DirectAccess.
- B. Configure folder redirection.
- C. Create a volume mount point.
- D. Implement additional DFS targets.

Correct Answer: D

Direct Access is a remote access solution and does not address the problem. Folder redirection does not address the problem Volume mount point would not solve this problem either

The Distributed File System is used to build a hierarchical view of multiple file servers and shares on the network. Instead of having to think of a specific machine name for each set of files, the user will only have to remember one name; which will be the '\\key\\' to a list of shares found on multiple servers on the network. Think of it as the home of all file shares with links that point to one or more servers that actually host those shares.

DFS has the capability of routing a client to the closest available file server by using Active Directory site metrics

Dfs target (or replica): This can be referred to as either a root or a link. If you have two identical shares, normally stored on different servers, you can group them together as Dfs Targets under the same link.



QUESTION 5

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. There are five Windows Server 2003 SP2 servers that have the Terminal Server component installed. A firewall server runs Microsoft Internet Security and Acceleration (ISA) Server 2006.

You plan to give remote users access to the Remote Desktop Services servers.

You need to create a remote access strategy for the Remote Desktop Services servers that meets the following requirements:

- Restricts access to specific Remote Desktop Services servers
- Encrypts all connections to the Remote Desktop Services servers
- Minimizes the number of open ports on the firewall server

What should you do?



- A. Implement SSL bridging on the ISA Server. Require authentication on all inbound connections to the ISA Server.
- B. Implement port forwarding on the ISA Server. Require authentication on all inbound connections to the ISA Server.
- C. Upgrade a Windows Server 2003 SP2 server to Windows Server 2008 R2. On the Windows Server 2008 R2 server, implement the Remote Desktop Gateway (RD Gateway) role service, and configure a Remote Desktop resource authorization policy (RD RAP).
- D. Upgrade a Windows Server 2003 SP2 server to Windows Server 2008 R2. On the Windows Server 2008 R2 server, implement the Remote Desktop Gateway (RD Gateway) role service, and configure a Remote Desktop connection authorization policy (RD CAP).

Correct Answer: C

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

Terminal Services Gateway TS Gateway allows Internet clients secure, encrypted access to Terminal Servers behind your organization's firewall without having to deploy a Virtual Private Network (VPN) solution. This means that you can have users interacting with their corporate desktop or applications from the comfort of their homes without the problems that occur when VPNs are configured to run over multiple Network Address Translation (NAT) gateways and the firewalls of multiple vendors.

TS Gateway works using RDP over Secure Hypertext Transfer Protocol (HTTPS), which is the same protocol used by Microsoft Office Outlook 2007 to access corporate Exchange Server 2007 Client Access Servers over the Internet. TS Gateway Servers can be configured with connection authorization policies and resource authorization policies as a way of differentiating access to Terminal Servers and network resources.

Connection authorization policies allow access based on a set of conditions specified by the administrator; resource authorization policies grant access to specific Terminal Server resources based on user account properties.

Resource Authorization Policies Terminal Services resource authorization policies (TS-RAPs) are used to determine the specific resources on an organization's network that an incoming TS Gateway client can connect to. When you create a TS-RAP you specify a group of computers that you want to grant access to and the group of users that you will allow this access to. For example, you could create a group of computers called AccountsComputers that will be accessible to members of the Accountants user group. To be granted access to internal resources, a remote user must meet the conditions of at least one TS-CAP and at least one TS-RAP.

QUESTION 6

You need to recommend a solution for deploying and managing App2. What should you recommend?

- A. Publish App2 as a RemoteApp program.
- B. Deploy App2 by using a Group Policy logon script.
- C. Assign App2 by using Group Policy software distribution.
- D. Publish App2 by using Group Policy software distribution.

Correct Answer: C

<http://support.microsoft.com/kb/816102>

This step-by-step article describes how to use Group Policy to automatically distribute programs to client computers or users. You can use Group Policy to distribute computer programs by using the following methods:



Assigning Software

You can assign a program distribution to users or computers. If you assign the program to a user, it is installed when the user logs on to the computer. When the user first runs the program, the installation is finalized. If you assign the program

to a computer, it is installed when the computer starts, and it is available to all users who log on to the computer. When a user first runs the program, the installation is finalized.

Publishing Software

You can publish a program distribution to users. When the user logs on to the computer, the published program is displayed in the Add or Remove Programs dialog box, and it can be installed from there.

QUESTION 7

A company has servers that run Windows Server 2008 R2 and a storage area network (SAN) that supports the virtual Disk Service (VDS).

You are designing a storage solution for the servers.

The storage solution must meet the following requirements:

Allow the creation of Fibre Channel (FC) and Internet SCSI (iSCSI) logical unit numbers (LUNs).

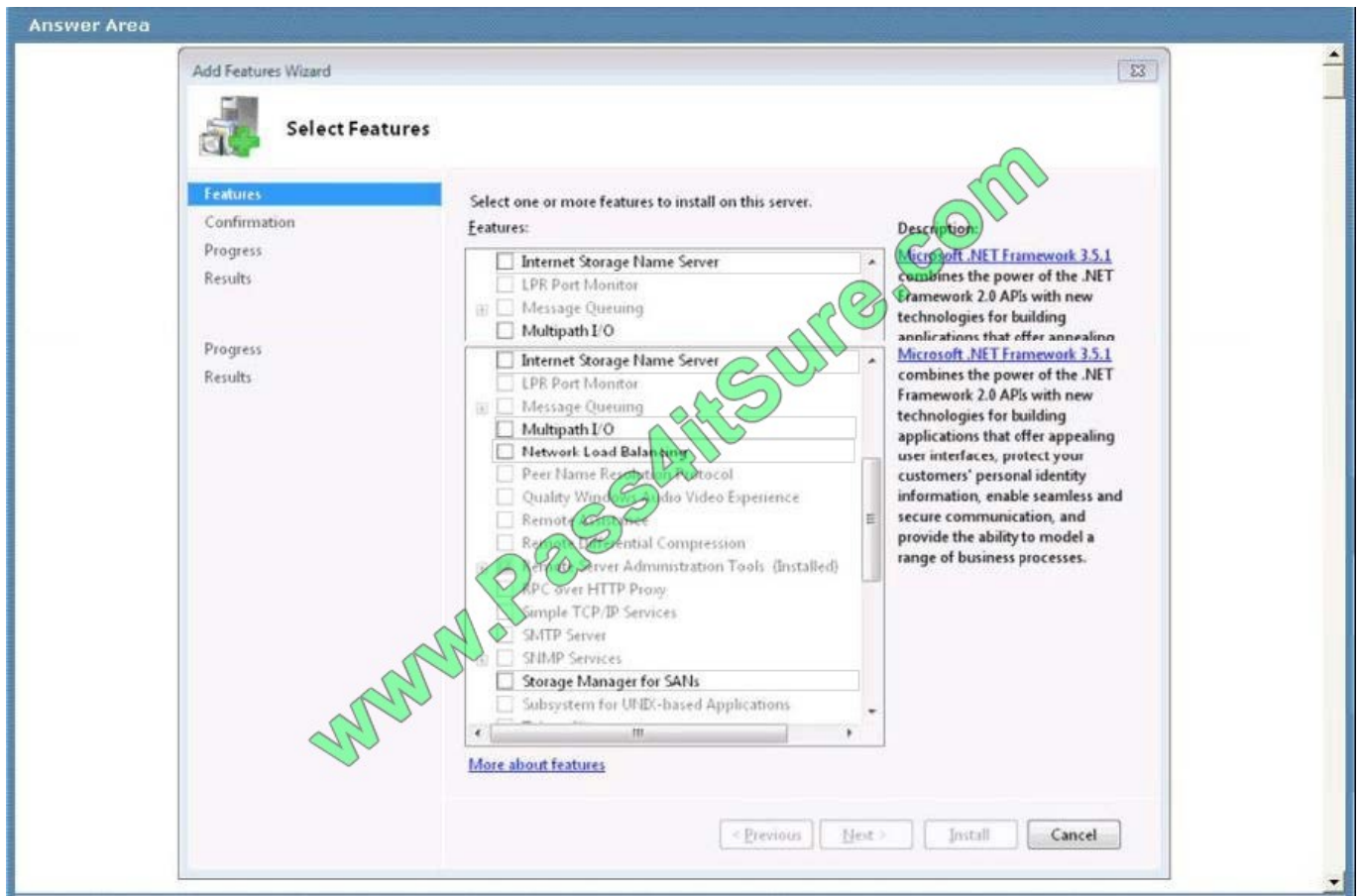
Allow the management of FC and iSCSI LUNs.

You need to ensure that the storage solution meets the requirements.

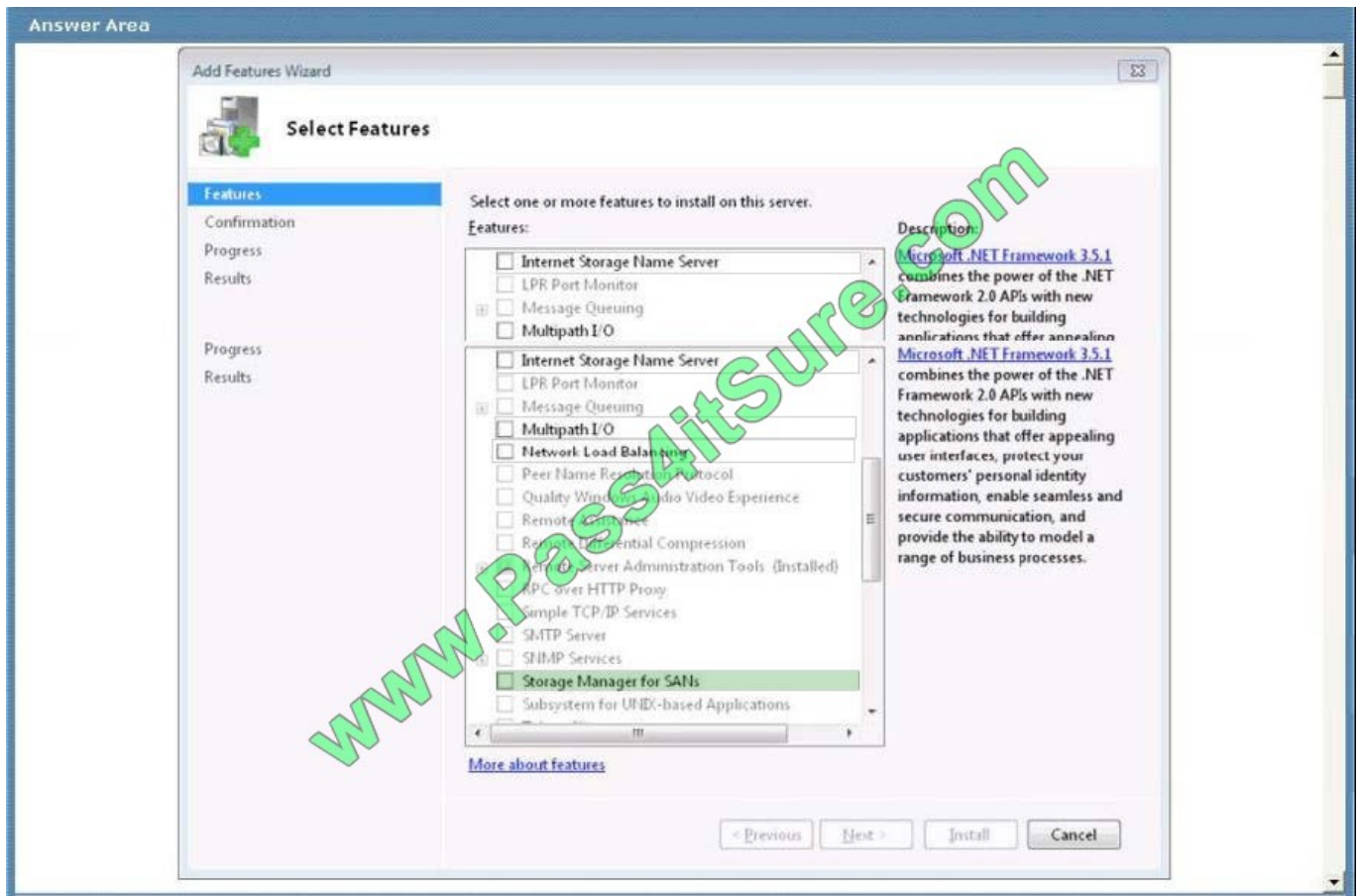
Which feature should you install?

To answer, select the appropriate feature in the answer area.

Hot Area:



Correct Answer:



Storage Manager for SANs helps you create and manage logical unit numbers (LUNs) on Fibre Channel and iSCSI disk drive subsystems that support Virtual Disk Service (VDS) in your storage area network (SAN).

A LUN is a logical reference to a portion of a storage subsystem. A LUN can comprise a disk, a section of a disk, a whole disk array, or a section of a disk array in the subsystem. Using LUNs simplifies the management of storage resources in your SAN because they serve as logical identifiers through which you can assign access and control privileges.

You can use Storage Manager for SANs to create and manage logical unit numbers (LUNs) on both Fibre Channel and iSCSI disk storage subsystems that support Virtual Disk Service (VDS).

Because of hardware, protocol, and security differences, LUN configuration and management on Fibre Channel and iSCSI environments is different. This section explains those differences, lists the types of LUNs that can be created, and

defines LUNs in the context of partitions and volumes.

Managing LUNs in a Fibre Channel environment In a Fibre Channel environment, LUNs created on a disk storage subsystem are assigned directly to a server or cluster, which accesses the LUN through one or more Fibre Channel host bus

adapter (HBA) ports. You only need to identify the server or cluster that will access the LUN, and then select which HBA ports on that server or cluster will be used for LUN traffic.

When a server or cluster is identified, Storage Manager for SANs automatically discovers the available Fibre Channel HBA ports on that server or cluster. You can also add ports manually by typing their World Wide Name (WWN).

Managing LUNs in an iSCSI environment



Unlike in a Fibre Channel environment, LUNs created on an iSCSI disk storage subsystem are not only assigned to a server or cluster. For iSCSI, LUNs are first assigned to logical entities called targets.

Targets are created in order to manage the connections between an iSCSI device and the servers that need to access it. A target defines the portals (IP addresses) that can be used to connect to the iSCSI device, as well as the security

settings (if any) that the iSCSI device requires in order to authenticate the servers that are requesting access to its resources.

To connect to a target, a server in the storage area network (SAN) uses an iSCSI initiator. An iSCSI initiator is a logical entity that enables the server to communicate with the target. The iSCSI initiator first logs on to the target, and only after

access is granted by the target, the server can start reading and writing to LUNs assigned to that target. Each iSCSI initiator can have one or more network adapters through which communication is established.

As with Fibre Channel environments, you only need to identify the server or cluster that will access the LUN, and Storage Manager for SANs automatically discovers the iSCSI initiators on that server or cluster, and lists all the available

adapters for those initiators. After the iSCSI initiator adapters have been discovered, you can select which adapters will be used for LUN traffic. Types of LUNs

Storage Manager for SANs supports the following types of LUNs.

LUN type	Description
Simple	Simple LUNs use only one physical drive or one portion of a physical drive. This is the most basic type of LUN.
Spanned	Spanned LUNs are simple LUNs that span multiple physical drives.
Striped	Striped LUNs write data across multiple physical drives. Data is divided into blocks and spread among all the drives. Since striping writes data across multiple drives, striped LUNs cannot be extended or mirrored, and do not offer fault tolerance. If one of the disks containing a striped LUN fails, the entire LUN is unavailable. Select this type of LUN when improved I/O performance is required.
Mirrored	Mirrored LUNs are fault-tolerant LUNs that provide data redundancy by creating identical copies of the LUN on two physical drives. All read data is available, but if one disk becomes unavailable, the LUN continues to be available using the unaffected disk. Select this type of LUN when fault tolerance is required.
Striped with parity	Striped LUNs with parity are fault-tolerant LUNs with data and parity spread intermittently across three or more physical disks. If a portion of the LUN becomes unavailable, the data can be reconstructed using the parity information. This type of LUN provides better read performance than a mirrored LUN, but write performance is reduced by the parity calculation. Select this type of LUN when fault tolerance is required and improved read performance is desired.

LUNs, partitions and volumes A LUN is a logical reference to a portion of a storage subsystem. A LUN can comprise a disk, a section of a disk, a whole disk array, or a section of a disk array in the subsystem. This logical reference, when it is assigned to a server in your SAN, acts as a physical disk drive that the server can read and write to. Using LUNs simplifies the management of storage resources in your SAN, because they serve as logical identifiers through which you can assign access and control privileges.

After a LUN has been assigned to a server, you can create one or more partitions on that LUN. Partitions define how much physical space is allocated for storage. For the operating system to start writing and reading data on partitions, you need to create volumes by formatting the partitions using a file system. Volumes define how much logical space is allocated for storage. They can expand over more than one partition.

**QUESTION 8**

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 9

You need to recommend a backup strategy for the servers in the San Francisco office. The strategy must meet the company's technical requirements. What should you include in the recommendation?

- A. native-boot virtual hard disks (VHDs)
- B. Microsoft System Center Data Protection Manager 2010
- C. system restore points
- D. Windows Server Backup

Correct Answer: D

You need to recommend a backup strategy for the servers in the San Francisco office. The strategy must meet the company's technical requirement.

Technical Requirement: Ensure that you can perform a bare metal recovery in the San Francisco Office Business Goal: Minimize costs whenever possible So the correct answer is Windows Server Backup because you can deploy Bare Metal

backups Previous answer below ...

<http://technet.microsoft.com/en-us/library/ff399260.aspx>



What is Data Protection Manager?

Microsoft System Center Data Protection Manager (DPM) 2010 is a member of the Microsoft System Center family of management products, designed to help IT professionals manage their Windows environment. DPM provides Windows

backup and recovery--delivering seamless data protection for Microsoft application and file servers by using integrated disk and tape media. DPM performs replication, synchronization, and recovery point creation to provide reliable protection

and rapid recovery of data for both system administrators and end-users.

QUESTION 10

You need to recommend a solution that meets the following requirements:

- Log access to all shared folders on TT-FILE02.
- Minimize administrative effort.
- Ensure that further administrative action is not required when new shared folders are added to TT-FILE02.

What should you recommend?

- A. Upgrade TT-FILE02 to Windows Server 2008 Enterprise and use Application control policies in Group Policy.
- B. Add the Connection Manager Administration Kit feature on TT-FILE02.
- C. Upgrade TT-FILE02 to Windows Server 2008 R2 Standard and use Advanced Audit Policy Configuration settings in Group Policy.
- D. Add the Network Policy and Access Services role to TT-FILE02.

Correct Answer: C

Security auditing enhancements in Windows Server 2008 R2 and Windows 7 can help your organization audit compliance with important business-related and security-related rules by tracking precisely defined activities, such as:

A group administrator has modified settings or data on servers that contain finance information.

An employee within a defined group has accessed an important file.

The correct system access control list (SACL) is applied to every file and folder or registry key on a computer or file share as a verifiable safeguard against undetected access. In Windows 7 and Windows Server 2008 R2, the number of audit settings for which success and failure can be tracked has increased to 53. Previously, there were nine basic auditing settings under Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy. These 53 new settings allow you to select only the behaviors that you want to monitor and exclude audit results for behaviors that are of little or no concern to you, or behaviors that create an excessive number of log entries. In addition, because Windows 7 and Windows Server 2008 R2 security audit policy can be applied by using domain Group Policy, audit policy settings can be modified, tested, and deployed to selected users and groups with relative simplicity.

<http://technet.microsoft.com/en-us/library/dd408940%28v=ws.10%29.aspx>

QUESTION 11



You need to recommend a solution to ensure that all of the client computers that run Windows 7 meet the company's security requirements. What should you include in the recommendation?

- A. Encrypted File System (EFS)
- B. the AppLocker Group Policy settings
- C. the IPSec enforcement method
- D. Windows BitLocker Drive Encryption (BitLocker)

Correct Answer: D

BitLocker Drive Encryption is a full disk encryption feature. It is designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm in CBC mode with a 128 bit key, combined with the Elephant diffuser for additional disk encryption-specific security not provided by AES.

The latest version of BitLocker, included in Windows 7 and Windows Server 2008 R2, adds the ability to encrypt removable drives. These can be read, but not written, by Windows XP using Microsoft BitLocker To Go Reader program

QUESTION 12

Your network consists of a single Active Directory domain. Your network contains 10 servers and 500 client computers. All domain controllers run Windows Server 2008 R2.

A Windows Server 2008 R2 server has Remote Desktop Services installed. All client computers run Windows XP Service Pack 3.

You plan to deploy a new line of business Application. The Application requires desktop themes to be enabled.

You need to recommend a deployment strategy that meets the following requirements:

- Only authorized users must be allowed to access the Application.
- Authorized users must be able to access the Application from any client computer.

-

Your strategy must minimize changes to the client computers.

-

Your strategy must minimize software costs. What should you recommend?

- A.
Migrate all client computers to Windows 7. Deploy the Application to all client computers by using a Group Policy object (GPO).
- B.
Migrate all client computers to Windows 7. Deploy the Application to the authorized users by using a Group Policy object (GPO).



C.

Deploy the Remote Desktop Connection (RDC) 7.0 software to the client computers. Install the Application on the Remote Desktop Services server. Implement Remote Desktop Connection Broker (RD Connection Broker).

D.

Deploy the Remote Desktop Connection (RDC) 7.0 software to the client computers. Enable the Desktop Experience feature on the Remote Desktop Services server. Install the Application on the Remote Desktop Services server.

Correct Answer: D

Desktop Experience

Configuring a Windows Server 2008 server as a terminal server lets you use Remote Desktop Connection 6.0 to connect to a remote computer from your administrator workstation and reproduces on your computer the desktop that exists on the remote computer. When you install Desktop Experience on Windows Server 2008, you can use Windows Vista features such as Windows Media Player, desktop themes, and photo management within the remote connection.

[Latest 70-646 Dumps](#)

[70-646 PDF Dumps](#)

[70-646 Braindumps](#)



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](#)

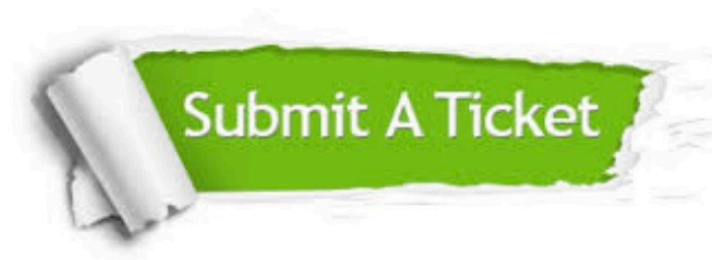
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4itsure.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 <p>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.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4itsure, All Rights Reserved.