PASS4SURES.COM

A Composite Solution With Just One Click

Microsoft

70-646 PRACTICE EXAM

Pro: Windows Server 2008 Server Administrator

Pro: Windows Server 2008, Server Administrator

Total Questions: 265/18CS

Question: 1

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.

Answer: D

Explanation:
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: 2

Your network consists of a single Active Directory domain. Your main office has an Internet connection. Your company plans to open a branch office. The branch office will connect to the main office by using a WAN link. The WAN link will have limited bandwidth. The branch office will not have access to the Internet. The branch office will contain 30 Windows Server 2008 R2 servers. You need to plan the deployment of the servers in the branch office. The deployment must meet the following requirements:
- Installations must be automated.
- Computers must be automatically activated.
- Network traffic between the offices must be minimized.

What should you include in your plan?

A. In the branch office, implement Key Management Service (KMS), a DHCP server, and Windows Deployment Services (WDS).
B. Use Multiple Activation Key (MAK) Independent Activation on the servers. In the main office, implement a DHCP server and Windows Deployment Services (WDS).
C. In the main office, implement Windows Deployment Services (WDS). In the branch office, implement a DHCP server and implement the Key Management Service (KMS).
D. Use Multiple Activation Key (MAK) Independent Activation on the servers. In the main office, implement a DHCP server. In the branch office, implement Windows Deployment Services (WDS).

Answer: A

Explanation:
The key here is that bandwidth from the branch to the main office is limited and there is no direct link to MS.
WDS and Product Activation
Although product activation does not need to occur during the actual installation process, administrators considering using WDS to automate deployment should also consider using volume activation to automate activation. Volume activation provides a simple centralized method that systems administrators can use for the activation of large numbers of deployed servers. Volume activation allows for two types of keys and three methods of activation. The key types are the Multiple Activation Key (MAK) and the Key Management Services (KMS) key.
Multiple Activation Keys allow activation of a specific number of computers. Each successful activation depletes the activation pool. For example, a MAK key that has 100 activations allows for the activation of 100 computers. The Multiple Activation Key can use the MAK Proxy Activation and the MAK Independent Activation activation methods. MAK Proxy Activation uses a centralized activation request on behalf of multiple products using a single connection to Microsoft's activation servers. MAK Independent Activation requires that each computer activates individually against Microsoft's activation servers.
The Branch office has no internet connection, so MAK is not the solution.
KMS requires at least 25 computers connecting before activation can occur, and activation must be renewed by reconnecting to the KMS server every 180 days.
You can use KMS and MAK in conjunction with one another. The number of computers, how often they connect to the network, and whether there is Internet connectivity determines which solution you should deploy. You should deploy MAK if substantial numbers of computers do not connect to the network for more than 180 days. If there is no Internet connectivity and more than 25 computers, you should deploy KMS. If there is no Internet connectivity and less than 25 computers, you will need to use MAK and activate each system over the telephone.

Question: 3

Your network contains a Webbased Application that runs on Windows Server 2003. You plan to migrate the Webbased Application to Windows Server 2008 R2. You need to recommend a server configuration to support the Webbased Application. The server configuration must meet the following requirements:

- Ensure that the Application is available to all users if a single server fails
- Support the installation of .NET Applications
- Minimize software costs

What should you recommend?

A. Install the Server Core installation of Windows Server 2008 R2 Standard on two servers. Configure the servers in a Network Load Balancing cluster.
B. Install the full installation of Windows Server 2008 R2 Web on two servers. Configure the servers in a Network Load Balancing cluster.
C. Install the full installation of Windows Server 2008 R2 Enterprise on two servers. Configure the servers in a failover

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

Answer: B

Explanation:
Web Edition meets the requirements
Windows Web Server 2008 R2
Windows Web Server 2008 R2 is designed to function specifically as a Web application server.
Other roles, such as Windows Deployment Server and Active Directory Domain Services (AD DS), are not supported on Windows Web Server 2008 R2. You deploy this server role either on a screened subnet to support a website viewable to external hosts or as an intranet server. As appropriate given its stripped-down role, Windows Web Server 2008 R2 does not support the high-powered hardware configurations that other editions of Windows Server 2008 R2 do. Windows Web Server 2008 R2 has the following properties:
: Supports a maximum of 32 GB of RAM and 4 sockets in symmetric multiprocessing (SMP) configuration
You should plan to deploy Windows Web Server 2008 R2 in the Server Core configuration, which minimizes its attack surface, something that is very important on a server that interacts with hosts external to your network environment. You should plan to deploy the full version of Windows Web Server 2008 R2 only if your organization's web applications rely on features that are not available in the Server Core version of Windows Web Server 2008 R2. Unlike the Server Core version of Windows Web Server 2008, Windows Web Server 2008 R2 supports a greater amount of Internet Information Services (IIS) functionality.
Configuring Windows Network Load Balancing
While DNS Round Robin is a simple way of distributing requests, Windows Server 2008 NLB is a much more robust form of providing high availability to applications. Using NLB, an administrator can configure multiple servers to operate as a single cluster and control the usage ot the cluster in near real-time.
Why Failover Cluster will not work.
Contrast DNS Round Robin and NLB with Failover Clustering, another availability technology in Windows Server 2008. Formerly known as server clustering, Failover Clustering creates a group of computers that all have access lo the same data store or disk resource or network share. The applicationsjunning on aJailoverCluster must be cluster-aware. Failover Clustering has had some changes since Windows Server 2003. Lesson 2 will cover these changes.

Question: 4

Your company purchases 15 new 64bit servers as follows:
- Five of the servers have a single processor.
- Five of the servers have a single dual core processor.
- Five of the servers have two quad core processors.

You plan to deploy Windows Server 2008 R2 on the new servers by using Windows Deployment Services (WDS). You need to recommend a WDS install image strategy that meets the following requirements:
- Minimizes the number of install images
- Supports the deployment of Windows Server 2008 R2

What should you recommend?

A. one install image file that contains three install images
B. one install image file that contains a single install image
C. two install image files that each contain a single install image
D. three install image files that each contain a single install image

Answer: B

Explanation:
You only need one image per processor type
Windows Deployment Services Images
Windows Deployment Services uses two different types of images: install images and boot images. Install images are the operating system images that will be deployed to Windows Server 2008 or Windows Vista client computers. A default installation image is located in the \Sources directory of the Windows Vista and Windows Server 2008 installation DVDs. If you are using WDS to deploy Windows Server 2008 to computers with different processor architectures, you will need to add separate installation images for each architecture to the WDS server. Architecture-specific images can be found on the architecture-specific installation media. For example, the Itanium image is located on the Itanium installation media and the x64 default installation image is located on the x64 installation media. Although you can create custom images, you only need to have one image per processor architecture. For example, deploying Windows Server 2008 Enterprise Edition x64 to a computer with 1 x64 processor and to a computer with 8 x64 processors in SMP configuration only requires access to the default x64 installation image. Practice exercise 2 at the end of this lesson covers the specifics ol adding a default installation image to a WDS server.

Question: 5

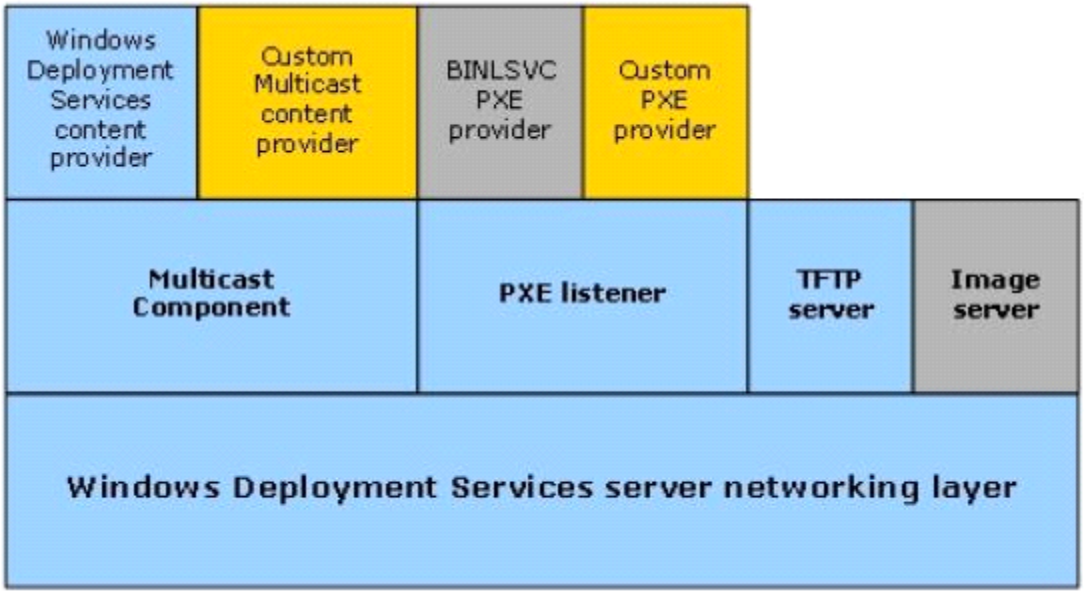
Your network contains a single Active Directory site. You plan to deploy 1,000 new computers that will run Windows 7 Enterprise. The new computers have Preboot Execution Environment (PXE) network adapters. You need to plan the deployment of the new computers to meet the following requirements:
•Support 50 simultaneous installations of Windows 7
•Minimize the impact of network operations during the deployment of the new computers
•Minimize the amount of time required to install Windows 7 on the new computers
What should you include in your plan?

A. Deploy the Windows Deployment Services (WDS) server role. Configure the IP Helper tables on all routers.
B. Deploy the Windows Deployment Services (WDS) server role. Configure each WDS server by using native mode.
C. Deploy the Windows Deployment Services (WDS) server role and the Transport Server feature. Configure the Transport Server to use a custom network profile.
D. Deploy the Windows Deployment Services (WDS) server role and the Transport Server feature. Configure the Transport Server to use a static multicast address range.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc726564%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc725964%28WS.10%29.aspx
WDS Multicast Server
Updated: November 21, 2007
Applies To: Windows Server 2008
The multicast server deploys an image to a large number of client computers concurrently without overburdening the network. When you create a multicast transmission for an image, the data is sent over the network only once, which can drastically reduce the network bandwidth that is used.
Using Transport Server
Updated: May 8, 2008
Applies To: Windows Server 2008
This topic only applies to Windows Server 2008. If you have Windows Server 2008 R2, see Configuring Transport Server.
You have two options when installing the Windows Deployment Services role in Windows Server 2008. You can install both the Deployment Server and Transport Server role services (which is the default) or you can install only the

Transport Server role service. The second configuration is for advanced scenarios, such as environments without Active Directory Domain Services (AD DS), Domain Name System (DNS), or Dynamic Host Configuration Protocol (DHCP). You can configure Transport Server to enable you to boot from the network using Pre-Boot Execution Environment (PXE) and Trivial File Transfer Protocol (TFTP), a multicast server, or both. Note that Transport Server does not contain or support the Windows Deployment Services image store.
Configure how to obtain IP addresses. If multiple servers are using multicast functionality on a network (Transport Server, Deployment Server, or another solution), it is important that each server is configured so that the multicast IP addresses do not collide. Otherwise, you may encounter excessive traffic when you enable multicasting. Note that each Windows Deployment Services server will have the same default range. To work around this issue, specify static ranges that do not overlap to ensure that each server is using a unique IP address, or configure each of the servers to obtain multicast addresses from a Multicast Address Dynamic Client Allocation Protocol (MADCAP) server.
The server architectures are illustrated in the following diagram. The blue parts are installed with Transport Server and the Deployment Server. The grey parts are installed with the Deployment Server only. The yellow parts are not installed with either, but can be written using guidelines in the Windows SDK.



Question: 6

Your network consists of a single Active Directory site that includes two network segments. The network segments connect by using a router that is RFC 1542 compliant. You plan to use Windows Deployment Services (WDS) to deploy Windows Server 2008 R2 servers. All new servers support PreBoot Execution Environment (PXE). You need to design a deployment strategy to meet the following requirements:
Support Windows Server?2008 R2
Deploy the servers by using WDS in both network segments
Minimize the number of servers used to support WDS
What should you include in your design?

A. Deploy one server. Install WDS and DHCP on the server. Configure the IP Helper tables on the route between the network segments.
B. Deploy two servers. Install WDS and DHCP on both servers. Place one server on each of the network segments. Configure both servers to support DHCP option 60.
C. Deploy two servers. Install WDS and DHCP on both servers. Place one server on each of the network segments. Configure both servers to support DHCP option 252.
D. Deploy two servers. Install WDS and DHCP on one server. Install DHCP on the other server. Place one server on each of the network segments. Configure both servers to support DHCP option 60.

Answer: A

Explanation:
http://support.microsoft.com/kb/926172
IP Helper table updates
The PXE network boot method uses DHCP packets for communication. The DHCP packets serve a dual purpose. They are intended to help the client in obtaining an IP address lease from a DHCP server and to locate a valid network boot server. If the booting client, the DHCP server, and the network boot server are all located on the same network segment, usually no additional configuration is necessary. The DHCP broadcasts from the client reach both the DHCP server and the network boot server.
However, if either the DHCP server or the network boot server are on a different network segment than the client, or if they are on the same network segment but the network is controlled by a switch or a router, you may have to update the routing tables for the networking equipment in order to make sure that DHCP traffic is directed correctly.
Such a process is known as performing IP Helper table updates. When you perform this process, you must configure the networking equipment so that all DHCP broadcasts from the client computer are directed to both a valid DHCP server and to a valid network boot server.
Note: It is inefficient to rebroadcast the DHCP packets onto other network segments. It is best to only forward the DHCP packets to the recipients that are listed in the IP Helper table.
After the client computer has obtained an IP address, it contacts the network boot server directly in order to obtain the name and the path of the network boot file to download. Again, this process is handled by using DHCP packets.
Note: We recommend that you update the IP Helper tables in order to resolve scenarios in which the client computers and the network boot server are not located on the same network segment.

Question: 7

Your company has 250 branch offices. Your network contains an Active Directory domain. The domain controllers run Windows Server 2008 R2. You plan to deploy Readonly Domain Controllers (RODCs) in the branch offices. You need to plan the deployment of the RODCs to meet the following requirements:

- Build each RODC at the designated branch office.
- Ensure that the RODC installation source files do not contain cached secrets.
- Minimize the bandwidth used during the initial synchronization of Active Directory Domain Services (AD?DS).

What should you include in your plan?

A. Use Windows Server Backup to perform a full backup of an existing domain controller. Use the backup to build the new RODCs.
B. Use Windows Server Backup to perform a custom backup of the critical volumes of an existing domain controller. Use the backup to build the new RODCs.
C. Create a DFS namespace that contains the Active Directory database from one of the existing domain controllers. Build the RODCs by using an answer file.
D. Create an RODC installation media. Build the RODCs from the RODC installation media.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc770654%28WS.10%29.aspx
Installing AD DS from Media
Applies To: Windows Server 2008, Windows Server 2008 R2
You can use the Ntdsutil.exe tool to create installation media for additional domain controllers that you are creating in a domain. By using the Install from Media (IFM) option, you can minimize the replication of directory data over the

network. This helps you install additional domain controllers in remote sites more efficiently.
Ntdsutil.exe can create four types of installation media, as described in the following table.
You must use read-only domain controller (RODC) installation media to install an RODC. For RODC installation media, the ntdsutil command removes any cached secrets, such as passwords. You can create RODC installation media either on an RODC or on a writeable domain controller. You must use writeable domain controller installation media to install a writeable domain controller. You can create writeable domain controller installation media only on a writeable domain controller.
If the source domain controller where you create the installation media and the destination server where you plan to install ActiveDirectory Domain Services (ADDS) both run Windows Server2008 with Service Pack2 or later or Windows Server2008R2, and if you are using Distributed File System (DFS) Replication for SYSVOL, you can run the ntdsutil ifm command with an option to include the SYSVOL shared folder in the installation media. If the installation media includes SYSVOL, you must use Robocopy.exe to copy the installation media from the source domain controller to the destination server. For more information, see Installing an Additional Domain Controller by Using IFM.

Type of installation media	Parameter	Description
Full (or writable) domain controller	**Create Full** *PathToMediaFolder*	Creates installation media for a writable domain controller or an Active Directory Lightweight Directory Services (AD LDS) instance in the folder that is identified in the path.
RODC	**Create RODC** *PathToMediaFolder*	Creates installation media for an RODC in the folder that is identified in the path.
Full (or writable) domain controller with SYSVOL **Important** This option works only for domain controllers that run Windows Server 2008 R2	**Create Sysvol Full** *PathToMediaFolder*	Creates installation media for a writable domain controller with SYSVOL in the folder that is identified in the path.
RODC with SYSVOL **Important** This option works only for domain controllers that run Windows Server 2008 R2	**Create Sysvol RODC** *PathToMediaFolder*	Creates installation media for an RODC with SYSVOL in the folder that is identified in the path.

Question: 8

Your network consists of a single Active Directory domain. The network is located on the 172.16.0.0/23 subnet. The company hires temporary employees. You provide user accounts and computers to the temporary employees. The temporary employees receive computers that are outside the Active Directory domain. The temporary employees use their computers to connect to the network by using wired connections and wireless connections. The company's security policy specifies that the computers connected to the network must have the latest updates for the operating system. You need to plan the network's security so that it complies with the company's security policy. What should you include in your plan?

A. Implement a Network Access Protection (NAP) strategy for the 172.16.0.0/23 subnet.
B. Create an extranet domain within the same forest. Migrate the temporary employees' user accounts to the extranet domain. Install the necessary domain resources on the 172.16.0.0/23 subnet.
C. Move the temporary employees' user accounts to a new organizational unit (OU). Create a new Group Policy object

(GPO) that uses an intranet Microsoft Update server. Link the new GPO to the new OU.
D. Create a new subnet in a perimeter network. Relocate the wireless access point to the perimeter network. Require authentication through a VPN server before allowing access to the internal resources.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/dd125338%28WS.10%29.aspx
Network Access Protection Design Guide
Updated: October 6, 2008
Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista
Network Access Protection (NAP) is one of the most anticipated features of the WindowsServer®2008 operating system. NAP is a new platform that allows network administrators to define specific levels of network access based on a client's identity, the groups to which the client belongs, and the degree to which the client complies with corporate governance policy. If a client is not compliant, NAP provides a mechanism for automatically bringing the client into compliance (a process known as remediation) and then dynamically increasing its level of network access. NAP is supported by Windows Server2008R2, Windows Server2008, Windows7, WindowsVista®, and Windows® XP with Service Pack 3 (SP3). NAP includes an application programming interface that developers and vendors can use to integrate their products and leverage this health state validation, access enforcement, and ongoing compliance evaluation. For more information about the NAP API, see Network Access Protection (http://go.microsoft.com/fwlink/?LinkId=128423).
The following are key NAP concepts:
NAP Agent.
A service included with Windows Server2008, WindowsVista, and Windows XP with SP3 that collects and manages health information for NAP client computers.
NAP client computer.
A computer that has the NAP Agent service installed and running, and is providing its health status to NAP server computers.
NAP-capable computer.
A computer that has the NAP Agent service installed and running and is capable of providing its health status to NAP server computers. NAP-capable computers include computers running Windows Server2008, WindowsVista, and Windows XP with SP3.
Non-NAP-capable computer. A computer that cannot provide its health status to NAP server components. A computer that has NAP agent installed but not running is also considered non-NAP-capable.
Compliant computer.
A computer that meets the NAP health requirements that you have defined for your network. Only NAP client computers can be compliant.
Noncompliant computer.
A computer that does not meet the NAP health requirements that you have defined for your network. Only NAP client computers can be noncompliant.
Health status.
Information about a NAP client computer that NAP uses to allow or restrict access to a network. Health is defined by a client computer's configuration state. Some common measurements of health include the operational status of Windows Firewall, the update status of antivirus signatures, and the installation status of security updates. A NAP client computer provides health status by sending a message called a statement of health (SoH).
NAP health policy server.
A NAP health policy server is a computer running Windows Server2008 with the Network Policy Server (NPS) role service installed and configured for NAP. The NAP health policy server uses NPS policies and settings to evaluate the health of NAP client computers when they request access to the network, or when their health state changes. Based on the results of this evaluation, the NAP health policy server instructs whether NAP client computers will be granted full or restricted access to the network.

Question: 9

Your company has a main office and two branch offices. The main office is located in London. The branch offices are located in New York and Paris. Your network consists of an Active Directory forest that contains three domains named contoso.com, paris.contoso.com, and newyork.contoso.com. All domain controllers run Windows Server 2008 R2 and have the DNS Server server role installed. The domain controllers for contoso.com are located in the London office. The domain controllers for paris.contoso.com are located in the Paris office. The domain controllers for newyork.contoso.com are located in the New York office. A domain controller in the contoso.com domain has a standard primary DNS zone for contoso.com. A domain controller in the paris.contoso.com domain has a standard primary DNS zone for paris.contoso.com. A domain controller in the newyork.contoso.com domain has a standard primary DNS zone for newyork.contoso.com. You need to plan a name resolution strategy for the Paris office that meets the following requirements:

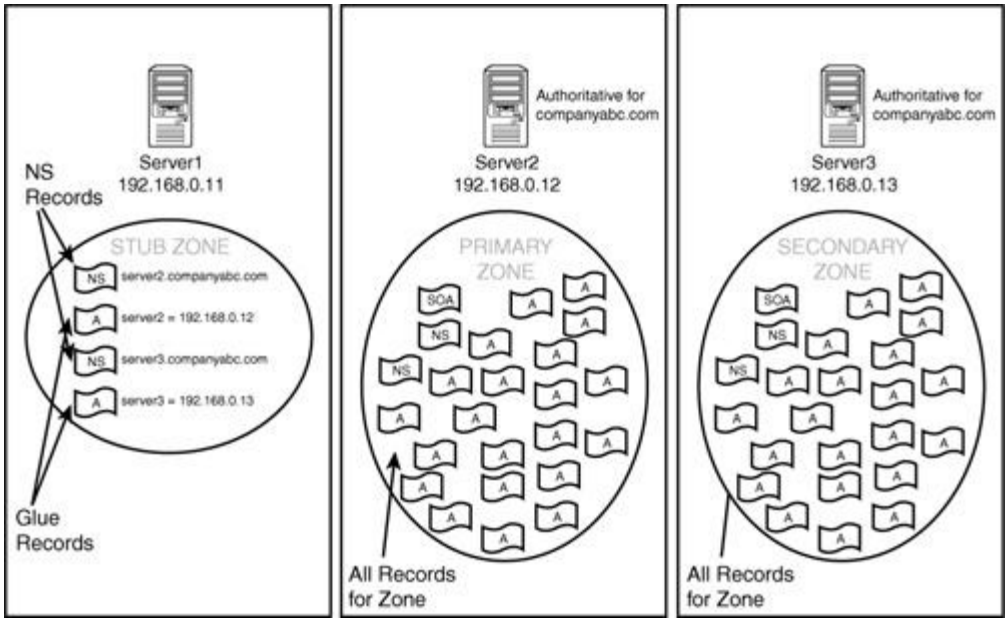
- If a WAN link fails, clients must be able to resolve hostnames for contoso.com.
- If a WAN link fails, clients must be able to resolve hostnames for newyork.contoso.com.
- The DNS servers in Paris must be updated when new authoritative DNS servers are added to newyork.contoso.com.

What should you include in your plan?

A. Configure conditional forwarding for contoso.com. Configure conditional forwarding for newyork.contoso.com.
B. Create a standard secondary zone for contoso.com. Create a standard secondary zone for newyork.contoso.com.
C. Convert the standard zone into an Active Directoryintegrated zone. Add all DNS servers in the forest to the root hints list.
D. Create an Active Directoryintegrated stub zone for contoso.com. Create an Active Directoryintegrated stub zone for newyork.contoso.com.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc771640.aspx
http://technet.microsoft.com/en-us/library/cc771898.aspx
Understanding Zone Delegation
Applies To: Windows Server 2008, Windows Server 2008 R2
Domain Name System (DNS) provides the option of dividing up the namespace into one or more zones, which can then be stored, distributed, and replicated to other DNS servers. When you are deciding whether to divide your DNS namespace to make additional zones, consider the following reasons to use additional zones:
• You want to delegate management of part of your DNS namespace to another location or department in your organization.
• You want to divide one large zone into smaller zones to distribute traffic loads among multiple servers, improve DNS name resolution performance, or create a more-fault-tolerant DNS environment.
• You want to extend the namespace by adding numerous subdomains at once, for example, to accommodate the opening of a new branch or site.
Secondary zone
When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.



Question: 10

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. You need to implement a Certificate Services solution that meets the following requirements:

- Automates the distribution of certificates for internal users
- Ensures that the network's certificate infrastructure is as secure as possible
- Gives external users access to resources that use certificate based authentication

What should you do?

A. Deploy an online standalone root certification authority (CA). Deploy an offline standalone root CA.
B. Deploy an offline enterprise root certification authority (CA). Deploy an offline enterprise subordinate CA.
C. Deploy an offline standalone root certification authority (CA). Deploy an online enterprise subordinate CA. Deploy an online standalone subordinate CA.
D. Deploy an online standalone root certification authority (CA). Deploy an online enterprise subordinate CA. Deploy an online standalone subordinate CA.

Answer: C

Explanation:
Certification authority hierarchies
The Microsoft public key infrastructure (PKI) supports a hierarchical certification authority (CA) model. A certification hierarchy provides scalability, ease of administration, and consistency with a growing number of commercial and other CA products.
In its simplest form, a certification hierarchy consists of a single CA. However, in general, a hierarchy will contain multiple CAs with clearly defined parent-child relationships. In this model, the child subordinate certification authorities are certified by their parent CA-issued certificates, which bind a certification authority's public key to its identity. The CA at the top of a hierarchy is referred to as the root authority, or root CA. The child CAs of the root CAs are called subordinate certification authorities (CAs).
A root certification authority (CA) is the top of a public key infrastructure (PKI) and generates a self-signed certificate. This means that the root CA is validating itself (self-validating). This root CA could then have subordinate CAs that effectively trust it. The subordinate CAs receive a certificate signed by the root CA, so the subordinate CAs can issue certificates that are validated by the root CA. This establishes a CA hierarchy and trust path.
http://social.technet.microsoft.com/wiki/contents/articles/2900.offline-root-certification-authority-ca.aspx

Certification authority hierarchies

The Microsoft public key infrastructure (PKI) supports a hierarchical certification authority (CA) model. A certification hierarchy provides scalability, ease of administration, and consistency with a growing number of commercial and other CA products.

In its simplest form, a certification hierarchy consists of a single CA. However, in general, a hierarchy will contain multiple CAs with clearly defined parent-child relationships. In this model, the child subordinate certification authorities are certified by their parent CA-issued certificates, which bind a certification authority's public key to its identity. The CA at the top of a hierarchy is referred to as the root authority, or root CA. The child CAs of the root CAs are called subordinate certification authorities (CAs).

Authentication and Authorization

Stand-alone CAs use local authentication for certificate requests, mainly through the Web enrollment interface.

Stand-alone CAs provide an ideal service provider or commercial PKI provider platform for issuing certificates to users outside of an Active Directory environment where the user identity is separately verified and examined before the request is submitted to the CA.

Offline and Online CAs

Traditionally, the decision of whether to use either an online or offline CAs involves a compromise between availability and usability versus security. The more sensitive that the key material is and the higher the security requirements are, the less accessible the CA should be to users.

Specifying CA Roles

An ideal PKI hierarchy design divides the responsibility of the CAs. A topology that is designed with requirements that have been carefully considered provides the most flexible and scalable enterprise configuration. In general, CAs are organized in hierarchies. Single tier hierarchies might not provide adequate security compartmentalization, extensibility and flexibility. Hierarchies with more than three tiers might not provide additional value regarding security, extensibility and flexibility.

The most important consideration is protecting the highest instance of trust as much as possible. Single-tier hierarchies are based on the need to compartmentalize risk and reduce the attack surface that is available to users who have malicious intent. A larger hierarchy is much more difficult to administer, with little security benefit.

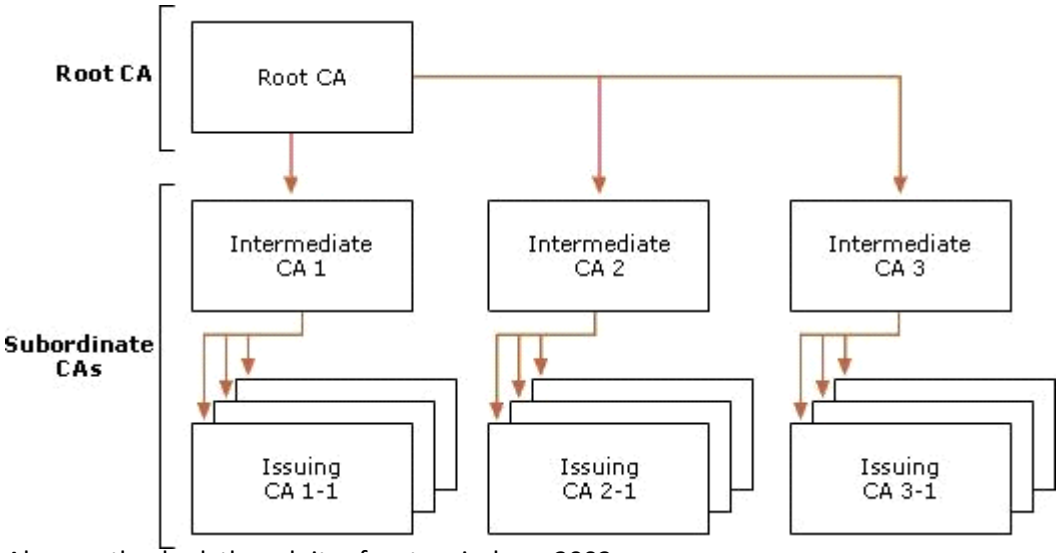
Depending on the organization's necessities, a PKI should consist of two or three logical levels that link several CAs in a hierarchy. Administrators who understand the design requirements for a three-level topology may also be able to build a two-level topology.

A three-tier CA hierarchy consists of the following components:

A root CA that is configured as a stand-alone CA without a network connection

One or more intermediate CAs that are configured as stand-alone CAs without a network connection

One or more issuing CAs that are configured as enterprise CAs that are connected to the network



Also worth a look though it refers to windows 2003

http://technet.microsoft.com/en-us/library/cc779714%28WS.10%29.aspx

Question: 11

Your network contains an Active Directory forest named contoso.com. You plan to deploy a new child domain named branch.contoso.com. The child domain will contain two domain controllers. Both domain controllers will have the DNS Server server role installed. All users and computers in the branch office will be members of the branch.contoso.com domain. You need to plan the DNS infrastructure for the child domain to meet the following requirements:

- Ensure resources in the root domain are accessible by fully qualified domain names.
- Ensure resources in the child domain are accessible by fully qualified domain names.
- Provide name resolution services in the event that a single server fails for a prolonged period of time.
- Automatically recognize when new DNS servers are added to or removed from the contoso.com domain.

What should you include in your plan?

A. On both domain controllers, add a conditional forwarder for contoso.com and create a standard primary zone for branch.contoso.com.
B. On both domain controllers, modify the root hints to include the domain controllers for contoso.com. On one domain controller, create an Active Directoryintegrated zone for branch.contoso.com.
C. On one domain controller create an Active Directoryintegrated zone for branch.contoso.com and create an Active Directoryintegrated stub zone for contoso.com.
D. On one domain controller, create a standard primary zone for contoso.com. On the other domain controller, create a standard secondary zone for contoso.com.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc772101.aspx
http://technet.microsoft.com/en-us/library/cc771898.aspx
Understanding DNS Zone Replication in Active Directory Domain Services
Applies To: Windows Server 2008, Windows Server 2008 R2
You can store Domain Name System (DNS) zones in the domain or application directory partitions of Active Directory Domain Services (AD DS). A partition is a data structure in AD DS that distinguishes data for different replication purposes. For more information, see Understanding Active Directory Domain Services Integration.
The following table describes the available zone replication scopes for AD DS-integrated DNS zone data.

Zone replication scope	Description
All DNS servers in the forest that are domain controllers running Windows Server 2003 or Windows Server 2008	Replicates zone data to all Windows Server 2003 and Windows Server 2008 domain controllers running the DNS Server service in the AD DS forest. This option replicates zone data to the ForestDNSZones partition. Therefore, it provides the broadest replication scope.
All DNS servers in the domain that are domain controllers running Windows Server 2003 or Windows Server 2008	Replicates zone data to all Windows Server 2003 and Windows Server 2008 domain controllers running the DNS Server service in the Active Directory domain. This option replicates zone data to the DomainDNSZone partition. It is the default setting for DNS zone replication in Windows Server 2003 and Windows Server 2008.
All domain controllers in the Active Directory domain	Replicates zone data to all domain controllers in the Active Directory domain. If you want Windows 2000 DNS servers to load an Active Directory–integrated zone, you must specify this scope for that zone.
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. For more information, see Create a DNS Application Directory Partition and Enlist a DNS Server in a DNS Application Directory Partition.

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.
Primary zone
When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master copy of zone data in a local file or in AD DS. When the zone is stored in a file, by default the primary zone file is named rone_name.dns and it is located in the %windir%\System32\Dns folder on the server.
Secondary zone
When a zone that this DNS server hosts is a secondary zone, this DNS server is a secondary source for information about this zone. The zone at this server must be obtained from another remote DNS server computer that also hosts the zone. This DNS server must have network access to the remote DNS server that supplies this server with updated information about the zone. Because a secondary zone is merely a copy of a primary zone that is hosted on another server, it cannot be stored in AD DS.
Stub zone
When a zone that this DNS server hosts is a stub zone, this DNS server is a source only for information about the authoritative name servers for this zone. The zone at this server must be obtained from another DNS server that hosts the zone. This DNS server must have network access to the remote DNS server to copy the authoritative name server information about the zone.
You can use stub zones to:
• Keep delegated zone information current. By updating a stub zone for one of its child zones regularly, the DNS server that hosts both the parent zone and the stub zone will maintain a current list of authoritative DNS servers for the child zone.
• Improve name resolution. Stub zones enable a DNS server to perform recursion using the stub zone's list of name servers, without having to query the Internet or an internal root server for the DNS namespace.
• Simplify DNS administration. By using stub zones throughout your DNS infrastructure, you can distribute a list of the authoritative DNS servers for a zone without using secondary zones. However, stub zones do not serve the same purpose as secondary zones, and they are not an alternative for enhancing redundancy and load sharing.
There are two lists of DNS servers involved in the loading and maintenance of a stub zone:
• The list of master servers from which the DNS server loads and updates a stub zone. A master server may be a primary or secondary DNS server for the zone. In both cases, it will have a complete list of the DNS servers for the zone.
• The list of the authoritative DNS servers for a zone. This list is contained in the stub zone using name server (NS) resource records.
When a DNS server loads a stub zone, such as widgets.tailspintoys.com, it quenes the master servers, which can be in different locations, for the necessary resource records of the authoritative servers for the zone widgets.tailspintoys.com. The list of master servers may contain a single server or multiple servers, and it can be changed anytime.

Question: 12

Your network is configured as shown in the following diagram.

You deploy an enterprise certification authority (CA) on the internal network. You also deploy a Microsoft Online Responder on the internal network. You need to recommend a secure method for Internet users to verify the validity of individual certificates. The solution must minimize network bandwidth. What should you recommend?

A. Deploy a subordinate CA on the perimeter network.
B. Install a standalone CA and the Network Device Enrollment Service (NDES) on a server on the perimeter network.
C. Install a Network Policy Server (NPS) on a server on the perimeter network. Redirect authentication requests to a server on the internal network.
D. Install Microsoft Internet Information Services (IIS) on a server on the perimeter network. Configure IIS to redirect requests to the Online Responder on the internal network.

Answer: D

Explanation:
http://www.ipsure.com/blog/2010/installation-and-configuration-of-active-directory-certificate-services-onwindows-server-2008-r2-1/
http://msdn.microsoft.com/en-us/library/cc732956.aspx

Components of an Online Responder

msdn

Applies To: Windows Server 2008 R2

The Online Responder role service in Windows Server 2008 R2 is made up of the following components.

Component	Description
Online Responder service	The Online Responder service decodes a revocation status request for a specific certificate, evaluates the status of this certificate, and sends back a signed response containing the requested certificate status information. The Online Responder service is a separate component from a certification authority (CA).
Online Responder	A computer on which the Online Responder service and Online Responder Web proxy are running. A computer that hosts a CA can also be configured as an Online Responder, but you should maintain CAs and Online Responders on separate computers. A single Online Responder can provide revocation status information for certificates issued by a single CA or multiple CAs. CA revocation information can be supported by more than one Online Responder. **Note** An Online Responder can be installed on any computer running Windows Server 2008 R2 Enterprise or Windows Server 2008 R2 Datacenter. The certificate revocation data is derived from a published certificate revocation list (CRL) that can come from a CA on a computer running Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, or Windows 2000 Server, or from a non-Microsoft CA.
Online Responder Web proxy	The service interface for the Online Responder is implemented as an Internet Server API (ISAPI) extension hosted by Internet Information Services (IIS). The Web proxy receives and decodes requests, and caches responses for a configurable period of time.
Revocation configuration	A revocation configuration includes all of the settings that are needed to respond to certificate status requests that have been issued by using a specific CA key. These configuration settings include the CA certificate, the signing certificate for the Online Responder, and the type of revocation provider to use.
Revocation provider	A revocation provider is the software module that, in conjunction with other revocation configuration settings, enables an Online Responder to check the status of a certificate. The revocation provider in Windows Server 2008 R2 uses data from CRLs to provide this status information.
Online Responder Array	An Online Responder Array contains one or more member Online Responders. Additional Online Responders can be added to an Online Responder Array for a number of reasons, including geographic considerations, scalability, network design considerations, or fault tolerance if an individual Online Responder becomes unavailable. Responders in an Online Responder Array are referred to as Array members.
Online Responder Array controller	When multiple Online Responders are combined in an Array, one member of the Array must be designated as the Array controller. Although each Online Responder in an Array can be configured and managed independently, in case of conflicts the configuration information for the Array controller will override configuration options set on other Array members.

Question: 13

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.

Answer: A

Explanation:
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.

Question: 14

Your company has a main office and three branch offices. The network consists of a single Active Directory domain. Each office contains an Active Directory domain controller. You need to create a DNS infrastructure for the network that meets the following requirements:

- The DNS infrastructure must allow the client computers in each office to register DNS names within their respective offices.
- The client computers must be able to resolve names for hosts in all offices.

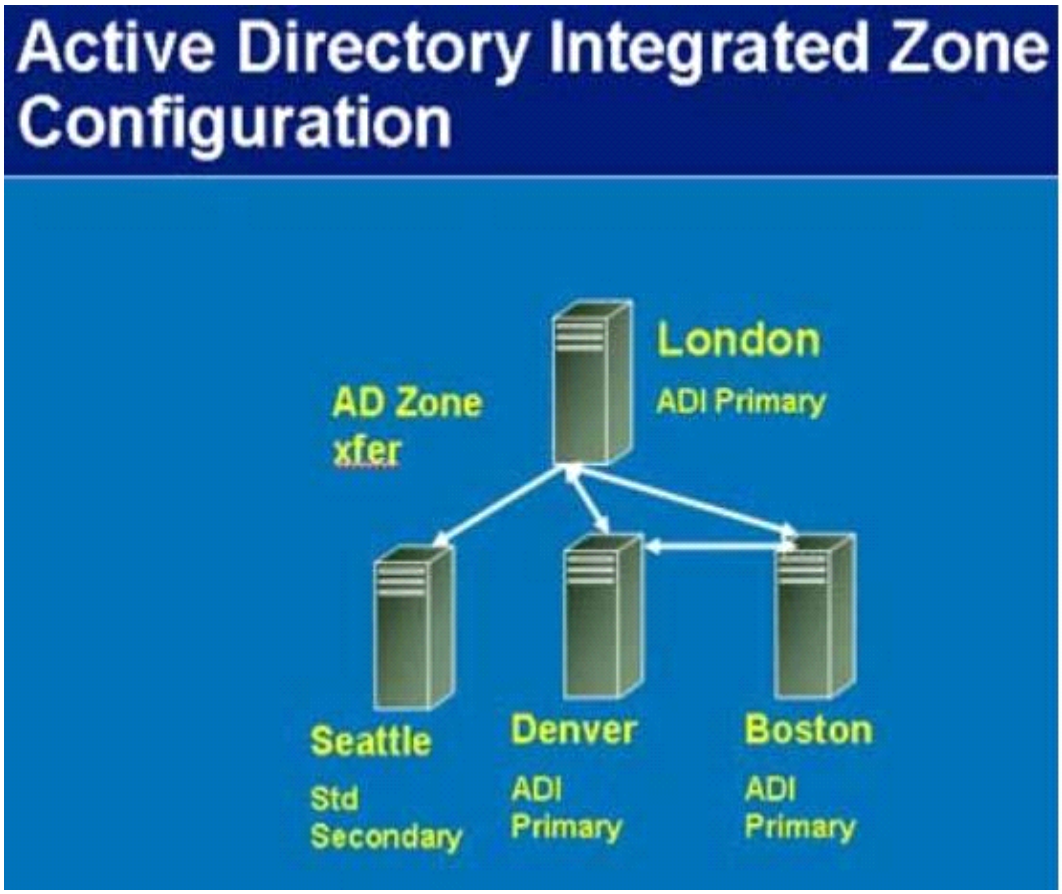
What should you do?

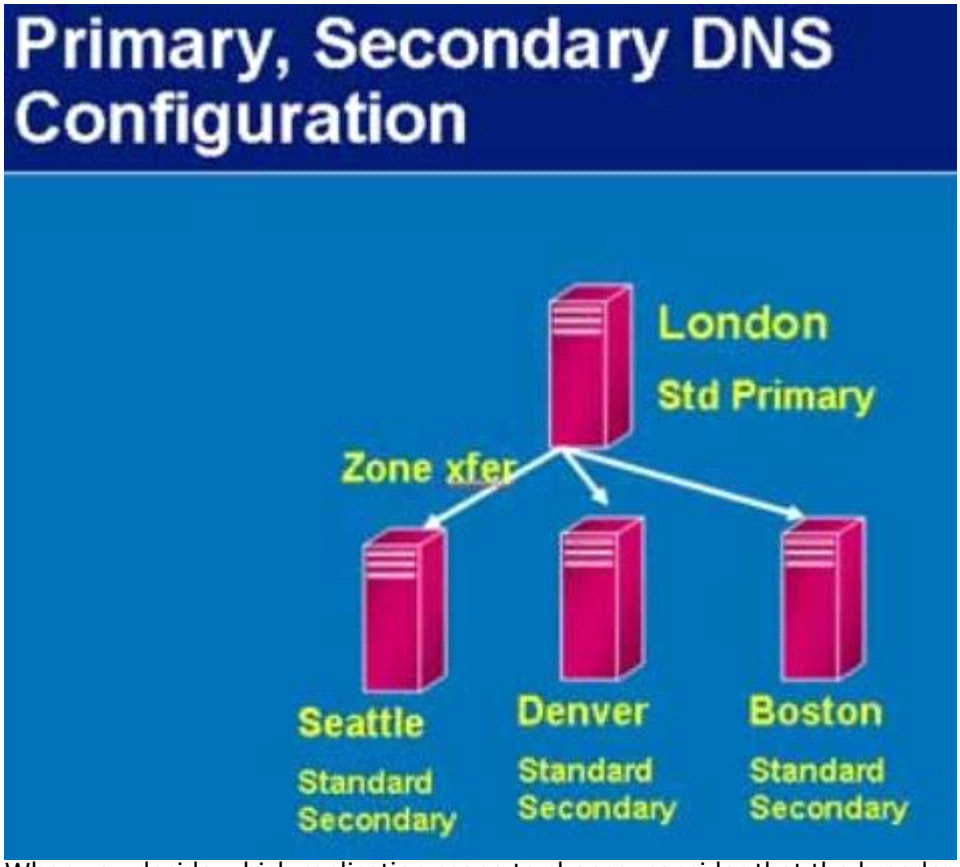
A. Create an Active Directoryintegrated zone at the main office site.

B. Create a standard primary zone at the main office site and at each branch office site.
C. Create a standard primary zone at the main office site. Create a secondary zone at each branch office site.
D. Create a standard primary zone at the main office site. Create an Active Directoryintegrated stub zone at each branch office site.

Answer: A

Explanation:
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.

Question: 15

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

- Manage the print queue from a central location.
- Make the print services available, even if one of the print devices fails.

What should you include in your plan?

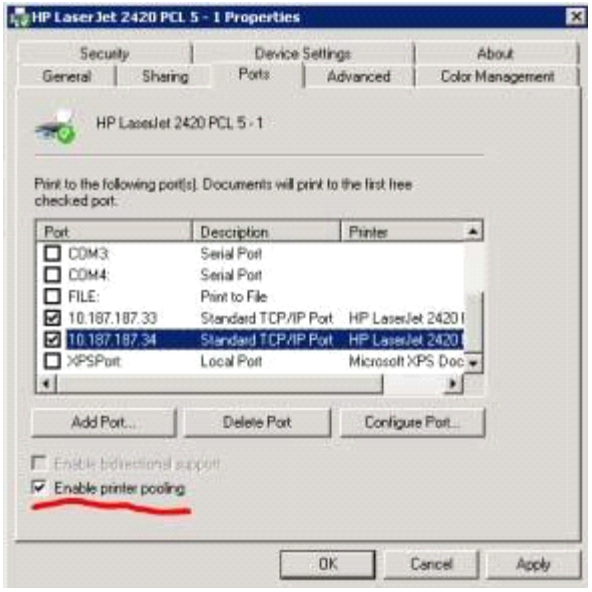
A. Install and share a printer on Server1. Enable printer pooling.

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

C. Install and share a printer on Server1. Install and share a printer on Server2. Use Print Management to install the printers on the client computers.
D. Add Server1 and Server2 to a Network Load Balancing cluster. Install a printer on each node of the cluster.

Answer: A

Explanation:
http://www.techrepublic.com/blog/datacenter/configure-printer-pooling-in-windows-server-2008/964
Managing printers can be the bane of a Windows administrator. One feature that may assist you with this task is the Windows printer pooling feature. Windows Server 2008 offers functionality that permits a collection of multiple like-configured printers to distribute the print workload.
Printer pooling makes one share that clients print to, and the jobs are sent to the first available printer. Configuring print pooling is rather straightforward in the Windows printer configuration applet of the Control Panel. Figure A shows two like-modeled printers being pooled.
To use pooling, the printer models need to be the same so that the driver configuration is transparent to the end device; this can also help control costs of toner and other supplies. But plan accordingly — you don't want users essentially running track to look for their print jobs on every printer in the office.



Question: 16

Your network contains two servers that run the Server Core installation of Windows Server 2008 R2. The two servers are part of a Network Load Balancing cluster. The cluster hosts a Web site. Administrators use client computers that run Windows 7. You need to recommend a strategy that allows the administrators to remotely manage the Network Load Balancing cluster. Your strategy must support automation. What should you recommend?

A. On the servers, enable Windows Remote Management (WinRM).
B. On the servers, add the administrators to the Remote Desktop Users group.
C. On the Windows 7 client computers, enable Windows Remote Management (WinRM).
D. On the Windows 7 client computers, add the administrators to the Remote Desktop Users group.

Answer: A

Explanation:
http://support.microsoft.com/kb/968929

http://msdn.microsoft.com/en-us/library/aa384291%28VS.85%29.aspx
WinRM 2.0
WinRM is the Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows for hardware and operating systems from different vendors to interoperate. The WS-Management Protocol specification provides a common way for systems to access and exchange management information across an IT infrastructure. WinRM 2.0 includes the following new features:
• The WinRM Client Shell API provides functionality to create and manage shells and shell operations, commands, and data streams on remote computers.
• The WinRM Plug-in API provides functionality that enables a user to write plug-ins by implementing certain APIs for supported resources and operations.
• WinRM 2.0 introduces a hosting framework. Two hosting models are supported. One is Internet Information Services (HS)-based and the other is WinRM service-based.
• Association traversal lets a user retrieve instances of Association classes by using a standard filtering mechanism.
• WinRM 2.0 supports delegating user credentials across multiple remote computers.
• Users of WinRM 2.0 can use Windows PowerShell cmdlets for system management.
• WinRM has added a specific set of quotas that provide a better quality of service and allocate server resources to concurrent users. The WinRM quota set is based on the quota infrastructure that is implemented for the IIS service.

About Windows Remote Management

Windows Remote Management is one component of the Windows Hardware Management features that manage server hardware locally and remotely. These features diagnosis and control through baseboard management controllers (*BMCs*), and a COM API and scripting objects that allow you to write applications that communicat about the public specification for WS-Management protocol, see Web Services for Management (WS-Management).

Components of WinRM and Hardware Management

The following is a list of components and features that are supplied by WinRM and hardware monitoring:

- WinRM Scripting API
  This scripting API enables you to obtain data from remote computers using scripts that perform WS-Management protocol operations.
- **Winrm.cmd**
  This command-line tool for system management is implemented in a Visual Basic Scripting Edition file (Winrm.vbs) written using the WinRM scripting API. Th manage resources. For more information, see the online help provided by the command line **Winrm /?**.

  Windows Server 2003 R2: For this command to work, the Hardware Management feature must be installed through **Add/Remove System Comp**
- **Winrs.exe**
  This command line tool enables administrators to remotely execute most Cmd.exe commands using the WS-Management protocol. For more information, see

  Windows Server 2003 R2: This command is not available.
- Intelligent Platform Management Interface (IPMI) driver and WMI provider
  Hardware management through the *Intelligent Platform Management Interface (IPMI)* provider and driver enables you to control and diagnose remote server deployed.

  For more information, see the IPMI Provider and Intelligent Platform Management Interface (IPMI) Classes.
- WMI service
  The WMI service continues to run side-by-side with WinRM and provides requested data or control through the *WMI plug-in*. You can continue to obtain data f IPMI-supplied data. For more information about configuration and installation required for WinRM, see Hardware Management Introduction.
- WS-Management protocol
  WS-Management protocol, a SOAP-based, firewall-friendly protocol, was designed for systems to locate and exchange management information. The intent o consistency for enterprise systems that have computers running on a variety of operating systems from different vendors.

  WS-Management protocol is based on the following standard web service specifications: HTTPS, SOAP over HTTP (WS-I profile), SOAP 1.2, WS-Addressing, W the current draft of the specification, see the Management Specifications Index Page.

Working with WinRM

For more information about writing WinRM scripts, see Using Windows Remote Management.

The following table lists topics that provide information about the WS-Management protocol, WinRM and WMI, how to specify management resources such as disk dr

Topic	Description
Installation and Configuration for Windows Remote Management	The WinRM *listener* requires configuration on both client and server computers.
Windows Remote Management Architecture	Diagram that illustrates the components of WinRM and which components are found on client and server computer
WS-Management Protocol	Description of the public standard WS-Management protocol for remotely sending and receiving management data
Scripting in Windows Remote Management	The WinRM scripting API is similar to the actions of the WS-Management protocol. Data retrieved by scripts is form
Authentication for Remote Connections	WS-Management protocol maintains security for data transfer between computers by supporting several standard
Windows Remote Management and WMI	Because WinRM is integrated with Windows Management Instrumentation (WMI), you can obtain WMI data with sc Winrm command-line tool.
Resource URIs	A *resource URI* is an identifier for a management operation or value. For example, disk drives represent a type of
Remote Hardware Management	The IPMI provider supplies classes and data that describe the baseboard management controller (BMC) hardware n the BMC sensors. Other objects represent the BMC System Event Log (SEL) and the messages in the log.
Events	You cannot obtain events through WinRM scripting, but you can use the Wevtutil.exe command-line tool to view Ev

USAGE
=====
(ALL UPPER-CASE = value that must be supplied by user.)
winrs [-/SWITCH[:VALUE]] COMMAND
COMMAND - Any string that can be executed as a command in the cmd.exe shell.
SWITCHES
========
(All switches accept both short form or long form. For example both -r and
-remote are valid.)
-r[emote]:ENDPOINT - The target endpoint using a NetBIOS name or the standard connect
ion URL: [TRANSPORT://]TARGET[:PORT]. If not specified
-r:localhost is used.
-un[encrypted] - Specify that the messages to the remote shell will not be encrypted. This is useful for troubleshooting, or when the network traffic is already encrypted using ipsec, or when physical security is enforced. By default the messages are encrypted
using Kerberos or NTLM keys. This switch is ignored when HTTPS transport is selected.
-u[sername]:USERNAME - Specify username on command line. If not specified the tool will
use Negotiate authentication or prompt for the name.
If -username is specified, -password must be as well.
-p[assword]:PASSWORD - Specify password on command line. If -password is not specified but -username is the tool will prompt for the password. If -password is specified, -user must be specified as well.
-t[imeout]:SECONDS - This option is deprecated.
-d[irectory]:PATH - Specifies starting directory for remote shell. If not specified the remote shell will start in the user's home directory defined by the environment variable %USERPROFILE%.
-env[ironment]:STRING=VALUE - Specifies a single environment variable to be set when shell starts, which allows changing default environment for shell. Multiple occurrences of this switch must be used to specify multiple environment variables.
-noe[cho] - Specifies that echo should be disabled. This may be necessary to ensure that user's answers to remote prompts are not displayed locally. By default echo is "on".
-nop[rofile] - Specifies that the user's profile should not be loaded. By default the server will attempt to load the user profile. If the remote user is not a local administrator on the target system then this option will be required (the default will result in error).
-a[llow]d[elegate] - Specifies that the user's credentials can be used to access a remote share, for example, found on a different machine than the target endpoint.
-comp[ression] - Turn on compression. Older installations on remote machines may not support compression so it is off by default.
-[use]ssl - Use an SSL connection when using a remote endpoint. Specifying this instead of the transport "https:" will use the default WinRM default port.
-? - Help

To terminate the remote command the user can type Ctrl-C or Ctrl-Break, which will be sent to the remote shell. The second Ctrl-C will force termination of winrs.exe.
To manage active remote shells or WinRS configuration, use the WinRM tool. The URI alias to manage active shells is shell/cmd. The URI alias for WinRS configuration is winrm/conf
ig/winrs. Example usage can be found in the WinRM tool by typing "WinRM -?".
Examples:
winrs -r:https://myserver.com command
winrs -r:myserver.com -usessl command
winrs -r:myserver command
winrs -r:http://127.0.0.1 command
winrs -r:http://169.51.2.101:80 -unencrypted command
winrs -r:https://[::FFFF:129.144.52.38] command
winrs -r:http://[1080:0:0:0:8:800:200C:417A]:80 command
winrs -r:https://myserver.com -t:600 -u:administrator -p:$%fgh7 ipconfig
winrs -r:myserver -env:PATH=^%PATH^%;c:\tools -env:TEMP=d:\temp config.cmd
winrs -r:myserver netdom join myserver /domain:testdomain /userd:johns /passwordd:$%fgh789
winrs -r:myserver -ad -u:administrator -p:$%fgh7 dir \\anotherserver\share

Question: 17

Your company has a main office and a branch office. You plan to deploy a Readonly Domain Controller (RODC) in the branch office. You need to plan a strategy to manage the RODC. Your plan must meet the following requirements:

- Allow branch office support technicians to maintain drivers and disks on the RODC
- Prevent branch office support technicians from managing domain user accounts

What should you include in your plan?

A. Configure the RODC for Administrator Role Separation.
B. Configure the RODC to replicate the password for the branch office support technicians.
C. Set NTFS permissions on the Active Directory database to Read & Execute for the branch office support technicians.
D. Set NTFS permissions on the Active Directory database to Deny Full Control for the branch office support technicians.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc753170%28WS.10%29.aspx

Administrator Role Separation

Updated: August 20, 2010

Applies To: Windows Server 2008

This topic explains how you can use Administrator Role Separation (ARS) on a read-only domain controller (RODC) to delegate RODC administration to a user who is

One problem encountered by administrators of domain controllers in perimeter networks is that domain controllers typically have to be set up and administered by d performing an offline defragmentation, or backing up the system, cannot be delegated.

With the introduction of RODCs, domain administrators can delegate both the installation and the administration of RODCs to any domain user, without granting ther ARS.

You can use ARS for two different purposes:

- **RODC installation**. You can promote an RODC in two stages:

  1. A domain administrator creates an account in the domain for the computer that is going to be promoted as an RODC. During this process, the domain the security principal (user or group) that, using this account, will have the right to promote and subsequently administer the RODC.
  2. In the site where the RODC is going to be located, the delegated administrator that the domain administrator specifies during the first stage can attach

- **RODC maintenance**. The delegated administrator for the RODC can log on to it to perform maintenance work, such as upgrading a driver or an application, i on. But the delegated administrator cannot log on to any other domain controller—including other RODCs—or perform any other administrative task in the do effectively manage the RODC without compromising the security of the rest of the domain.

For more information about how to configure ARS for an RODC, see RODC Administration (http://go.microsoft.com/fwlink/?LinkID=133521).

Question: 18

Your network consists of a single Active Directory domain. The network contains five Windows Server 2008 R2 servers that host Web Applications. You need to plan a remote management strategy to manage the Web servers. Your plan must meet the following requirements:

- Allow Web developers to configure features on the Web sites
- Prevent Web developers from having full administrative rights on the Web servers

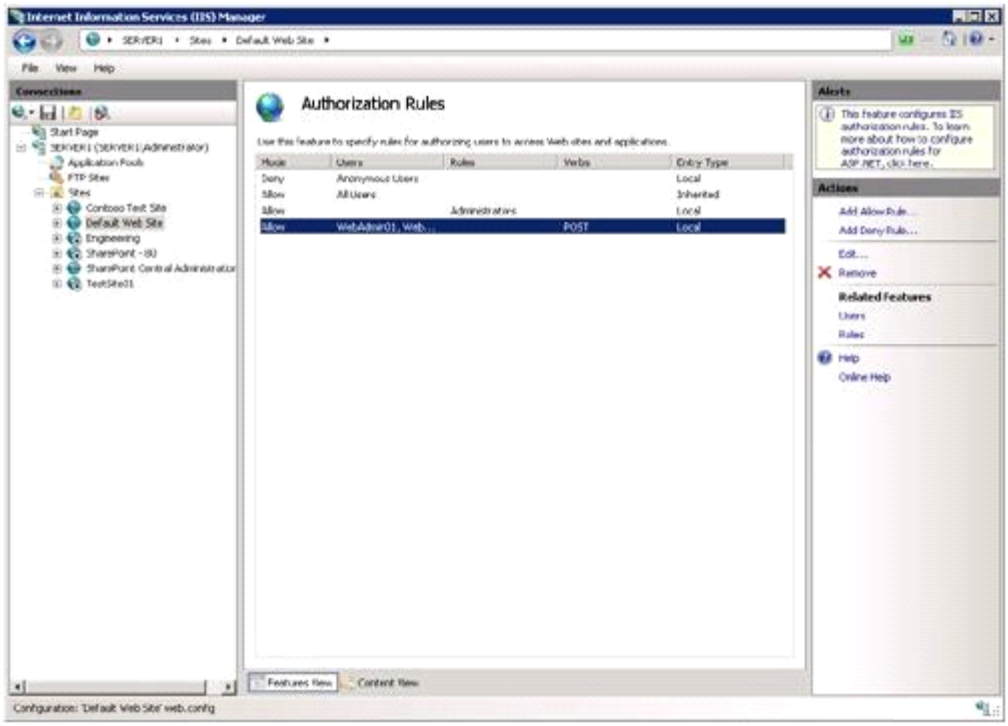
What should you include in your plan?

A. Configure request filtering on each Web server.
B. Configure authorization rules for Web developers on each Web server.
C. Configure the security settings in Internet Explorer for all Web developers by using a Group Policy.
D. Add the Web developers to the Account Operators group in the domain.

Answer: B

Explanation:
http://mscerts.programming4.us/windows_server/windows%20server%202008%20%20%20controlling%20access%20to%20web%20services%20%28part%205%29%20-%20managing%20url%20authorization%20rules.aspx
Managing URL Authorization Rules
Authorization is a method by which systems administrators can determine which resources and content are available to specific users Authorization relies on authentication to validate the identity of a user. Once the identity has been proven, authorization rules determine which actions a user or computer can perform IIS provides methods of securing different types of content using URL-based authorization. Because Web content is generally requested using a URL that includes a full path to the content being requested, you can configure authorization settings easily, using IIS Manager
Creating URL Authorization Rules
To enable URL authorization, the UrlAuthorizationModule must be enabled Authorization rules can be configured at the level of the Web server for specific Web sites, for specific Web applications, and for specific files (based on a complete URL path). URL authorization rules use inheritance so that lower-level objects inherit authorization settings from their parent objects (unless they are specifically overridden).
To configure authorization settings, select the appropriate object in the left pane of IIS Manager, and then select Authorization Rules in Features View. Figure 6 shows an example of multiple rules configured for a Web site.

Figure 6. Viewing authorization rules for a Web site



There are two types of rules: Allow and Deny. You can create new rules by using the Add Allow Rule and Add Deny Rule commands in the Actions pane The available options for both types of rules are the same. (See Figure 7) When creating a new rule, the main setting is to determine to which users the rule applies. The options are:

- All Users
- All Anonymous Users
- Specific Roles Or User Groups
- Specific Users

Figure 7. Creating a new Allow Rule for a Web application

When you choose to specify users or groups to which the rule applies, you can type the appropriate names in a command-separated list. The specific users and groups are defined using NET role providers. This is a standard feature that is available to ASP NET Web developers. Developers can create their own roles and user accounts and can define permissions within their applications. Generally, information about users and roles is stored in a relational database or relies on a directory service such as Active Directory.

In addition to user and role selections, you can further configure an authorization rule based on specific HTTP verbs. For example, if you want to apply a rule only for POST commands (which are typically used to send information from a Web browser to a Web server), add only the POST verb to the rule

Managing Rule Inheritance

As mentioned earlier in this section, authorization rules are inherited automatically by lower-level objects This is useful when your Web site and Web content is organized hierarchically based on intended users or groups The Entry Type column shows whether a rule has been inherited from a higher level or whether it has been defined locally IIS Manager automatically will prevent you from creating duplicate rules. You can remove rules at any level, including both Inherited and Local entry types

Question: 19

Your network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2008 R2. The domain contains 200 Windows Server 2008 R2 servers. You need to plan a monitoring solution that meets the following requirements:

- Sends a notification by email to the administrator if an Application error occurs on any of the servers
- Uses the minimum amount of administrative effort

What should you include in your plan?

A. On one server, create event subscriptions for each server. On the server, attach tasks to the Application error events.
B. On one server, create an Event Trace Sessions Data Collector Set. On all servers, create a System Performance Data Collector Set.
C. On all servers, create event subscriptions for one server. On all servers, attach a task for the Application error events.
D. On all servers, create a System Performance Data Collector Set. On one server, configure the report settings for the new Data Collector set.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc749183.aspx
http://technet.microsoft.com/en-us/library/cc748890.aspx
http://technet.microsoft.com/en-us/library/cc722010.aspx
Event Subscriptions
Applies To: Windows 7, Windows Server 2008 R2, Windows Vista
Event Viewer enables you to view events on a single remote computer. However, troubleshooting an issue might require you to examine a set of events stored in multiple logs on multiple computers.
Windows Vista includes the ability to collect copies of events from multiple remote computers and store them locally. To specify which events to collect, you create an event subscription. Among other details, the subscription specifies exactly which events will be collected and in which log they will be stored locally. Once a subscription is active and events are being collected, you can view and manipulate these forwarded events as you would any other locally stored events.
Using the event collecting feature requires that you configure both the forwarding and the collecting computers. The functionality depends on the Windows Remote Management (WinRM) service and the Windows Event Collector (Wecsvc) service. Both of these services must be running on computers participating in the forwarding and collecting process. To learn about the steps required to configure event collecting and forwarding computers, see Configure Computers to Forward and Collect Events.
Additional Considerations
• You can subscribe to receive events from an existing subscription on a remote computer.
Configure Computers to Forward and Collect Events
Applies To: Windows 7, Windows Server 2008 R2, Windows Vista

Before you can create a subscription to collect events on a computer, you must configure both the collecting computer collected (collector) and each computer from which events will be collected (source). Updated information about event subscriptions may be available online at Event Subscriptions.
To configure computers in a domain to forward and collect events
1. Log on to all collector and source computers. It is a best practice to use a domain account with administrative privileges.
2. On each source computer, type the following at an elevated command prompt:

```
winrm quickconfig
```

Note

If you intend to specify an event delivery optimization of **Minimize Bandwidth** or **Minimize Latency**, then you must also run the above command on the collector computer.

3. On the collector computer, type the following at an elevated command prompt:

```
wecutil qc
```

4. Add the computer account of the collector computer to the local Administrators group on each of the source computers.

Note

By default, the **Local Users and Groups** MMC snap-in does not enable you to add computer accounts. In the **Select Users, Computers, or Groups** dialog box, click the **Object Types** button and select the **Computers** check box. You will then be able to add computer accounts.

5. The computers are now configured to forward and collect events. Follow the steps in Create a New Subscription to specify the events you want to have forwarded to the collector.

Additional Considerations

- In a workgroup environment, you can follow the same basic procedure described above to configure computers to forward and collect events. However, there are some additional steps and considerations for workgroups:
    - You can only use Normal mode (Pull) subscriptions.
    - You must add a Windows Firewall exception for Remote Event Log Management on each source computer.
    - You must add an account with administrator privileges to the Event Log Readers group on each source computer. You must specify this account in the Configure Advanced Subscription Settings dialog when creating a subscription on the collector computer.
    - Type `winrm set winrm/config/client @{TrustedHosts="<sources>"}` at a command prompt on the collector computer to allow all of the source computers to use NTLM authentication when communicating with WinRM on the collector computer. Run this command only once. Where `<sources>` appears in the command, substitute a list of the names of all of the participating source computers in the workgroup. Separate the names by commas. Alternatively, you can use wildcards to match the names of all the source computers. For example, if you want to configure a set of source computers, each with a name that begins with "msft", you could type this command `winrm set winrm/config/client @{TrustedHosts="msft*"}` on the collector computer. To learn more about this command, type `winrm help config`.
- If you configure a subscription to use the HTTPS protocol by using the **HTTPS** option in **Advanced Subscription Settings**, you must also set corresponding Windows Firewall exceptions for port 443. For a subscription that uses **Normal** (PULL mode) delivery optimization, you must set the exception only on the source computers. For a subscription that uses either **Minimize Bandwidth** or **Minimize Latency** (PUSH mode) delivery optimizations, you must set the exception on both the source and collector computers.
- If you intend to specify a user account by using the **Specific User** option in **Advanced Subscription Settings** when creating the subscription, you must ensure that account is a member of the local Administrators group on each of the source computers in step 4 instead of adding the machine account of the collector computer. Alternatively, you can use the Windows Event Log command-line utility to grant an account access to individual logs. To learn more about this command-line utility, type wevtutil sl -? at a command prompt.

Create a New Subscription

Applies To: Windows 7, Windows Server 2008 R2, Windows Vista

To receive forwarded events on a computer, you must set up one or more event subscriptions. Before setting up a subscription, you must configure both the computer that will receive the forwarded events, and the computer or computers that will forward the events. To learn how to configure the computers, see Configure Computers to Forward and Collect Events.

Once you have configured the computers, you create a subscription to specify which events to collect.

To create a new subscription

1. On the collector computer, run Event Viewer as an administrator.
2. Click **Subscriptions** in the console tree.

   Note

   If the Windows Event Collector service is not started, you will be prompted to confirm that you want to start it. This service must be started to create subscriptions and collect events. You must be a member of the Administrators group to start this service.

3. On the **Actions** menu, click **Create Subscription**.
4. In the **Subscription Name box**, type a name for the subscription.
5. In the **Description box**, enter an optional description.
6. In the **Destination Log box**, select the log file where collected events are to be stored. By default, collected events are stored in the ForwardedEvents log.
7. Click **Add** and select the computers from which events are to be collected.

   Note

   After adding a computer, you can test connectivity between it and the local computer by selecting the computer and clicking **Test**.

8. Click **Select Events** to display the **Query Filter** dialog box. Use the controls in the **Query Filter** dialog box to specify the criteria that events must meet to be collected.
9. Click **OK** on the **Subscription Properties** dialog box. The subscription will be added to the **Subscriptions** pane and, if the operation was successful, the Status of the subscription will be Active.

Events raised on the forwarder computers that meet the criteria of the subscription will be copied to the collector computer log specified in step 6.

Additional Considerations

- You cannot use Event Viewer to create a subscription while it is connected to a remote computer.
- You can use the filter from a previously defined Custom View by choosing **Copy from existing Custom View**. Additionally, you can paste an XPATH query into the text box on the XML tab of the **Query Filter** dialog box.
- If a newly created subscription does not activate, you can open the **Subscription Properties** dialog box and select individual source computers to view the status for each of them.

Question: 20

Your network consists of a single Active Directory domain. The network includes a branch office named Branch1. Branch1 contains 50 member servers that run Windows Server 2008 R2. An organizational unit (OU) named Branch1Servers contains the computer objects for the servers in Branch1. A global group named Branch1admins contains the user accounts for the administrators. Administrators maintain all member servers in Branch1. You need to recommend a solution that allows the members of Branch1admins group to perform the following tasks on the Branch1 member servers.

- Stop and start services
- Change registry settings

What should you recommend?

A. Add the Branch1admins group to the Power Users local group on each server in Branch1.
B. Add the Branch1admins group to the Administrators local group on each server in Branch1.
C. Assign the Branch1admins group change permissions to the Branch1Servers OU and to all child objects.
D. Assign the Branch1admins group Full Control permissions on the Branch1Servers OU and to all child objects.

Answer: B

Explanation:
Local admins have these rights.
Power Users do not
By default, members of the power users group have no more user rights or permissions than a standard user account. The Power Users group in previous versions of Windows was designed to give users specific administrator rights and permissions to perform common system tasks. In this version of Windows, standard user accounts inherently have the ability to perform most common configuration tasks, such as changing time zones. For legacy applications that require the same Power User rights and permissions that were present in previous versions of Windows, administrators can

apply a security template that enables the Power Users group to assume the same rights and permissions that were present in previous versions of Windows.

Question: 21

Your network consists of a single Active Directory domain. The network includes a branch office named Branch1. Branch1 contains a Read only Domain Controller (RODC) named Server1. A global group named Branch1admins contains the user accounts for administrators. Administrators manage the client computers and servers in Branch1. You need to recommend a solution for delegating control of Server1. Your solution must meet the following requirements:

- Allow the members of the Branch1admins group to administer Server1 including, change device drivers and install operating system updates by using Windows Update.
- Provide the Branch1admins group rights on Server1 only.
- Prevent Branch1admins group from modifying Active Directory objects.

What should you recommend?

A. Add the Branch1admins global group to the Server Operators builtin local group.
B. Add the members of the Branch1admins global group to the Administrators builtin local group of Server1.
C. Grant Full Control permission on the Server1 computer object in the domain to the Branch1admins group
D. Move the Server1 computer object to a new organizational unit (OU) named Branch1servers. Grant Full Control permission on the Branch1servers OU to the Branch1admins group.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc753223%28WS.10%29.aspx
Administrator role separation
Administrator role separation specifies that any domain user or security group can be delegated to be the local administrator of an RODC without granting that user or group any rights for the domain or other domain controllers. Accordingly, a delegated administrator can log on to an RODC to perform maintenance work, such as upgrading a driver, on the server. But the delegated administrator is not able to log on to any other domain controller or perform any other administrative task in the domain. In this way, a security group that comprises branch users, rather than members of the Domain Admins group, can be delegated the ability to effectively manage the RODC in the branch office, without compromising the security of the rest of the domain.

Question: 22

Your network consists of a single Active Directory forest. The forest functional level is Windows Server 2008 R2. The forest contains two domains named contoso.com and na.contoso.com. Contoso.com contains a user named User1. Na.contoso.com contains an organizational unit (OU) named Security. You need to give User1 administrative rights so that he can manage Group Policies for the Security OU. You want to achieve this goal while meeting the following requirements:

- User1 must be able to create and configure Group Policies in na.contoso.com.
- User1 must be able to link Group Policies to the Security OU.
- User1 must be granted the least administrative rights necessary to achieve the goal.

What should you do?

A. Add User1 to the Administrators group for na.contoso.com.
B. Add User1 to the Group Policy Creator Owners group in contoso.com. Modify the permissions on the Security OU.
C. Run the Delegation of Control Wizard on the Security OU. In the Group Policy Management Console, modify the

permissions of the Group Policy Objects container in the na.contoso.com domain.
D. Run the Delegation of Control Wizard on na.contoso.com. In the Group Policy Management Console, modify the permissions of the Group Policy Objects container in the contoso.com domain.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd145442.aspx
http://technet.microsoft.com/en-us/library/dd145338.aspx
http://technet.microsoft.com/en-us/library/dd145594.aspx

Tasks to Delegate

Updated: December 30, 2008

Applies To: Windows Server 2008, Windows Server 2008 R2

Item	Details
Delegate the following common tasks	The following are common tasks that you can select to delegate control of them: • Create, delete, and manage user accounts • Reset user passwords and force password change at next logon • Read all user information • Modify the membership of a group • Join a computer to a domain • Manage Group Policy links • Generate Resultant Set of Policy (Planning) • Generate Resultant Set of Policy (Logging) • Create, delete, and manage inetOrgPerson accounts • Reset inetOrgPerson passwords and force password change at next logon • Read all inetOrgPerson information
Create a custom task to delegate	Select this option to create a custom task if the task that you want to delegate does not appear in the list of common tasks.

Active Directory Object Type

Updated: December 30, 2008

Applies To: Windows Server 2008, Windows Server 2008 R2

Control	Details
This folder, existing objects in this folder, and creation of new objects in this folder	Select this option if you want to delegate full control of this folder and all its existing object contents, as well as any future objects that it might contain.
Only the following objects in the folder	Select this option if you want to delegate control of only selected types of objects in this folder. The types of objects that are available are determined by the Active Directory schema. For more information about specific object types, see Active Directory Domain Services Reference (http://go.microsoft.com/fwlink/?LinkId=80181).
Create selected objects in this folder check box	Select this check box to create objects of the types that are selected in the object type list.
Delete selected objects in this folder check box	Select this check box to remove objects of the types that are selected in the object type list.

Permissions

Updated: December 30, 2008

Applies To: Windows Server 2008, Windows Server 2008 R2

Control	Details
Show these permissions	Select among the following check boxes: • **General**. This is the default view. When you select this check box, the list of permissions displays only the core permissions that are common to all the selected objects on the previous wizard page. These permissions include Full Control, Read, Write, Read All Properties, and Write All Properties. • **Property-specific**. Select this check box to update the listed permissions to include properties that are specific to the types of objects that you selected on the previous wizard page. For example, if you selected account objects, any properties that are specific to the account object type, such as **Read adminDescription** and **Write adminDescription**, appear in the permissions list. • **Creation/deletion of specific child objects**. Select this check box to update the listed permissions to include properties that are specific to the creation and deletion of child objects for the object types that you selected on the previous wizard page.
Permissions	You can delegate control by using the check boxes that correspond to each of the available permissions. For example, to delegate full control over the object types that you selected previously in the wizard, select the **Full Control** check box. For more information, see Best practices for assigning permissions on Active Directory objects (http://go.microsoft.com/fwlink/?LinkID=63971).

Question: 23

Your network contains several branch offices. All servers run Windows Server 2008 R2. Each branch office contains a domain controller and a file server. The DHCP Server server role is installed on the branch office domain controllers. Each office has a branch office administrator. You need to delegate the administration of DHCP to meet the following requirements:

- Allow branch office administrators to manage DHCP scopes for their own office
- Prevent the branch office administrators from managing DHCP scopes in other offices
- Minimize administrative effort

What should you do?

A. In the Active Directory domain, add the branch office administrators to the Server Operators builtin local group.
B. In the Active Directory domain, add the branch office administrators to the Network Configuration Operators builtin local group.
C. In each branch office, migrate the DHCP Server server role to the file server. On each file server, add the branch office administrator to the DHCP Administrators local group.
D. In each branch office, migrate the DHCP Server server role to the file server. In the Active Directory domain, add the branch office administrators to the DHCP Administrators domain local group.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd379494%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/dd379483%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/dd379535%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc737716%28WS.10%29.aspx

DHCP Server Migration: Appendix A

Updated: April 29, 2009

Applies To: Windows Server 2008 R2

Migration tools

Migration tools are provided in Windows Server 2008 R2. The tools for earlier versions of the Windows operating system are also available in Windows Server 2008 R2.

Follow these steps to access the tools on the destination server:

1. Open Server Manager.
2. Click **Action**, and then select **Add Features**. The Add Features Wizard opens.
3. On the **Select Features** page, from the **Features** list, select **Windows Server Migration Tools**, and then click **Next**.
4. Complete the steps in the wizard, and then click **Close**.

The previous steps do not work for Server Core installations. To install the migration tools on a Server Core installation, see Windows Server Migration Tools Installation, Access, and Removal (http://go.microsoft.com/fwlink/?LinkID=134763).

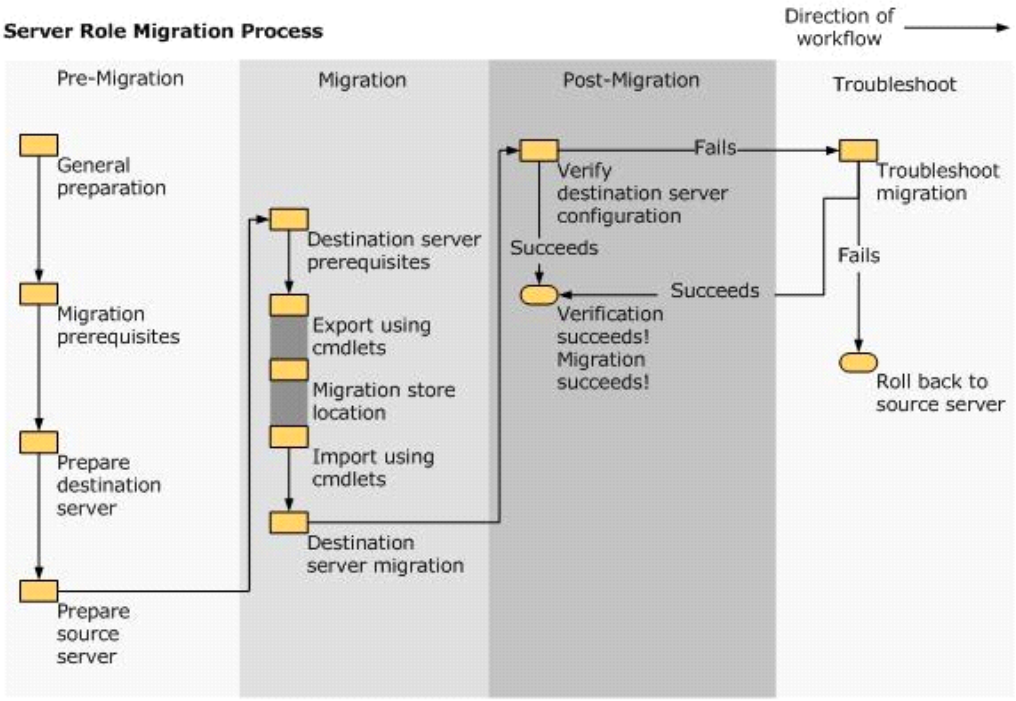
Installing and using Windows PowerShell with migration cmdlets
To access, download, and install migration tools (the migration toolkit), any role-specific tools, and Windows PowerShell, see Windows Server Migration Tools Installation, Access, and Removal (http://go.microsoft.com/fwlink/?LinkID=134763).

Known issues
If the DHCP installation on the source server has a database path that varies from the default, before you perform the import, provide the destination server with a volume with the same drive letter on which the DHCP server database exists on the source server. For example, if the DHCP server database on the source server is located on D:\, then the destination server should have a volume with the driver letter D.

If you cannot match the volume on the destination server that has the same driver letter as that shown for the source DHCP server database, then the DHCP database path on the source server must be changed back to the default path (%systemroot%\system32\dhcp) before you start the migration.

DHCP Server migration process

As shown in the following illustration, the pre-migration process involves the manual collection of data, followed by procedures on the destination and source servers. The migration process includes source and destination server procedures that use the **Export** and **Import** cmdlets to automatically collect, store, and then migrate server role settings. Post-migration procedures include verifying that the destination server successfully replaced the source server and then retiring or repurposing the source server. If the verification procedure indicates that the migration failed, troubleshooting begins. If troubleshooting fails, rollback instructions are provided to return to the use of the original source server.



DHCP Administrators

Members of the DHCP Administrators group can view and modify any data at the DHCP server. DHCP Administrators can create and delete scopes, add reservations, change option values, create superscopes, or perform any other activity needed to administer the DHCP server, including export or import of the DHCP server configuration and database. DHCP Administrators perform these tasks using the Netsh commands for DHCP or the DHCP console. For more information, see DHCP tools.

Members of the DHCP Administrators group do not have unlimited administrative rights. For example, if a DHCP server is also configured as a DNS server, a member of the DHCP Administrators group can view and modify the DHCP configuration but cannot modify DNS server configuration on the same computer.

Because members of the DHCP Administrators group have rights on the local computer only, DHCP Administrators cannot authorize or unauthorize DHCP servers in Active Directory. Only members of the Domain Admins group can perform this task. If you want to authorize or unauthorize a DHCP server in a child domain, you must have enterprise administrator credentials for the parent domain. For more information about authorizing DHCP servers in Active Directory, see Authorizing DHCP servers and Authorize a DHCP server in Active Directory.

Using groups to administer DHCP servers in a domain

When you add a user or group to a DHCP Users or DHCP Administrators group on a DHCP server, the rights of the DHCP group member do not apply to all of the DHCP servers in the domain. The rights apply only to the DHCP service on the local computer.

Question: 24

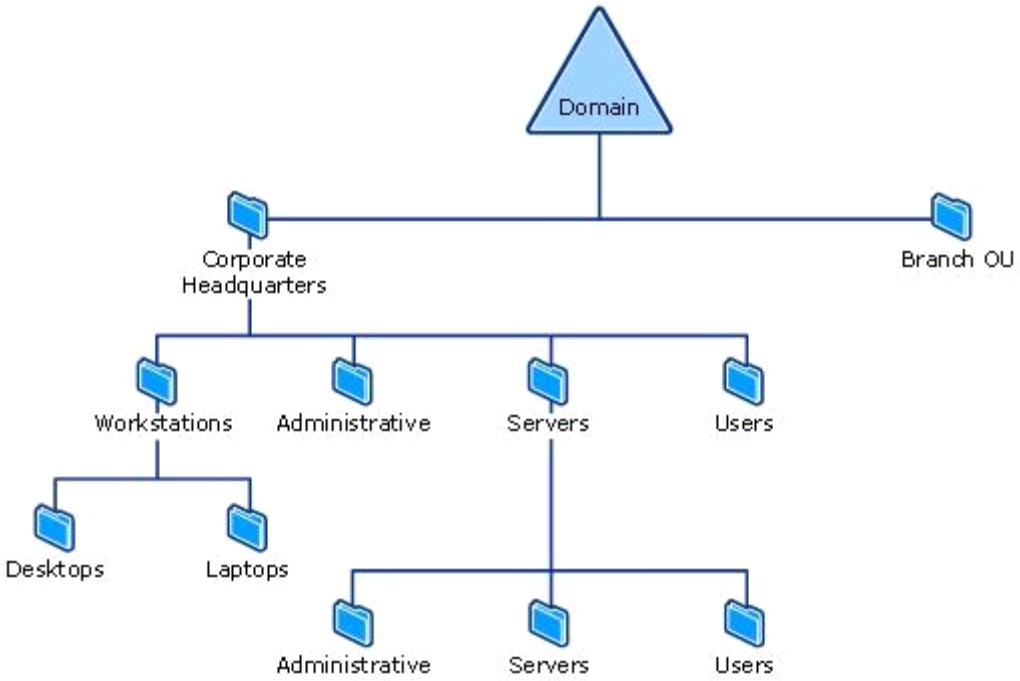
Your company has a single Active Directory domain. You have 30 database servers that run Windows Server 2008 R2. The computer accounts for the database servers are stored in an organizational unit (OU) named Data. The user accounts for the database administrators are stored in an OU named Admin. The database administrators are

members of a global group named D_Admins. You must allow the database administrators to perform administrative tasks on the database servers. You must prevent the database administrators from performing administrative tasks on other servers. What should you do?

A. Deploy a Group Policy to the Data OU.
B. Deploy a Group Policy to the Admin OU.
C. Add D_Admins to the Domain Admins global group.
D. Add D_Admins to the Server Operators built-in local group.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc754948%28WS.10%29.aspx
Group Policy Planning and Deployment Guide
You can use Windows Server 2008 Group Policy to manage configurations for groups of computers and users, including options for registry-based policy settings, security settings, software deployment, scripts, folder redirection, and preferences. Group Policy preferences, new in Windows Server 2008, are more than 20 Group Policy extensions that expand the range of configurable policy settings within a Group Policy object (GPO). In contrast to Group Policy settings, preferences are not enforced. Users can change preferences after initial deployment. For information about Group Policy Preferences, see Group Policy Preferences Overview.
Using Group Policy, you can significantly reduce an organization's total cost of ownership. Various factors, such as the large number of policy settings available, the interaction between multiple policies, and inheritance options, can make Group Policy design complex. By carefully planning, designing, testing, and deploying a solution based on your organization's business requirements, you can provide the standardized functionality, security, and management control that your organization needs.
Overview of Group Policy
Group Policy enables Active Directory–based change and configuration management of user and computer settings on computers running Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP. In addition to using Group Policy to define configurations for groups of users and computers, you can also use Group Policy to help manage server computers, by configuring many server-specific operational and security settings.
By using a structure in which OUs contain homogeneous objects, such as either user or computer objects but not both, you can easily disable those sections of a GPO that do not apply to a particular type of object. This approach to OU design, illustrated in Figure 1, reduces complexity and improves the speed at which Group Policy is applied. Keep in mind that GPOs linked to the higher layers of the OU structure are inherited by default, which reduces the need to duplicate GPOs or to link a GPO to multiple containers.
When designing your Active Directory structure, the most important considerations are ease of administration and delegation.



Question: 25

Your network consists of a single Active Directory forest that contains a root domain and two child domains. All servers run Windows Server 2008 R2. A corporate policy has the following requirements:

- All local guest accounts must be renamed and disabled.
- All local administrator accounts must be renamed.
- You need to recommend a solution that meets the requirements of the corporate policy.

What should you recommend?

A. Implement a Group Policy object (GPO) for each domain.
B. Implement a Group Policy object (GPO) for the root domain.
C. Deploy Network Policy and Access Services (NPAS) on all domain controllers in each domain
D. Deploy Active Directory Rights Management Services (AD RMS) on the root domain controllers.

Answer: A

Explanation:
http://www.windowsecurity.com/articles/protecting-administrator-account.html
http://www.pctips3000.com/enable-or-disable-group-policy-object-in-windows-server-2008/
http://blogs.technet.com/b/chenley/archive/2006/07/13/441642.aspx

In addition to the basic steps that can be performed to protect this account, here are some advanced tricks that you can employ to take the access and security of the Administrator account to a new level.

1. Disable the Administrator account – This is a Group Policy setting which allows you to disable this account within the domain and on local SAMs of Windows XP and Windows Server 2003 computers. The policy is under the following GPO setting:

   Computer Configuration|Windows Settings|Security Settings|Local Policies|Security Options|Accounts: Administrator account status

   This policy setting can be seen in Figure 2, and just needs to be set to Enabled to enforce the setting.

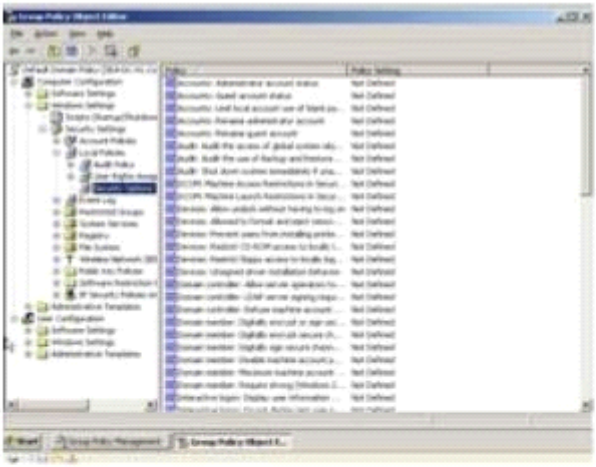
Figure 2: GPO setting that allows you to disable the Administrator account

2. Rename Administrator account using GPOs – It will be hard to disable every Administrator account on every computer due to applications and other requirements. In these cases you can take an easy approach for ensuring the Administrator account is renamed. You can configure the following GPO setting, which can rename the Administrator account on any Windows 2000, XP, or Server 2003 computer.

   Computer Configuration|Windows Settings|Security Settings|Local Policies|Security Options|Accounts: Rename Administrator account

3. Deny "Access this computer from the network" User Right – By default the Administrator account is grouped into the Everyone and Authenticated Users groups, which gives the account the ability to access all computers over the network by default. Since the Administrator account is not being used for routine administration, there is really no need for the account to be accessing any resource, on any server, over the network. If you configure the following Group Policy User Right setting for the Administrator account, it can go a long way to reduce the attack surface that attackers have on the Administrator account.

   Computer Configuration|Windows Settings|Security Settings|Local Policies|User Rights Assignment|Deny access to this computer from the network



Answer: To disable local administrative accounts throughout the domain I would use group policy to accomplish the task. The GPO can be created by using the Computer Policy | Windows Settings | Security Settings | Local policies | Security Options and then using the Accounts:Administrator account status setting. If this setting is GPO is linked to the domain level it can effective disable all of the local admin accounts.

Question: 26

Your network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2008 R2. All domain controllers run Windows Server 2008 R2. A corporate policy requires that the users from the research department have higher levels of account and password security than other users in the domain. You need to recommend a solution that meets the requirements of the corporate policy. Your solution must minimize hardware and software costs. What should you recommend?

A. Create a new Active Directory site. Deploy a Group Policy object (GPO) to the site.
B. Create a new Password Settings Object (PSO) for the research department's users.
C. Create a new organizational unit (OU) named Research in the existing domain. Deploy a Group Policy object (GPO) to the Research OU.
D. Create a new domain in the forest. Add the research department's user accounts to the new domain. Configure a new security policy in the new domain.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc770842%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc754461%28WS.10%29.aspx

- **Exceptional PSOs:** If you want a certain group member to conform to a policy that is different from the policy that is assigned to the entire group, you can assign the exceptional PSO directly to that particular user. If you apply a PSO directly to the user (that is, if you apply it to the group that the user is a member of), it takes precedence over all implicit PSOs that might be linked to it when **msDS-ResultantPSO** for that user is being determined. However, if there are two or more exceptional PSOs that are applied directly to the user object (this is not recommended), the exceptional PSO with the smallest globally unique identifier (GUID) takes precedence.

To create a PSO using ADSI Edit

1. Click **Start**, click **Run**, type **adsiedit.msc**, and then click **OK**.

> **Note**
>
> If you are running ADSI Edit for the first time on a domain controller, proceed to step 2. Otherwise, proceed to step 4.

2. In the ADSI Edit snap-in, right-click **ADSI Edit**, and then click **Connect to**.
3. In **Name**, type the fully qualified domain name (FQDN) of the domain in which you want to create the PSO, and then click **OK**.
4. Double-click the domain.
5. Double-click **DC=<domain_name>**.
6. Double-click **CN=System**.
7. Click **CN=Password Settings Container**.

   All the PSO objects that have been created in the selected domain appear.
8. Right-click **CN=Password Settings Container**, click **New**, and then click **Object**.
9. In the **Create Object** dialog box, under **Select a class**, click **msDS-PasswordSettings**, and then click **Next**.
10. In **Value**, type the name of the new PSO, and then click **Next**.
11. Continue with the wizard, and enter appropriate values for all **mustHave** attributes.

Question: 27

Your network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2008 R2. All servers run Windows Server 2008 R2. A corporate security policy requires complex passwords for user accounts that have administrator privileges. You need to design a strategy that meets the following requirements:

- Ensures that administrators use complex passwords
- Minimizes the number of servers required to support the solution

What should you include in your design?

A. Implement Network Access Protection (NAP).
B. Implement Active Directory Rights Management Services (AD RMS).
C. Create a new Password Settings Object (PSO) for administrator accounts.
D. Create a new child domain in the forest. Move all nonadministrator accounts to the new domain. Configure a complex password policy in the root domain.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc770842%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc754461%28WS.10%29.aspx

- **Exceptional PSOs:** If you want a certain group member to conform to a policy that is different from the policy that is assigned to the entire group, you can assign the exceptional PSO directly to that particular user. If you apply a PSO directly to the user (that is, if you apply it to the group that the user is a member of), it takes precedence over all implicit PSOs that might be linked to it when **msDS-ResultantPSO** for that user is being determined. However, if there are two or more exceptional PSOs that are applied directly to the user object (this is not recommended), the exceptional PSO with the smallest globally unique identifier (GUID) takes precedence.

To create a PSO using ADSI Edit

1. Click **Start**, click **Run**, type **adsiedit.msc**, and then click **OK**.

   Note

   If you are running ADSI Edit for the first time on a domain controller, proceed to step 2. Otherwise, proceed to step 4.

2. In the ADSI Edit snap-in, right-click **ADSI Edit**, and then click **Connect to**.
3. In **Name**, type the fully qualified domain name (FQDN) of the domain in which you want to create the PSO, and then click **OK**.
4. Double-click the domain.
5. Double-click **DC=<domain_name>**.
6. Double-click **CN=System**.
7. Click **CN=Password Settings Container**.

   All the PSO objects that have been created in the selected domain appear.

8. Right-click **CN=Password Settings Container**, click **New**, and then click **Object**.
9. In the **Create Object** dialog box, under **Select a class**, click **msDS-PasswordSettings**, and then click **Next**.
10. In **Value**, type the name of the new PSO, and then click **Next**.
11. Continue with the wizard, and enter appropriate values for all **mustHave** attributes.

Question: 28

Your network consists of a single Active Directory domain. The domain contains three organizational units (OUs) named Test, Application, and Database. You need to redesign the layout of the OUs to support the following requirements:
- Prevent Group Policy objects (GPOs) that are linked to the domain from applying to computers located in the Applications OU
- Minimize the number of GPOs
- Minimize the number of Ous
What should you include in your design?

A. Create a Starter GPO.
B. Create a Windows Management Instrumentation (WMI) filter.
C. Delegate permissions on the Application OU.
D. Configure block inheritance on the Application OU.

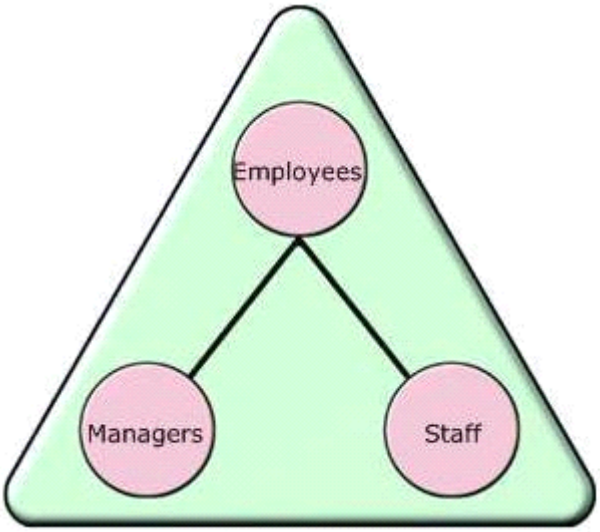
Answer: D

Explanation:
Understanding Group Policy
You already know that Group Policy settings contained in Group Policy objects (GPOs) can be linked to OUs, and that OUs can either inherit settings from parent OUs or block inheritance and obtain their specific settings from their own linked GPOs. You also know that some policies—specifically, security policies—can be set to “no override” so that they cannot be blocked or overwritten and force child OUs to inherit the settings from their parents.

Question: 29

Your network consists of a single Active Directory domain. The relevant portion of the Active Directory domain is

configured as shown in the following diagram.



The Staff organizational unit (OU) contains all user accounts except for the managers' user accounts. The Managers OU contains the managers' user accounts and the following global groups:

- Sales
- Finance
- Engineering

You create a new Group Policy object (GPO) named GPO1, and then link it to the Employees OU.
Users from the Engineering global group report that they are unable to access the Run command on the Start menu. You discover that the GPO1 settings are causing the issue. You need to ensure that the users from the Engineering global group are able to access the Run command on the Start menu. What should you do?

A. Configure GPO1 to use the Enforce Policy option.
B. Configure Block Inheritance on the Managers OU.
C. Configure Group Policy filtering on GPO1 for the Engineering global group.
D. Create a new child OU named Engineering under the Employees OU. Move the Engineering global group to the new Engineering child OU.

Answer: C

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration.
No administrator likes exceptions, but we are required to implement them. Typically you might have configured security filtering, Windows Management Instrumentation (WMI) filters, block inheritance settings, no-override settings, loopback processing, and slow-link settings. You need to check that these settings are not affecting normal GPO processing.

Question: 30

Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. You need to recommend a Group Policy deployment strategy. Your strategy must support the following requirements:

- Domainlevel Group Policy objects (GPOs) must not be overwritten by organizational unit (OU) level GPOs.
- OUlevel GPOs must not Apply to members of the Server Operators group.

What should you recommend?

A. Enable Block Inheritance for the domain, and then modify the permissions of all GPOs linked to OUs.

B. Enable Block Inheritance for the domain, and then enable Loopback Processing policy mode. Add the Server Operators group to the Restricted Groups list.
C. Set all domain level GPOs to Enforced, and then modify the permissions of the GPOs that are linked to OUs.
D. Set all domain level GPOs to Enforced, and then enable Loopback Processing policy mode. Add the Server Operators group to the Restricted Groups list.

Answer: C

Explanation:
http://www.petri.co.il/working_with_group_policy.htm
http://technet.microsoft.com/en-us/library/bb742376.aspx

GPO behavior

Group Policy is processed in the following order:

Local Policy > Site GPO > Domain GPO > OU GPO > Child OU GPO

and so on.

GPOs inherited from the Active Directory are always stronger than local policy. When you configure a Site policy it is being overridden by Domain policy, and Domain policy is being overridden by OU policy. If there is an OU under the previous OU, its GPO is stronger the previous one.

The rule is simple, as more you get closer to the object that is being configured, the GPO is stronger.

What does it mean "stronger"? If you configure a GPO and linke it to "Organization" OU, and in it you configure Printer installation – allowed and then at the "Dallas" OU you configured other GPO but do not allow printer installation, then the Dallas GPO is more powerful and the computers in it will not allow installation of printers.

The example above is true when you have different GPOs that have similar configuration, configured with opposite settings. When you apply couple of GPOs at different levels and every GPO has its own settings, all settings from all GPOs are merged and inherited by the computers or users.

Linking a GPO to Multiple Sites, Domains, and OUs
This section demonstrates how you can link a GPO to more than one container (site, domain, or OU) in the Active Directory. Depending on the exact OU configuration, you can use other methods to achieve similar Group Policy effects; for example, you can use security group filtering or you can block inheritance. In some cases, however, those methods do not have the desired affects. Whenever you need to explicitly state which sites, domains, or OUs need the same set of policies, use the method outlined below:
To link a GPO to multiple sites, domains, and OUs
1. Open the saved MMC console GPWalkthrough, and then double-click the Active Directory User and Computers node.
2. Double-click the reskit.com domain, and double-click the Accounts OU.
3. Right-click the Headquarters OU, select Properties from the context menu, and then click the Group Policy tab.
4. In the Headquarters Properties dialog box, on the Group Policy tab, click New to create a new GPO named Linked Policies.
5. Select the Linked Policies GPO, and click the Edit button.
6. In the Group Policy snap-in, in the User Configuration node, under Administrative Templates node, click Control Panel, and then click Display.
7. On the details pane, click the Disable Changing Wallpaper policy, and then click Enabled in the Disable Changing

Wallpaper dialog box and click OK.
8. Click Close to exit the Group Policy snap-in.
9. In the Headquarters Properties page, click Close.
Next you will link the Linked Policies GPO to another OU.
1. In the GPWalkthrough console, double-click the Active Directory User and Computers node, double-click the reskit.com domain, and then double-click the Accounts OU.
2. Right-click the Production OU, click Properties on the context menu, and then click the Group Policy tab on the Production Properties dialog box.
3. Click the Add button, or right-click the blank area of the Group Policy objects links list, and select Add on the context menu.
4. In the Add a Group Policy Object Link dialog box, click the down arrow on the Look in box, and select the Accounts.reskit.com OU.
5. Double-click the Headquarters.Accounts.reskit.com OU from the Domains, OUs, and linked Group Policy objects list.
6. Click the Linked Policies GPO, and then click OK.
You have now linked a single GPO to two OUs. Changes made to the GPO in either location result in a change for both OUs. You can test this by changing some policies in the Linked Policies GPO, and then logging onto a client in each of the affected OUs, Headquarters and Production.

Question: 31

Your network consists of three Active Directory forests. Forest trust relationships exist between all forests. Each forest contains one domain. All domain controllers run Windows Server 2008 R2. Your company has three network administrators. Each network administrator manages a forest and the Group Policy objects (GPOs) within that forest. You need to create standard GPOs that the network administrators in each forest will use. The GPOs must meet the following requirements:

- The GPOs must only contain settings for either user configurations or computer configurations.
- The number of GPOs must be minimized.

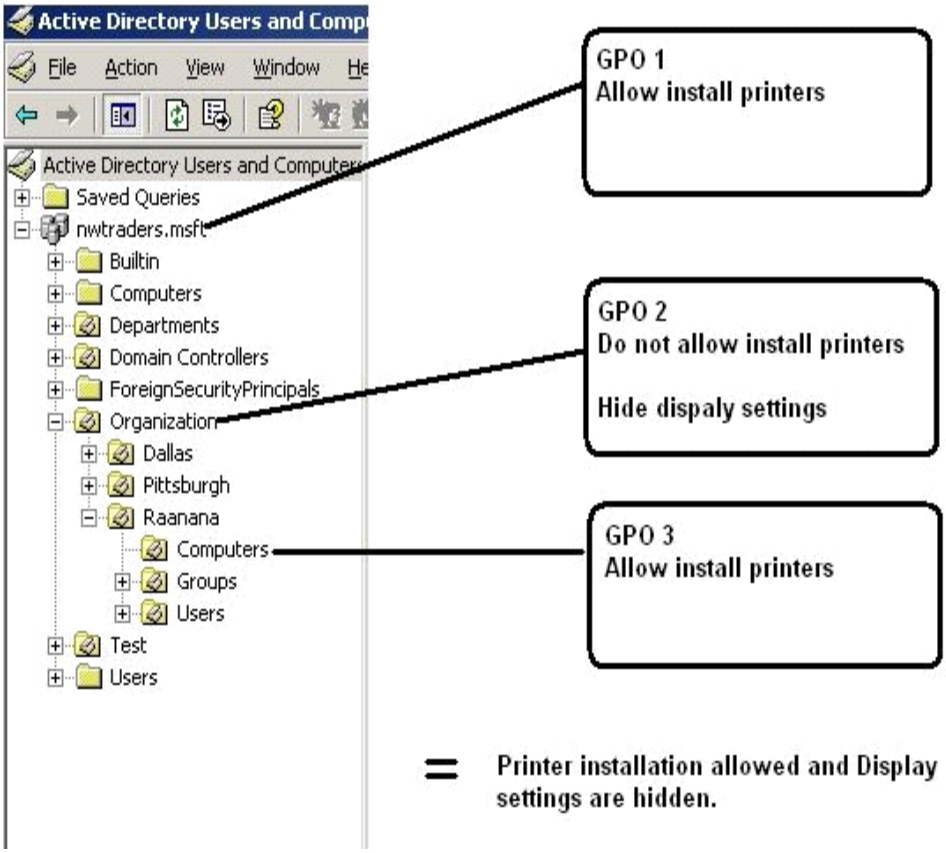
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Export the new GPOs to .cab files. Ensure that the .cab files are available to the network administrator in each forest.
B. Create two new GPOs. Configure both GPOs to use the required user configurations and the required computer configurations.
C. Create two new GPOs. Configure one GPO to use the required user configuration. Configure the other GPO to use the required computer configuration.
D. Back up the Sysvol folder that is located on the domain controller where the new GPOs were created. Provide the backup to the network administrator in each forest.

Answer: A, C

Explanation:
http://technet.microsoft.com/en-us/library/ee390958.aspx
http://www.petri.co.il/working_with_group_policy.htm
Export a GPO to a File
Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2
You can export a controlled Group Policy object (GPO) to a CAB file so that you can copy it to a domain in another forest and import the GPO into Advanced Group Policy Management (AGPM) in that domain. For information about how to import GPO settings into a new or existing GPO, see Import a GPO from a File.
A user account with the Editor or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management (AGPM) is required to complete this procedure. Review the details in "Additional considerations"

in this topic.
To export a GPO to a file
1. In the Group Policy Management Console tree, click Change Control in the forest and domain in which you want to manage GPOs.
2. On the Contents tab, click the Controlled tab to display the controlled GPOs.
3. Right-click the GPO, and then click Export to.
4. Enter a file name for the file to which you want to export the GPO, and then click Export. If the file does not exist, it is created. If it already exists, it is replaced.
Additional considerations
• By default, you must be an Editor or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have List Contents, Read Settings, and Export GPO permissions for the GPO.
Group Policy sections
Each GPO is built from 2 sections:
• Computer configuration contains the settings that configure the computer prior to the user logon combo-box.
• User configuration contains the settings that configure the user after the logon. You cannot choose to apply the setting on a single user, all users, including administrator, are affected by the settings.



Question: 32

Your company has a branch office that contains a Windows Server 2008 R2 computer. The Windows Server 2008 R2 computer runs Windows Server Update Services (WSUS). The WSUS server is configured to store updates locally. The company opens four new satellite offices. Each satellite office connects to the branch office by using a dedicated WAN link. Internet access is provided through the branch office. You need to design a strategy for patch management that meets the following requirements:

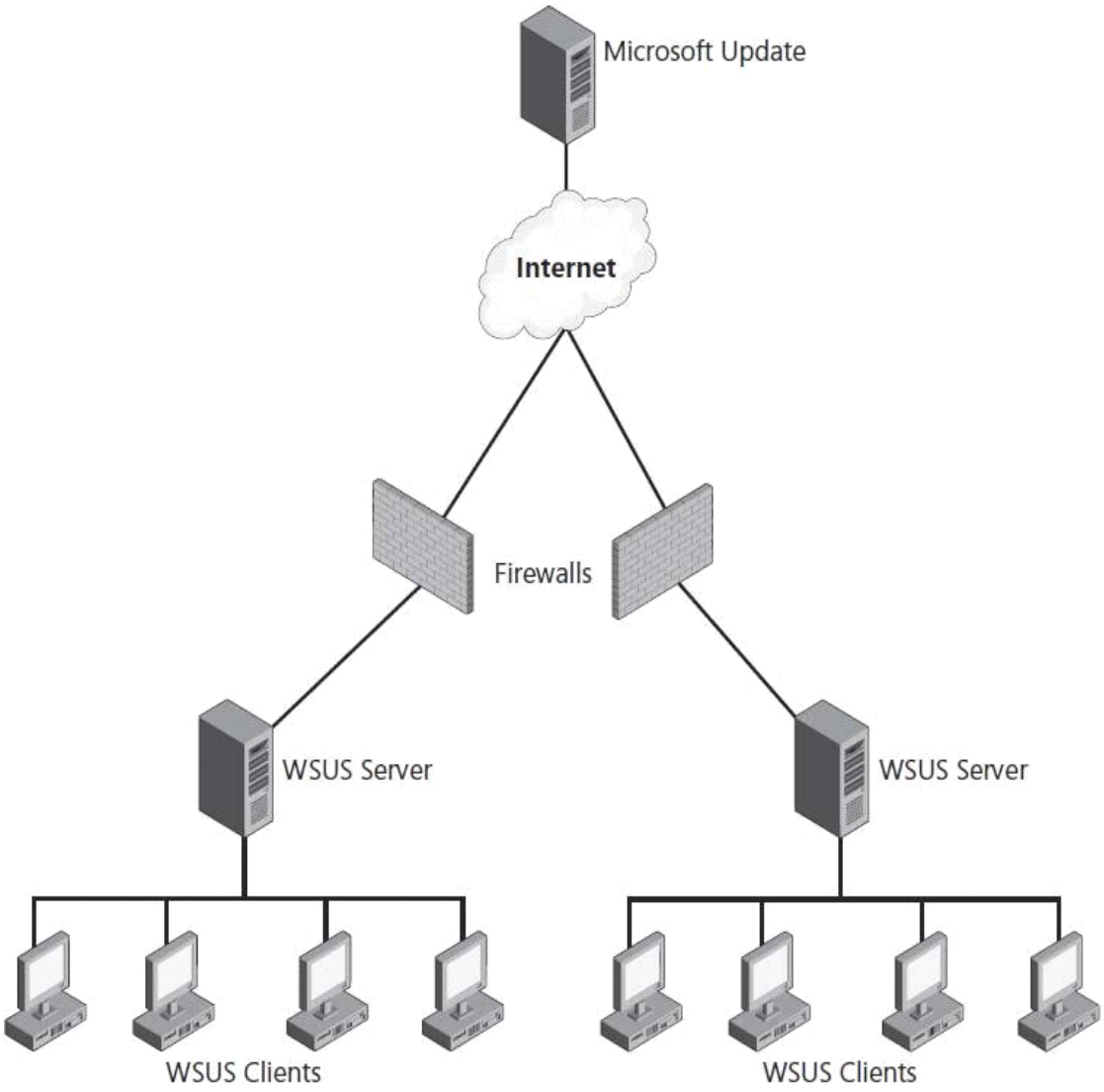
- WSUS updates are approved independently for each satellite office.
- Internet traffic is minimized.

What should you include in your design?

A. In each satellite office, install a WSUS server. Configure each satellite office WSUS server as an autonomous server.
B. In each satellite office, install a WSUS server. Configure each satellite office WSUS server as a replica of the branch office WSUS server.
C. In each satellite office, install a WSUS server. Configure each satellite office WSUS server to use the branch office WSUS server as an upstream server.
D. For each satellite office, create organizational units (OUs). Create and link the Group Policy objects (GPOs) to the OUs. Configure different schedules to download updates from the branch office WSUS server to the client computers in each satellite office.

Answer: C

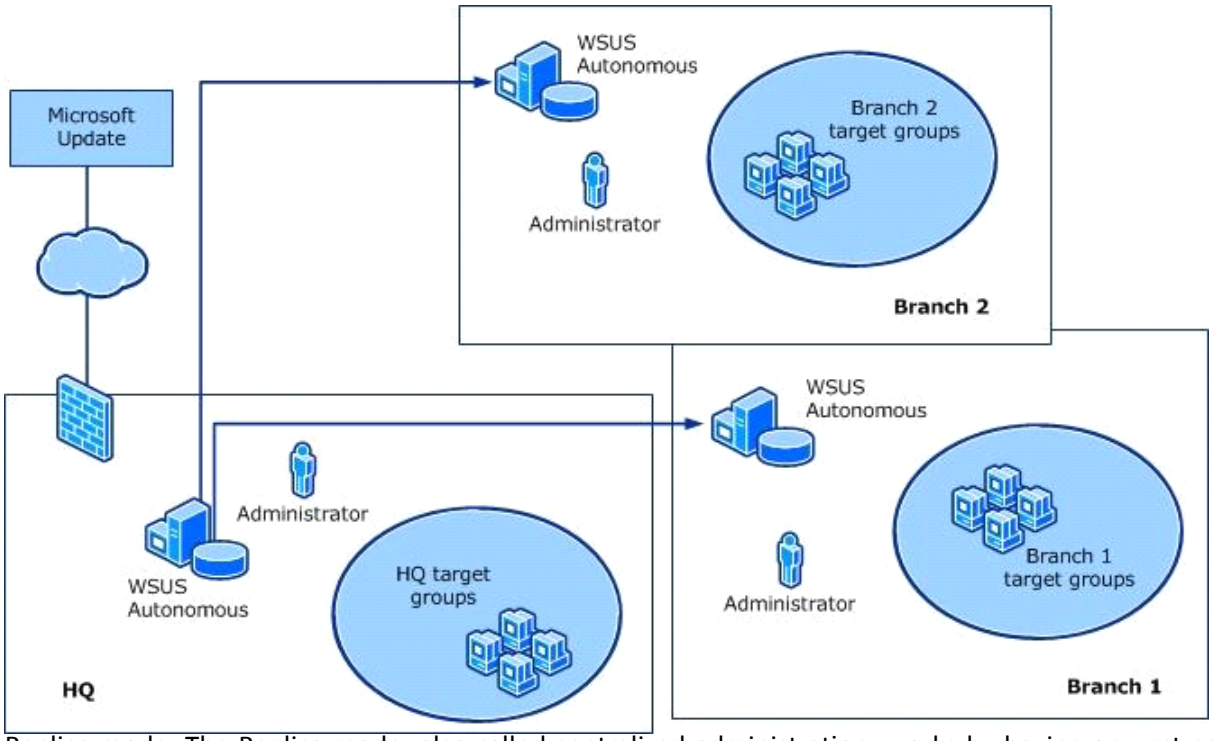
Explanation:
http://technet.microsoft.com/en-us/library/hh852344.aspx
In addition, a Windows Server 2008 server running WSUS server can act as an upstream server—an update source for other WSUS servers within your organization. At least one WSUS server in your network must connect to the Microsoft Update Web site to get available update information. How many other servers connect directly to Microsoft Update is something you need to determine as part of your planning process, and depends upon network configuration and security requirements.



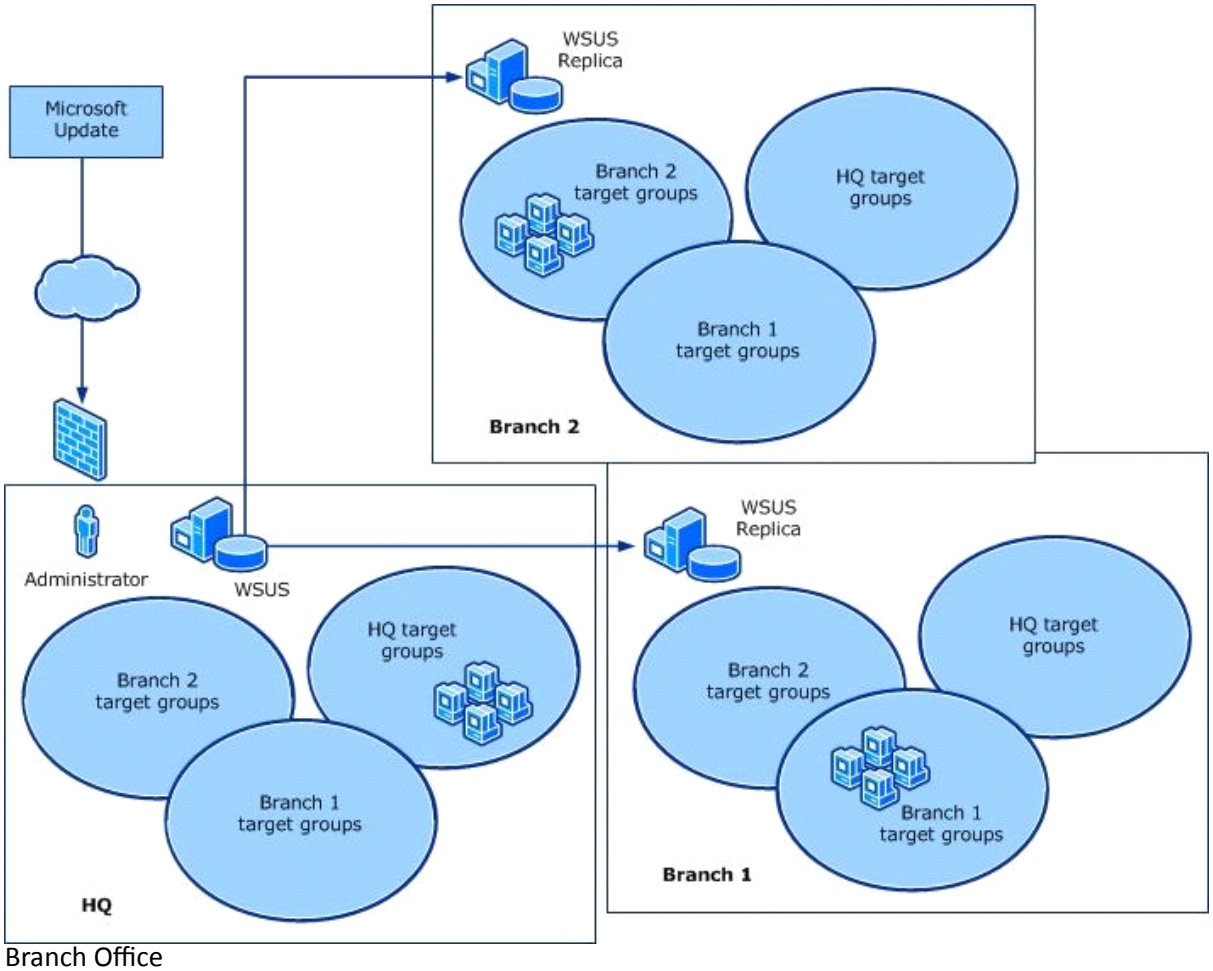
In this deployment model, the WSUS server that receives updates from the Microsoft Update server is designated as

the upstream server. A WSUS server that retrieves updates from another WSUS server is designated as a downstream server.

Autonomous mode: The Autonomous mode, also called distributed administration, is the default installation option for WSUS. In Autonomous mode, an upstream WSUS server shares updates with downstream servers during synchronization. Downstream WSUS servers are administered separately, and they do not receive update approval status or computer group information from the upstream server. By using the distributed management model, each WSUS server administrator selects update languages, creates computer groups, assigns computers to groups, tests and approves updates, and makes sure that the correct updates are installed to the appropriate computer groups. The following image shows how you might deploy autonomous WSUS servers in a branch office environment:



Replica mode: The Replica mode, also called centralized administration, works by having an upstream WSUS server that shares updates, approval status, and computer groups with downstream servers. Replica servers inherit update approvals and are not administered separately from the upstream WSUS server. The following image shows how you might deploy replica WSUS servers in a branch office environment.



Branch Office

You can leverage the Branch Office feature in Windows to optimize WSUS deployment. This type of deployment offers the following advantages:

Helps reduce WAN link utilization and improves application responsiveness. To enable BranchCache acceleration of content that is served by the WSUS server, install the BranchCache feature on the server and the clients, and ensure that the BranchCache service has started. No other steps are necessary.

In branch offices that have low-bandwidth connections to the central office but high-bandwidth connections to the Internet, the Branch Office feature can also be used. In this case you may want to configure downstream WSUS servers to get information about which updates to install from the central WSUS server, but download the updates from Microsoft Update.

Question: 33

Your network contains several Windows Server 2008 R2 servers that run Windows Server Update Services (WSUS). The WSUS servers distribute updates to all computers on the internal network. Remote users connect from their personal computers to the internal network by using a splittunnel VPN connection. You need to plan a strategy for patch management that deploys updates on the remote users' computers. Your strategy must meet the following requirements:

- Minimize bandwidth use over the VPN connections
- Require updates to be approved on the WSUS servers before they are installed on the client computers.

What should you include in your plan?

A. Create a Group Policy object (GPO) to perform clientside targeting.

B. Create a computer group for the remote users' computers. Configure the remote users' computers to use the internal WSUS server.

C. Create a custom connection by using the Connection Manager Administration Kit (CMAK). Deploy the custom connection to all of the remote users' computers.
D. Deploy an additional WSUS server. Configure the remote users' computers to use the additional WSUS server. Configure the additional WSUS server to leave the updates on the Microsoft Update Web site.

Answer: D

Explanation:
Performance and Bandwidth Optimization
Branch offices with slow WAN connections to the central server but broadband connections to the Internet can be configured to get metadata from the central server and update content from the Microsoft Update Web site.

Question: 34

Your company has a branch office that contains a Windows Server 2008 R2 server. The server runs Windows Server Update Services (WSUS). The company opens four new satellite offices. Each satellite office connects to the branch office by using a dedicated WAN link. You need to design a strategy for patch management that meets the following requirements:

- WSUS updates are approved from a central location.
- WAN traffic is minimized between the branch office and the satellite offices.

What should you include in your design?

A. In each satellite office, install a WSUS server. Configure each satellite office WSUS server as a replica of the branch office WSUS server.
B. In each satellite office, install a WSUS server. Configure each satellite office WSUS server as an autonomous server that synchronizes to the branch office WSUS server.
C. On the branch office WSUS server, create a computer group for each satellite office. Add the client computers in each satellite office to their respective computer groups.
D. For each satellite office, create an organizational unit (OU). Create and link a Group Policy object (GPO) to each OU. Configure different schedules to download updates from the branch office WSUS server to the client computers in each satellite office.

Answer: A

Explanation:
Replica Mode and Autonomous Mode
You have two options when configuring the administration model for your organization’s downstream WSUS servers. The first option, shown in Figure 8-5, is to configure the downstream WSUS server as a replica of the upstream server. When you configure a WSUS server as a replica, all approvals, settings, computers, and groups from the upstream server are used on the downstream server. The downstream server cannot be used to approve updates when configured in replica mode, though you can change a replica server to the second mode—called autonomous mode—if an update urgently needs to be deployed.

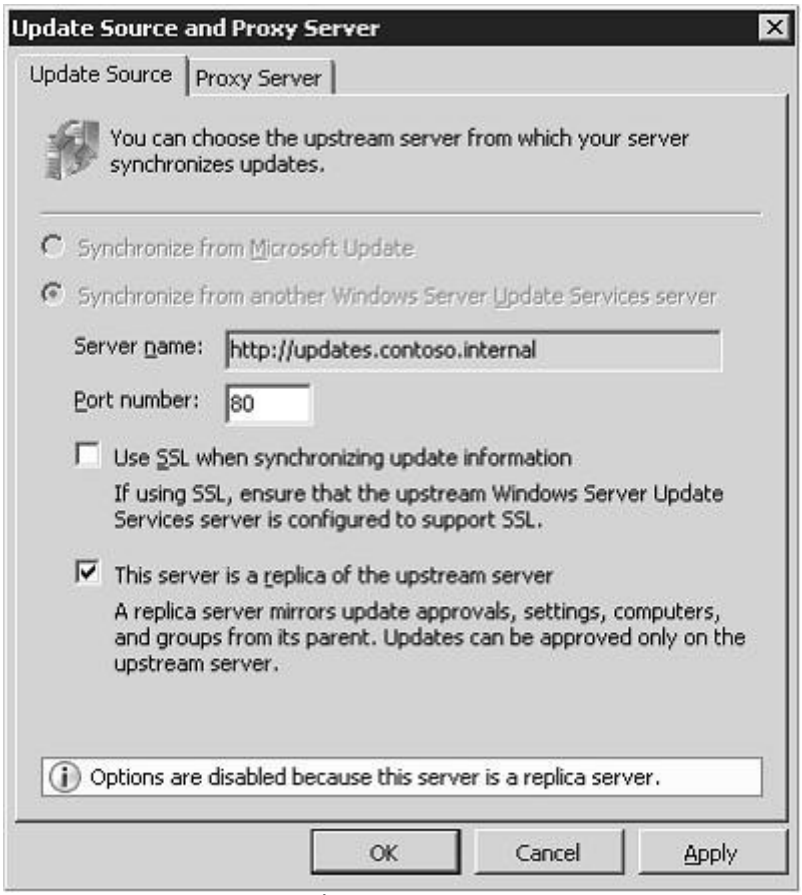


Figure 8-5Downstream replica server

Question: 35

You need to design a Windows Server Update Services (WSUS) infrastructure that meets the following requirements:
·The updates must be distributed from a central location.
·All computers must continue to receive updates in the event that a server fails.
What should you include in your design?

A. Configure two WSUS servers in a Microsoft SQL Server 2008 failover cluster. Configure each WSUS server to use a local database.
B. Configure a single WSUS server to use multiple downstream servers. Configure each WSUS server to use a RAID 1 mirror and a local database.
C. Configure a single WSUS server to use multiple downstream servers. Configure each WSUS server to use a RAID 5 array and a local database.
D. Configure a Microsoft SQL Server 2008 failover cluster. Configure two WSUS servers in a Network Load Balancing cluster. Configure WSUS to use the remote SQL Server 2008 database instance.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/dd939812(v=WS.10).aspx
WSUS database
WSUS 3.0 SP2 requires a database for each WSUS server. WSUS supports the use of a database that resides on a different computer than the WSUS server, with some restrictions. For a list of supported databases and remote database limitations, see WSUS database requirements.

The WSUS database stores the following information:
• WSUS server configuration information
• Metadata that describes each update
• Information about client computers, updates, and interactions
If you install multiple WSUS servers, you must maintain a separate database for each WSUS server, whether it is an autonomous or a replica server. (For more information about WSUS server types, see Design the WSUS Server Layout.) You cannot store multiple WSUS databases on a single instance of SQL Server, except in Network Load Balancing (NLB) clusters that use SQL Server failover. For more about this configuration, see
Configure WSUS for Network Load Balancing.
SQL Server, SQL Server Express, and Windows Internal Database provide the same performance characteristics for a single server configuration, where the database and the WSUS service are located on the same computer. A single server configuration can support several thousand WSUS client computers.
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 ClusteringFailover 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: 36

Your network consists of a single Active Directory forest. The sales department in your company has 600 Windows Server 2008 R2 servers. You need to recommend a solution to monitor the performance of the 600 servers. Your solution must meet the following requirements:
- Generate alerts when the average processor usage is higher than 90 percent for 20 minutes.
- Automatically adjust the processor monitoring threshold to allow for temporary changes in the workload.

What should you recommend?

A. Install Windows System Resource Manager (WSRM) on each server.
B. Deploy Microsoft System Center Operations Manager (OpsMgr).
C. Deploy Microsoft System Center Configuration Manager (SysMgr).
D. Configure Reliability and Performance Monitor on each server

Answer: B

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Microsoft System Center Operations Manager 2007
When planning the centralized monitoring and management of large numbers of Windows Server 2008 computers, you should consider implementing Microsoft System Center Operations Manager 2007. System
Center Operations Manager 2007 was touched on briefly during Chapter 4, “Application Servers and Services.”Microsoft System Center Operations Manager 2007 allows you to centrally manage and monitor thousands of servers and applications and provides a complete overview of the health of your network environment. System Center Operations Manager 2007 is the most recent version of Microsoft Operations Manager 2005 (MOM). System Center Operations Manager 2007 provides the following features:
■Proactive alerts that recognize conditions that are likely to lead to failure of critical services, applications, and

servers in the future
■The ability to configure tasks to automatically execute to resolve problems when given events occur
■The collection of long-term trend data from all servers and applications across the organization with the ability to generate comparison reports against current performance
■ Correlation of auditing data generated across the organization, allowing the detection of trends that might not be apparent when examining server auditing data in isolation

Question: 37

Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. A server named Server1 has the Remote Desktop Services server role installed. You notice that several users consume more than 30 percent of the CPU resources throughout the day. You need to prevent users from consuming more than 15 percent of the CPU resources. Administrators must not be limited by the amount of CPU resources that they can consume. What should you do?

A. Implement Windows System Resource Manager (WSRM), and configure user policies.
B. Implement Windows System Resource Manager (WSRM), and configure session policies.
C. Configure Performance Monitor, and create a userdefined Data Collector Set.
D. Configure Performance Monitor, and create an Event Trace Session Data Collector Set.

Answer: A

Explanation:
You can use tools such as the Windows System Resource Manager and Performance Monitor to determine memory and processor usage of Terminal Services clients. Once you understand how the Terminal Server's resources are used, you can determine the necessary hardware resources and make a good estimate as to the Terminal Server's overall client capacity. Terminal Server capacity directly influences your deployment plans: A server that has a capacity of 100 clients is not going to perform well when more than 250 clients attempt to connect. Monitoring tools are covered in more detail in "Monitoring Terminal Services" later in this lesson.

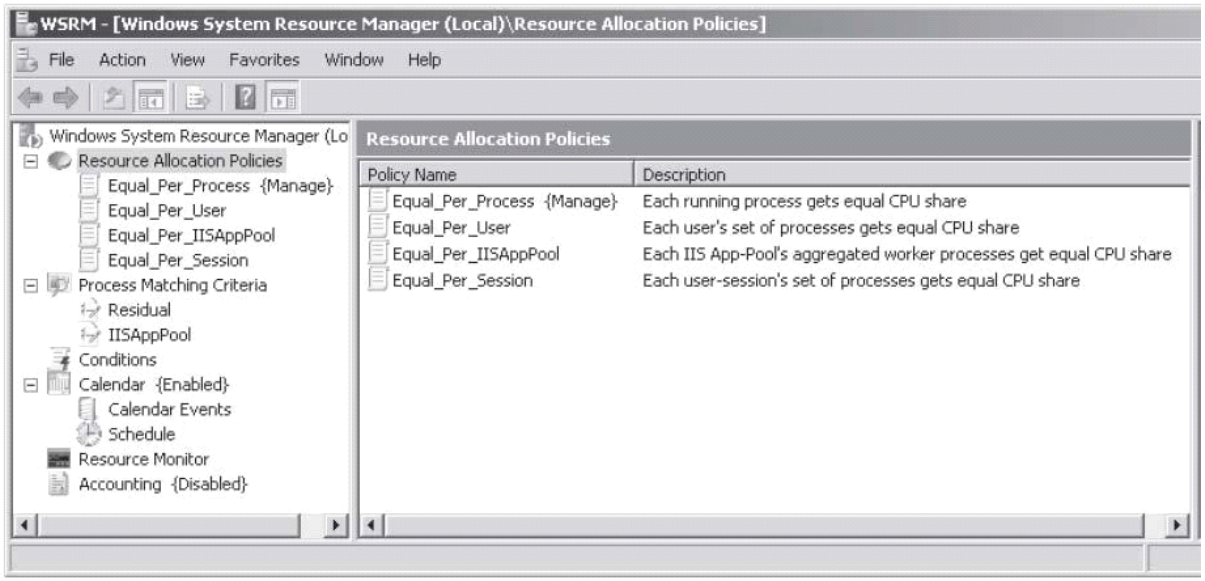


Figure 5-9 The WSRM console

Windows System Resource Manager
Windows System Resource Manager (WSRM) is a feature that you can install on a Windows Server 2008 computer that controls how resources are allocated. The WSRM console, shown in Figure 5-9, allows an administrator to apply

WSRM policies. WSRM includes four default policies and also allows administrators to create their own. The two policies that will most interest you as someone responsible for planning and deploying Terminal Services infrastructure are Equal_Per_User and Equal_Per_Session.
The Equal_Per_User WSRM policy ensures that each user is allocated resources equally, even when one user has more sessions connected to the Terminal Server than other users. Apply this policy when you allow users to have multiple sessions to the Terminal Server—it stops any one user from monopolizing hardware resources by opening multiple sessions. The Equal_Per_Session policy ensures that each session is allocated resources equally. If applied on a Terminal Server where users are allowed to connect with multiple sessions, this policy can allow those users to gain access to a disproportionate amount of system resources in comparison to users with single sessions.

Question: 38

Your network contains a standalone root certification authority (CA). You have a server named Server1 that runs Windows Server 2008 R2. You issue a server certificate to Server1. You deploy Secure Socket Tunneling Protocol (SSTP) on Server1. You need to recommend a solution that allows external partner computers to access internal network resources by using SSTP. What should you recommend?

A. Enable Network Access Protection (NAP) on the network.
B. Deploy the Root CA certificate to the external computers.
C. Implement the Remote Desktop Connection Broker role service.
D. Configure the firewall to allow inbound traffic on TCP Port 1723.

Answer: B

Explanation:
Lesson 1: Configuring Active Directory Certificate Services
Certificate Authorities are becoming as integral to an organization's network infrastructure as domain controllers, DNS, and DHCP servers. You should spend at least as much time planning the deployment of Certificate Services in your organization's Active Directory environment as you spend planning the deployment of these other infrastructure servers. In this lesson, you will learn how certificate templates impact the issuance of digital certificates, how to configure certificates to be automatically assigned to users, and how to configure supporting technologies such as Online Responders and credential roaming. Learning how to use these technologies will smooth the integration of certificates into your organization's Windows Server 2008 environment.
After this lesson, you will be able to:
Install and manage Active Directory Certificate Services.■
■ Configure autoenrollment for certificates.
■ Configure credential roaming.
■ Configure an Online Responder for Certificate Services.
Estimated lesson time: 40 minutes
Types of Certificate Authority
When planning the deployment of Certificate Services in your network environment, you must decide which type of Certificate Authority best meets your organizational requirements. There are four types of Certificate Authority (CA):
■Enterprise Root
■Enterprise Subordinate
■Standalone Root
■Standalone Subordinate
The type of CA you deploy depends on how certificates will be used in your environment and the state of the existing environment. You have to choose between an Enterprise or a Standalone CA during the installation of the Certificate Services role, as shown in Figure 10-1. You cannot switch between any of the CA types after the
CA has been deployed.

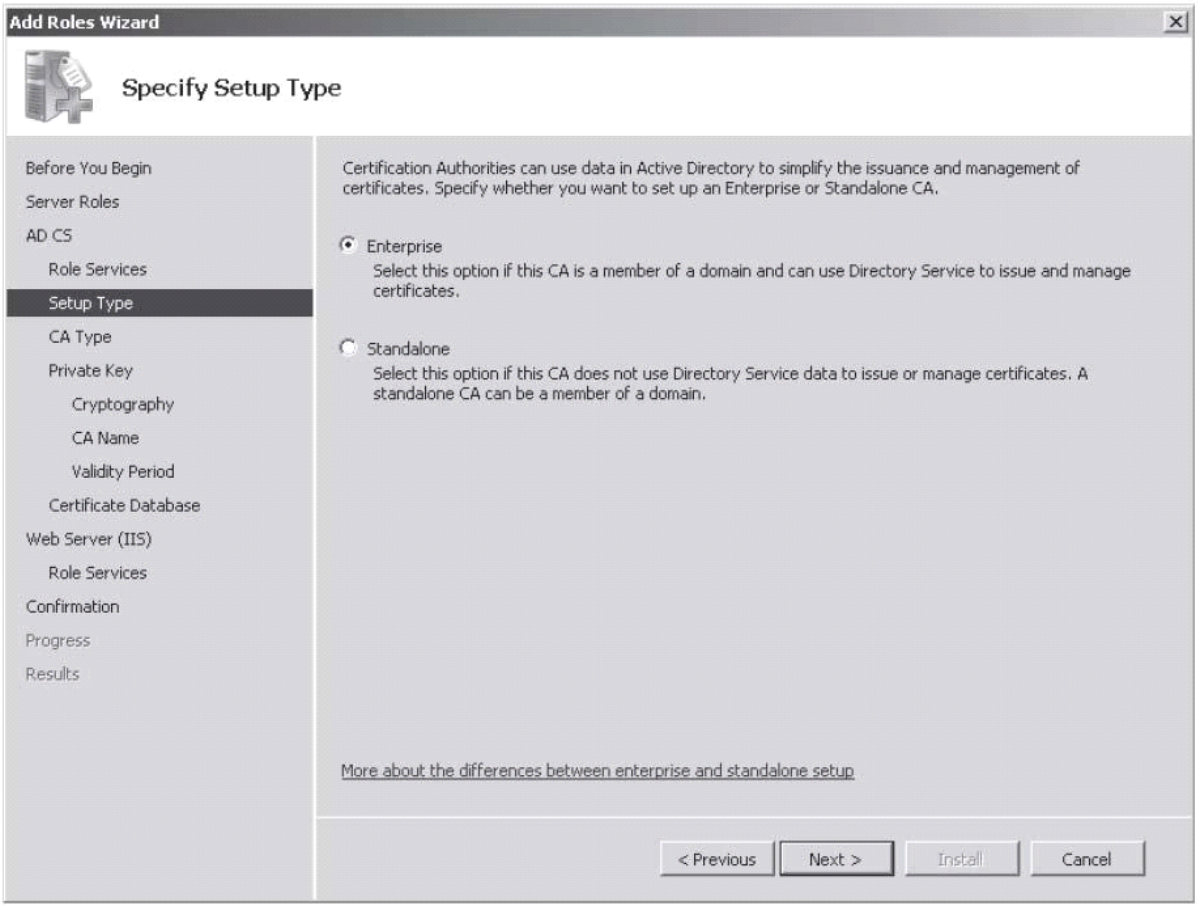


Figure 10-1Selecting an Enterprise or Standalone CA

Enterprise CAs require access to Active Directory. This type of CA uses Group Policy to propagate the certificate trust lists to users and computers throughout the domain and publish certificate revocation lists to Active Directory. Enterprise CAs issue certificates from certificate templates, which allow the following functionality:

■Enterprise CAs enforce credential checks on users during the certificate enrollment process. Each certificate template has a set of security permissions that determine whether a particular user is authorized to receive certificates generated from that template.

■ Certificate names are automatically generated from information stored within Active Directory. The method by which this is done is determined by certificate template configuration.

■ Autoenrollment can be used to issue certificates from Enterprise CAs, vastly simplifying the certificate distribution process. Autoenrollment is configured through applying certificate template permissions.

In essence, Enterprise CAs are fully integrated into a Windows Server 2008 environment. This type of CA makes the issuing and management of certificates for Active Directory clients as simple as possible.

Standalone CAs do not require Active Directory. When certificate requests are submitted to Standalone CAs, the requestor must provide all relevant identifying information and manually specify the type of certificate needed. This process occurs automatically with an Enterprise CA. By default, Standalone CA requests require administrator approval. Administrator intervention is necessary because there is no automated method of verifying a requestor's credentials. Standalone CAs do not use certificate templates, limiting the ability for administrators to customize certificates for specific organizational needs.

You can deploy Standalone CAs on computers that are members of the domain. When installed by a user that is a member of the Domain Admins group, or one who has been delegated similar rights, the Standalone CA's information will be added to the Trusted Root Certificate Authorities certificate store for all users and computers in the domain. The CA will also be able to publish its certificate revocation list to Active Directory.

Whether you install a Root or Subordinate CA depends on whether there is an existing certificate infrastructure.

Root CAs are the most trusted type of CA in an organization's public key infrastructure (PKI) hierarchy. Root CAs sit at the top of the hierarchy as the ultimate point of trust and hence must be as secure as possible. In many environments,

a Root CA is only used to issue signing certificates to Subordinate CAs. When not used for this purpose, Root CAs are kept offline in secure environments as a method of reducing the chance that they might be compromised.
If a Root CA is compromised, all certificates within an organization's PKI infrastructure should be considered compromised. Digital certificates are ultimately statements of trust. If you cannot trust the ultimate authority from which that trust is derived, it follows that you should not trust any of the certificates downstream from that ultimate authority.
Subordinate CAs are the network infrastructure servers that you should deploy to issue the everyday certificates needed by computers, users, and services. An organization can have many Subordinate CAs, each of which is issued a signing certificate by the Root CA. In the event that one Subordinate CA is compromised, trust of that CA can be revoked from the Root CA. Only the certificates that were issued by that CA will be considered untrustworthy. You can replace the compromised Subordinate CA without having to replace the entire organization's certificate infrastructure. Subordinate CAs can be replaced, but a compromised Enterprise Root CA usually means you have to redeploy the Active Directory forest from scratch. If a Standalone Root CA is compromised, it also necessitates the replacement of an organization's PKI infrastructure.

Question: 39

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. You need to plan an auditing strategy that meets the following requirements:

- Audits all changes to Active Directory Domain Services (AD DS)
- Stores all auditing data in a central location

What should you include in your plan?

A. Configure an audit policy for the domain. Configure Event Forwarding.
B. Configure an audit policy for the domain controllers. Configure Data Collector Sets.
C. Implement Windows Server Resource Manager (WSRM) in managing mode.
D. Implement Windows Server Resource Manager (WSRM) in accounting mode.

Answer: A

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
The configuration of a subscription filter is more like the configuration of a custom view in that you are able to specify multiple event log sources, rather than just a single Event Log source. In addition, the subscription will be saved whereas you need to re-create a filter each time you use one. By default, all collected Event Log data will be written to the Forwarded Event Event Log. You can forward data to other logs by configuring the properties of the subscription. Even though you use a filter to retrieve only specific events from source computers and place them in the destination log, you can still create and apply a custom view to data that is located in the destination log. You could create a custom view for each source computer, which would allow you to quickly limit events to that computer rather than viewing data from all source computers at the same time.
You configure collector initiated subscriptions through the application of Group Policy. To do this you must configure the collector computer in the same manner as you did in the previous steps. When configuring the subscription type, select Source Computer Initiated rather than Collector Initiated. To set up the source computers, apply a GPO where you have configured the Computer Configuration\Policies\AdministrativeTemplates\Windows Components\Event Forwarding node and configure the Server Address, Refresh Interval, And Issuer Certificate policy with the details of the collector computer, as shown in Figure 7-10.
■ Auditing enhancements You can use the new Directory Service Changes audit policy subcategory when auditing Windows Server 2008 AD DS. This lets you log old and new values when changes are made to AD DS objects and their attributes. You can also use this new feature when auditing Active Directory Lightweight Directory Services (AD LDS).
Planning AD DS Auditing
In Windows Server 2008, the global audit policy Audit Directory Service Access is enabled by default. This policy

controls whether auditing for directory service events is enabled or disabled. If you configure this policy setting by modifying the Default Domain Controllers Policy, you can specify whether to audit successes, audit failures, or not audit at all. You can control what operations to audit by modifying the System Access Control List (SACL) on an object. You can set a SACL on an AD DS object on the Security tab in that object's
Properties dialog box.
As an administrator one of your tasks is to configure audit policy. Enabling success or failure auditing is a straightforward procedure. Deciding which objects to audit; whether to audit success, failure or both; and whether to record new and old values if changes are made is much more difficult. Auditing everything is never an option—too much information is as bad as too little. You need to be selective. In Windows 2000 Server and Windows Server 2003, you could specify only whether DS access was audited. Windows Server 2008 gives you more granular control. You can audit the following:
■DS access
■DS changes (old and new values)
■DS replication

Question: 40

Your network contains a single Active Directory domain. All domain controllers run Windows Server 2008 R2. There are 1,000 client computers that run Windows 7 and that are connected to managed switches. You need to recommend a strategy for network access that meets the following requirements:
·Users are unable to bypass network access restrictions.
·Only client computers that have uptodate service packs installed can access the network.
·Only client computers that have uptodate antimalware software installed can access the network. What should you recommend?

A. Implement Network Access Protection (NAP) that uses DHCP enforcement.
B. Implement Network Access Protection (NAP) that uses 802.1x enforcement.
C. Implement a Network Policy Server (NPS), and enable IPsec on the domain controllers.
D. Implement a Network Policy Server (NPS), and enable Remote Authentication DialIn User Service (RADIUS) authentication on the managed switches.

Answer: B

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
■Integration with network access protection (NAP)System Center Configuration Manager 2007 lets your organization enforce compliance of software updates on client computers. This helps protect the integrity of the corporate network through integration with the Microsoft Windows Server 2008 NAP policy enforcement platform. NAP policies enable you to define which software updates to include in your system health requirements. If a client computer attempts to access your network, NAP and System Center Configuration
Manager 2007 work together to determine the client's health state compliance and determine whether the client is granted full or restricted network access. If the client is noncompliant, System Center Configuration Manager 2007 can deliver the necessary software updates so that the client can meet system health requirements and be granted full network access.
■Restrict network accessSystem Center Configuration Manager 2007 NAPenables you to include software updates in your system health requirements.NAP policies define which software updates need to be included, and the System Center Configuration Manager 2007 System Health Validator point passes the client's compliant or noncompliant health state to the Network Policy Server, which determines whether to grant the client full or restricted network access. Noncompliant clients can be automatically brought into compliance through remediation. This requires the System Center Configuration Manager 2007 software updates feature to be configured and operational.
NAP Enforcement Methods

When a computer is found to be noncompliant with the enforced health policy, NAPenforces limited network access. This is done through an Enforcement Client (EC). Windows Vista, Windows XP Service Pack 3, and Windows Server 2008 include NAPEC support for IPsec, IEEE 802.1X, Remote Access VPN, and DHCP enforcement methods. Windows Vista and Windows Server 2008 also support NAP enforcement for Terminal Server Gateway connections.
NAP enforcement methods can either be used individually or can be used in conjunction with each other to limit the network access of computers that are found not to be in compliance with configured health policies. Hence you can apply the remote access VPN and IPsec enforcement methods to ensure that internal clients and clients coming in from the Internet are only granted access to resources if they meet the appropriate client health benchmarks.
802.1X 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.

Question: 41

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. The network contains 100 servers and 5,000 client computers. The client computers run either Windows XP Service Pack 1 or Windows 7.
You need to plan a VPN solution that meets the following requirements:
·Stores VPN passwords as encrypted text
·Supports Suite B cryptographic algorithms
·Supports automatic enrollment of certificates
·Supports client computers that are configured as members of a workgroup
What should you include in your plan?

A. Upgrade the client computers to Windows XP Service Pack 3. Implement a standalone certification authority (CA). Implement an IPsec VPN that uses certificate based authentication.
B. Upgrade the client computers to Windows XP Service Pack 3. Implement an enterprise certification authority (CA) that is based on Windows Server?2008 R2. Implement an IPsec VPN that uses Kerberos authentication.
C. Upgrade the client computers to Windows 7. Implement an enterprise certification authority (CA) that is based on Windows Server 2008 R2. Implement an IPsec VPN that uses preshared keys.
D. Upgrade the client computers to Windows 7. Implement an enterprise certification authority (CA) that is based on Windows Server 2008 R2. Implement an IPsec VPN that uses certificate based authentication.

Answer: D

Explanation:
This is as close as I could get to an answer to this.
In essence, Enterprise CAs are fully integrated into a Windows Server 2008 environment. This type of CA makes the issuing and management of certificates for Active Directory clients as simple as possible.
Standalone CAs do not require Active Directory. When certificate requests are submitted to Standalone CAs, the requestor must provide all relevant identifying information and manually specify the type of certificate needed. This process occurs automatically with an Enterprise CA. By default, Standalone CA requests require administrator approval. Administrator intervention is necessary because there is no automated method of verifying a requestor's credentials. Standalone CAs do not use certificate templates, limiting the ability for administrators to customize certificates for specific organizational needs.
■L2TP/IPsecL2TP connections use encryption provided by IPsec. L2TP/IPsec is the protocol that you need to deploy if you are supporting Windows XP remote access clients, because these clients cannot use SSTP. L2TP/IPsec provides per-packet data origin authentication, data integrity, replay protection, and data confidentiality.
L2TP/IPsec connections use two levels of authentication. Computer-level authentication occurs either using digital certificates issued by a CA trusted by the client and VPN server or through the deployment of pre-shared keys. PPP authentication protocols are then used for user-level authentication. L2TP/IPsec supports all of the
VPN authentication protocols available on Windows Server 2008.
Supports Suite B cryptographic algorithms
When using the Certificate Templates console, note that you cannot configure the autoenrollment permission for a level 1 certificate template. Level 1 certificates have Windows 2000 as their minimum supported CA. Level 2 certificate templates have Windows Server 2003 as a minimum supported CA. Level 2 certificate templates are also the minimum level of certificate template that supports autoenrollment. Level 3 certificates templates are supported only by client computers running Windows Server 2008 or Windows Vista. Level 3 certificate templates allow administrators to configure advanced Suite B cryptographic settings. These settings are not required to allow certificate autoenrollment and most administrators find level 2 certificate templates are adequate for their organizational needs.

Question: 42

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. All servers run Windows Server 2008 R2. All client computers run Windows 7. You need to generate a monthly report on the status of software updates for the client computers. Your solution must meet the following requirements:

- Display all of the operating system updates that installed successfully
- Display all of the Microsoft Application updates that installed successfully
- Display all of the operating system updates that failed to install
- Display all of the Microsoft Application updates that failed to install
- Minimize administrative effort
- Minimize costs

What should you do?

A. Install Microsoft System Center Essentials (Essentials) 2007. Deploy management agents on all client computers.
B. Install Microsoft System Center Configuration Manager (SysMgr) 2007. Deploy management agents on all client computers.
C. Install Windows Server Update Services (WSUS) 3.0 SP2. Configure Windows Update by using a Group Policy object (GPO).
D. Deploy Microsoft Baseline Security Analyzer (MBSA) 2.1 on the client computers. Run MBSA on each client computer, and save the report to a shared folder on the network.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd939886%28WS.10%29.aspx
What's new in this release?
• Integration with Windows Server® 2008 R2
• Support for the BranchCache® feature in Windows Server 2008 R2
• Support for Windows® 7 client computers New features
• Automatic approval rules include the ability to specify the approval deadline date and time for all computers or for specific computer groups.
• Improved handling of language selection for downstream servers includes a new warning dialog that appears when you decide to download updates only for specified languages.
• New Update and Computer Status reports let you filter updates that are approved for installation. You can run these reports from the WSUS administration console or use the application programming interface (API) to incorporate this functionality into your own reports.
Windows Update Agent improvements
• Client computer scan time is faster than previous versions.
• Computers that are managed by WSUS servers can now run "scoped" scans against those servers, instead of performing a full scan. This results in faster scans for applications that use Microsoft Update APIs such as Windows Defender.
• User experience improvements help users organize updates and provide greater clarity on update value and behavior.
• Imaged computers are more clearly displayed in the WSUS administration console.
For more information, see article 903262 in the Microsoft Knowledge Base.
• Prevents APIs that are called by non-local system callers in a non-interactive session from failing.
• Prevents error code 0x80070057 when you try to install 80 or more updates at the same time from the Windows Update Web page or from the Microsoft Update Web page.
• Improves scan times for Windows Update
• Improves the speed at which signature updates are delivered
• Enables support for Windows Installer reinstallation functionality
• Improves error messaging

Question: 43

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. Your company and an external partner plan to collaborate on a project. The external partner has an Active Directory domain that contains Windows Server 2008 R2 domain controllers. You need to design a collaboration solution that meets the following requirements:
- Allows users to prevent sensitive documents from being forwarded to untrusted recipients or from being printed.
- Allows users in the external partner organization to access the protected content to which they have been granted rights.
- Sends all interorganizational traffic over port 443.
- Minimizes the administrative effort required to manage the external users.

What should you include in your design?

A. Establish a federated trust between your company and the external partner. Deploy a Windows Server 2008 R2 server that has Microsoft SharePoint Foundation 2010 installed.
B. Establish a federated trust between your company and the external partner. Deploy a Windows Server 2008 R2 server that runs Microsoft SharePoint 2010 and that has the Active Directory Rights Management Services (AD RMS) role installed.

C. Establish an external forest trust between your company and the external partner. Deploy a Windows Server 2008 R2 server that has the Active Directory Certificate Services server role installed. Implement Encrypting File System (EFS).
D. Establish an external forest trust between your company and the external partner. Deploy a Windows Server 2008 R2 server that has the Active Directory Rights Management Service (AD RMS) role installed and Microsoft SharePoint Foundation 2010 installed.

Answer: B

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Active Directory Federation Services
You can create forest trusts between two or more Windows Server 2008 forests (or Windows Server 2008 and Windows Server 2003 forests). This provides cross-forest access to resources that are located in disparate business units or organizations. However, forest trusts are sometimes not the best option, such as when access across organizations needs to be limited to a small subset of individuals. Active Directory Federation Services (AD FS) enables organizations to allow limited access to their infrastructure to trusted partners. AD
FS acts like a cross-forest trust that operates over the Internet and extends the trust relationship to Web applications (a federated trust). It provides Web single-sign-on (SSO) technologies that can authenticate a user over the life of a single online session. AD FS securely shares digital identity and entitlement rights (known asclaims) across security and enterprise boundaries.
Windows Server 2003 R2 introduced AD FS and Windows Server 2008 expands it. New AD FS features introduced in Windows Server 2008 include the following:
■Improved application supportWindows Server 2008 integrates AD FS with Microsoft Office SharePoint Server 2007 and Active Directory Rights Management Services (AD RMS).
■Improved installationAD FS is implemented in Windows Server 2008 as a server role. The installation wizard includes new server validation checks.
■Improved trust policyImprovements to the trust policy import and export functionality help to minimize configuration issues that are commonly associated with establishing federated trusts.
AD FS extends SSO functionality to Internet-facing applications. Partners experience the same streamlined SSO user experience when they access the organization's Web-based applications as they would when accessing resources through a forest trust. Federation servers can be deployed to facilitate businesstobusiness (B2B) federated transactions.
AD FS provides a federated identity management solution that interoperates with other security products by conforming to the Web Services Federation(WS-Federation) specification. This specification makes it possible for environments that do not use Windows to federate with Windows environments. It also provides an extensible architecture that supports the Security Assertion Markup Language (SAML) 1.1 token type and Kerberos authentication. AD FS can perform claim mapping—for example, modifying claims using business logic variables in an access request. Organizations can modify AD FS to coexist with their current security infrastructure and business policies.
Finally, AD FS supports distributed authentication and authorization over the Internet. You can integrate it into an organization's existing access management solution to translate the claims that are used in the organization into claims that are agreed on as part of a federation. AD FS can create, secure, and verify claims that move between organizations. It can also audit and monitor the communication activity between organizations and departments to help ensure secure transactions.

Question: 44

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 need to create a remote access strategy for the

Remote Desktop Services servers that meets the following requirements:
- Restricts access to specific users
- Minimizes the number of open ports on the firewall
- Encrypts all remote connections to the Remote Desktop Services servers

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).

Answer: D

Explanation:
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.
Connection Authorization Policies
Terminal Services connection authorization policies (TS-CAPs) specify which users are allowed to connect through the TS Gateway Server to resources located on your organization's internal network. This is usually done by specifying a local group on the TS Gateway Server or a group within Active Directory. Groups can include user or computer accounts. You can also use TS-CAPs to specify whether remote clients use password or smart-card authentication to access internal network resources through the TS Gateway Server. You can use TS-CAPs in conjunction with NAP; this scenario is covered in more detail by the next lesson.

Question: 45

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).

Answer: C

Explanation:
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: 46

Your network consists of a single Active Directory domain. All domain controllers run Windows Server 2008 R2. There are five servers that run Windows Server 2003 SP2. The Windows Server 2003 SP2 servers have the Terminal Server component installed. A firewall server runs Microsoft Internet Security and Acceleration (ISA) Server 2006. All client computers run Windows 7. 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:

- Minimizes the number of open ports on the firewall server
- Encrypts all remote connections to the Remote Desktop Services servers
- Prevents network access to client computers that have Windows Firewall disabled

What should you do?

A. Implement port forwarding on the ISA Server. Implement Network Access Quarantine Control on the ISA Server.
B. 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 implement Network Access Protection (NAP).
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 connection authorization policy (RD?CAP).
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 resource authorization policy (RD RAP).

Answer: B

Explanation:
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.
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.

Question: 47

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.

Answer: D

Explanation:

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.

Question: 48

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.

Answer: D

Explanation:
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: 49

Your network contains an Active Directory domain. The domain contains a Remote Desktop Services server that runs Windows Server 2008 R2. All client computers run Windows 7. You need to deploy a new line of business Application. The deployment must meet the following requirements:

- Users must have access to the Application from the company portal.
- Users must always have access to the latest version of the Application.
- You must minimize the number of Applications installed on the client computers.

What should you do?

A. Publish the Application to the users by using a Group Policy object (GPO).
B. Publish the Application as a RemoteApp. Enable Remote Desktop Web Access (RD Web Access).
C. Assign the Application to the client computers by using a Group Policy object (GPO).
D. Deploy the Application by using Microsoft System Center Configuration Manager (SCCM) 2007 R2.

Answer: B

Question: 50

Your network consists of a single Active Directory domain. The domain contains a server that runs Windows Server 2008 R2 and that has the Remote Desktop Services server role installed. The server has six custom Applications installed. The custom Applications are configured as RemoteApps. You notice that when a user runs one of the Applications, other users report that the server seems slow and that some Applications become unresponsive. You need to ensure that active user sessions receive equal access to system resources. What should you do?

A. Implement Remote Desktop Web Access.
B. Implement Remote Desktop Connection Broker.
C. Configure Performance Monitor.

D. Implement Windows System Resource Manager.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc771218%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc732553%28WS.10%29.aspx
Terminal Services and Windows System Resource Manager
Windows® System Resource Manager (WSRM) on Windows Server® 2008 allows you to control how CPU and memory resources are allocated to applications, services, and processes on the computer. Managing resources in this way improves system performance and reduces the chance that applications, services, or processes will take CPU or memory resources away from one another and slow down the performance of the computer. Managing resources also creates a more consistent and predictable experience for users of applications and services running on the computer.
You can use WSRM to manage multiple applications on a single computer or users on a computer on which Terminal Services is installed.
Resource-Allocation Policies
WSRM uses resource-allocation policies to determine how computer resources, such as CPU and memory, are allocated to processes running on the computer. There are two resource-allocation policies that are specifically designed for computers running Terminal Services. The two Terminal Services-specific resource-allocation policies are:
Equal_Per_User
Equal_Per_Session

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

Question: 51

Your network contains an Active Directory domain. You have a server that runs Windows Server 2008 R2 and has the Remote Desktop Services server role enabled. All client computers run Windows 7. You need to plan the deployment of a new line of business Application to all client computers. The deployment must meet the following requirements:

- Users must access the Application from an icon on their desktops.
- Users must have access to the Application when they are not connected to the network.

What should you do?

A. Publish the Application as a RemoteApp.
B. Publish the Application by using Remote Desktop Web Access (RD Web Access).
C. Assign the Application to the Remote Desktop Services server by using a Group Policy object (GPO).
D. Assign the Application to all client computers by using a Group Policy object (GPO).

Answer: D

Question: 52

Your network contains a single Active Directory domain. You have 100 servers that run Windows Server 2008 R2 and 5,000 client computers that run Windows 7. You plan to deploy Applications to the client computers. You need to recommend an Application deployment strategy that meets the following requirements:
·Applications must be deployed only to client computers that meet the minimum hardware requirements.
·Deployments must be scheduled to occur outside business hours.
·Detailed reports on the success or failure of the Application deployments must be provided.
What should you recommend?

A. Deploy Applications by using Group Policy.
B. Implement Windows Server Update Services (WSUS).
C. Implement Microsoft System Center Operations Manager (SCOM) 2007 R2.
D. Implement Microsoft System Center Configuration Manager (SCCM) 2007 R2.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/bb680651.aspx
Welcome to Microsoft System Center Configuration Manager 2007. Configuration Manager 2007 contributes to a more effective Information Technology (IT) department by enabling secure and scalable operating system and application deployment and desired configuration management, enhancing system security, and providing comprehensive asset management of servers, desktops, and mobile devices.
Post-Setup Configuration Tasks
After Setup has run, there are still a few tasks you must perform to have a functioning Configuration Manager 2007 site. For example, you might need to assign new site system roles and install clients. For more information, see Checklist for Required Post Setup Configuration Tasks.
Common Configuration Manager Tasks
For more information about how to do common Configuration Manager 2007 tasks, see the following topics.

- Planning and Deploying the Server Infrastructure for Configuration Manager 2007
- Planning and Deploying Clients for Configuration Manager 2007
- Collect hardware and software asset information
- Distribute software
- Deploy software updates
- Deploy operating systems
- Manage desired configurations
- Remotely administer a computer
- Restrict non-compliant computers from accessing the network
- Manage mobile devices like Smartphones and Pocket PCs

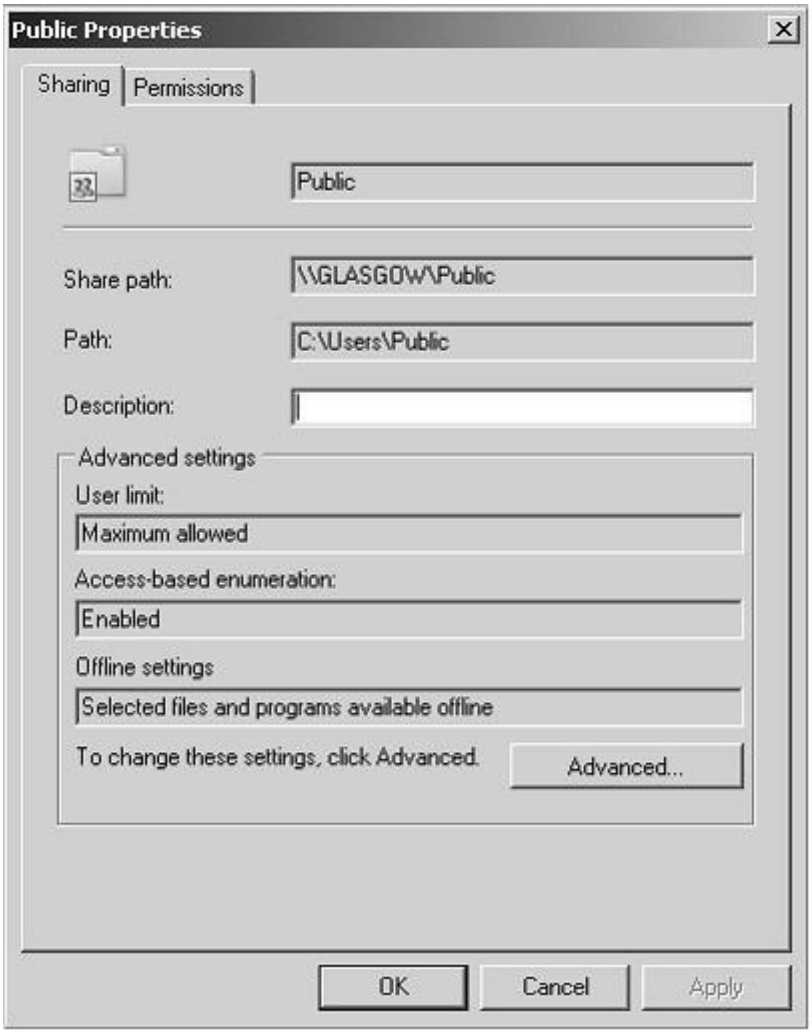
Question: 53

Your company has a main office and two branch offices. Each office has a domain controller and file servers. Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. You need to plan the deployment of Distributed File System (DFS) to meet the following requirements:
·Ensure that users see only the folders to which they have access
·Ensure that users can access the data locally
·Minimize the bandwidth required to replicate data
What should you include in your plan?

A. Deploy a standalone DFS namespace. Enable accessbased enumeration and use DFS Replication.
B. Deploy a standalone DFS namespace. Enable accessbased enumeration and use File Replication Service (FRS).
C. Deploy a domainbased DFS namespace and use DFS Replication. Modify each share to be a hidden share.
D. Deploy a domainbased DFS namespace and use File Replication Service (FRS). Modify each share to be a hidden share.

Answer: A

Explanation:
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.
This lesson summarizes DFS only very briefly as part of your planning considerations. Lesson 2 of this chapter discusses the topic in much more depth.
Exam TipPrevious Windows Server examinations have contained a high proportion of DFS questions. There is no reason to believe 70-646 will be any different.
You can also use Share And Storage Management to view and modify the properties of a shared folder or volume, including the local NTFS permissions and the network access permissions for that shared resource. To do this you again select the shared resource on the Shares tab and select Properties in the Actions pane.
Figure 6-6 shows the Properties dialog box for the share folder Public. The Permissions tab lets you specify share and NTFS permissions. Clicking Advanced lets you configure user limits and caching and disable or enable access-based enumeration (ABE). ABE is enabled by default and lets you hide files and folders from users who do not have access to them.



Question: 54

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?

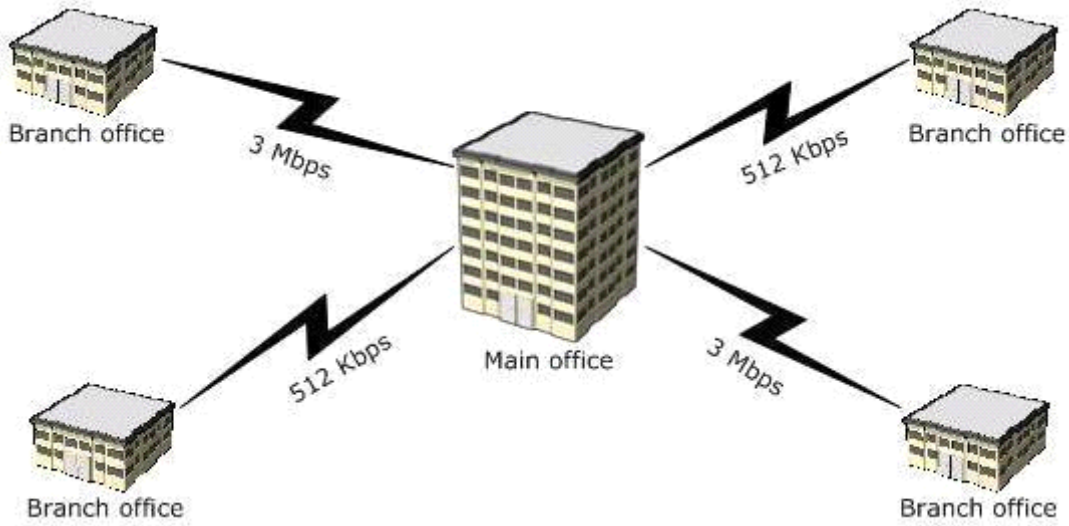
A. File Server Resource Manager (FSRM)
B. Volume Shadow Copy Service (VSS)
C. Microsoft SharePoint Foundation 2010
D. Windows System Resource Manager (WSRM)

Answer: C

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

Question: 55

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

Answer: D

Explanation:
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: 56

Your network consists of a single Active Directory domain. The domain contains a file server named Server1 that runs Windows Server 2008 R2. The file server contains a shared folder named UserDocs. Each user has a subfolder in UserDocs that they use to store personal data. You need to design a data management solution that meets the following requirements:

- Limits the storage space that is available to each user in UserDocs
- Sends a notification to the administrator if a users attempts to save multimedia files in UserDocs
- Minimizes administrative effort

What should you include in your design?

A. Configure NTFS quotas on UserDocs. Configure a task in Event Viewer to send an email notification.
B. Configure NTFS quotas on UserDocs. Schedule a script to monitor the contents of UserDocs and send an email notification if a multimedia file is found.
C. Install the File Server Resource Manager (FSRM) role service on Server1. Configure event subscriptions.
D. Install the File Server Resource Manager (FSRM) role service on Server1. Configure hard quotas and file screening.

Answer: D

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Creating Quotas
If the FSRM File Services server role is installed, you can use FSRM to create quotas. The Create Quota dialog box is shown in Figure 6-13. Note that you will be unable to access this box if you have not installed the appropriate server role, which you will do in the practice session later in this lesson.

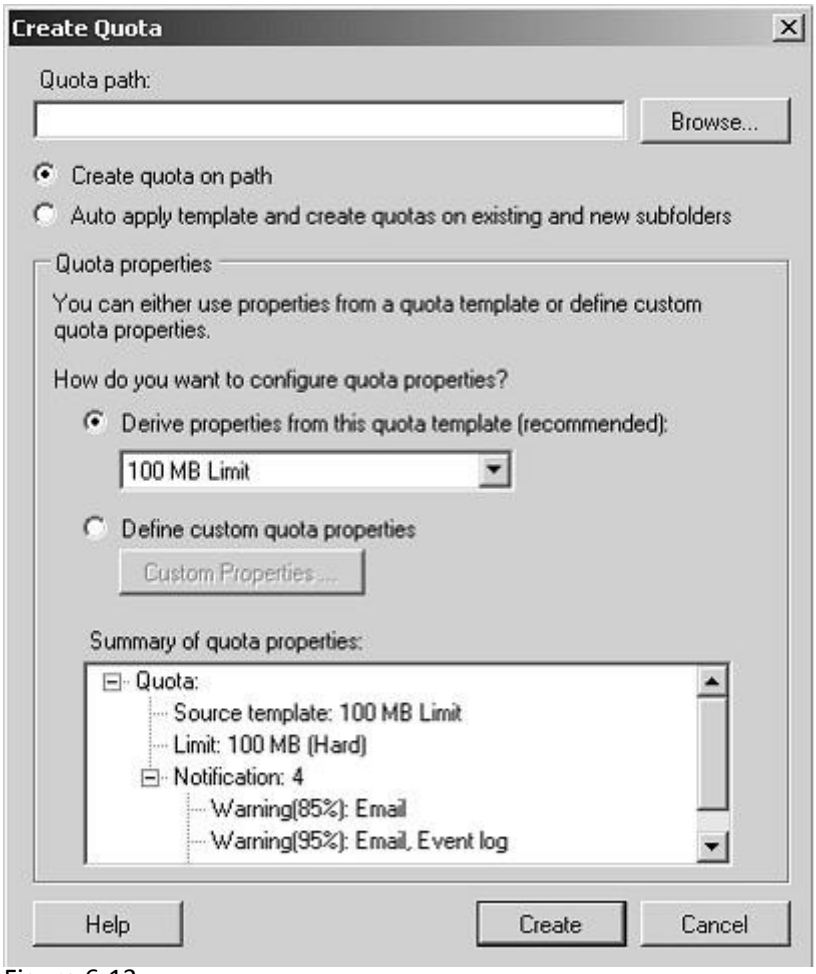


Figure 6-13

The Create Quota dialog box

You specify a path to the volume or folder for which you want to create the quota and then specify whether you want to create a quota only on that path or whether a template-based quota will be automatically generated and applied to existing and new subfolders on the path of the parent volume or folder. To specify the latter action, select Auto Apply Template And Create Quotas On Existing And New Subfolders. Typically you would select Derive Properties From This Quota Template (Recommended) and select a template. You can, if you want, define custom quota properties, but this is not recommended. You can select templates that specify the quota size that is allocated to each user and whether the quota is hard or soft. A hard quota cannot be exceeded. A user can exceed a soft quota, but typically exceeding the quota limit generates a report in addition to sending an e-mail notification and logging the event. Soft quotas are used for monitoring. Quota templates include the following:

■100 MB Limit This is a hard quota. It e-mails the user and specified administrators if the100 percent quota limit has been reached and writes an event to the event log.

■200 MB Limit Reports to User This is a hard quota. It generates a report, sends e-mails, and writes an event to the event log if the 100 percent quota limit has been reached.

■200 MB Limit with 50 MB Extension Technically this is a hard quota because it performs an action when the user attempts to exceed the limit, rather than merely monitoring the exceeded limit. The action is to run a program that applies the 250 MB Extended Limit template and effectively gives the user an additional 50 MB.

E-mails are sent and the event is logged when the limit is extended.

■250 MB Extended Limit The 250 MB limit cannot be exceeded. E-mails are sent and the event is logged when the limit is reached.

■Monitor 200 GB Volume Usage This is a soft quota that can be applied only to volumes. It is used for monitoring.

■Monitor 50 MB Share Usage This is a soft quota that can be applied only to shares. It is used for monitoring.

Managing File Screens

You can use FSRM to create and manage file screens that control the types of files that users can save, and generate

notifications when users attempt to save unauthorized files. You can also define file screening templates that you can apply to new volumes or folders and use across your organization.
FSRM also enables you to create file screening exceptions that extend the flexibility of the file screening rules.
You could, for example, ensure that users do not store music files in personal folders, but you could allow storage of specific types of media files, such as training files that comply with company policy. You could also create an exception that allows members of the senior management group to save any type of file they want to (provided they comply with legal restrictions).
You can also configure your screening process to notify you by e-mail when an executable file is stored on a shared folder. This notification can include information about the user who stored the file and the file's exact location.
Exam Tip File screens are not specifically included on the objectives for the 70-646 examination. You should know what they are, what they do, and that you can manage them from FSRM. You probably will not come across detailed questions about file screen configuration.

Question: 57

Your company has two branch offices that connect by using a WAN link. Each office contains a server that runs Windows Server 2008 R2 and that functions as a file server. Users in each office store data on the local file server. Users have access to data from the other office. You need to plan a data access solution that meets the following requirements:

- Folders that are stored on the file servers must be available to users in both offices.
- Network bandwidth usage between offices must be minimized.
- Users must be able to access all files in the event that a WAN link fails.

What should you include in your plan?

A. On both servers, implement DFS Replication.
B. On both servers, install and configure File Server Resource Manager (FSRM) and File Replication Service (FRS).
C. On one server, install and configure File Server Resource Manager (FSRM). On the other server, install and configure File Replication Service (FRS).
D. On one server, install and configure Distributed File System (DFS). On the other server, install and configure the Background Intelligent Transfer Service (BITS).

Answer: A

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
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.
■ File Replication Service (FRS) The File Replication Service (FRS) enables you to synchronize folders with file servers that use FRS. Where possible you should use the DFS Replication (DFSR) service. You should install FRS only if your Windows Server 2008 server needs to synchronize folders with servers that use FRS with the Windows Server 2003 or Windows 2000 Server implementations of DFS.
The main tool for implementing shared folder replication in a Windows Server 2008 network is DFS Replication.
Using DFS Namespace to Plan and Implement a Shared Folder Structure and Enhance Data Availability
When you add the DFS Management role service to the Windows Server 2008 File Services Server role, the DFS Management console is available from the Administrative Tools menu or from within Server Manager. This console provides the DFS Namespaces and DFS Replication tools as shown in Figure 6-31 DFS Namespaces lets you group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.
This structure increases availability. You can use the efficient, multiple-master replication engine provided by DFSR to replicate a DFS Namespace within a site and across WAN links. A user connecting to files within the shared folder

structures contained in the DFS Namespace will automatically connect to shared folders in the same AD DS site (when available) rather than across a WAN. You can have several DFS Namespace servers in a site and spread over several sites, so if one server goes down, a user can still access files within the shared folder structure.
Because DFSR is multimaster, a change to a file in the DFS Namespace on any DFS Namespace server is quickly and efficiently replicated to all other DFS Namespace servers that hold that namespace. Note that DFSR replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the AD DS SYSVOL folder in domains that use the Windows Server 2008 domain functional level. You can install FRS Replication as part of the Windows Server 2003 File Services role service, but you should use it only if you need to synchronize with servers that use FRS with the Windows Server 2003 or Windows 2000 Server implementations of DFS.

Question: 58

Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. All client computers run Windows 7. Users store all of their files in their Documents folder. Many users store large files. You plan to implement roaming user profiles for all users by using Group Policy. You need to recommend a solution that minimizes the amount of time it takes users to log on and log off of the computers that use the roaming user profiles. What should you recommend?

A. Modify the Group Policy object (GPO) to include folder redirection.
B. Modify the Group Policy object (GPO) to include Background Intelligent Transfer Service (BITS) settings.
C. On the server that hosts the roaming user profiles, enable caching on the profiles share.
D. On any server, install and configure the Background Intelligent Transfer Service (BITS) server extensions.

Answer: A

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Planning and Managing Group Policy
Planning your Group Policy is in part planning your organizational structure. If you have a huge number of OUs—some inheriting policies, others blocking inheritance, several OUs linking to the same GPO, and several GPOs linking to the same OU—you have a recipe for disaster. While too few OUs and GPOs is also a mistake, most of us err on the side of having too many. Keep your structures simple. Do not link OUs and GPOs across site boundaries. Give your OUs and GPOs meaningful names.
When you are planning Group Policy you need to be aware of the Group Policy settings that are provided with Windows Server 2008. These are numerous and it is not practical to memorize all of them, but you should know what the various categories are. Even if you do not edit any policies, exploring the Group Policy structure in Group Policy Management Editor is worthwhile. You will develop a feel for what is available and whether you need to generate custom policies by creating ADMX files.
You also need a good understanding of how Group Policy is processed at the client. This happens in the following two phases:
■Core processing When a client begins to process Group Policy, it must determine whether it can reach a DC, whether any GPOs have been changed, and what policy settings must be processed. The core Group Policy engine performs the processing of this in the initial phase.
■Client-side extension (CSE) processing In this phase, Group Policy settings are placed in various categories, such as Administrative Templates, Security Settings, Folder Redirection, Disk Quota, and Software Installation. A specific
CSE processes the settings in each category, and each CSE has its own rules for processing settings. The core Group Policy engine calls the CSEs that are required to process the settings that apply to the client.
CSEs cannot begin processing until core Group Policy processing is completed. It is therefore important to plan your Group Policy and your domain structure so that this happens as quickly and reliably as possible. The troubleshooting section later in this lesson discusses some of the problems that can delay or prevent core
Group Policy processing.

Question: 59

Your network contains a Windows Server 2008 R2 server that functions as a file server. All users have laptop computers that run Windows 7. The network is not connected to the Internet. Users save files to a shared folder on the server. You need to design a data provisioning solution that meets the following requirements:

- Users who are not connected to the corporate network must be able to access the files and the folders in the corporate network.
- Unauthorized users must not have access to the cached files and folders.

What should you do?

A. Implement a certification authority (CA). Configure IPsec domain isolation.
B. Implement a certification authority (CA). Configure Encrypting File System (EFS) for the drive that hosts the files.
C. Implement Microsoft SharePoint Foundation 2010. Enable Secure Socket Layer (SSL) encryption.
D. Configure caching on the shared folder. Configure offline files to use encryption.

Answer: D

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Lesson 2: Provisioning Data
Lesson 1 in this chapter introduced the Share And Storage Management tool, which gives you access to the Provision Storage Wizard and the Provision A Shared Folder Wizard. These tools allow you to configure storage on the volumes accessed by your server and to set up shares. When you add the Distributed File System (DFS) role service to the File Services server role you can create a DFS Namespace and go on to configure DFSR. Provisioning data ensures that user files are available and remain available even if a server fails or a WAN link goes down. Provisioning data also ensures that users canwork on important files when they are not connected to the corporate network.
In a well-designed data provisioning scheme, users should not need to know the network path to their files, or from which server they are downloading them. Even large files should typically download quickly—files should not be downloaded or saved across a WAN link when they are available from a local server. You need to configure indexing so that users can find information quickly and easily. Offline files need to be synchronized quickly and efficiently, and whenever possible without user intervention. A user should always be working with the most up-to-date information (except when a shadow copy is specified) and fast and efficient replication should ensure that where several copies of a file exist on a network they contain the same information and latency is minimized.
You have several tools that you use to configure shares and offline files, configure storage, audit file access, prevent inappropriate access, prevent users from using excessive disk resource, and implement disaster recovery. However, the main tool for provisioning storage and implementing a shared folder structure is DFS Management, specifically DFS Namespaces. The main tool for implementing shared folder replication in a
Windows Server 2008 network is DFS Replication.

Question: 60

Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. All client computers run Windows 7. Some users have laptop computers and work remotely from home. You need to plan a data provisioning infrastructure to secure sensitive files. Your plan must meet the following requirements:

- Files must be stored in an encrypted format.
- Files must be accessible by remote users over the Internet.
- Files must be encrypted while they are transmitted over the Internet.

What should you include in your plan?

A. Deploy one Microsoft SharePoint Foundation 2010 site. Require users to access the SharePoint site by using a Secure Socket Transmission Protocol (SSTP) connection.
B. Deploy two Microsoft SharePoint Foundation 2010 sites. Configure one site for internal users. Configure the other site for remote users. Publish the SharePoint sites by using HTTPS.
C. Configure a Network Policy and Access Services (NPAS) server to act as a VPN server. Require remote users to access the files by using an IPsec connection to the VPN server.
D. Store all sensitive files in folders that are encrypted by using Encrypting File System (EFS). Require remote users to access the files by using Secure Socket Transmission Protocol (SSTP).

Answer: D

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Encrypting File System Encrypting File System (EFS) is another method through which you can ensure the integrity of data. Unlike BitLocker, which encrypts all data on a volume using a single encryption key that is tied to the computer, EFS allows for the encryption of individual files and folders using a public encryption key tied to a specific user account. The encrypted file can only be decrypted using a private encryption key that is accessible only to the user. It is also possible to encrypt documents to other user's public EFS certificates. A document encrypted to another user's public EFS certificate can only be decrypted by that user's private certificate.
Security Groups cannot hold encryption certificates, so the number of users that can access an encrypted document is always limited to the individual EFS certificates that have been assigned to the document. Only a user that originally encrypts the file or a user whose certificate is already assigned to the file can add another user's certificate to that file. With EFS there is no chance that an encrypted file on a departmental shared folder might be accessed by someone who should not have access because of incorrectly configured NTFS or Shared Folder permissions. As many administrators know, teaching regular staff to configure NTFS permissions can be challenging. The situation gets even more complicated when you take into account Shared Folder permissions. Teaching staff to use EFS to limit access to documents is significantly simpler than explaining NTFS ACLs.
If you are considering deployment of EFS throughout your organization, you should remember that the default configuration of EFS uses self-signed certificates. These are certificates generated by the user's computer rather than a Certificate Authority and can cause problems with sharing documents because they are not necessarily accessible from other computers where the user has not encrypted documents. A more robust solution is to modify the default EFS Certificate Template that is provided with a Windows Server 2008
Enterprise Certificate Authority to enable autoenrollment. EFS certificates automatically issued by an Enterprise CA can be stored in Active Directory and applied to files that need to be shared between multiple users.
Another EFS deployment option involves smart cards. In organizations where users authenticate using smart cards, their private EFS certificates can be stored on a smart card and their public certificates stored within Active Directory. You can learn more about configuring templates for autoenrollment in Chapter 10, "Certificate Services and Storage Area Networks."
MORE INFO More on EFS
For more information on Encrypting File System in Windows Server 2008, consult the following TechNet article:
http://technet2.microsoft.com/windowsserver2008/en/library/f843023b-bedd-40dd9e5b-f1619eebf7821033.mspx?mfr=true.
Quick Check
1. From a normal user's perspective, in terms of encryption functionality, how does EFS differ from BitLocker?
2. What type of auditing policy should you implement to track access to sensitive files?
Quick Check Answers
1. BitLocker works on entire volumes and is transparent to the user. EFS works on individual files and folders and be configured by the user.
2. Auditing Object Access.
Windows Server 2008 VPN Protocols
Windows Server 2008 supports three different VPN protocols: Tunneling Protocol (PPTP), Layer Two Tunneling

Protocol over IPsec (L2TP/IPsec), and Secure Socket Tunneling Protocol (SSTP). The factors that will influence the protocol you choose to deploy in your own network environment include client operating system, certificate infrastructure, and how your organization's firewall is deployed.
Windows XP remote access clients, because these clients cannot use SSTP
■ SSTP Secure Socket Tunneling Protocol (SSTP) is a VPN technology that makes its debut with Windows Server 2008. SSTP VPN tunnels allow traffic to pass across firewalls that block traditional PPTP or L2TP/IPsec VPN traffic. SSTP works by encapsulating Point-to-Point Protocol (PPP) traffic over the Secure Sockets Layer (SSL) channel of the Secure Hypertext Transfer Protocol (HTTPS) protocol. Expressed more directly, SSTP piggybacks PPP over HTTPS. This means that SSTP traffic passes across TCP port 443, which is almost certain to be open on any firewall between the Internet and a public-facing Web server on an organization's screened subnet.
When planning for the deployment of SSTP, you need to take into account the following considerations:
■ SSTP is only supported with Windows Server 2008 and Windows Vista with Service Pack 1.
■ SSTP requires that the client trust the CA that issues the VPN server's SSL certificate.
■ The SSL certificate must be installed on the server that will function as the VPN server prior to the installation of Routing and Remote Access; otherwise, SSTP will not be available.
■ The SSL certificate subject name and the host name that external clients use to connect to the VPN server must match, and the client Windows Vista SP1 computer must trust the issuing CA.
■ SSTP does not support tunneling through Web proxies that require authentication.
■ SSTP does not support site-to-site tunnels. (PPTP and L2TP do.)
MORE INFO More on SSTP
To learn more about SSTP, see the following SSTP deployment walkthrough document at http://download.microsoft.com/download/b/1/0/b106fc39-936c-4857-a6ea-3fb9d1f37063/ Deploying%20SSTP %20Remote%20Access%20Step%20by%20Step%20Guide.doc.

Question: 61

Your company has a main office and a branch office. Your network contains a single Active Directory domain. You install 25 Windows Server 2008 R2 member servers in the branch office. You need to recommend a storage solution that meets the following requirements:

- Encrypts all data on the hard disks
- Allows the operating system to start only when the authorized user is present

What should you recommend?

A. Encrypting File System (EFS)
B. File Server Resource Manager (FSRM)
C. Windows BitLocker Drive Encryption (BitLocker)
D. Windows System Resource Manager (WSRM)

Answer: C

Explanation:
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, BitLockerensures 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 Volume Configuration

One of the most important things to remember is that a computer must be configured to support BitLocker prior to the installation of Windows Server 2008. The procedure for this is detailed at the start of Practice 2 at the end of this lesson, but involves creating a separate 1.5-GB partition, formatting it, and making it active as the System partition prior to creating a larger partition, formatting it, and then installing the Windows Server 2008 operating system. Figure 1-6 shows a volume configuration that supports BitLocker. If a computer's volumes are not correctly configured prior to the installation of Windows Server 2008, you will need to perform a completely new installation of Windows Server 2008 after repartitioning the volume correctly. For this reason you should partition the hard disk drives of all computers in the environment on which you are going to install Windows Server 2008 with the assumption that at some stage in the future you might need to deploy BitLocker.

If BitLocker is not deployed, it has cost you only a few extra minutes of configuration time. If you later decide to deploy BitLocker, you will have saved many hours of work reconfiguring the server to support full hard drive encryption.

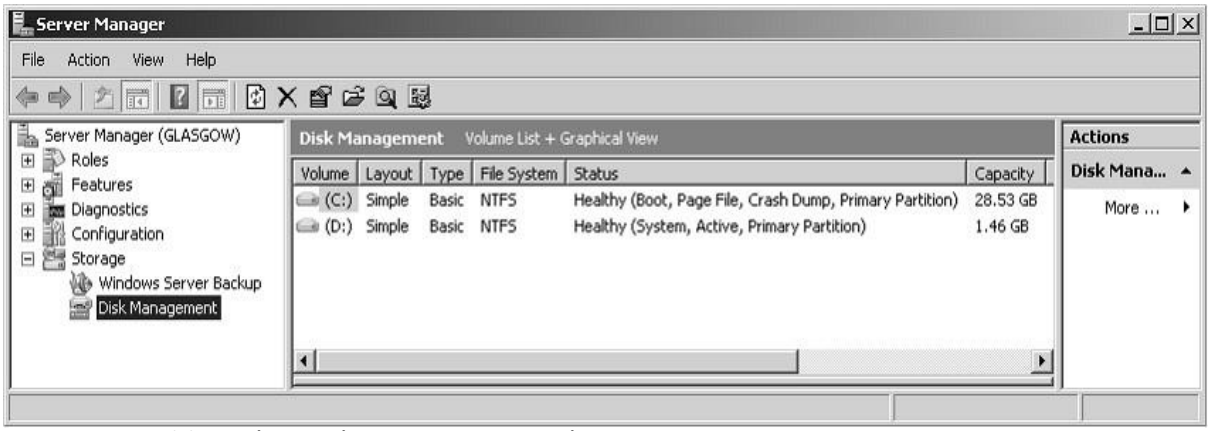


Figure 1-6Partition scheme that supports BitLocker

The necessity of having specifically configured volumes makes BitLocker difficult to implement on Windows Server 2008 computers that have been upgraded from Windows Server 2003. The necessary partition scheme would have had to be introduced prior to the installation of Windows Server 2003, which in most cases would have occurred before most people were aware of BitLocker.

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.

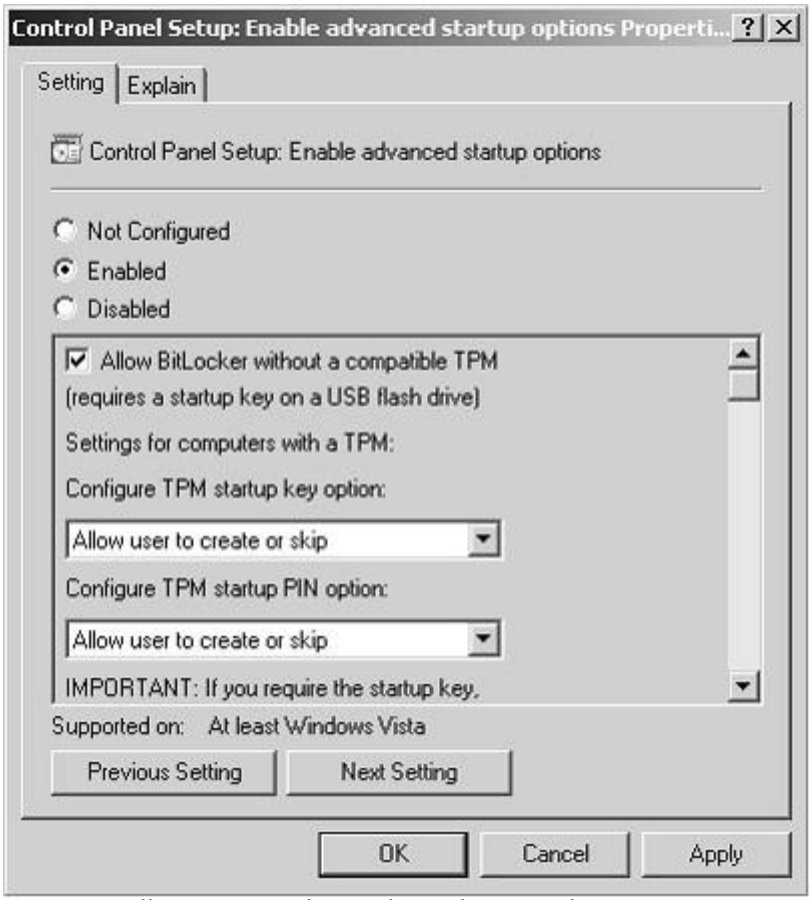


Figure 1-7Allowing BitLocker without the TPM chip

Other BitLocker policies include:

■Turn On BitLocker Backup To Active Directory Domain ServicesWhen 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 FolderWhen enabled, this policy sets the default folder to which computer recovery keys can be stored.

■Control Panel Setup: Configure Recovery OptionsWhen enabled, this policy can be used to disable the recovery password and the recovery key. If both the recovery password and the recovery key are disabled, the policy that backs up the recovery key to Active Directory must be enabled.

■Configure Encryption MethodThis policy allows the administrator to specify the properties of the AES encryption method used to protect the hard disk drive.

■Prevent Memory Overwrite On RestartThis policy speeds up restarts, but increases the risk of BitLocker being compromised.

■Configure TMP Platform Validation ProfileThis policy configures how the TMP security hardware protects the BitLocker encryption key.

Encrypting File System vs. BitLocker

Although both technologies implement encryption, there is a big difference between Encrypting File System (EFS) and BitLocker. EFS is used to encrypt individual files and folders and can be used to encrypt these items for different users. BitLockerencrypts the whole hard disk drive. A user with legitimate credentials can log on to a file server that is protected by BitLocker and will be able to read any files that she has permissions for. This user will not, however be able to read files that have been EFS encrypted for other users, even if she is granted permission, because you can only read EFS-encrypted files if you have the appropriate digital certificate. EFS allows organizations to protect

sensitive shared files from the eyes of support staff who might be required to change file and folder permissions as a part of their job task, but should not actually be able to review the contents of the file itself. BitLocker provides a transparent form of encryption, visible only when the server is compromised. EFS provides an opaque form of encryption—the content of files that are visible to the person who encrypted them are not visible to anyone else, regardless of what file and folder permissions are set.

Turning Off BitLocker

In some instances you may need to remove BitLocker from a computer. For example, the environment in which the computer is located has been made much more secure and the overhead from the BitLocker process is causing performance problems. Alternatively, you may need to temporarily disable BitLocker so that you can perform maintenance on startup files or the computer's BIOS. As Figure 1-8 shows, you have two options for removing BitLocker from a computer on which it has been implemented: disable BitLocker or decrypt the drive.

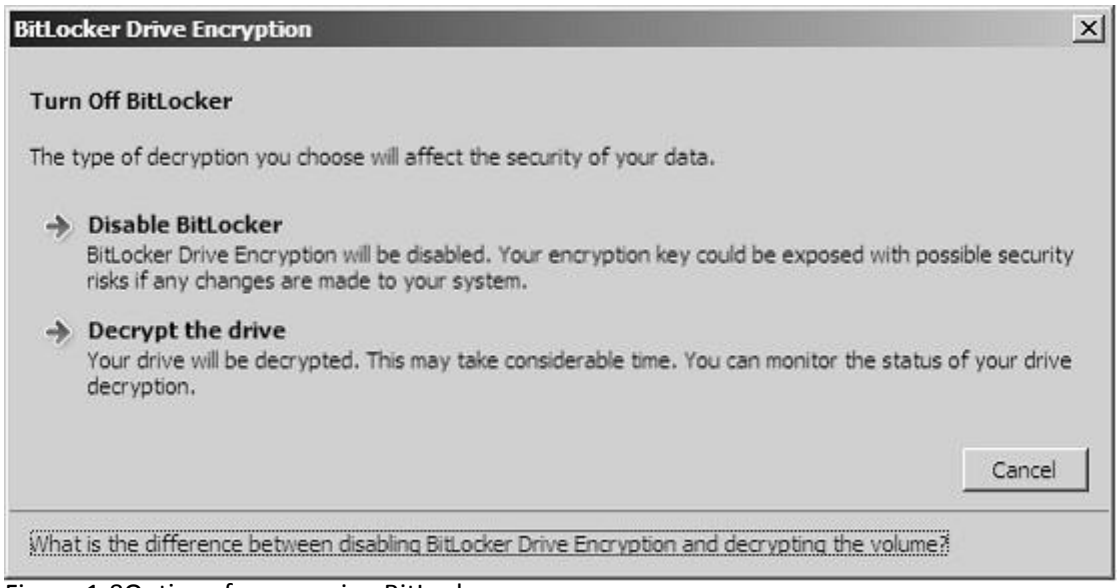


Figure 1-8Options for removing BitLocker

Disabling BitLocker removes BitLocker protection without decrypting the encrypted volumes. This is useful if a TPM chip is present, but it is necessary to update a computer's BIOS or startup files. If you do not disable

BitLocker when performing this type of maintenance, BitLocker—when implemented with a TPM chip—will lock the computer because the diagnostics will detect that the computer has been tampered with. When you disable BitLocker, a plaintext key is written to the hard disk drive. This allows the encrypted hard disk drive to be read, but the presence of the plaintext key means that the computer is insecure. Disabling BitLocker using this method provides no performance increase because the data remains encrypted—it is just encrypted in an insecure way. When BitLocker is re-enabled, this plaintext key is removed and the computer is again secure.

Exam Tip Keep in mind the conditions under which you might need to disable BitLocker. Also remember the limitations of BitLocker without a TPM 1.2 chip.

Select Decrypt The Drive when you want to completely remove BitLocker from a computer. This process is as time-consuming as performing the initial drive encryption—perhaps more so because more data might be stored on the computer than when the initial encryption occurred. After the decryption process is finished, the computer is returned to its pre-encrypted state and the data stored on it is no longer protected byBitLocker.

Decrypting the drive will not decrypt EFS-encrypted files stored on the hard disk drive.

Question: 62

Your company plans to deploy eight file servers that run Windows Server 2008 R2. All file servers will connect to Ethernet switches. You need to plan a data storage solution that meets the following requirements:

- Allocates storage to the servers as needed
- Utilizes the existing network infrastructure
- Maximizes performance

- Maximizes fault tolerance

Which actions should you include in your plan?

A. Install Windows Server 2008 R2 Datacenter on each server. Deploy the servers in a failover cluster. Deploy an iSCSI storage area network (SAN).
B. Install Windows Server 2008 R2 Standard on each server. Deploy the servers in a Network Load Balancing (NLB) cluster. Implement RAID?5 on each server.
C. Install Windows Server 2008 R2 Enterprise on each server. Deploy the servers in a failover cluster. Deploy a Fibre Channel (FC) storage area network (SAN).
D. Install Windows Server 2008 R2 Enterprise on each server. Deploy the servers in a Network Load Balancing (NLB) cluster. Map a network drive on each server to an external storage array.

Answer: A

Explanation:
DataCenter has Failover Cluster and of course a SAN with ISCSI will utilize the existing network topology.

Question: 63

You plan to deploy a distributed database Application that runs on multiple Windows Server 2008 R2 servers.
You need to design a storage strategy that meets the following requirements:
·Allocates storage to servers as required
·Uses the existing network infrastructure
·Uses standard Windows management tools
·Ensures that data is available if a single disk fails
What should you include in your design?

A. An iSCSI disk storage subsystem that supports Microsoft Multipath I/O. Configure the storage subsystem as a RAID?0 array.
B. An iSCSI disk storage subsystem that supports Virtual Disk Service (VDS). Configure the storage subsystem as a RAID?5 array.
C. A Fibre Channel (FC) disk storage subsystem that supports Microsoft Multipath I/O. Configure the storage subsystem as a RAID?0 array.
D. A Fibre Channel (FC) disk storage subsystem that supports the Virtual Disk Service (VDS). Configure the storage subsystem as a RAID?5 array.

Answer: B

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Virtual Disk Service (VDS)
Virtual Disk Service (VDS) provides a standard set of application programming interfaces (APIs) that provide a single interface through which disks can be managed. VDS provides a complete solution for managing storage hardware and disks and enables you to create volumes on those disks. This means that you can use a single tool to manage devices in a mixed storage environment rather than tools provided by different hardware vendors. Before you can manage a LUN using Storage Manager For SANs, you must install its VDS hardware provider. This will usually be provided by the hardware vendor. Prior to purchasing a storage device to be used on your organization's SAN, you should verify that a compatible VDS hardware provider exists.
VDS defines a software and a hardware provider interface. Each of these providers implements a different portion of the VDS API. The software provider is a program that runs on the host and is supported by a kernelmode driver.

Software providers operate on volumes, disks, and partitions. The hardware provider manages the actual storage subsystem. Hardware providers are usually disk array or adapter cards that enable the creation of logical disks for each LUN type. The LUN type that can be configured will depend on the options allowed by the VDS hardware provider. For example, some VDS hardware providers will allow the RAID-5 (Striped with Parity) LUN type to be implemented, while others might be limited to providing the Mirrored or Spanned LUN types.
MORE INFO More on VDS
For more information on the functionality of VDS, consult the following TechNet article:http://technet2.microsoft.com/windowsserver/en/library/dc77e7c7-ae44-4483-878b-6bc3819e64dc1033.mspx?mfr=true
Storage Manager For SANs
You can use the Storage Manager For SANs console to create LUNs on Fibre Channel and iSCSI storage arrays. You install Storage Manager For SANs as a Windows Server 2008 feature. To use Storage Manager
For SANs to manage LUNs, the following criteria must be met:
■The storage subsystems that you are going to manage must support VDS.
■The VDS hardware provider for each subsystem must already be installed on the Windows Server 2008 computer. When you open Storage Manager For SANs from the Administrative Tools menu, you are presented with three main nodes, which have the following functionality:
■LUN ManagementThis node lists all of the LUNs created with Storage Manager For SANs. From this node you can create new LUNs, extend the size of existing LUNs, assign and unassign LUNs, and delete LUNs. You can also use this node to configure the Fibre Channel and iSCSI connections that servers use to access LUNs.
■SubsystemsThis node lists all of the storage subsystems currently discovered within the SAN environment. You can rename subsystems using this node.
■DrivesThis node lists all of the drives in the storage subsystems discovered in the SAN. You can identify drives that you are working with by making the drive light blink from this node.
You can use any LUN type that is supported by the storage subsystem that you are deploying. The different
LUN types are:
■SimpleA simple LUN uses either an entire physical drive or a portion of that drive. The failure of a disk in a simple LUN means that all data stored on the LUN is lost.
■SpannedA spanned LUN is a simple LUN that spans multiple physical drives. The failure of any one disk in a spanned LUN means that all data stored on the LUN is lost.
■StripedData is written across multiple physical disks. This type of LUN, also known as RAID-0 has improved
I/O performance because data can be read and written to multiple disks simultaneously, but like a spanned LUN, all data will be lost in the event that one disk in the array fails.
■MirroredThis LUN type, also known as RAID-1, is fault tolerant. Identical copies of the LUN are created on two physical drives. All read and write operations occur concurrently on both drives. If one disk fails, the LUN continues to be available on the unaffected disk.
■Striped with ParityThis LUN type, also known as RAID-5, offers fault tolerance and improved read performance, although write performance is hampered by parity calculation. This type requires a minimum of three disks and the equivalent of one disk's worth of storage is lost to the storage of parity information across the disk set. This LUN type will retain data if one disk is lost, but all data will be lost if two disks in the array fail at the same time. In the event that one disk fails, it should be replaced as quickly as possible.

Question: 64

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

Answer: C

Explanation:
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: 65

Your company has a main office and a branch office. Your network contains a single Active Directory domain. The functional level of the domain is Windows Server 2008 R2. An Active Directory site exists for each office. All servers run Windows Server 2008 R2. You plan to deploy file servers in each office. You need to design a file sharing strategy to meet the following requirements:

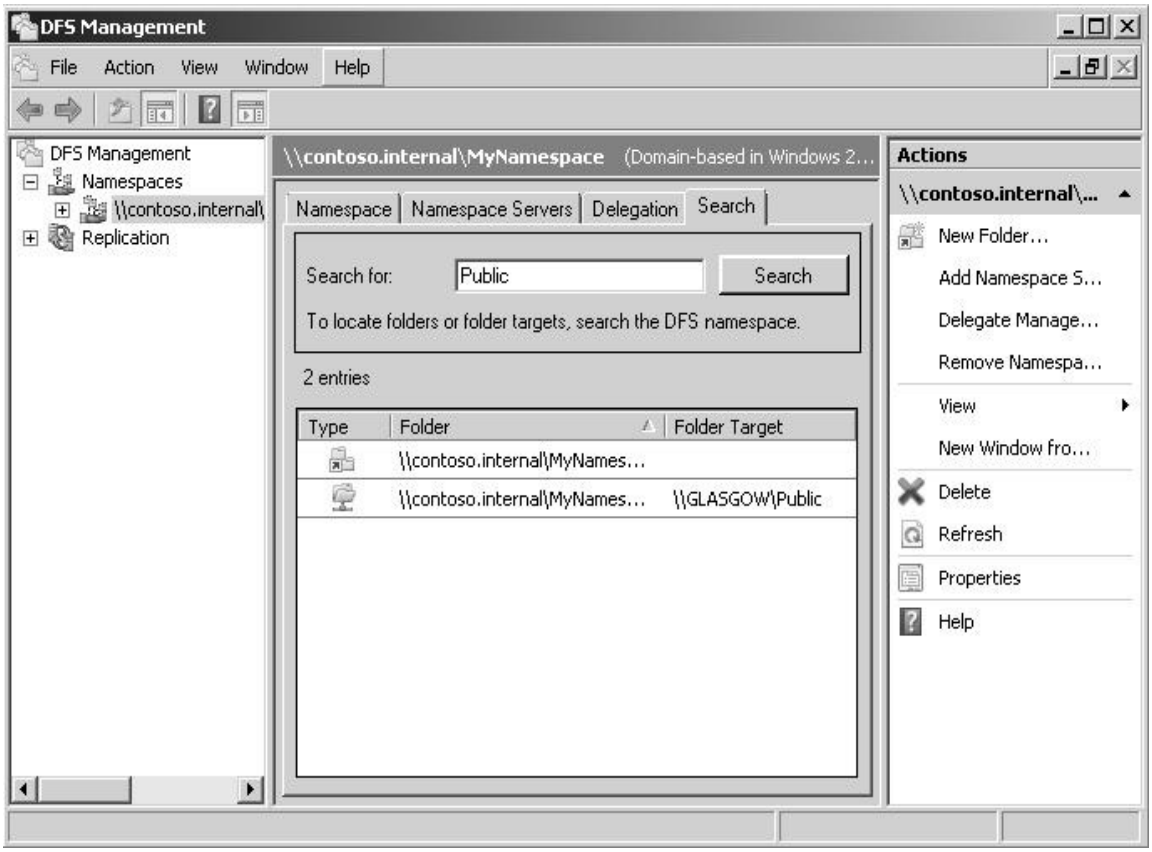
- Users in both offices must be able to access the same files.
- Users in both offices must use the same Universal Naming Convention (UNC) path to access files.
- The design must reduce the amount of bandwidth used to access files.
- Users must be able to access files even if a server fails.

What should you include in your design?

A. A standalone DFS namespace that uses replication.
B. A domainbased DFS namespace that uses replication.
C. A multisite failover cluster that contains a server located in the main office and another server located in the branch office.
D. A Network Load Balancing cluster that contains a server located in the main office and another server located in the branch office.

Answer: B

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
Domain-Based Namespaces
You can create domain-based namespaces on one or more member servers or DCs in the same domain.
Metadata for a domain-based namespaces is stored by AD DS. Each server must contain an NTFS volume to host the namespace. Multiple namespace servers increase the availability of the namespace and ensure failover protection. A domain-based namespace cannot be a clustered resource in a failover cluster. However, you can locate the namespace on a server that is also a node in a failover cluster provided that you configure the namespace to use only local resources on that server. A domain-based namespace in Windows Server
2008 mode supports access-based enumeration. Windows Server 2008 mode is discussed later in this lesson.
You choose a domain-based namespace if you want to use multiple namespace servers to ensure the availability of the namespace, or if you want to make the name of the namespace server invisible to users.
When users do not need to know the UNC path to a namespace folder it is easier to replace the namespace server or migrate the namespace to another server.
If, for example, a stand-alone namespace called \\Glasgow\Books needed to be transferred to a server called Brisbane, it would become \\Brisbane\Books. However, if it were a domain-based namespace (assuming Brisbane and Glasgow are both in the Contoso.internal domain), it would be \\Contoso.internal\Books no matter which server hosted it, and it could be transferred from one server to the other without this transfer being apparent to the user, who would continue to use \\Contoso.internal\Books to access it.



Question: 66

Your network consists of a single Active Directory domain. The network contains a file server that runs Windows Server 2008 R2. All servers use internal storage only. You plan to deploy a client/server Application. You need to deploy the Application so that it is available if a single server fails. You must achieve this goal while minimizing costs. What should you do?

A. Deploy RemoteApp.
B. Deploy a failover cluster that uses No Majority: Disk Only.
C. Deploy a failover cluster that uses Node and File Share Disk Majority.
D. Deploy Distributed File System (DFS) and configure replication.

Answer: C

Explanation:
Understanding Cluster Quorum Models
Quorums are used to determine the number of failures that can be tolerated within a cluster before the cluster itself has to stop running. This is done to protect data integrity and prevent problems that could occur because of failed or failing communication between nodes.
Quorums describe the configuration of the cluster and contain information about the cluster components such as network adapters, storage, and the servers themselves. The quorum exists as a database in the registry and is maintained on the witness disk or witness share. The witness disk or share keeps a copy of this configuration data so that servers can join the cluster at any time, obtaining a copy of this data to become part of the cluster.
One server manages the quorum resource data at any given time, but all participating servers also have a copy.
You can use the following four quorum models with Windows Server 2008 Failover Clusters:
■Node Majority Microsoft recommends using this quorum model in Failover Cluster deployments that contain an odd

number of cluster nodes. A cluster that uses the Node Majority quorum model is called a Node Majority cluster and remains up and running if the number of available nodes exceeds the number of failed nodes—that is, half plus one of its nodes is available. For example, for a seven-node cluster to remain online, four nodes must be available. If four nodes fail in a seven-node Node Majority cluster, the entire cluster shuts down. You should use Node Majority clusters in geographically or network-dispersed cluster nodes. To operate successfully this model requires an extremely reliable network, high-quality hardware, and a third-party mechanism to replicate back-end data.

■Node and Disk Majority Microsoft recommends using this quorum model in clusters that contain even numbers of cluster nodes. Provided that the witness disk remains available, a Node and Disk Majority cluster remains up and running when one-half or more of its nodes are available. A six-node cluster will not shut down if three or more nodes plus its witness disk are available. In this model, the cluster quorum is stored on a cluster disk that is accessible to all cluster nodes through a shared storage device using Serial Attached SCSI (SAS), Fibre Channel, or iSCSI connections. The model consists of two or more server nodes connected to a shared storage device and a single copy of the quorum data is maintained on the witness disk. You should use the Node and Disk Majority quorum model in Failover Clusters with shared storage, all connected on the same network and with an even number of nodes. In the case of a witness disk failure, a majority of the nodes need to remain up and running. For example, a six-node cluster will run if (at a minimum) three nodes and the witness disk are available. If the witness disk is offline, the same six-node cluster requires that four nodes are available.

Exam Tip If the 70-646 examination asks which quorum model is the closest to the traditional single-quorum device cluster configuration model, the answer is the Node and Disk Majority quorum model.

■Node and File Share Majority This configuration is similar to the Node and Disk Majority model, but the quorum is stored on a network share rather than on a witness disk. A Node and File Share Majority cluster can be deployed in a similar fashion to a Node Majority cluster, but as long as the witness file share is available the cluster can tolerate the failure of half its nodes. You should use the Node and File Share Majority quorum model in clusters with an even number of nodes that do not utilize shared storage.

■No Majority: Disk Only Microsoft recommends that you do not use this model in a production environment because the disk containing the quorum is a single point of failure. No Majority: Disk Only clusters are best suited for testing the deployment of built-in or custom services and applications on a Windows Server 2008 Failover Cluster. In this model, provided that the disk containing the quorum remains available, the cluster can sustain the failover of all nodes except one.

MORE INFO Quorum models webcast

Four quorum models are available with Windows Server 2008. For more information on the models, view the TechNet webcast at http://msevents.microsoft.com/CUI/WebCastEventDetails .aspx?EventID=1032364841&EventCategory=4&culture=en-US&CountryCode=US

Question: 67

Your company has a main office and a branch office. The offices connect by using WAN links. The network consists of a single Active Directory domain. An Active Directory site exists for each office. Servers in both offices run Windows Server 2008 R2 Enterprise. You plan to deploy a failover cluster solution to service users in both offices.

You need to plan a failover cluster to meet the following requirements:

·Maintain the availability of services if a single server fails

·Minimize the number of servers required

What should you include in your plan?

A. Deploy a failover cluster that contains one node in each office.

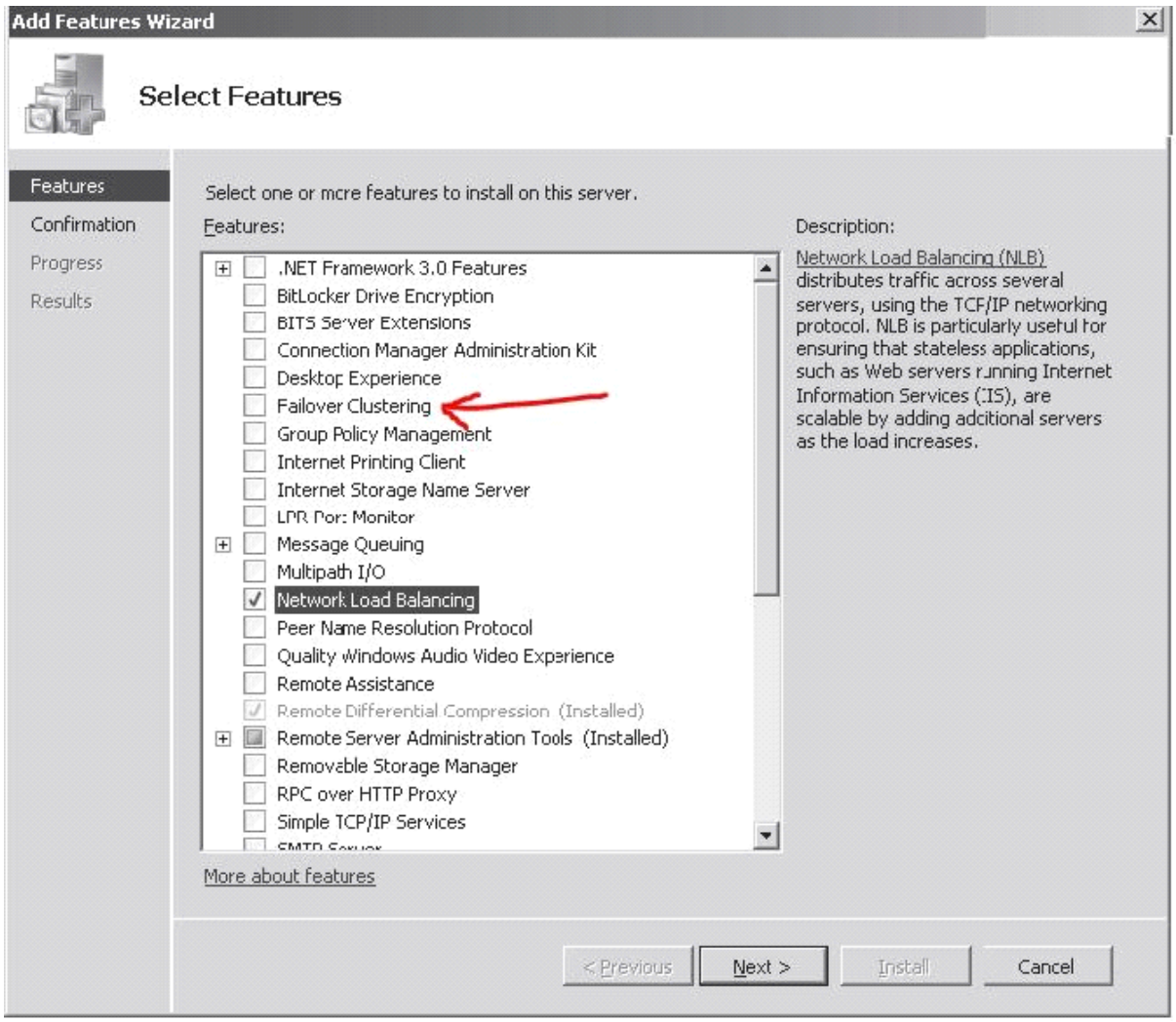
B. Deploy a failover cluster that contains two nodes in each office.

C. In the main office, deploy a failover cluster that contains one node. In the branch office, deploy a failover cluster that contains one node.

D. In the main office, deploy a failover cluster that contains two nodes. In the branch office, deploy a failover cluster that contains two nodes.

Answer: A

Explanation:
MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:
■Failover Clustering Failover 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.
■Failover clustering The Failover Clustering feature enables multiple servers to work together to increase the availability of services and applications. If one of the clustered servers (or nodes) fails, another node provides the required service through failover and is available in Windows Server 2008 Enterprise and Datacenter editions and is not available in Windows Server 2008 Standard or Web editions.
Failover clustering - Formerly known as server clustering, Failover Clustering creates a logical grouping of servers, also known as nodes, that can service requests for applications with shared data stores.



Question: 68

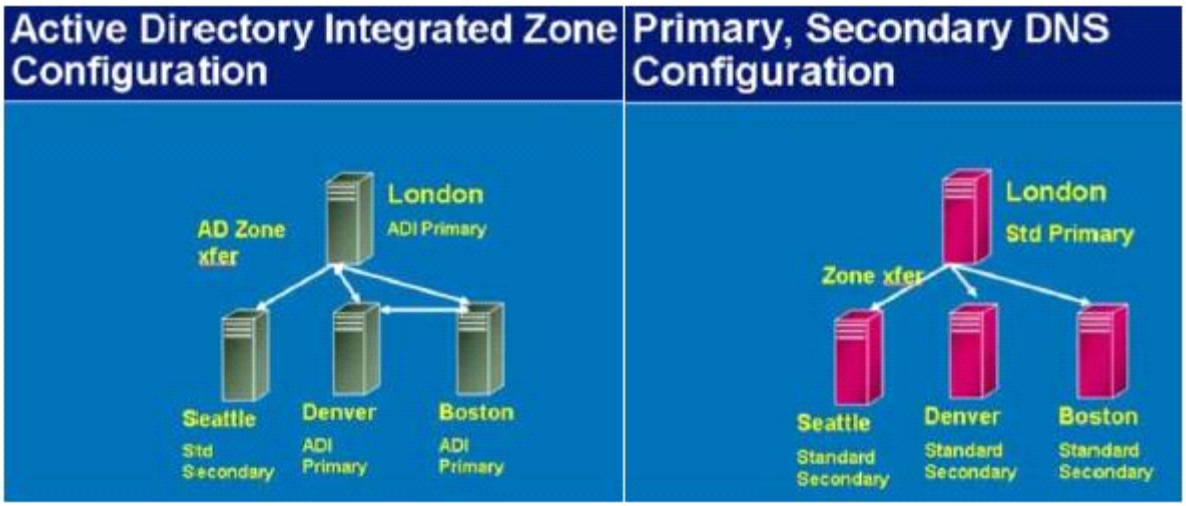
Your company has a main office and a branch office. Your network contains a single Active Directory domain. An Active Directory site exists for each office. All domain controllers run Windows Server 2008 R2. You plan to modify the DNS infrastructure. You need to plan the new DNS infrastructure to meet 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.

Answer: B

Explanation:
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.

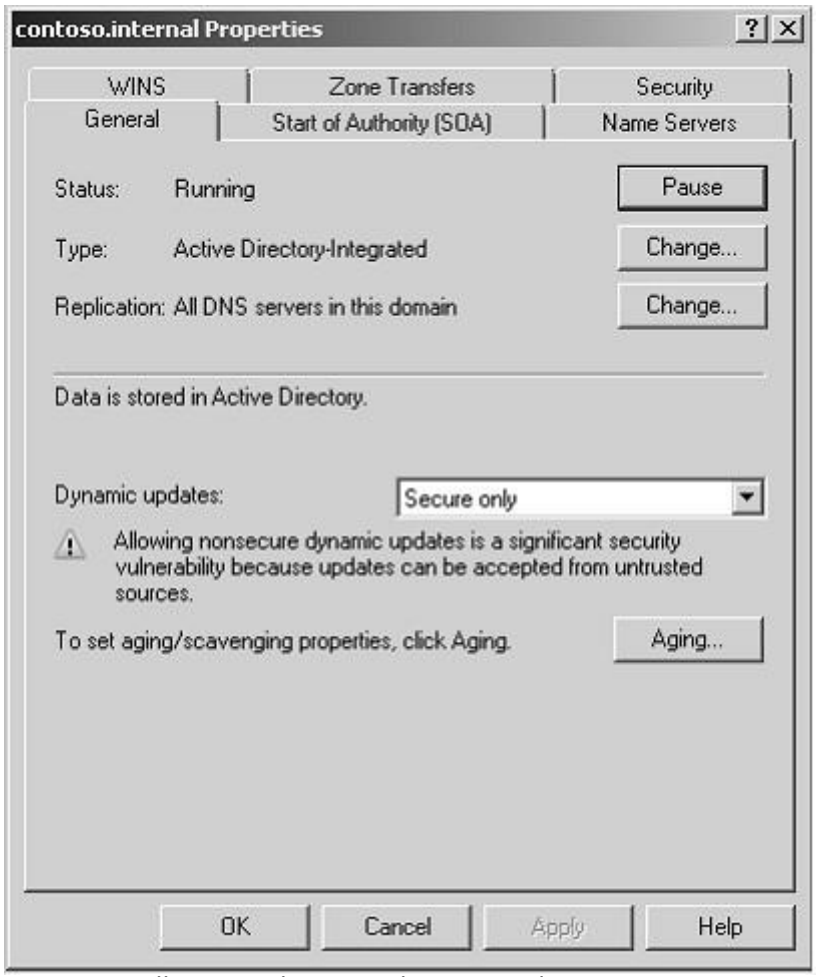


Figure 2-22Allowing only secure dynamic updates
MORE INFODynamic update protocol
For more information about the dynamic update protocol, see http://www.ietf.org/rfc/rfc2136.txt and http://www.ietf.org/rfc/rfc3007
NOTE Secure dynamic updates
Secure dynamic updates are only available for zones that are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

Question: 69

Your network consists of a single Active Directory domain. All servers run Windows Server 2008 R2. You plan to publish a Web site on two Web servers. You need to deploy an availability solution for your Web servers that meets the following requirements:

- Supports the addition of more Web servers without interrupting client connections
- Ensures that the Web site is accessible even if a single server fails

What should you do?

A. Configure a failover cluster.
B. Configure a Web garden on each Web server.
C. Create a Network Load Balancing cluster.
D. Create two Application pools on each Web server.

Answer: C

Explanation:
Windows Web Server 2008
Windows Web Server 2008 is designed to function specifically as a Web applications server. Other roles, such as Windows Deployment Server and Active Directory Domain Services, are not supported on Windows Web Server 2008. You deploy this server role either on a screened subnet to support a Web site viewable to external hosts or as an intranet server. As appropriate given its stripped-down role, Windows Web Server 2008 does not support the high-powered hardware configurations that other editions of Windows Server 2008 do.
Windows Web Server 2008 has the following properties:
- The 32-bit version (x86) supports a maximum of 4 GB of RAM and 4 processors in SMP configuration.
- The 64-bit version (x64) supports a maximum of 32 GB of RAM and 4 processors in SMP configuration.
- Supports Network Load Balancing clusters.

You should plan to deploy Windows Web Server 2008 in the Server Core configuration, which minimizes its attack surface, something that is very important on a server that interacts with hosts external to your network environment. You should only plan to deploy the full version of Windows Web Server 2008 if your organization's Web applications rely on features such as ASP.NET, because the .NET Framework is not included in a Server Core installation.
Configuring Windows Network Load Balancing
While DNS Round Robin is a simple way of distributing requests, Windows Server 2008 NLB is a much more robust form of providing high availability to applications. Using NLB, an administrator can configure multiple servers to operate as a single cluster and control the usage of the cluster in near real-time.
NLB operates differently than DNS Round Robin in that NLB uses a virtual network adapter on each host. This virtual network adapter gets a single IP and media access control (MAC) address, which is shared among the hosts participating in the load-balancing cluster. Clients requesting services from an NLB cluster have their requests sent to the IP address of the virtual adapter, at which point it can be handled by any of the servers in the cluster.
NLB automatically reconfigures as nodes are added and removed from the cluster. An administrator can add and remove nodes through the NLB Manager interface or the command line. For example, an administrator might remove each node in turn to perform maintenance on the nodes individually and cause no disruption in service to the end user.
Servers within NLB clusters are in constant communication with each other, determining which servers are available with a process known as heartbeats and convergence. The heartbeat consists of a server participating in an NLB cluster that sends out a message each second to its NLB-participating counterparts.
When five (by default) consecutive heartbeats are missed, convergence begins. Convergence is the process by which the remaining hosts determine the state of the cluster.
During convergence, the remaining hosts listen for heartbeats from the other servers to determine the host with the highest priority, which is then selected as the default host for the NLB cluster. Generally, two scenarios can trigger convergence. The first is the missed heartbeat scenario mentioned earlier; the second is removal or addition of a server to the cluster by an administrator. The heartbeat is reduced by one half during convergence. A less common reason for convergence is a change in the host configuration, such as a host priority.

Question: 70

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

Answer: D

Explanation:
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 ofWindows 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.

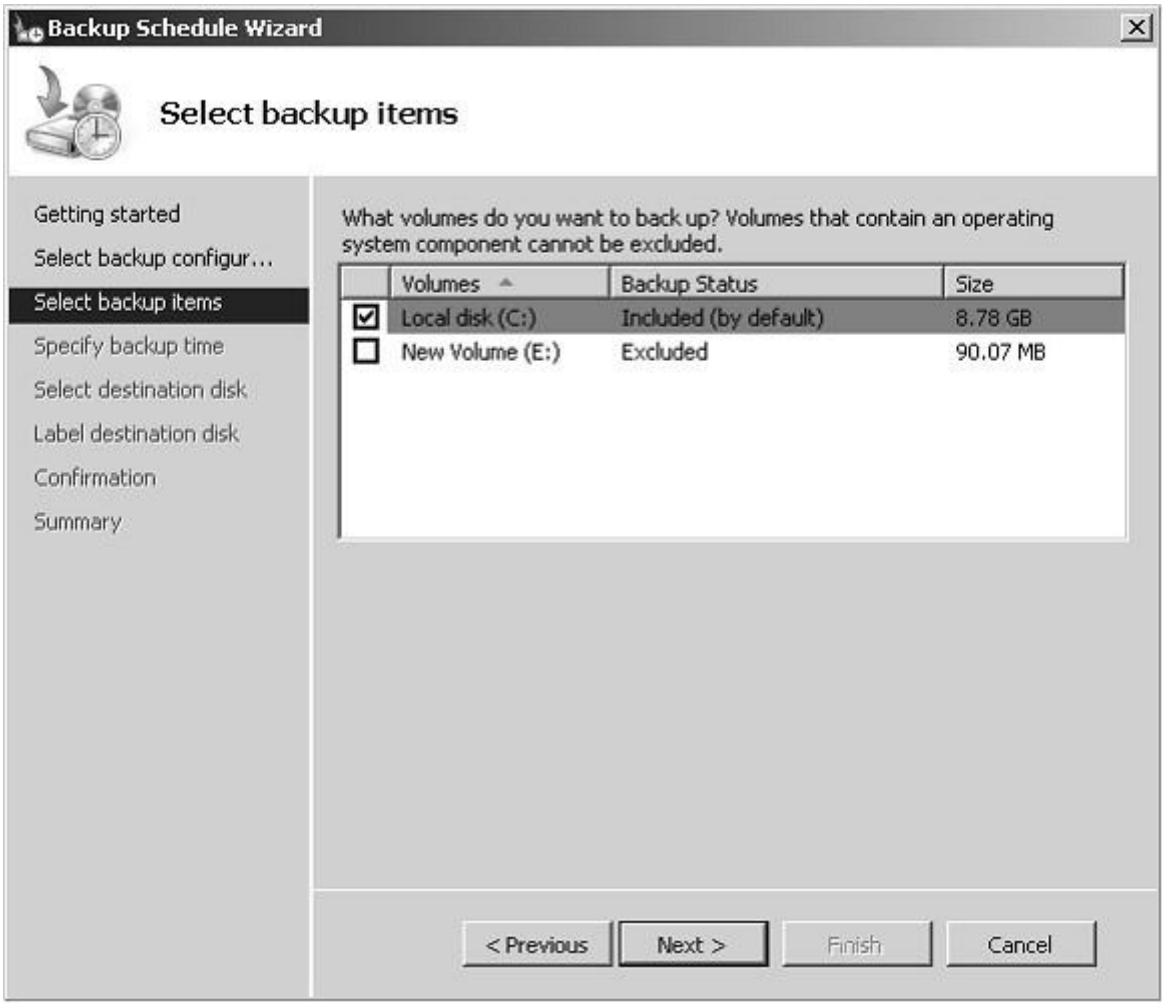


Figure 12-3Selecting backup items
3.The default backup schedule is once a day at 9:00 P.M. You can configure multiple backups to be taken during the

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.

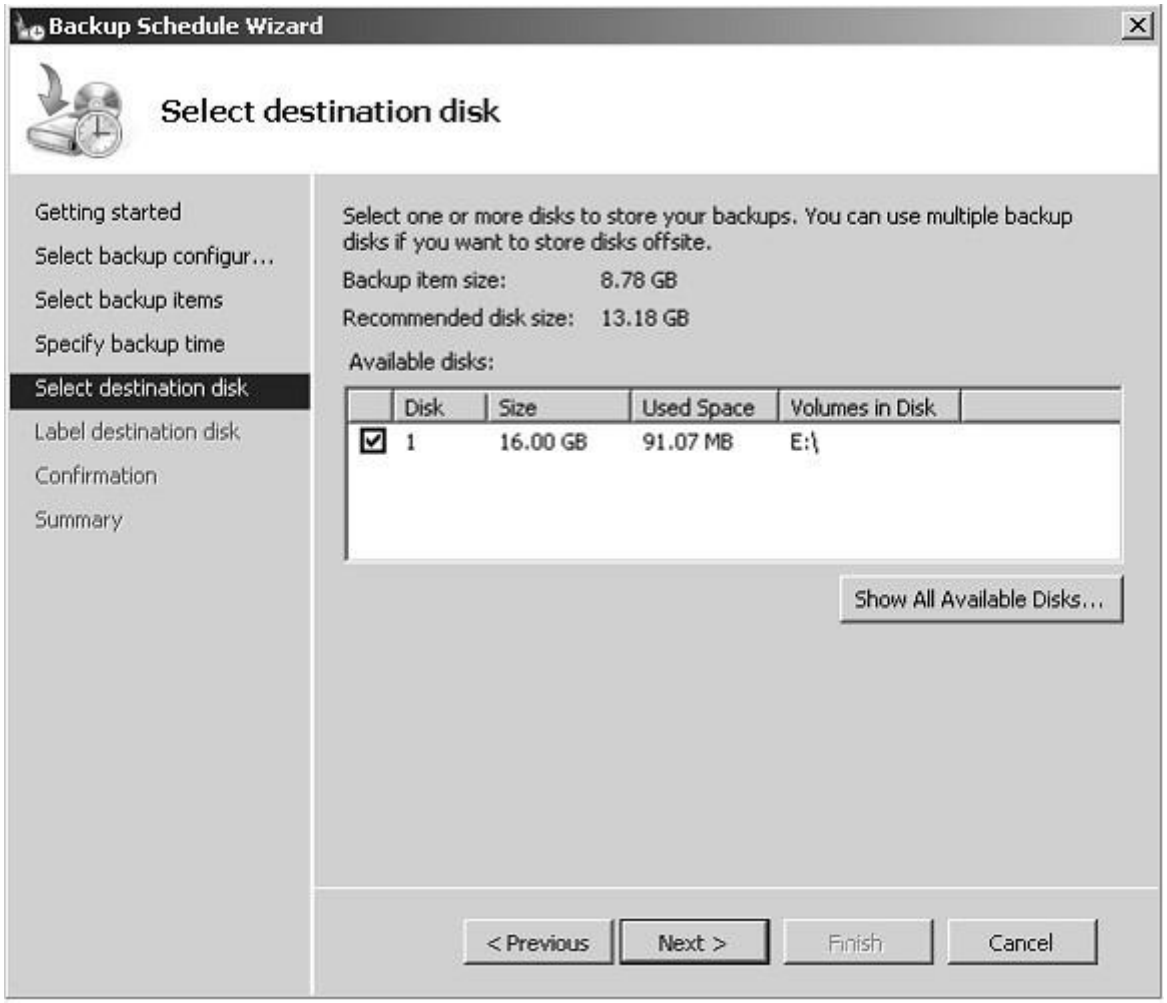


Figure 12-4Selecting a destination disk

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 BackupUse 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 BackupUse 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.

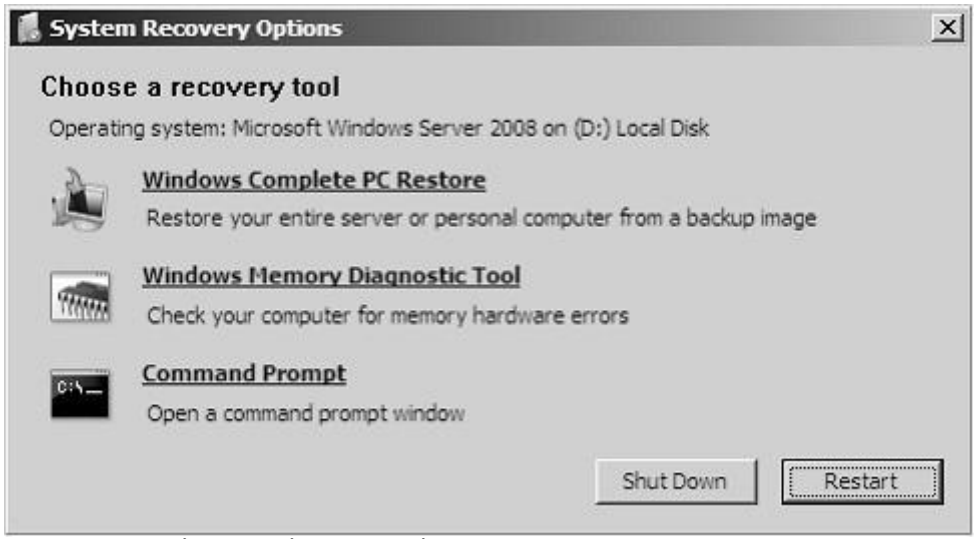


Figure 12-13Select Windows Complete PC Restore

Question: 71

Your network consists of a single Active Directory forest. The forest contains one Active Directory domain. The domain contains eight domain controllers. The domain controllers run Windows Server 2003 Service Pack 2. You upgrade one of the domain controllers to Windows Server 2008 R2. You need to recommend an Active Directory recovery strategy that supports the recovery of deleted objects. The solution must allow deleted objects to be recovered for up to one year after the date of deletion. What should you recommend?

A. Increase the tombstone lifetime for the forest.
B. Increase the interval of the garbage collection process for the forest.
C. Configure daily backups of the Windows Server 2008 R2 domain controller.
D. Enable shadow copies of the drive that contains the Ntds.dit file on the Windows Server 2008 R2 domain controller.

Answer: A

Explanation:
The tombstone lifetime must be substantially longer than the expected replication latency between the domain controllers. The interval between cycles of deleting tombstones must be at least as long as the maximum replication propagation delay across the forest. Because the expiration of a tombstone lifetime is based on the time when an object was deleted logically, rather than on the time when a particular server received that tombstone through replication, an object's tombstone is collected as garbage on all servers at approximately the same time. If the tombstone has not yet replicated to a particular domain controller, that DC never records the deletion. This is the reason why you cannot restore a domain controller from a backup that is older than the tombstone lifetime
By default, the Active Directory tombstone lifetime is sixty days. This value can be changed if necessary. To change this value, the tombstoneLifetime attribute of the CN=Directory Service object in the configuration partition must be modified.
This is related to server 2003 but should still be relelvant http://www.petri.co.il/
changing_the_tombstone_lifetime_windows_ad.htm
Authoritative Restore
When a nonauthoritative restore is performed, objects deleted after the backup was taken will again be deleted when the restored DC replicates with other servers in the domain. On every other DC the object is marked as deleted so that when replication occurs the local copy of the object will also be marked as deleted. The authoritative restore process marks the deleted object in such a way that when replication occurs, the object is restored to active status across the domain. It is important to remember that when an object is deleted it is not instantly removed from Active Directory, but gains an attribute that marks it as deleted until the tombstone lifetime is reached and the object is removed. The tombstone lifetime is the amount of time a deleted object remains in Active Directory and has a default value of 180 days.
To ensure that the Active Directory database is not updated before the authoritative restore takes place, you use the Directory Services Restore Mode (DSRM) when performing the authoritative restore process. DSRM allows the administrator to perform the necessary restorations and mark the objects as restored before rebooting the DC and allowing those changes to replicate out to other DCs in the domain.

Question: 72

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).

Answer: B

Explanation:
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.

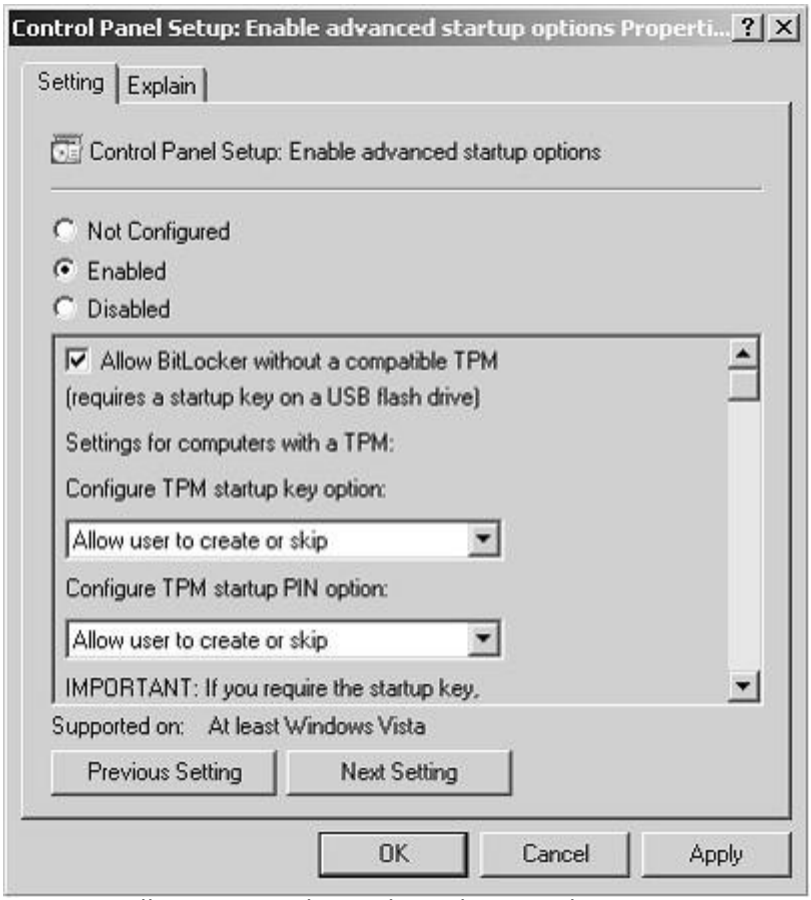


Figure 1-7Allowing BitLocker without the TPM chip

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: 73

Your network consists of a single Active Directory domain. The domain controllers run Windows Server 2008 R2. Your company's enterprise security policy states that the domain controllers cannot contain optical drives. You need to recommend a backup and recovery plan that restores the domain controllers in the event of a catastrophic server failure. What should you recommend?

A. Use Windows Server Backup to back up each domain controller to a local disk. Create a Windows Recovery Environment (Windows RE) partition on each domain controller.

B. Use Windows Server Backup to back up each domain controller to a local disk. Use Windows Deployment Services (WDS) to deploy the Windows Recovery Environment (Windows RE).

C. Use Windows Server Backup to back up each domain controller to a remote network share. Create a Windows Recovery Environment (Windows RE) partition on each domain controller.

D. Use Windows Server Backup to back up each domain controller to a remote network share. Use Windows Deployment Services (WDS) to deploy the Windows Recovery Environment (Windows RE).

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/cc766048(WS.10).aspx
http://technet.microsoft.com/en-us/library/cc765966(v=WS.10).aspx
(Must Read)
http://technet.microsoft.com/en-us/magazine/2008.10.desktopfiles.aspx
Special considerations
You must be a member of the Administrators group or Backup Operators group to use Windows Server Backup.
In Windows Server 2008, the firewall has been enabled by default. If you are managing the backups of another computer using the Windows Server Backup snap-in, your connectivity to the remote computer may be affected and can be resolved by changes in the firewall rules.
While working on the local computer, you are not affected.
Also, if you are a current user of the previous backup feature (Ntbackup.exe) that shipped in earlier versions of Windows, and plan to switch to the new Windows Server Backup, you might be affected by the following issues and changes:
Settings for creating backups will not be upgraded when you upgrade to Windows Server
2008. You will need to reconfigure settings.
You will need a separate, dedicated disk for running scheduled backups.
Only NTFS-formatted volumes on a locally attached disk can be backed up.
You can no longer back up to tape. (However, support of tape storage drivers is still included in Windows Server 2008.)
Windows Server Backup supports backing up to external and internal disks, DVDs, and shared folders.
You cannot recover backups that you created with Ntbackup.exe by using Windows Server
Backup. However, a version of Ntbackup.exe is available as a download to Windows Server
2008 for users who want to recover data from backups created using Ntbackup.exe. The downloadable version of Ntbackup.exe is only for recovering backups for older versions of
Windows and cannot be used to create new backups in Windows Server 2008.
Windows Server 2008 R2 including:
The ability to backup System State as a separate job as well as the ability to do incremental System State backups.
The ability to exclude specific file types, file folders, and specific files instead of having to backup an entire volume.
The ability to backup to a volume or a network share instead of requiring a dedicated disk for backups.
Windows Recovery Technical Reference
Windows Recovery Environment (Windows RE) is an extensible recovery platform based on Windows Preinstallation Environment (Windows PE). When the computer fails to start, Windows automatically fails over into this environment, and the Startup Repair tool in Windows RE automates the diagnosis and repair of an unbootable Windows Vista installation. Furthermore, Windows RE is a starting point for various tools for manual system recovery. The primary audience of this technology includes original equipment manufacturers
(OEMs), original device manufacturers (ODMs), and corporate IT professionals.
Image-based Recovery from Windows RE
In the event that the Windows installation cannot be repaired with Startup Repair or other manual repair steps, Windows RE can be used to launch an image-based recovery tool.
User-created Recovery Image
Windows Vista provides end users with the ability to create a backup image of their entire operating system.
End users can do this by using the Backup tool. The system image can be stored on an external hard disk, on a hard disk partition other than those imaged, or on a DVD. To restore the computer by using this system image, users must launch the restore interface from the list of Windows RE manual tools.
Factory-created Recovery Image
To facilitate restoring a computer to its factory state, a recovery image can be placed on the Windows RE partition. This eliminates the need for a separate recovery media in most cases.
If the Windows image format is used in the manufacturing process, the same operating system image can be used for recovery as well. A computer manufacturer can develop an application by using the Imaging APIs for Windows and the Windows image to restore the operating system volume. This application can be launched from the Windows RE user interface (UI) by using customizations provided by the ODM.

Question: 74

Your company has Windows Server 2008 R2 file servers.
You need to recommend a data recovery strategy that meets the following requirements:
·Backups must have a minimal impact on performance.
·All data volumes on the file server must be backed up daily.
·If a disk fails, the recovery strategy must allow individual files to be restored.
·Users must be able to retrieve previous versions of files without the intervention of an administrator. What should you recommend?

A. Deploy File Server Resource Manger (FSRM). Use Windows Server Backup to perform a daily backup to an external disk.
B. Deploy Windows Automated Installation Kit (Windows AIK). Enable shadow copies for the volumes that contain shared user data. Store the shadow copies on a separate physical disk.
C. Use Windows Server Backup to perform a daily backup to an external disk. Enable shadow copies for the volumes that contain shared user data. Store the shadow copies on a separate physical disk.
D. Use Windows Server Backup to perform a daily backup to a remote network share. Enable shadow copies for the volumes that contain shared user data. Store the shadow copies in the default location.

Answer: C

Explanation:
Shadow Copies of Shared Folders
Implementing Shadow Copies of Shared Folders will reduce an administrator's restoration workload dramatically because it almost entirely eliminates the need for administrator intervention in the recovery of deleted, modified, or corrupted user files. Shadow Copies of Shared Folders work by taking snapshots of files stored in shared folders as they exist at a particular point in time. This point in time is dictated by a schedule and the default schedule for Shadow Copies of Shared Folders is to be taken at 7:00 A.M. and 12:00 P.M. every weekday. Multiple schedules can be applied to a volume and the default schedule is actually two schedules applied at the same time.
To enable Shadow Copies of Shared Folders, open Computer Management from the Administrative Tools menu, right-click the Shared Folders node, click All Tasks and then click Configure Shadow Copies. This will bring up the Shadow Copies dialog box, shown in Figure 12-1. This dialog box allows you to enable and disable Shadow Copies on a per-volume basis. It allows you to edit the Shadow Copy of Shared Folder settings for a particular volume. It also allows you to create a shadow copy of a particular volume manually.

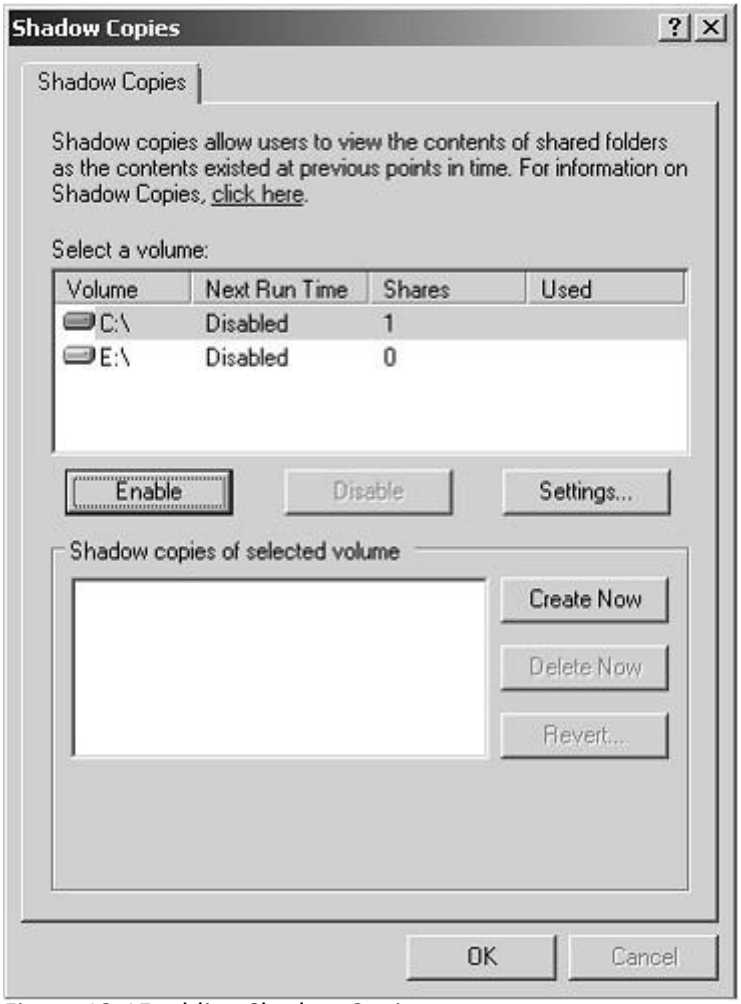


Figure 12-1Enabling Shadow Copies

Enabling Shadow Copies on a volume will automatically generate an initial shadow copy for that volume.

Clicking Settings launches the dialog box shown in Figure 12-2. From this dialog box, you can configure the storage area, the maximum size of the copy store, and the schedule of when copies are taken. Clicking Schedules allows you to configure how often shadow copies are generated. On volumes hosting file shares that contain files that are updated frequently, you would use a frequent shadow copy schedule. On a volume hosting file shares where files are updated less frequently, you should configure a less frequent shadow copy schedule.

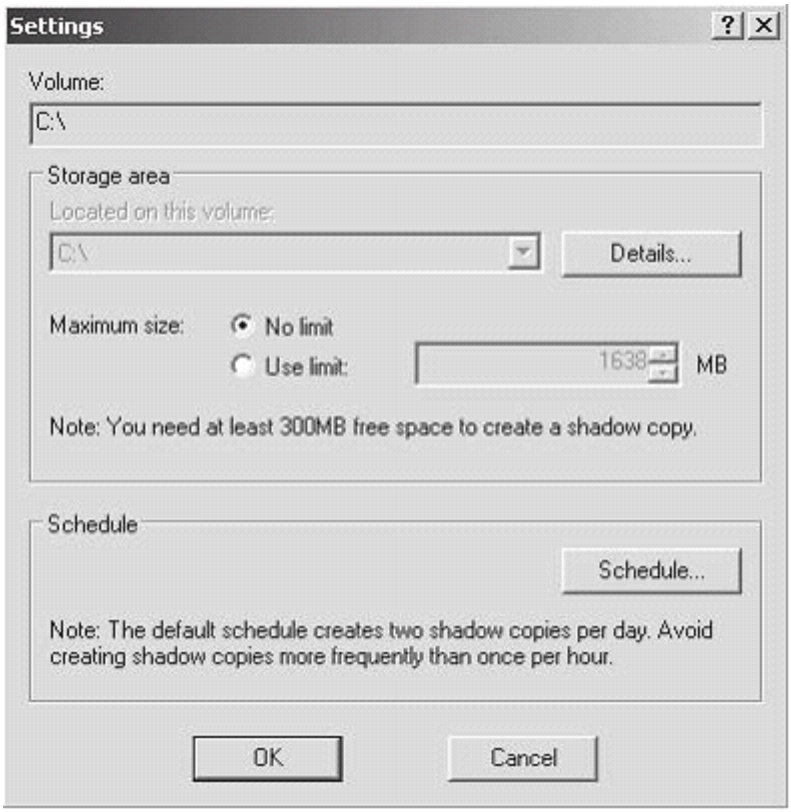


Figure 12-2Shadow Copy settings

When a volume regularly experiences intense read and write operations, such as a commonly used file share, you can mitigate the performance impact of Shadow Copies of Shared Folders by storing the shadow copy data on a separate volume. If a volume has less space available than the set limit, the service will remove the oldestshadow copies that it has stored as a way of freeing up space. Finally, no matter how much free space is available, a maximum of 64 shadow copies can be stored on any one volume. When you consider how scheduling might be configured for a volume, you will realize how this directly influences the length of shadow copy data retention. Where space is available, a schedule where shadow copies are taken once every Monday, Wednesday, and Friday allows shadow copies from 21 weeks previously to be retrieved. The default schedule allows for the retrieval of up to 6 weeks of previousshadow copies.

When planning the deployment of Shadow Copies of Shared Folders, it is important to remember that you configure settings on a per-volume basis. This means that the storage area, maximum size, and schedules for different volumes can be completely separate. If you plan shares in such a way that each volume hosts a single share, you can optimize the shadow copy settings for that share based on how the data is used, rather than trying to compromise in finding an effective schedule for very different shared folder usage patterns.

Quick Check

1.On what basis (server, volume, share, disk, or folder) are Shadow Copies of Shared Folders enabled?

2.What happens to shadow copy data when the volume that hosts it begins to run out of space?

Quick Check Answers

1.Shadow Copies of Shared Folders are enabled on a per-volume basis.

2.The oldest shadow copy data is automatically deleted when volumes begin to run out of space.

Question: 75

Your network consists of an Active Directory domain. The domain controllers run Windows Server 2008 R2. Client computers run Windows 7. You need to implement Encrypting File System (EFS) for all client computers. You want to achieve this goal while meeting the following requirements:

- You must minimize the amount of data that is transferred across the network when a user logs on to or off from a client computer.
- Users must be able to access their EFS certificates on any client computers.

- If a client computer's disk fails, EFS certificates must be accessible.

What should you do?

A. Enable credential roaming.
B. Enable roaming user profiles.
C. Enable a Data Recovery Agent.
D. Issue smart cards to all users.

Answer: A

Explanation:
Configuring Credential Roaming
Credential roaming allows for the storage of certificates and private keys within Active Directory. For example, a user's encrypting file system certificate can be stored in Active Directory and provided to the user when she logs on to different computers within the domain. The same EFS certificate will always be used to encrypt files.
This means that the user can encrypt files on an NTFS-formatted USB storage device on one computer and then decrypt them on another, because the EFS certificate will be transferred to the second computer's certificate store during the logon process.Credential roaming also allows for all of a user's certificates and keys to be removed when he logs off of the computer.
Credential roaming is enabled through the Certificate Services Client policy, located under User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies and shown in Figure 10-4.

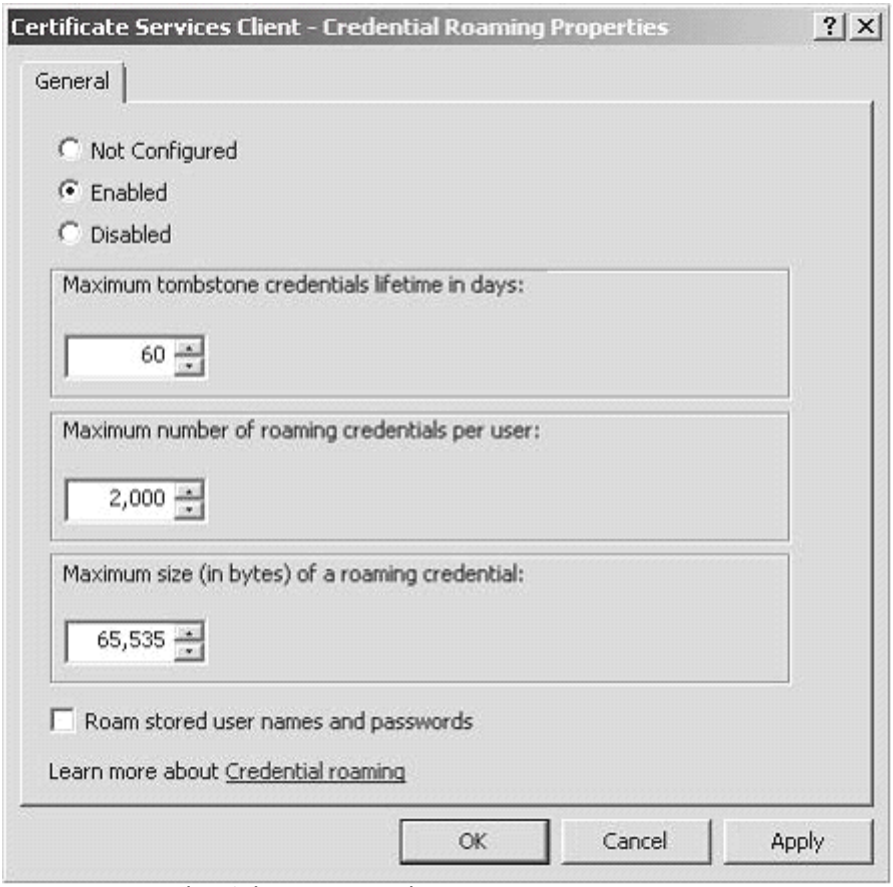


Figure 10-4Credential Roaming Policy
Credential roaming works in the following manner. When a user logs on to a client computer in a domain where the Credential Roaming Policy has been enabled, the certificates in the user's store on the client computer are compared to certificates stored for the user within Active Directory.
■If the certificates in the user's certificate store are up to date, no further action is taken.

■If more recent certificates for the user are stored in Active Directory, these credentials are copied to the client computer.
■If more recent certificates are located in the user's store, the certificates stored in Active Directory are updated.
Credential roaming synchronizes and resolves any conflicts between certificates and private keys from any number of client computers that a user logs on to, as well as certificates and private keys stored within Active Directory. Credential roaming is triggered whenever a private key or certificate in the local certificate store changes, whenever the user locks or unlocks a computer, and whenever Group Policy refreshes. Credential roaming is supported on Windows Vista, Windows Server 2008, Windows XP SP2, and Windows Server 2003
SP1.
MORE INFO More on credential roaming
For more information on configuring credential roaming, consult the following TechNet link:http://technet2.microsoft.com/windowsserver2008/en/library/fabc1c44-f2a2-43e1-b52e-9b12a1f19a331033.mspx?mfr=true

Question: 76

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.

Answer: B, C

Question: 77

You need to recommend a security strategy for WebApp2 that meets the company's Application requirements. What should you include in the recommendation?

A. Basic authentication and connection security rules
B. Basic authentication and SSL
C. Digest authentication and connection security rules
D. Digest authentication and SSL

Answer: B

Question: 78

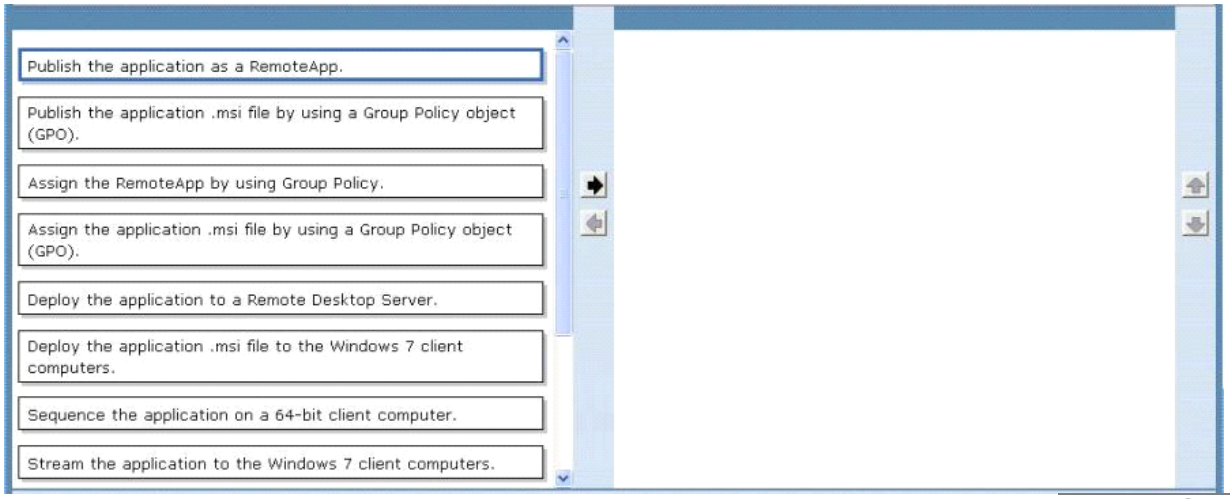
You need to ensure that Admin1 can administer the Web servers to meet the company's technical requirements. To which group should you add Admin1?

A. the Administrators local group on each Web server
B. the Backup Operators domain local group
C. the Backup Operators local group on each Web server
D. the Domain Admins global group

Answer: B

Question: 79

DRAG DROP
A company has servers that run Windows Server 2008 R2 and client computers that run 32-bit Windows 7 Enterprise. The environment includes Microsoft Application Visualization (App-V). You plan to deploy a 64-bit only Application. You need to ensure that users can run the Application. The Application must be automatically available on the client computers. 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.)



Answer:

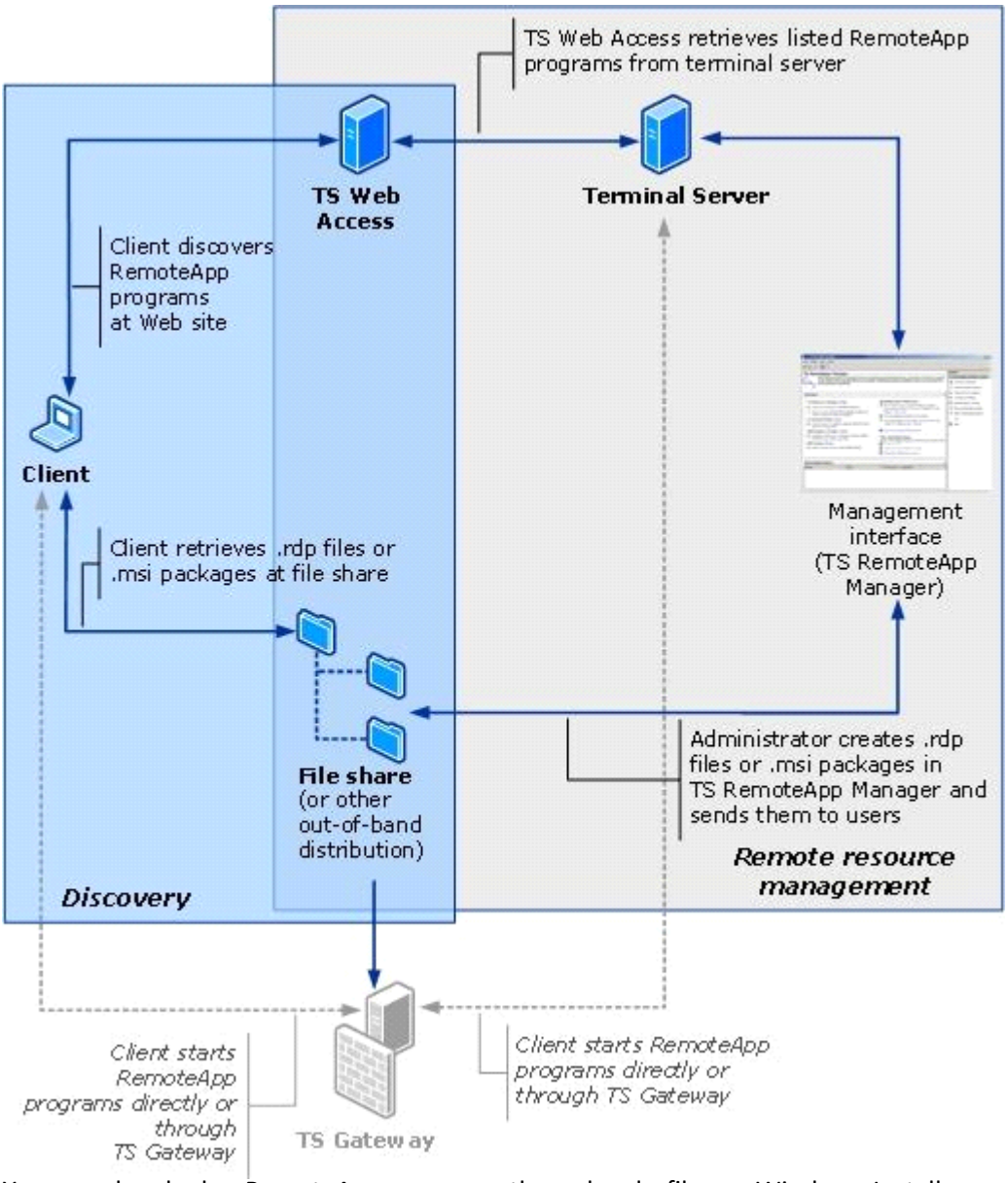
Explanation:
You have a 64bit application to be installed on 32 bit client PCs, the app is incompatible with these clients for this reason. So you create a remote desktop server (formally terminal server) and install the 64 bit version on this (step 1 of the answer) you then create a RemoteApp that os compatable to the 32bit clients (step 2) and finally you assign that using GPO to those clients that need it (step 3)
What are RemoteApp programs?
RemoteApp programs are programs that are accessed remotely through Terminal Services and appear as if they are running on the end user's local computer. Instead of being presented to the user in the desktop of the remote terminal server, the RemoteApp program is integrated with the client's desktop, running in its own resizable window with its own entry in the taskbar. Users can run RemoteApp programs side-by-side with their local programs. If a user is running more than one RemoteApp program on the same terminal server, the
RemoteApp programs will share the same Terminal Services session.
In Windows Server 2008, users can access RemoteApp programs in several ways, depending on the deployment method that you choose. They can:
Access a link to the program on a Web site by using TS Web Access.
Double-click a Remote Desktop Protocol (.rdp) file that has been created and distributed by their administrator.
Double-click a program icon on their desktop or Start menu that has been created and distributed by their administrator with a Windows Installer (.msi) package.
Double-click a file where the file name extension is associated with a RemoteApp program. This can be configured by their administrator with a Windows Installer package.
The .rdp files and Windows Installer packages contain the settings that are needed to run RemoteApp programs. After opening a RemoteApp program on their local computer, the user can interact with the program that is running on the terminal server as if it were running locally.
How should I deploy RemoteApp programs?

Before you configure TS RemoteApp, you should decide how you want to distribute RemoteApp programs to users. You can use either of the following deployment methods:

You can make RemoteApp programs available on a Web site by distributing the RemoteApp programs through TS Web Access.

You can distribute RemoteApp programs as .rdp files or Windows Installer packages through a file share, or through other distribution mechanisms such as Microsoft Systems Management Server or Active Directory software distribution.

Deploying RemoteApp programs through a file share or other distribution mechanism



You can also deploy RemoteApp programs through .rdp files or Windows Installer packages that are made available through file sharing, or through other distribution mechanisms such as Microsoft Systems Management Server or Active Directory software distribution. These methods enable you to distribute RemoteApp programs to users without using TS Web Access.

1. Configure the server that will host RemoteApp programs. This includes installing Terminal Server, installing programs, and verifying remote connection settings.
2. Use TS RemoteApp Manager to add RemoteApp programs and to configure global deployment settings.
3. Use TS RemoteApp Manager to create .rdp files or Windows Installer packages from RemoteApp programs.

Group Policy settings to control client behavior when opening a digitally signed .rdp file

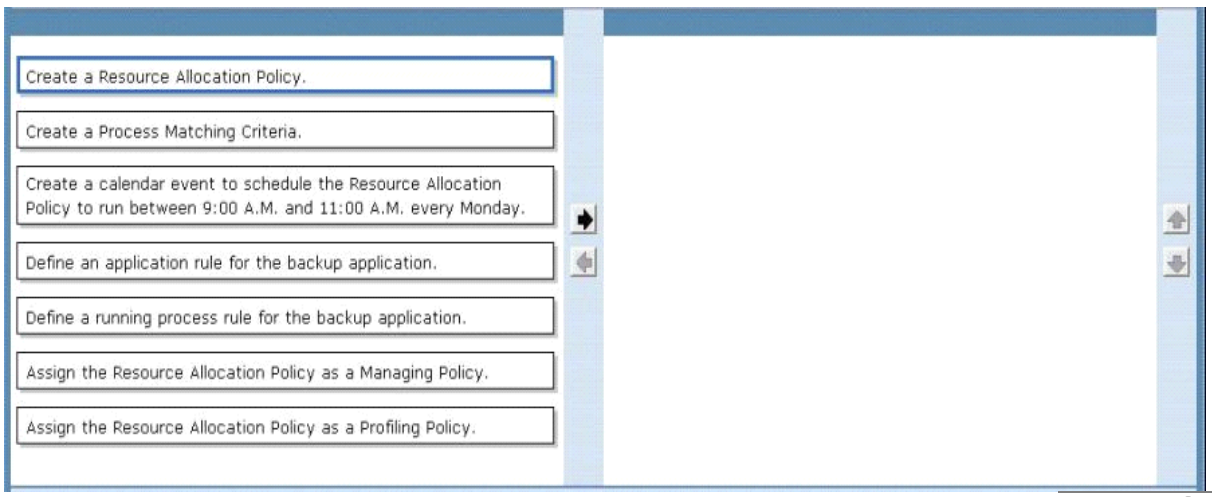
You can use Group Policy to configure clients to always recognize RemoteApp programs from a particular publisher as

trusted. You can also configure whether clients will block RemoteApp programs and remote desktop connections from external or unknown sources. By using these policy settings, you can reduce the number and complexity of security decisions that users face. This reduces the chances of inadvertent user actions that may lead to security vulnerabilities.
The relevant Group Policy settings are located in the Local Group Policy Editor at the following location, in both the Computer Configuration and in the User Configuration node:
Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client
The available policy settings are:
Specify SHA1 thumbprints of certificates representing trusted .rdp publishers
This policy setting allows you to specify a list of Secure Hash Algorithm 1 (SHA1) certificate thumbprints that represent trusted .rdp file publishers. If you enable this policy setting, any certificate with an SHA1 thumbprint that matches a thumbprint on the list will be considered trusted.
Allow .rdp files from valid publishers and user's default .rdp settings
This policy setting allows you to specify whether users can run .rdp files from a publisher that signed the file with a valid certificate. This policy setting also controls whether the user can start an RDP session by using default .rdp settings, such as when a user directly opens the RDC client without specifying an .rdp file.
Allow .rdp files from unknown publishers
This policy setting allows you to specify whether users can run unsigned .rdp files and .rdp files from unknown publishers on the client computer.

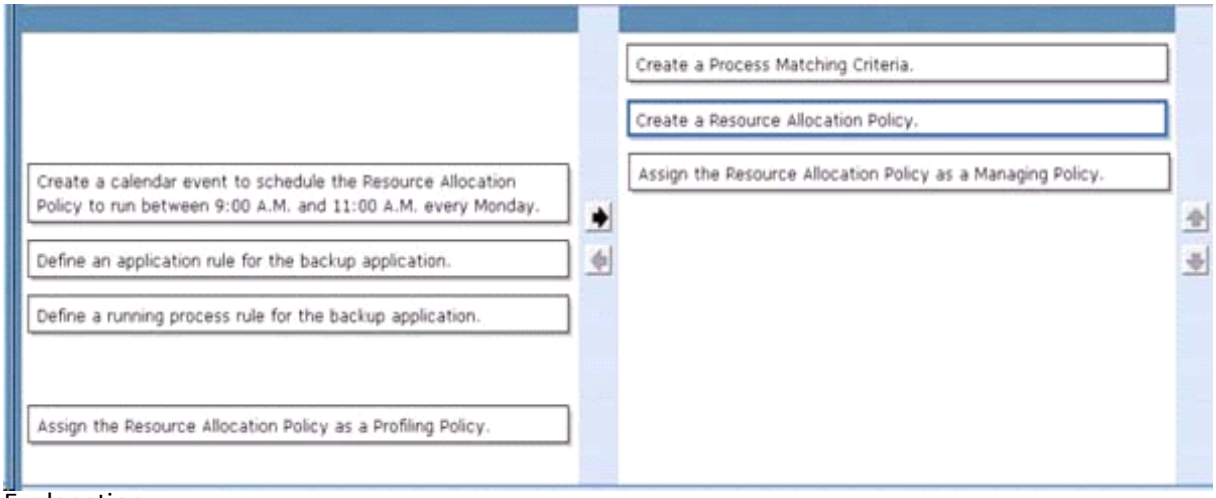
Question: 80 DRAG DROP

A company currently has a Remote Desktop Services (RDS) farm consisting of three Remote Desktop Session Hosts (RD Session Hosts) and one Remote Desktop Session Broker (RD Session Broker). The RD Session Hosts are configured to use Windows Network Load Balancing.
The RDS servers run slowly every Monday morning between 9:00 A.M. and 11:00 A.M.
You establish that your third-party backup solution is running on the RDS servers at these times and is causing the poor performance. Company policy mandates that the backup must occur at this time.
You have the following requirements:
- Implement Windows System Resource Manager (WSRM) on each of the RDS servers to minimize the system resources utilized by the backup Application.
- Ensure that WSRM runs only when required.

You need to configure WSRM.
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.)



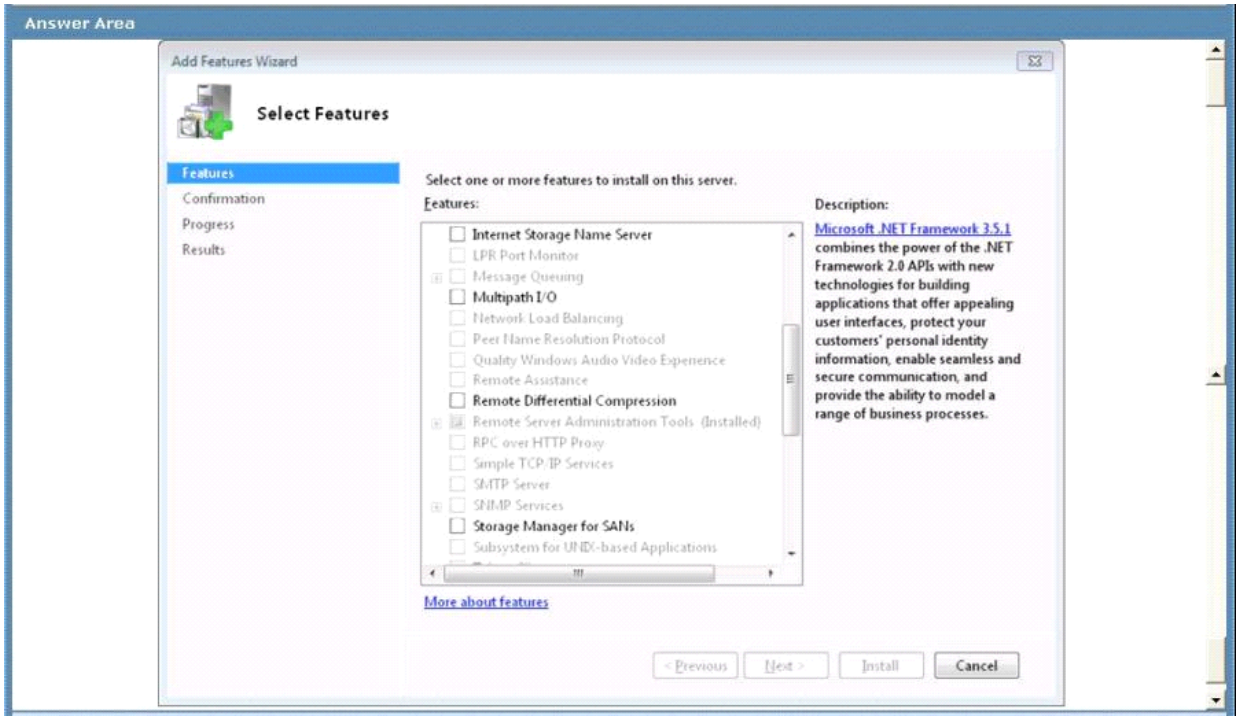
Answer:



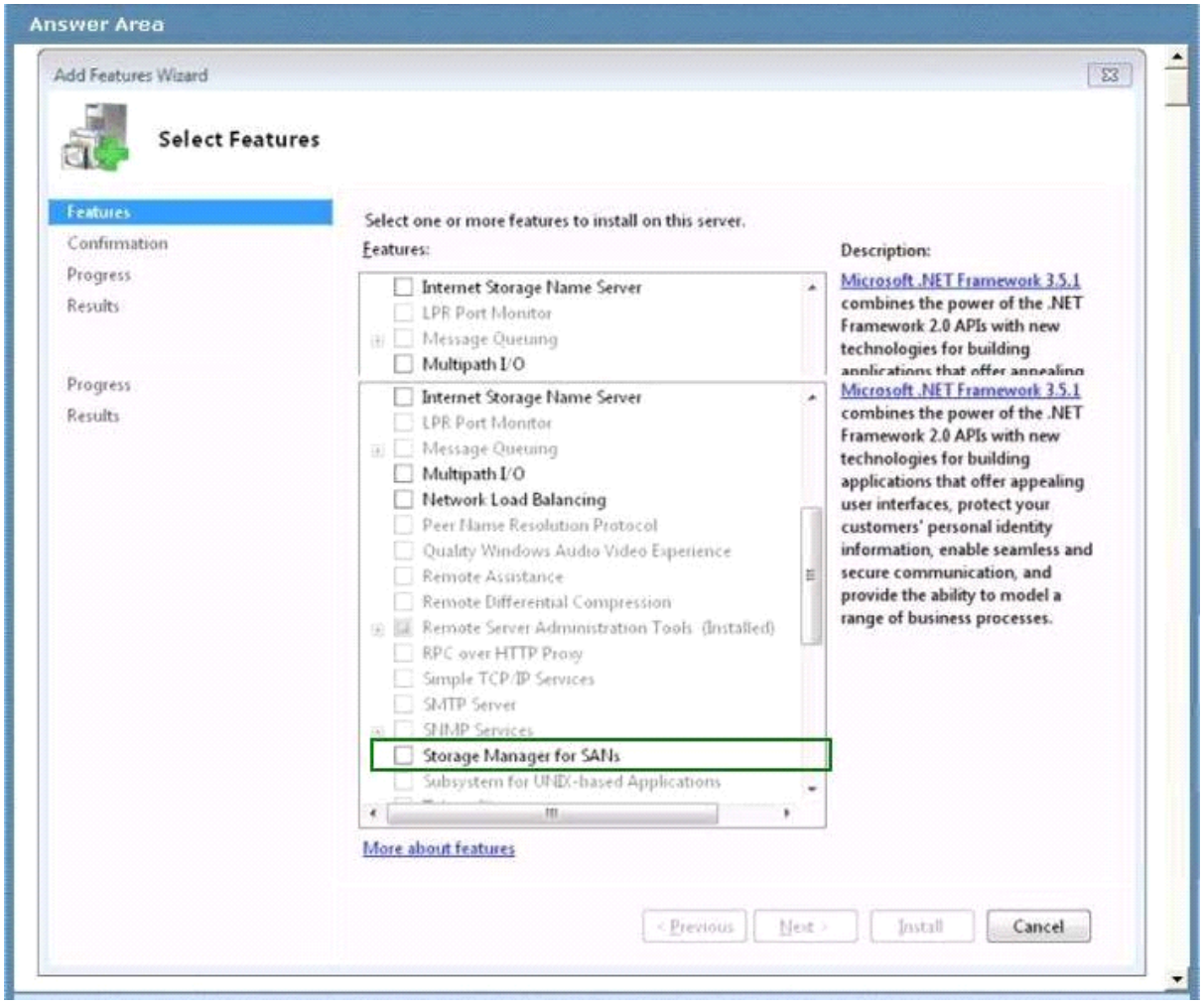
Explanation:
Process Matching Criteria
The WSRM process-matching criteria performance object, installed with Windows System Resource Manager (WSRM), consists of counters that monitor the CPU usage and memory usage of the processes matched by the process-matching criteria. The criteria are included in the managing resource-allocation policy. Each object will have as many instances as the number of process-matching criteria within the current active policy.
Resource Allocation Policy
Allocate processor and memory resources to processes that are specified by the process matching criteria that you create.
Also see
http://www.techrepublic.com/article/use-windows-system-resource-manager-to-control-a-serverspowers/5178054

Question: 81
HOTSPOT

A company has servers that run Windows Server 2008 R2. You are designing a storage solution for the servers. The storage solution includes Fibre Channel (FC) and Internet SCSI (iSCSI) disk drive subsystems, and supports the Virtual Disk Service (VDS). You need to ensure that you can create and manage logical unit numbers (LUNs) on the storage solution. Which feature should you install?
To answer, select the appropriate feature in the answer area.


Answer Area
Add Features Wizard
Select Features
Features
Confirmation
Progress
Results
Select one or more features to install on this server.
Features:
Internet Storage Name Server
LPR Port Monitor
Message Queuing
Multipath I/O
Network Load Balancing
Peer Name Resolution Protocol
Quality Windows Audio Video Experience
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools (Installed)
RPC over HTTP Proxy
Simple TCP/IP Services
SMTP Server
SNMP Services
Storage Manager for SANs
Subsystem for UNIX-based Applications
Description:
Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
More about features
< Previous
Next >
Install
Cancel

Answer:


Answer Area
Add Features Wizard
Select Features
Features
Confirmation
Progress
Results
Progress
Results
Select one or more features to install on this server.
Features:
Internet Storage Name Server
LPR Port Monitor
Message Queuing
Multipath I/O
Network Load Balancing
Peer Name Resolution Protocol
Quality Windows Audio Video Experience
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools (Installed)
RPC over HTTP Proxy
Simple TCP/IP Services
SMTP Server
SNMP Services
Storage Manager for SANs
Subsystem for UNIX-based Applications
Description:
Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building
Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
More about features
< Previous
Next >
Install
Cancel

Explanation:
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.

Question: 82

A company has servers that run a Server Core installation of Windows Server 2008. You are designing the migration of the servers to Windows Server 2008 R2. After the migration, you will install the Remote Desktop Services server role and the Print and Document Services server role on the servers. You need to ensure that shared resources on the servers are available after the migration, and minimize administrative effort. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Deploy new servers with a Server Core installation of Windows Server 2008 R2. Migrate the shared resources to the new servers.
B. Upgrade the existing servers to a Server Core installation of Windows Server 2008 R2, and then upgrade the servers to a full installation of Windows Server 2008 R2.
C. Move the shared resources off of the existing servers. Perform a clean installation of Windows Server 2008 R2 on the servers. Move the shared resources back onto the servers.
D. Deploy new servers with Windows Server 2008 R2 installed. Migrate the shared resources to the new servers.

Answer: D

Explanation:
The key here is minimize effort & remote desktop services.
Server core wouldn't allow remote desktop services as it has no GUI so that would rule out answer A you also cant upgrade from core to full see http://www.windowsitpro.com/article/tips/can-i-upgrade-fromserver-core-2008-to-the-full-windows-server-2008- or http://serverfault.com/questions/92523/upgrade-fromwindows-2008-server-core-to-full-windows-2008-server upgrade considerations for server core installations of windows server 2008 so that rules our B
You can use the server core installation option only by performing a clean installation.
You cannot upgrade from earlier versions of windows to server core installations of windows server 2008.
You cannot upgrade from non-server core installations of windows server 2008 to server core installations of windows server 2008.
You cannot convert server core installations of windows server 2008 to non-server core installations of windows server 2008.
You can upgrade server core installations of windows server 2008 only to windows server core r2 when it is released.
Answer C is possible but again you're asked to minimize effort so D would be 1 step less thus reducing your effort and possible down time.

Question: 83

As part of a Windows Server 2008 R2 Active Directory deployment, you are designing a Group Policy object (GPO) hierarchy. Client computers run Windows 7 and Windows XP. All client computers are in an organizational unit (OU) named Client Computers. Additional Windows 7 and Windows XP client computers will be joined to the domain over the next six months. You have the following requirements:

- Install the antivirus Application on all Windows XP computers.
- Do not install the antivirus Application on the Windows 7 computers.

- Do not make changes to the existing Active Directory logical structure.

You need to design a Group Policy strategy that meets the requirements.
Which GPO configuration should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Publish the antivirus application to client computers. Link the GPO to the domain. Use security filtering to prevent the Windows 7 client computers from receiving the GPO.
B. Assign the antivirus application to client computers. Link the GPO to the Client Computers OU. Create a WMI Filter that queries whether the client computer's Win32_OperatingSystem caption contains "Windows 7" . Associate the WMI filter with the GPO.
C. Assign the antivirus application to client computers. Link the GPO to the domain. Place all the Windows 7 computers in a security group. Use security filtering to prevent the Windows 7 client computers from receiving the GPO.
D. Assign the antivirus application to client computers. Link the GPO to the Client Computers OU. Create a WMI Filter that queries whether the client computer's Win32_OperatingSystem caption contains "Windows XP" . Associate the WMI Filter with the GPO.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc947846%28v=ws.10%29.aspx &
http://technet.microsoft.com/enus/library/cc947846%28v=ws.10%29.aspx#bkmk_1
Depending on which OS you're asked to install the AV app on your answer could change. There are reports that you're now being asked to install the AV on the Win7 clients. if that is the case then you would select the Windows 7 option

Question: 84

A company has servers that run Windows Server 2008 R2. Administrators use a graphic-intensive Application to remotely manage the network. You are designing a remote network administration solution. You need to ensure that authorized administrators can connect to internal servers over the Internet from computers that run Windows 7 or Windows Vista. Device redirection enforcement must be enabled for these connections. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Deploy and configure a server with the Remote Desktop Web Access server role. Enable Forms-based authentication. Ensure that administrators use RDC 6.1 when accessing internal servers remotely.
B. Deploy and configure a server with the Remote Desktop Web Access server role. Enable Forms-based authentication. Ensure that administrators use RDC 7.0 when accessing internal servers remotely,
C. Deploy and configure a server with the Remote Desktop Gateway server role. Ensure that administrators use RDC 7.0 when accessing internal servers remotely.
D. Deploy and configure a server with the Remote Desktop Gateway server role. Ensure that administrators use RDC 6.1 when accessing internal servers remotely.

Answer: C

Explanation:
http://windows.microsoft.com/en-us/windows7/What-is-a-Remote-Desktop-Gateway-server
A Remote Desktop Gateway (RD Gateway) server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer with an Internet connection. RD Gateway uses the Remote Desktop Protocol (RDP) along with the HTTPS protocol to help create a more secure, encrypted connection.
http://technet.microsoft.com/en-us/library/dd560672%28v=ws.10%29.aspx

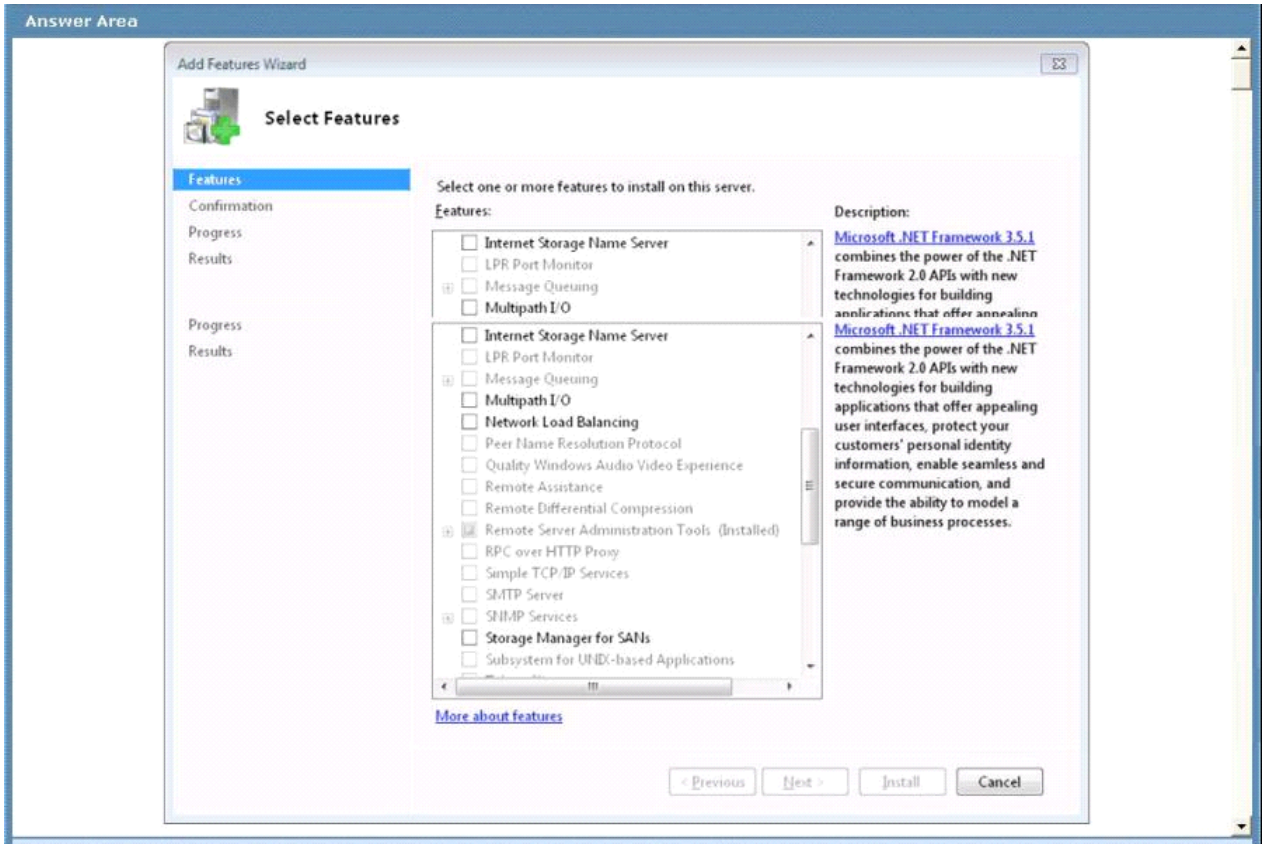
Device redirection enforcement
An RD Gateway server running Windows Server 2008 R2 includes the option to allow remote desktop clients to only connect to RD Session Host servers that enforce device redirection. RDC 7.0 is required for device redirection to be enforced by the RD Session Host server running Windows Server 2008 R2.
Device redirection enforcement is configured on the Device Redirection tab of the RD CAP by using Remote Desktop Gateway Manager.

Question: 85
HOTSPOT

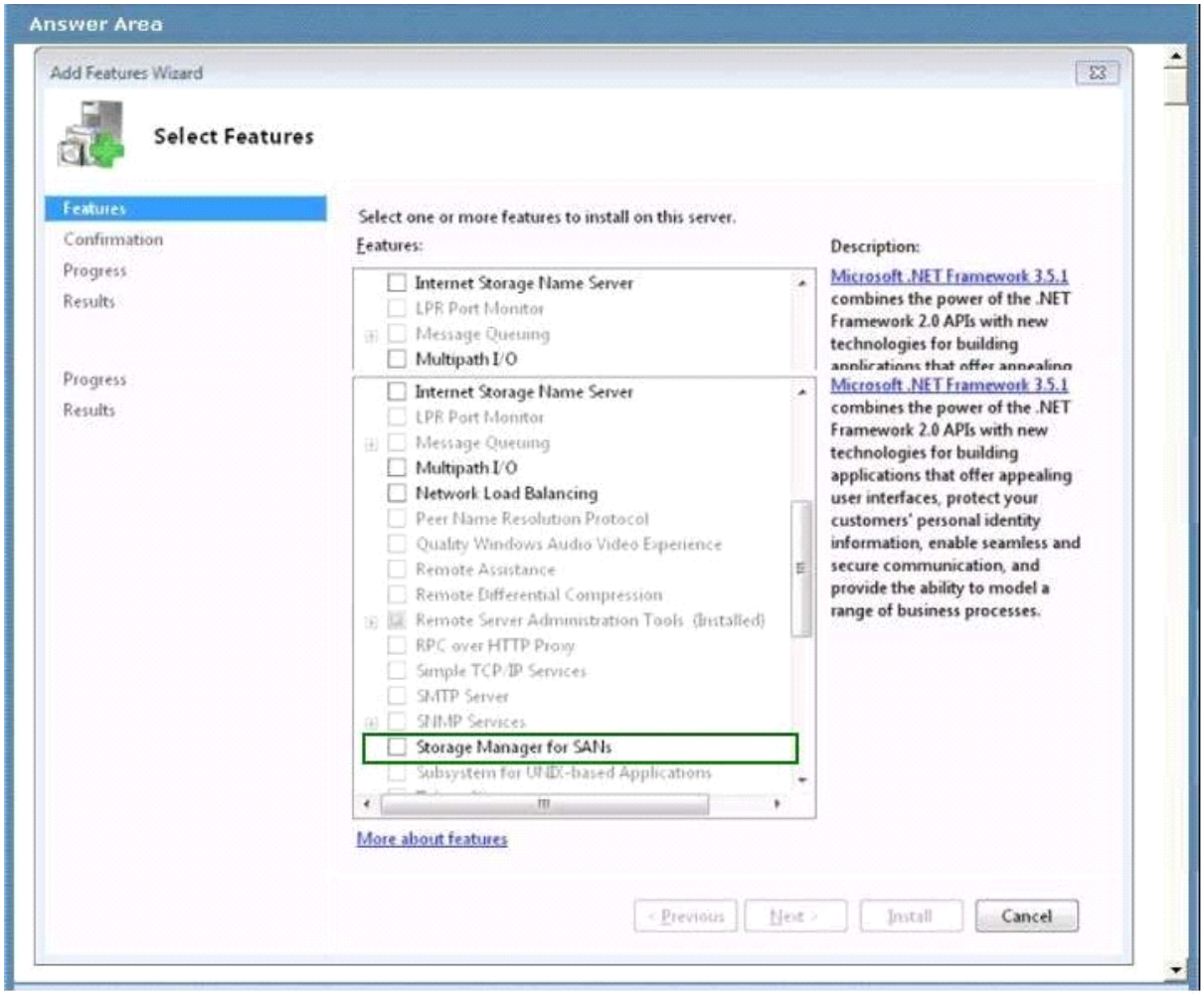
A company has servers that run Windows Server 2008 R2 and a storage area network (SAN) that supports the virtual Disk Service (VDS). You are designing a storage solution for the servers. The storage solution must meet the following requirements:

- 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.



Answer:



Explanation:

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 di 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 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 reac disk becomes unavailable, but 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 c information. This type of LUN provides better read performance than a mirrored LUN, but write performance is reduced by the parity calcu 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: 86

You are designing a server infrastructure to support a new stateful Application. The server infrastructure must meet the following requirements:

- Use two servers, each with two NIC cards and 32 GB of RAM.
- Provide access to the Application in the event of the failure of a single server.
- Provide the ability to scale up the Application.
- Minimize the attack surface of each server.
- Minimize server disk space requirements.

You need to design a server infrastructure that meets the requirements.
What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Perform a Server Core installation of Windows Server 2008 R2 Standard Edition. Configure both servers in a failover cluster.
B. Perform a Server Core installation of Windows Server 2008 R2. Configure both servers in a Windows Network Load Balancing array,
C. Install Windows Server 2008 R2 on both servers. Use DNS Round Robin to balance the load between the servers.
D. Install Windows Server 2008 R2 on both servers. Configure both servers in a Windows Network Load Balancing array.

Answer: B

Explanation:
All the requirements point to a server core install ie attack surface, disk space (no gui no need to waste disk space on it) that narrows it down to A & B
http://technet.microsoft.com/en-us/library/dd184075.aspx
NOTE: Theres some confusion over this question. in its current form no answer is 100% correct.
Answer A is the only answer to mention the edition of the OS. but Standard Edition does not support Fail Over Clustering.
The question mentions the new application will be stateful and network load balancers are not intended for the use of stateful apps. however if you look at http://technet.microsoft.com/en-us/library/cc757745%28v=ws.10%29.aspx,
Network Load Balancing and stateful connections
Application servers maintain two kinds of stateful connections:
Interclient state: A state whose updates must be synchronized with transactions performed for other clients, such as merchandise inventory at an e-commerce site.
Intraclient state: A state that must be maintained for a given client throughout a session (that can span multiple connections), such as a shopping cart process at an e-commerce site.
Network Load Balancing should not be used to scale applications that directly update interclient state, such as Microsoft SQL Server, because these applications generally were not designed to permit multiple instances to simultaneously access a shared database and synchronize updates. Instead, Network Load Balancing should be used to scale stateless front-end services, such as Microsoft Internet Information Services, that might access a shared back-end database server.
However, Network Load Balancing can be used to scale applications that manage intraclient state within a session that spans multiple connections. When client affinity is enabled, Network Load Balancing directs all TCP connections to the same cluster host. This allows session state to be maintained in host memory. Client/server applications that embed state within cookies or push it to a back-end database do not need client affinity to be maintained.
so it is possible the answer is B also the question suggests selecting the BEST answer, answer B would be the one that meets the requirements best
What Is Server Core
The Server Core option is a new minimal installation option that is available when you are deploying the Standard, Enterprise, or Datacenter edition of Windows Server 20081. Server Core provides you with a minimal installation of Windows Server 2008 that supports installing only certain server roles:

Server Role	Available in Full Installation	Available in Server Core
Active Directory Certificate Services (AD CS)	✓	
Active Directory Domain Services (AD DS)	✓	✓
Active Directory Federation Services (AD FS)	✓	
Active Directory Lightweight Directory Services (AD LDS)	✓	✓
Active Directory Rights Management Services (AD RMS)	✓	
Application Server	✓	
DHCP Server	✓	✓
DNS Server	✓	✓
Fax Server	✓	
File Services	✓	✓
Hyper-V	✓	✓
Network Policy and Access Services	✓	
Print Services	✓	✓
Streaming Media Services	✓	✓
Terminal Services	✓	
UDDI Services	✓	
Web Server (IIS)	✓	✓
Windows Deployment Services	✓	

if you look at http://community.spiceworks.com/topic/110578-difference-between-nlb-and-windows-failovercluster then consider your requirement of "Provide the ability to scale up the application" a fail over cluster wouldnt do this because it doesnt spread the load as only one server is live at any one time Availability, scalability, and clustering technologies

Windows Server 2008 R2 provides two clustering technologies: failover clusters and Network Load Balancing (NLB). Failover clusters primarily provide high availability; Network Load Balancing provides scalability and at the same time helps increase availability of Web-based services. Your choice of cluster technologies (failover clusters or Network Load Balancing) depends primarily on whether the applications you run have long-running

in-memory state:

What are failover clusters?

By using a failover cluster, you can ensure that users have nearly constant access to important server-based resources. A failover cluster is a set of independent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide service through a process known as failover.

In Windows Server 2008, the changes to failover clusters (formerly known as server clusters) are aimed at simplifying cluster setup and management, making the clusters more secure and stable, improving networking in clusters, and improving how failover clusters communicate with storage. A failover cluster is a group of independent servers that are running Windows Server 2008 and working together to increase the availability of services and applications. When a failure occurs on one computer in a cluster, resources are redirected and the workload is redistributed to another computer in the cluster. You can use failover clusters to ensure that users have nearly constant access to important server-based resources. Failover clusters are designed for applications that have long-running in-memory state, or that have large, frequently updated data states.

These are called stateful applications, and they include database applications and messaging applications.

Typical uses for failover clusters include file servers, print servers, database servers, and messaging servers.
What are NLB clusters?
A single computer running Windows can provide a limited level of server reliability and scalable performance. However, by combining the resources of two or more computers running one of the products in Windows Server 2008 R2 into a single virtual cluster, NLB can deliver the reliability and performance that Web servers and other mission-critical servers need. Each host runs a separate copy of the desired server applications (such as applications for Web, FTP, and Telnet servers). NLB distributes incoming client requests across the hosts in the cluster. The load weight to be handled by each host can be configured as necessary. You can also add hosts dynamically to the cluster to handle increased load. In addition, NLB can direct all traffic to a designated single host, which is called the default host.
NLB allows all of the computers in the cluster to be addressed by the same set of cluster IP addresses, and it maintains a set of unique, dedicated IP addresses for each host. For load-balanced applications, when a host fails or goes offline, the load is automatically redistributed among the computers that are still operating. When a computer fails or goes offline unexpectedly, active connections to the failed or offline server are lost. However, if you bring a host down intentionally, you can use the drainstop command to service all active connections prior to bringing the computer offline. In any case, when it is ready, the offline computer can transparently rejoin the cluster and regain its share of the workload, which allows the other computers in the cluster to handle less traffic. Network Load Balancing is intended for applications that do not have long-running in-memory state. These are called stateless applications. A stateless application treats each client request as an independent operation, and therefore it can load-balance each request independently. Stateless applications often have read-only data or data that changes infrequently. Front-end Web servers, virtual private networks (VPNs), File Transfer Protocol (FTP) servers, and firewall and proxy servers typically use Network Load Balancing. Network Load Balancing clusters can also support other TCP- or UDP-based services and applications.
However if you look here http://technet.microsoft.com/en-us/library/dd443539%28v=ws.10%29.aspx at the bottom it says:
Which editions include failover clustering?
The failover cluster feature is available in Windows Server 2008 R2 Enterprise and Windows Server 2008 R2 Datacenter. The feature is not available in Windows Web Server 2008 R2 or Windows Server 2008 R2 Standard.
So we have a problem, its obvious a Core install based on the requirements, the application being stateful means it must be a Failover Cluster but the OS edition doesnt support fail over clustering.

Question: 87

You are planning to deploy new servers that will run Windows Server 2008 R2. Each server will have 32 GB of RAM. The servers must support installation of the following role services:

- Routing and Remote Access
- Remote Desktop Services Gateway

You need to deploy the minimum edition of Windows Server 2008 R2 that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Windows Server 2008 R2 Standard
B. Windows Server 2008 R2 Enterprise
C. Windows Server 2008 R2 Web
D. Windows Server 2008 R2 Datacenter

Answer: A

Explanation:
http://www.microsoft.com/en-us/server-cloud/windows-server/2008-r2-standard.aspx
R2 Standard provides these services and is the mimimum edition they are availible on.
32 GB RAM is also supported if its a 64 bit version http://technet.microsoft.com/en-us/windowsserver/bb414778.aspx

Question: 88

A company wants to prevent employees who access the company's Remote Desktop Session Hosts (RD Session Hosts) from introducing malware onto the corporate network. You have the following requirements:

- Ensure that only client computers that have an up-to-date antivirus program installed can connect to the RD Session Hosts.
- Display a notification when a client computer that does not meet the antivirus requirements attempts to connect to an RD Session Host. Provide information about how to resolve the connection problem.
- Ensure that client computers can access only the RD Session Hosts.

You need to recommend a Remote Desktop Services (RDS) management strategy that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Deploy a Remote Desktop Gateway in a perimeter network. Install and configure a Network Policy and Access Services server. Configure the System Health Validator. Enable the Remote Desktop Gateway Network Access Protection Enforcement Client. Configure Remote Desktop Connection Authorization Policies and Remote Desktop Resource Authorization Polices.
B. Deploy the Routing and Remote Access Service in a perimeter network to support VPN connections. Install and configure a Network Policy and Access Services server. Enable the Network Access Protection VPN Enforcement Client. Configure the System Health Validator. Configure static routes on the VPN server to allow access only to the RD Session Hosts.
C. Deploy a Remote Desktop Gateway in a perimeter network. Configure Remote Desktop Connection Authorization Policies and Remote Desktop Resource Authorization Polices. Configure a logon message.
D. Deploy the Routing and Remote Access Service in a perimeter network to support VPN connections. Configure Connection Request Policies to specify which computers can connect to the corporate network. Configure static routes on the VPN server to allow access only to the RD Session Hosts.

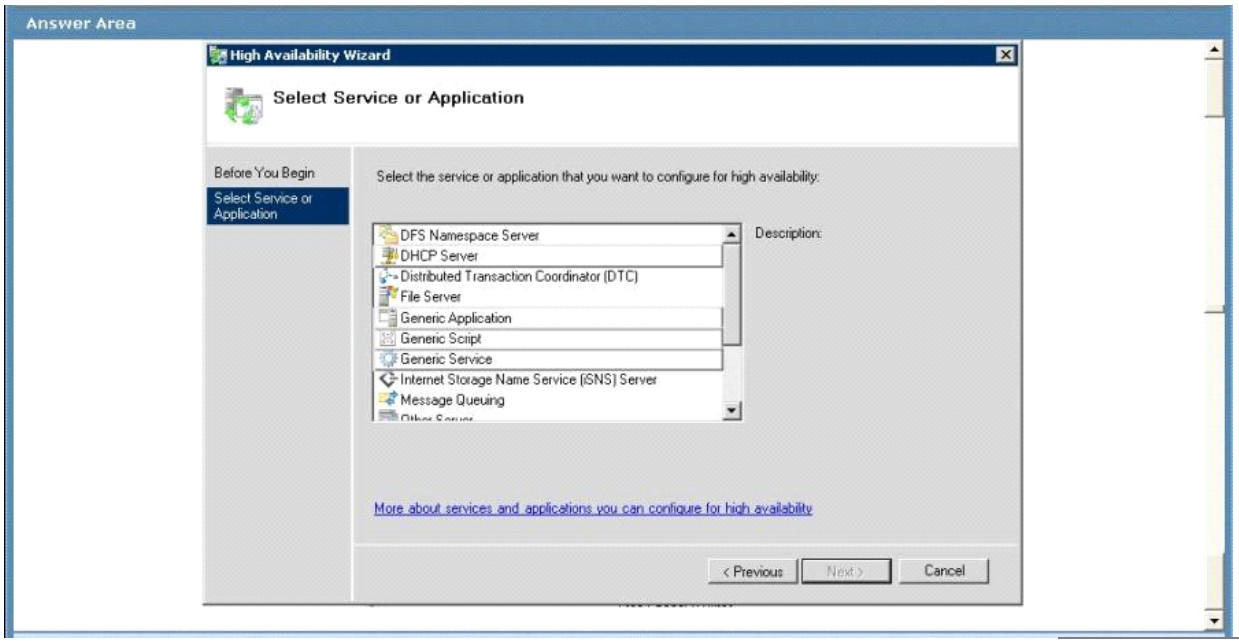
Answer: A

Explanation:
NAP with SHVs configured will ensure that the AV is installed and up to date. if they ar not you can direct them to a quatantine/remediation server to update
http://www.techrepublic.com/article/solutionbase-configuring-network-access-protection-for-windows-server-2008/178022
RD RAP
Remote Desktop resource authorization policies (RD RAPs) allow you to specify the internal network resources (computers) that remote users can connect to through an RD Gateway server.
http://technet.microsoft.com/en-us/library/cc730630
RD CAP
Remote Desktop connection authorization policies (RD CAPs) allow you to specify who can connect to an RD Gateway server
http://technet.microsoft.com/en-us/library/cc731544

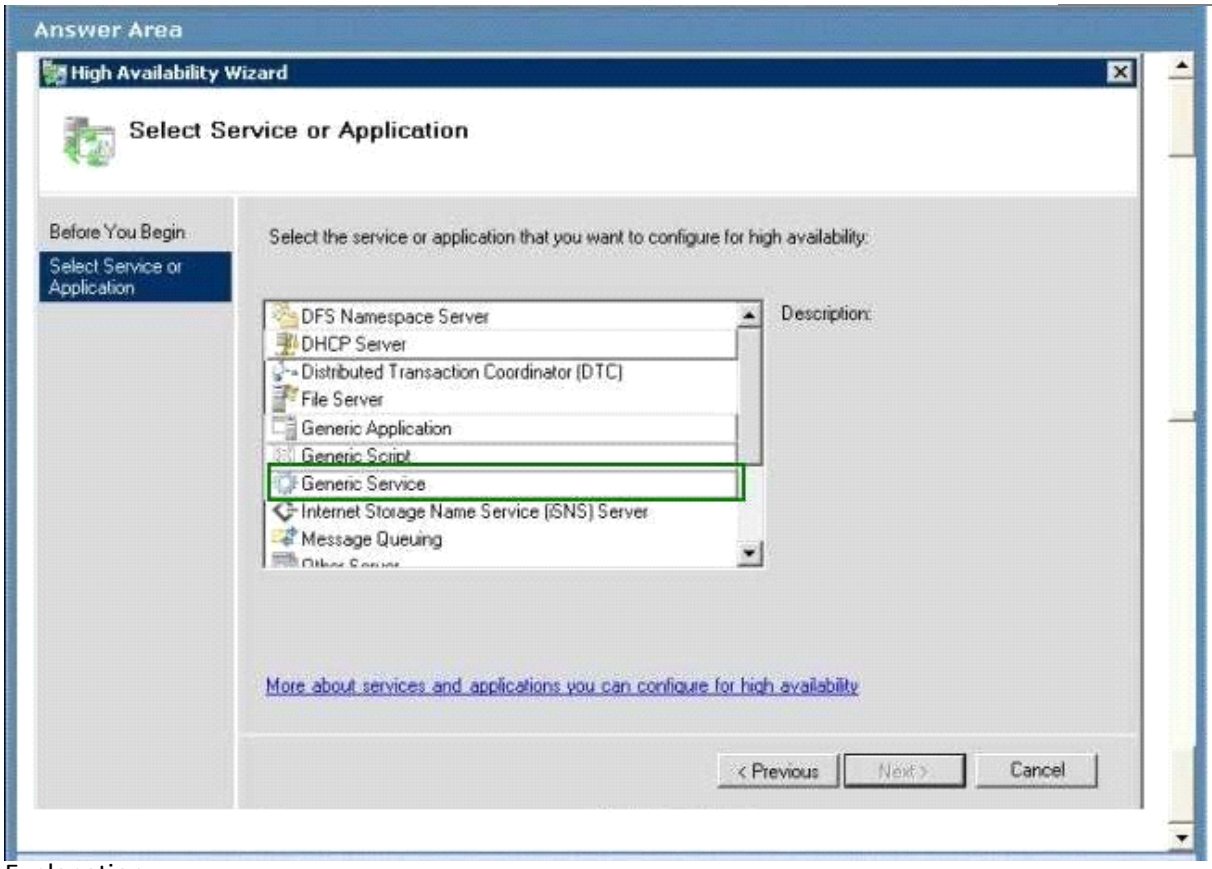
Question: 89
HOTSPOT

A company runs a third-party DHCP Application on a windows Server 2008 R2 server. The Application runs as a service that launches a background process upon startup. The company plans to migrate the DHCP Application to a Windows Server 2008 R2 failover cluster. You need to provide high availability for the DHCP Application. Which service or Application should you configure?

To answer, select the appropriate service or Application in the answer area.



Answer:



Explanation:

Windows Server 2008 (and R2) Failover Clustering supports virtually every workload which comes with Windows Server, however there are many custom and 3rd party applications which take advantage of our infrastructure to provide high-availability. Additionally there are some applications which were not originally designed to run in a failover cluster. These can be created, managed by and integrated with Failover Clustering using a generic container, with applications using the Generic Application resource type.

We use the Generic Application resource type to enable such applications to run in a highly-available environment which can benefit from clustering features (i.e. high availability, failover, etc.).

When a generic application resource is online, it means that the application is running. When a generic application is offline, it means that the application is not running.
http://blogs.msdn.com/b/clustering/archive/2009/04/10/9542115.aspx
A cluster-unaware application is distinguished by the following features.
The application does not use the Failover Cluster API. Therefore, it cannot discover information about the cluster environment, interact with cluster objects, detect that it is running in a cluster, or change its behavior between clustered and non-clustered systems.
If the application is managed as a cluster resource, it is managed as a Generic Application resource type or Generic Service resource type. These resource types provide very basic routines for failure detection and application shutdown. Therefore, a cluster-unaware application might not be able to perform the initialization and cleanup tasks needed for it to be consistently available in the cluster.
Most older applications are cluster-unaware. However, a cluster-unaware application can be made clusteraware by creating resource types to manage the application. A custom resource type provides the initialization, cleanup, and management routines specific to the needs of the application.
There is nothing inherently wrong with cluster-unaware applications. As long as they are functioning and highly available to cluster resources when managed as Generic Applications or Generic Services, there is no need to make them cluster-aware. However, if an application does not start, stop, or failover consistently when managed by the generic types, it should be made cluster-aware.

Question: 90

A network includes servers that run Windows Server 2008 R2 with the Network Policy Server (NPS) server role installed. You are planning to deploy a remote network administration solution. The remote administration solution must meet the following requirements:

- Include fault tolerance.
- Define the users who have remote access and the resources they can remotely access.

You need to design a remote administration solution that meets the requirements.
What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Deploy and configure multiple servers with the Remote Desktop Gateway server role. Create a central Remote Desktop Connection Authorization Policy (RD CAP) and a Resource Authorization Policy (RD RAP).
B. Deploy and configure multiple servers with the Remote Desktop Gateway server role. Create a local Remote Desktop Connection Authorization Policy (RD CAP) and a Resource Authorization Policy (RD RAP).
C. Deploy and configure one server with the Remote Desktop Web Access server role. Create a central Remote Desktop Connection Authorization Policy (RD CAP) and a Resource Authorization Policy (RD RAP).
D. Deploy and configure one server with the Remote Desktop Web Access server role. Create a local Remote Desktop Connection Authorization Policy (RD CAP) and a Resource Authorization Policy (RD RAP).

Answer: A

Explanation:
You can also configure RD Gateway to use Remote Desktop connection authorization policies (RD CAPs) that are stored on another server that runs the Network Policy Server (NPS) service. By doing this, you are using the server running NPS, formerly known as a Remote Authentication Dial-In User Service (RADIUS) server, to centralize the storage, management, and validation of RD CAPs. If you have already deployed a server running NPS for remote access scenarios such as VPN and dial-up networking, using the existing server running NPS for RD Gateway scenarios as well can enhance your deployment.
RAP
Remote Desktop resource authorization policies (RD RAPs) allow you to specify the internal network resources (computers) that remote users can connect to through an RD Gateway server.
Remote users connecting to the network through an RD Gateway server are granted access to computers on the

internal network if they meet the conditions specified in at least one RD CAP and one RD RAP.
CAP
Remote Desktop connection authorization policies (RD CAPs) allow you to specify who can connect to an RD Gateway server

Question: 91

You are designing a monitoring solution to log performance on member servers that run Windows Server 2008 R2. The monitoring solution must meet the following requirements for members of the Operations team:

- Create and modify Data Collector Sets.
- Display log file data and real-time performance data in Performance Monitor.

You need to design a monitoring solution that meets the requirements.
What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Add members of the Operations team to the Performance Monitor Users group. Assign the Act as part of the operating system user right to the Performance Monitor Users group
B. Add members of the Operations team to the Performance Log Users group
C. Add members of the Operations team to the Administrators group
D. Add members of the Operations team to the Power Users group

Answer: B

Explanation:
A Data Collector Set is the building block of performance monitoring and reporting in Windows Performance Monitor. It organizes multiple data collection points into a single component that can be used to review or log performance. A Data Collector Set can be created and then recorded individually, grouped with other Data Collector Set and incorporated into logs, viewed in Performance Monitor, configured to generate alerts when thresholds are reached, or used by other non-Microsoft applications. It can be associated with rules of scheduling for data collection at specific times. Windows Management Interface (WMI) tasks can be configured to run upon the completion of Data Collector Set collection.
Data Collector Sets can contain the following types of data collectors:
Performance counters
Event trace data
System configuration information (registry key values)
You can create a Data Collector Set from a template, from an existing set of Data Collectors in a Performance Monitor view, or by selecting individual Data Collectors and setting each individual option in the Data Collector Set properties.
http://technet.microsoft.com/en-us/library/cc722148
You can create a Data Collector Set from counters in the current Performance Monitor display. Membership in the local Performance Log Users or Administrators group, or equivalent, is the minimum required to complete this procedure.

Question: 92

A company has 10,000 client computers that run Windows 7. The company has a single domain Active Directory Domain Services (AD DS) forest with domain controllers that run Windows Server 2008 R2. Users have local administrative rights on client computers. You need to design a Group Policy solution that deploys a printer and enforces printer settings. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Use the Local Security Policy.
B. Use Group Policy preferences (GPPs).
C. Use a Group Policy object (GPO) Windows setting.
D. Use Starter Group Policy objects (GPOs).

Answer: B

Explanation:
Group Policy preferences, new for the Windows Server 2008 operating system, include more than 20 new Group Policy extensions that expand the range of configurable settings within a Group Policy object (GPO). These new extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC), under the new Preferences item. Examples of the new Group Policy preference extensions include folder options, mapped drives, printers, scheduled tasks, services, and Start menu settings.
In addition to providing significantly more coverage, better targeting, and easier management, Group Policy preferences enable you to deploy settings to client computers without restricting the users from changing the settings. This capability provides you with the flexibility to decide which settings to enforce and which settings to not enforce. You can deploy settings that you do not want to enforce by using Group Policy preferences.
System requirements and installation steps
To use Group Policy preferences, complete the following steps:
Install the set of client-side extensions (CSEs) on client computers. Supported operating systems: Windows Vista RTM or later, Windows XP with Service Pack 2 or later, Windows Server 2003 with Service Pack 1 or later
Download locations: Windows Vista (x86): http://go.microsoft.com/fwlink/?LinkId=111859Windows Vista (x64): http://go.microsoft.com/fwlink/?LinkID=111857Windows XP (x86): http://go.microsoft.com/fwlink/?LinkId=111851Windows XP (x64): http://go.microsoft.com/fwlink/?LinkId=111862Windows Server 2003 (x86): http://go.microsoft.com/fwlink/?LinkId=111852Windows Server 2003 (x64): http://go.microsoft.com/fwlink/?LinkId=111863
For more information, see Article 943729 in the Microsoft Knowledge Base.
Install the XMLLite low-level XML parser on client computers that are not running Windows Vista.
Supported operating systems: Windows XP SP2 or later, Windows Server 2003 SP1 or later
Download location: http://go.microsoft.com/fwlink/?LinkId=111843 worth looking at:
GP Policy vs. Preference vs. GP preferences
http://blogs.technet.com/b/grouppolicy/archive/2008/03/04/gp-policy-vs-preference-vs-gp-preferences.aspx

Question: 93

A company has a single Active Directory Domain Services (AD DS) domain and a single Remote Desktop Session Host (RD Session Host). The RD Session Host is approaching full memory capacity. All servers run Windows Server 2008 R2. You are designing a Remote Desktop Services (RDS) infrastructure. The infrastructure must meet the following requirements:

- Allow infrastructure capacity to increase.
- Minimize the number of physical servers.
- Do not require administrative action on the client computers if the infrastructure capacity increases.

You need to design an RDS infrastructure that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Migrate the RD Session Host to a virtual machine (VM) running in Microsoft Hyper-V. Add memory to the VM as demand increases.
B. Add RD Session Hosts as demand increases, and use Group Policy to direct users to the correct server.
C. Install and configure Windows Server Resource Manager (WSRM) on the RD Session Host to control user resource allocation.

D. Implement an RD Session Host server farm and add servers as required.

Answer: A

Explanation:
Virtualization meets the requirements easily enough, as capacity needs grow the VMs can be migrated to more powerful physical servers, again virtualization reduces the number of physical servers and finally as the actual RD Session Host wont change regardless of the location of that VM it will meet the third requirement Ans D does not meet the 3rd requirement
Ans C wont resolve the problem of running out of memory only that addition of RAM will resolve that issue
Ans B again does not meet the 3rd requirement

Question: 94

You are planning to deploy new servers that will run Windows Server 2008 R2. Each server will have 32 GB of RAM. The servers must support installation of the following role services:

- Routing and Remote Access
- Remote Desktop Services Gateway
- Minimize CPU and RAM usage

You need to deploy the minimum edition of Windows Server 2008 R2 that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. A Server Core installation of Windows Server 2008 R2 Datacenter.
B. A Full Installation of Windows Server 2008 R2 Enterprise.
C. A Full Installation of Windows Server 2008 R2 Standard.
D. A Server Core installation Windows Server 2008 R2 Web.

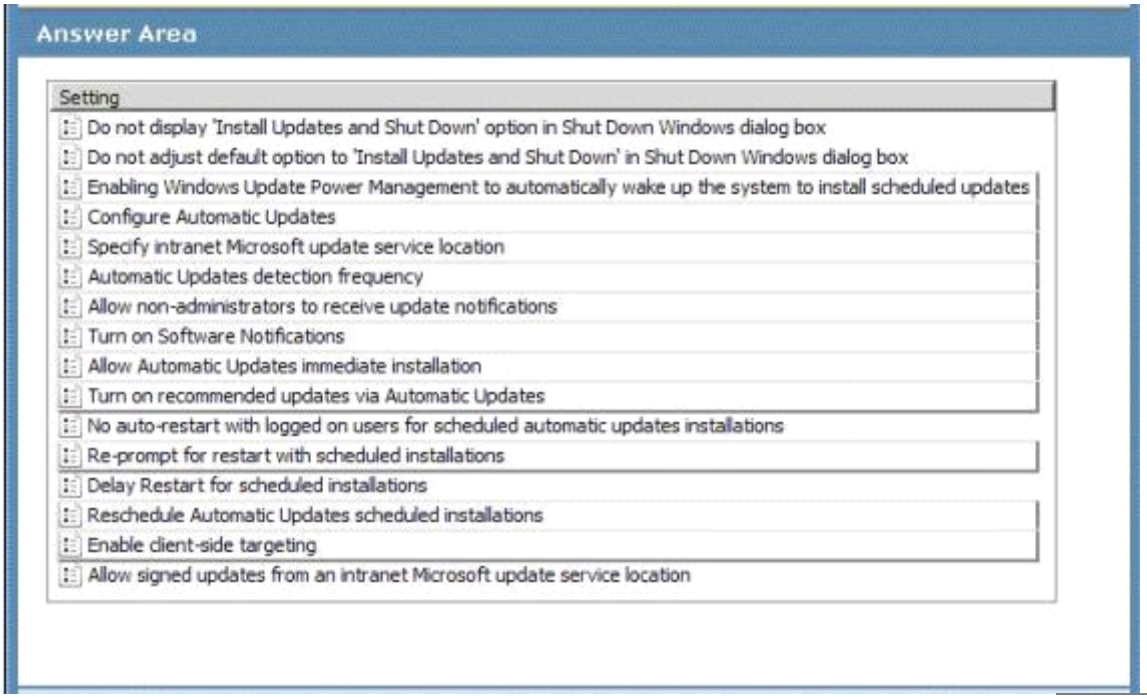
Answer: C

Question: 95
HOTSPOT

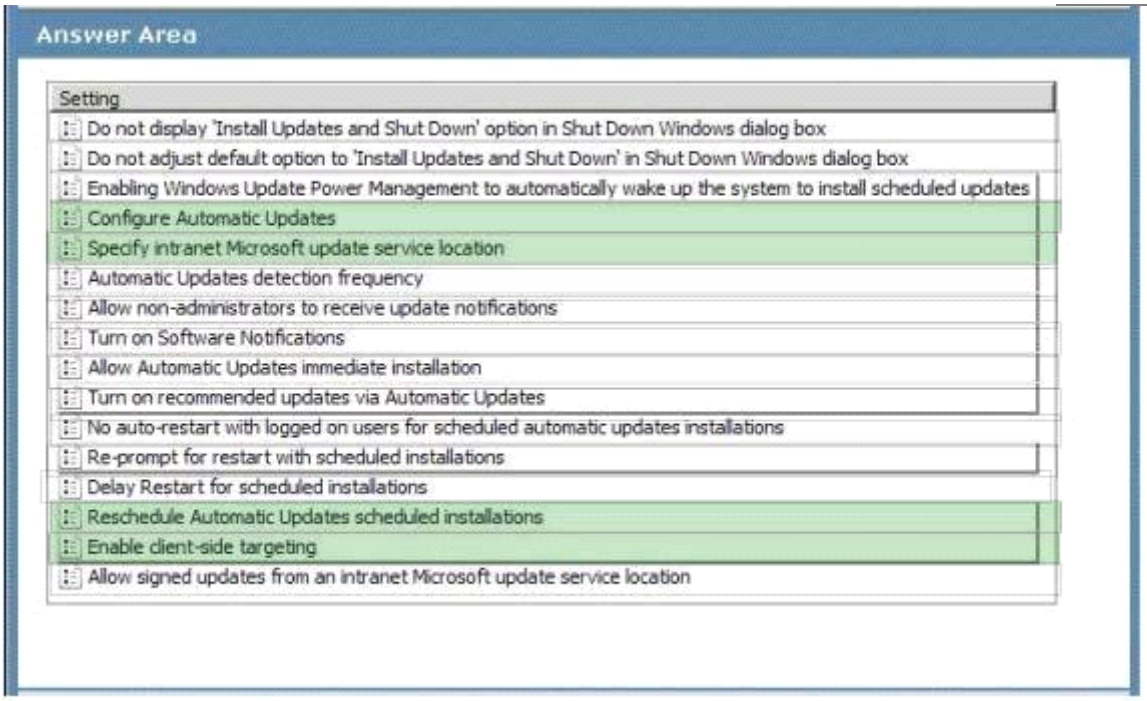
Your company has recently implemented Windows Server Update Services (WSUS). All client computers run Windows 7 Enterprise Edition. Only some users have local administrative privileges. You are designing a Group Policy object (GPO) to configure the client computers. The GPO must Apply only the following settings:

- Updates must be downloaded from the WSUS server.
- Automatically download and install updates every Thursday at 12:00 P.M.
- Configure WSUS client-side targeting through Group Policy.
- Delay the installation of updates until 20 minutes after a client computer is started, if the client computer was shut down at the specified installation time. You need to design the GPO to meet the requirements. Which settings should you configure to meet the requirements?

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



Answer:



Explanation:
Configure Automatic Updates
By enabling this setting you enable your computer to receive updates through Automatic Updates on a computer or computer group. To complete this setting, you must then select one of the following four options:
Notify before downloading any updates and notify again before installing them.
Download the updates automatically and notify when they are ready to be installed (default setting)
Automatically download updates and install them on the schedule specified below
Allow local administrators to select the configuration mode that Automatic Updates should notify and install updates
Best preactices http://technet.microsoft.com/en-us/library/cc720525%28v=ws.10%29.aspx deployment http://www.windows-noob.com/forums/index.php?/topic/588-how-can-i-configure-wsus-todeploy-updates/

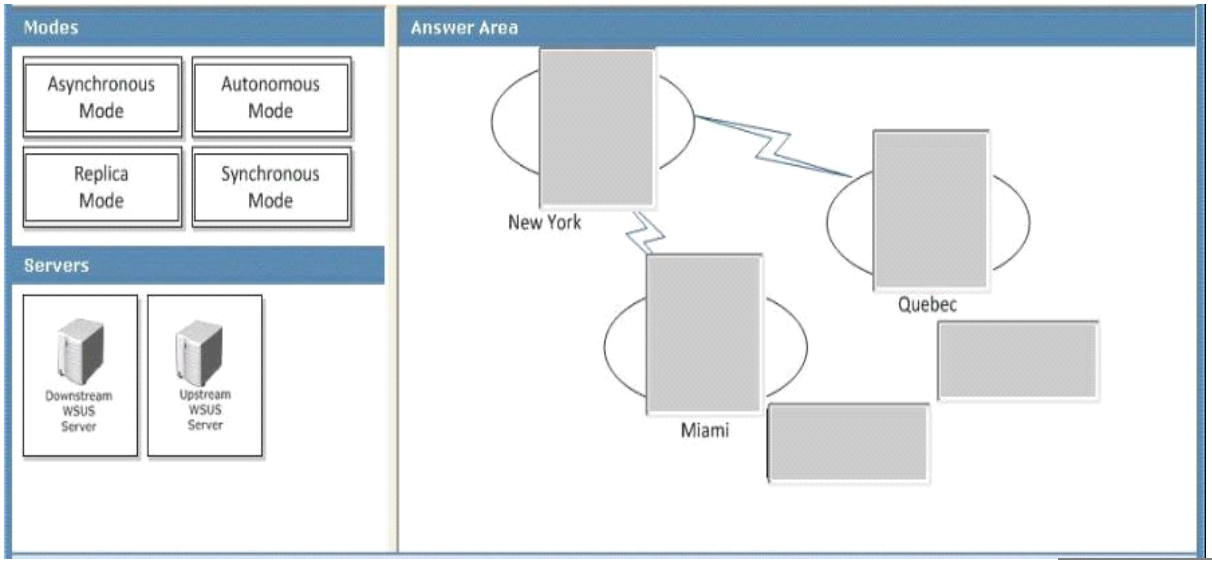
Question: 96 DRAG DROP

A company has its main office in New York and branch offices in Miami and Quebec. All sites are connected by reliable WAN links. You are designing a Windows Server Update Services (WSUS) deployment strategy. The deployment strategy must meet the following requirements:

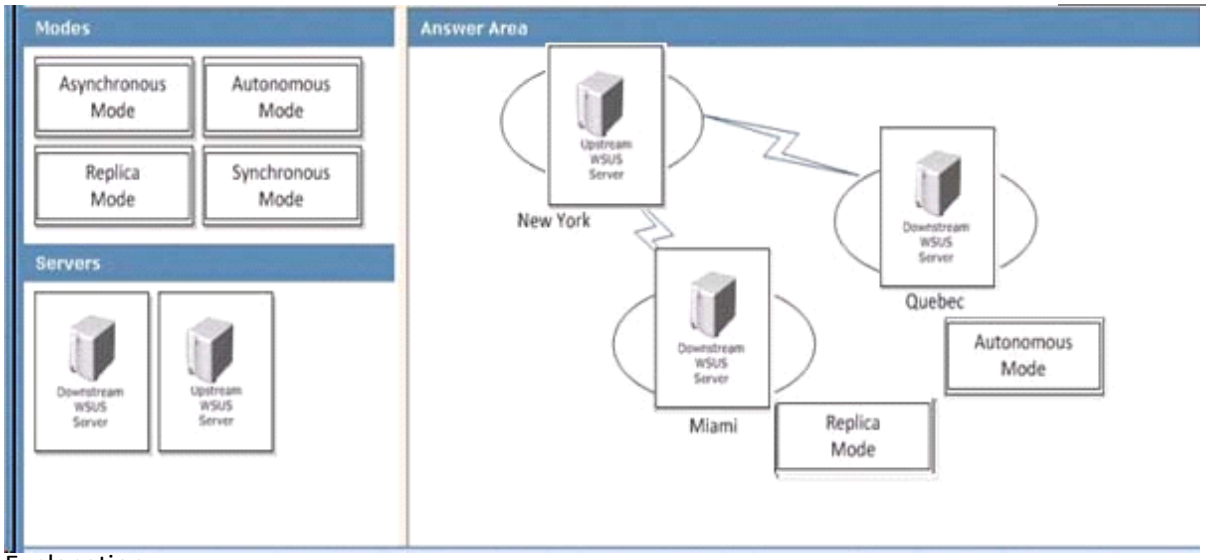
- Download updates from Windows Update only in the New York office.
- Ensure that the update language can be specified for the Quebec office.

You need to design a deployment strategy that meets the requirements. How should you configure the servers and hierarchy types?

To answer, drag the appropriate server types and hierarchy types from the list to the correct location or locations in the answer area.



Answer:



Explanation:

The most basic WSUS deployment consists of a server inside the corporate firewall that serves client computers on a private intranet, as shown in the "Simple WSUS Deployment" illustration below. The WSUS server connects to Microsoft Update to download updates. This is known as synchronization. During synchronization, WSUS determines if any new updates have been made available since the last time you synchronized. If it is your first time synchronizing WSUS, all updates are made available for download.

WSUS server hierarchies.

You can create complex hierarchies of WSUS servers. Since you can synchronize one WSUS server with another WSUS server instead of with Microsoft Update, you need to have only a single WSUS server that is connected to Microsoft Update. When you link WSUS servers together, there is an upstream WSUS server and a downstream WSUS server, as shown in the "WSUS Server Hierarchy" illustration below.

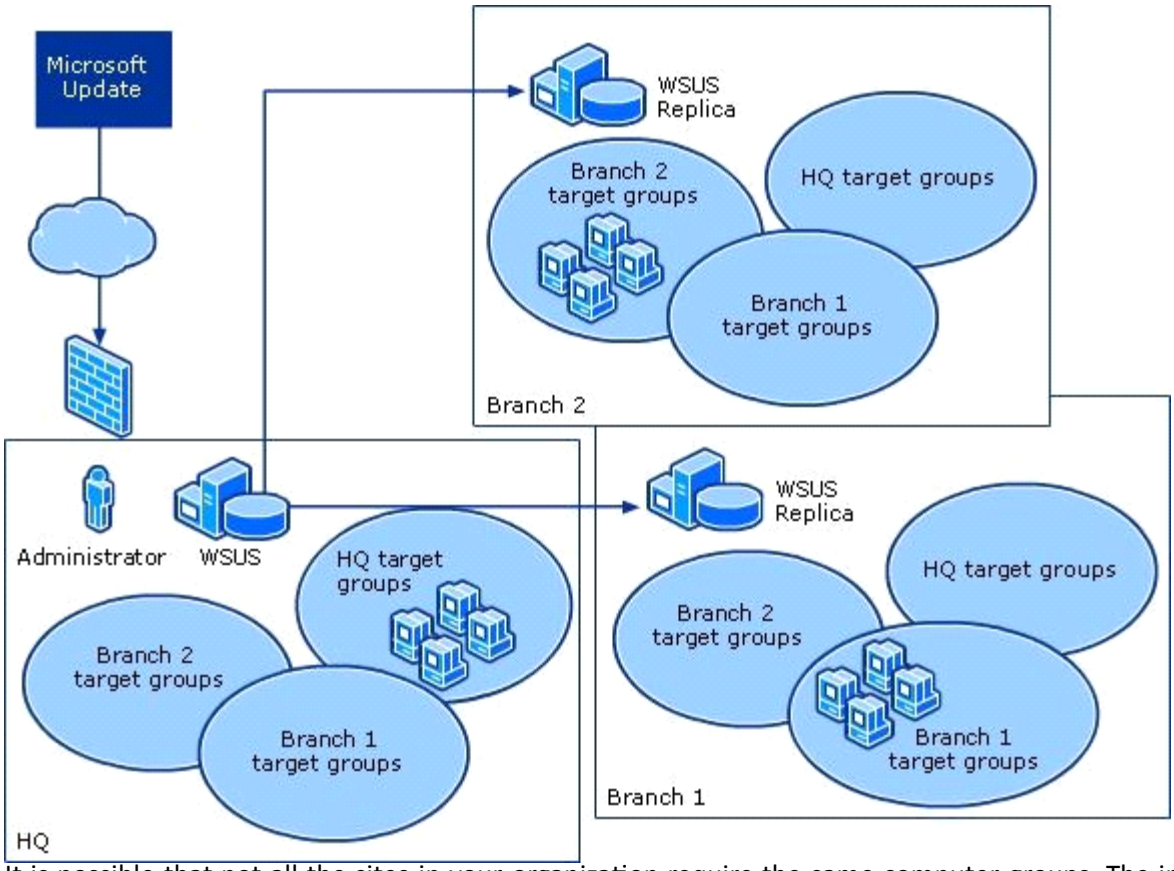
There are two ways to link WSUS servers together:

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.

Centralized management

Centrally managed WSUS servers utilize replica servers. Replica servers are not administered separately, and are used only to distribute approvals, groups, and updates. The approvals and targeting groups you create on the master server are replicated throughout the entire organization, as shown in the "WSUS Centralized Management (Replica Servers)" illustration below. Remember that computer group membership is not distributed throughout the replica group, only the computer groups themselves. In other words, you always have to load client computers into computer groups.



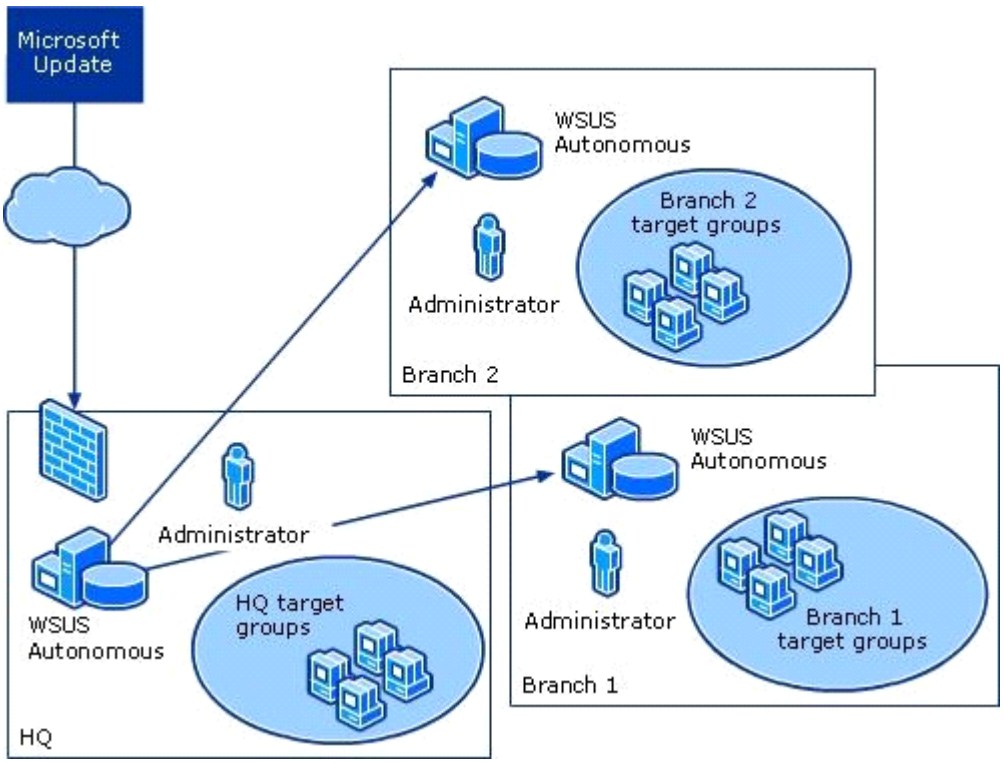
It is possible that not all the sites in your organization require the same computer groups. The important thing is to create enough computer groups on the administered server to satisfy the needs of the rest of the organization. Computers at different sites can be moved into a group appropriate for the site. Meanwhile, computer groups inappropriate for a particular site simply remain empty. All update approvals, like computer groups, must be created on the master server. For step-by-step instructions, see Create Replica Servers later in this guide.

You should also make sure that the upstream server is configured for all the languages required by its replica servers. If you add languages to the upstream server, you should copy the new updates to its replica servers.

Changing language options on the upstream server alone might result in a mismatch between the number of updates that are approved on the central server and the number of updates approved on the replica servers.

Distributed management

Distributed management offers you full control over approvals and computer groups for the WSUS server, as shown in the "WSUS Distributed Management" illustration below. With the distributed management model, there is usually an administrator at each site who decides which update languages are needed, creates computer groups, assigns computers to groups, tests and approves updates, and ensures that the correct updates are installed on the right computer groups. Distributed management is the default installation option for all WSUS installations.



Question: 97

A company has client computers that run Windows 7. The company has Windows Server Update Services (WSUS) 3.0 with Service Pack 2 (SP2) deployed on a server that runs Windows Server 2008 R2. You are designing an update management solution for the company's client computers. The solution must meet the following requirements:

- Client computers must use WSUS for the installation of updates.
- Only administrators should receive update notifications from WSUS.

You need to design an update management solution that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Define the WSUS settings in the Computer Configuration area of the Group Policy Management Console.
B. Define the WSUS settings in the User Configuration area of the Group Policy Management Console.
C. Define the WSUS settings in the User Configuration area of the Local Group Policy on client computers.
D. Define the WSUS settings in the Computer Configuration area of the Local Group Policy on client computers.

Answer: A

Explanation:
FROM Step by Step guide to setting up WSUS 3.0 SP2 http://technet.microsoft.com/en-us/library/cc708519%28v=ws.10%29 or http://blogs.microsoft.co.il/blogs/yanivf/archive/2007/09/23/install-wsus-3-0-stepby-step.aspx
To configure Automatic Updates
In Group Policy Object Editor, expand Computer Configuration, expand Administrative Templates, expand Windows Components, and then click Windows Update.

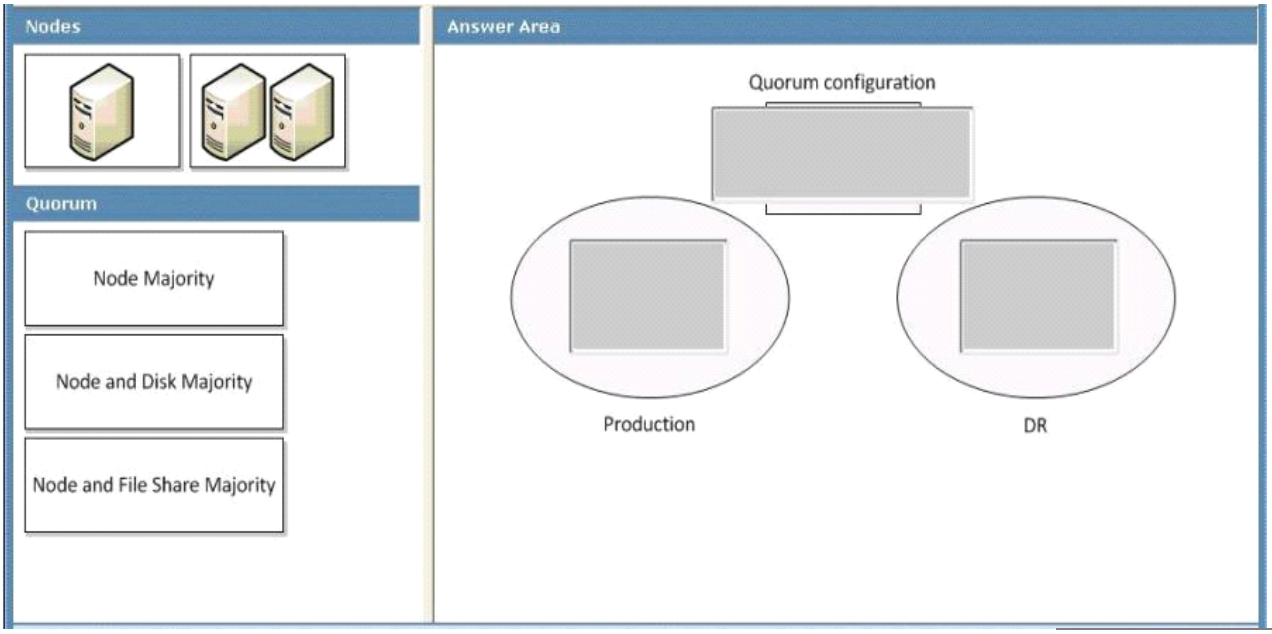
In the details pane, double-click Configure Automatic Updates.
Click Enabled, and then click one of the following options:
Notify for download and notify for install: This option notifies a logged-on administrative user before the download and before the installation of the updates.
Auto download and notify for install: This option automatically begins downloading updates and then notifies a logged-on administrative user before installing the updates.
Auto download and schedule the install: If Automatic Updates is configured to perform a scheduled installation, you must also set the day and time for the recurring scheduled installation.
Allow local admin to choose setting: With this option, local administrators are allowed to use Automatic Updates in Control Panel to select a configuration option of their choice. For example, they can choose their own scheduled installation time. Local administrators are not allowed to disable Automatic Updates.
Click OK.
Set Up E-Mail Notifications
http://technet.microsoft.com/en-us/library/cc708608%28v=ws.10%29.aspx
In the WSUS Administration console, click Options in the left pane.
In the center pane, click E-Mail Notifications.
Click the General tab.
If you want update notifications, select the Send e-mail notification when new updates are synchronized check box.
In the Recipients box, type the e-mail addresses of the people who should receive update notifications.
Separate the names with semi-colons.
If you want status reports, select the Send status reports check box.
In the Frequency box, select either Daily or Weekly.
In the Send reports at box, set the time at which you want status reports to be sent.
In the Recipients box type the e-mail addresses of the people who should receive status reports, delimited by semicolons.
In the Language box, select the language in which the status reports should be sent.
Click Apply to save these settings.

Question: 98

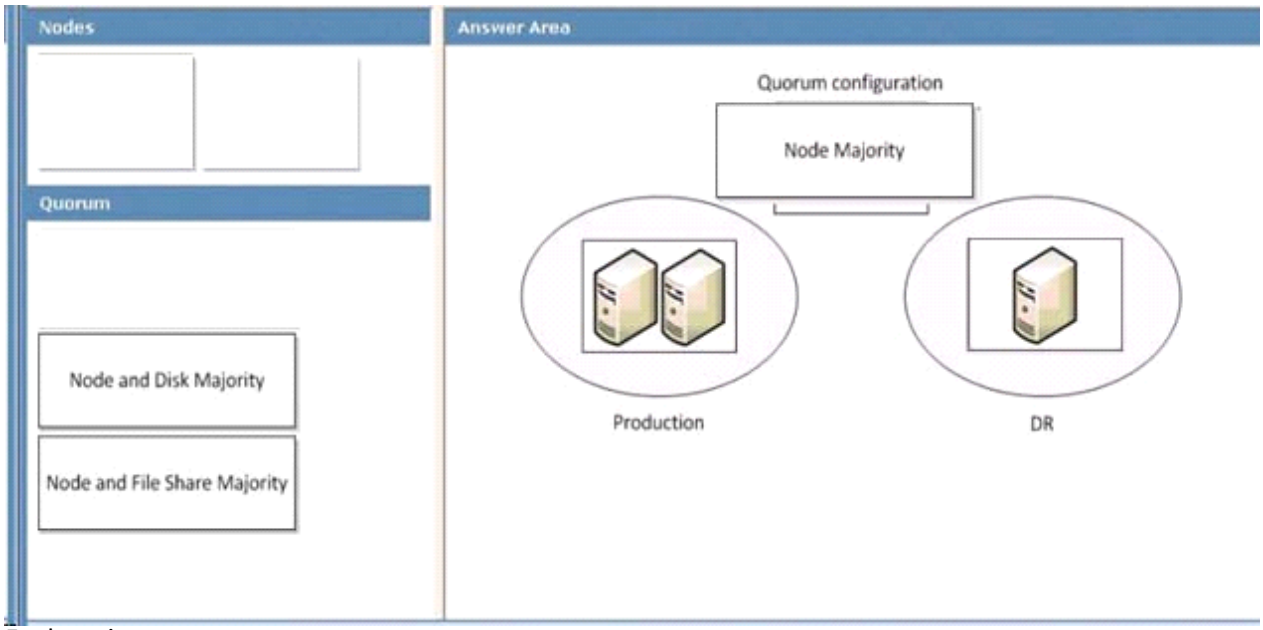
DRAG DROP
You are designing a highly available virtual environment running on Windows Server 2008 R2. The design must meet the following requirements:

- Provide high availability within the Production site to ensure that a failure of a node in the Production site does not stop the cluster from running.
- Provide the ability to withstand a failure of the Disaster Recovery (DR) site.
- Minimize the number of nodes and votes in the cluster.

You need to design the virtual environment to meet the requirements. What should you do?
To answer, drag the appropriate nodes and quorum configuration to the correct location or locations in the answer area.



Answer:



Explanation:
Having two nodes in the Production site provides high availability in that site.
Node Majority (recommended for clusters with an odd number of nodes)
Can sustain failures of half the nodes (rounding up) minus one. For example, a seven node cluster can sustain three node failures.

Question: 99

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

Answer: C

Explanation:
There's a lot of debate about this answer, is it A or C?
It's 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:

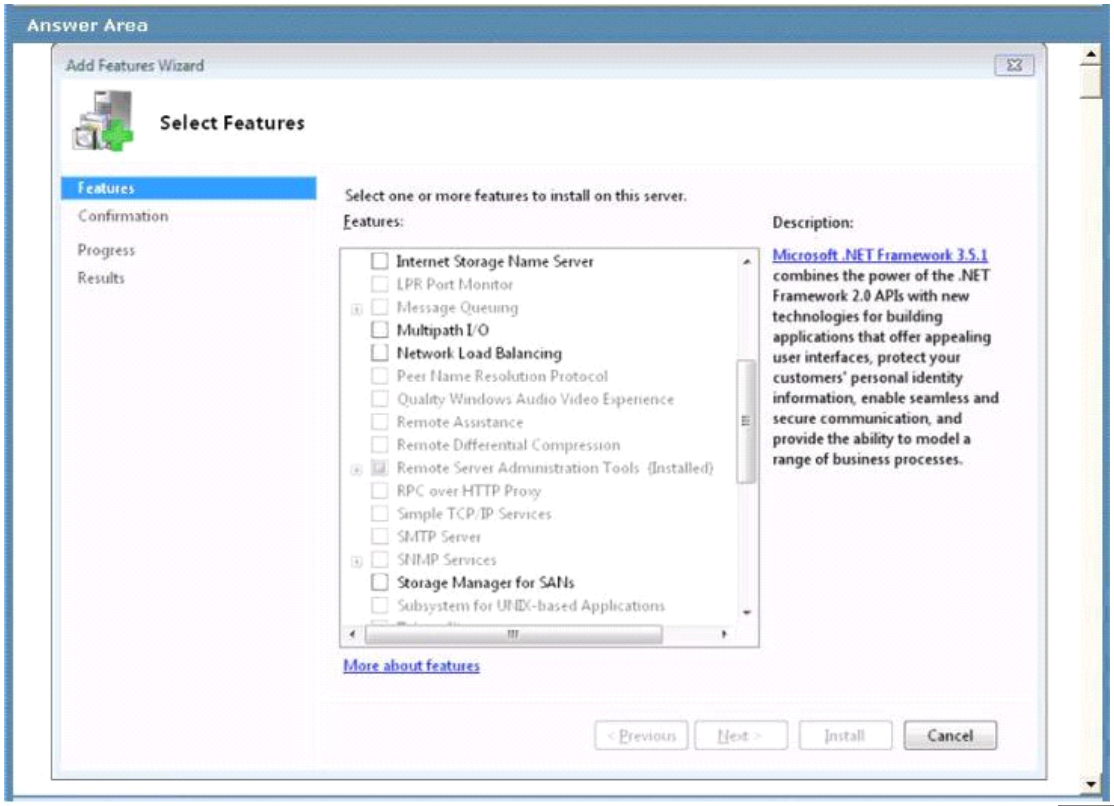
Who can connect to internal network resources (in other words, the user groups who can connect).
What network resources (computer groups) users can connect to.
Whether client computers must be members of Active Directory security groups.
Whether device redirection is allowed.
Whether clients need to 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: 100
HOTSPOT

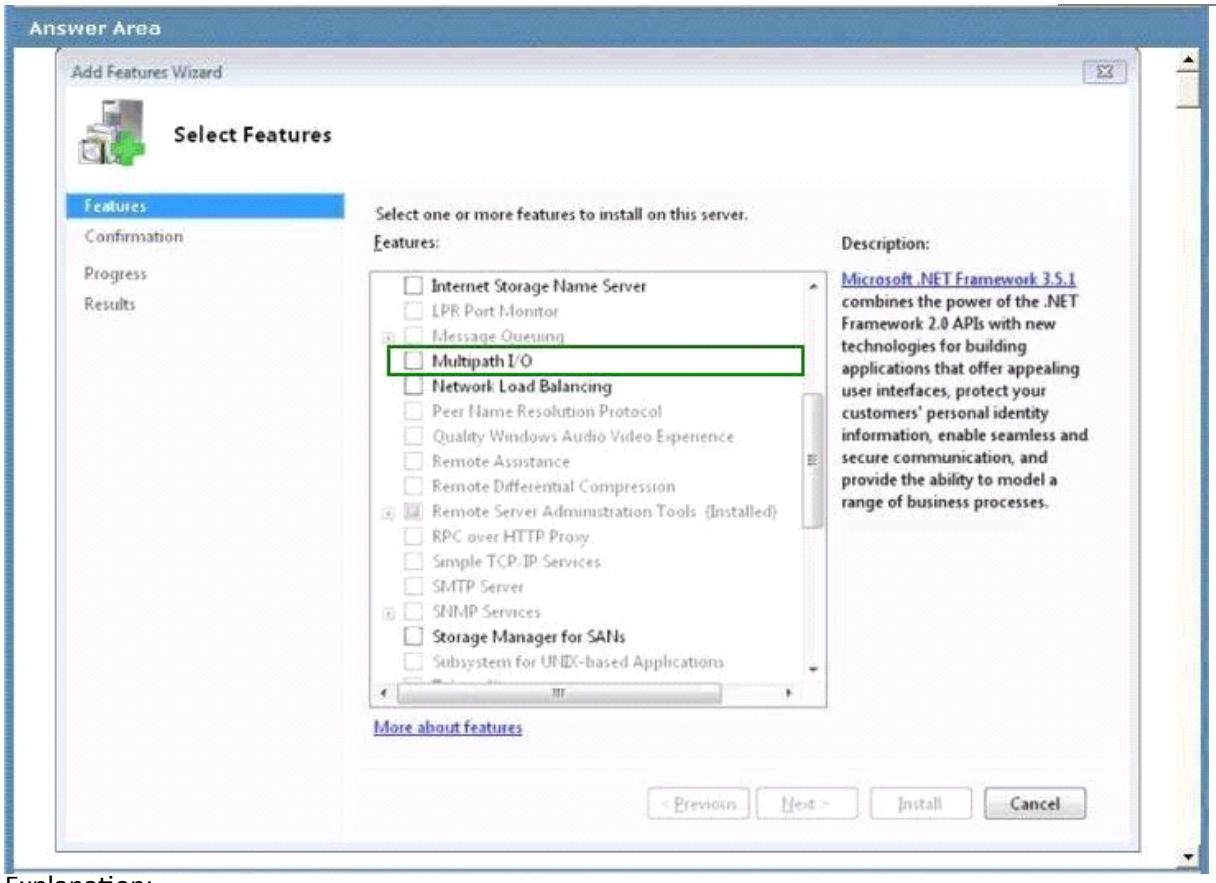
A company has servers that run Windows Server 2008 R2. You are designing a storage solution for the servers. The storage solution must meet the following requirements:

- Allow the use of Fibre Channel (FC), Internet SCSI (iSCSI), and Serial Attached SCSI (SAS) interfaces for connectivity to storage arrays.
- Support storage load balancing.

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.



Answer:



Explanation:

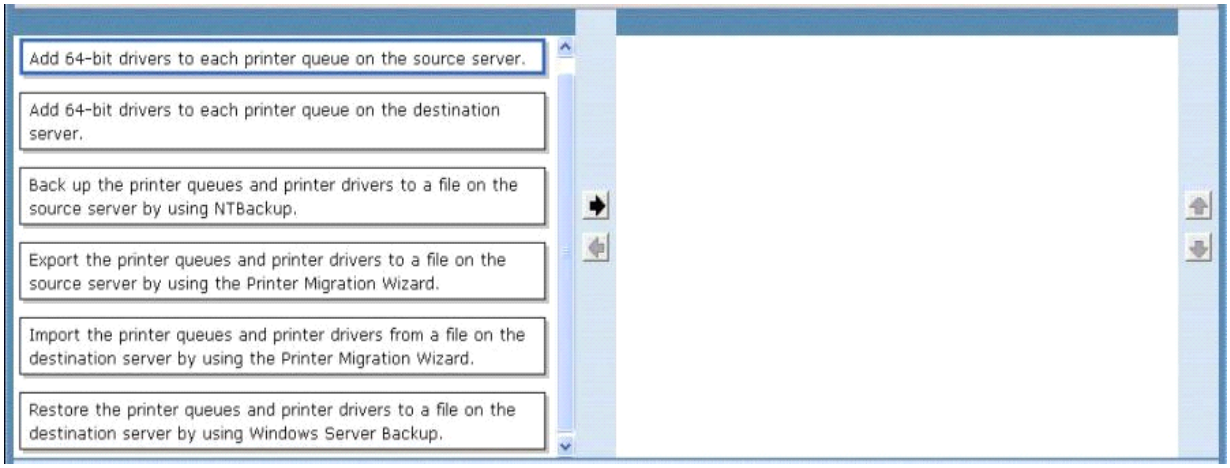
A growing number of organizations require that their data be available at all times. To meet this requirement, centralized storage must be readily available and immune to outages. Multipathing is the ability of a system to use more than one read/write path to a storage device. It is a solution that provides fault tolerance against a single point-

of-failure in hardware components.
The Microsoft® Multipath I/O (MPIO) framework helps ensure that your data is available at all times. MPIO supports multiple data paths to storage, improves the fault tolerance of the storage connection, and in some cases, provides greater aggregate throughput by using multiple paths at the same time. This helps improve system and application performance.
Multipathing Support for High Availability
Windows Server® 2008 includes many enhancements for the connectivity of a computer running a Windows server-class operating system to storage area networking (SAN) devices.
Among the enhancements enabling high availability for connecting Windows-based servers to SANs is integrated Multipath I/O (MPIO) support. Microsoft MPIO architecture supports iSCSI, Fibre Channel and serial attached storage (SAS) SAN connectivity by establishing multiple sessions or connections to the storage array. Multipathing solutions use redundant physical path components — adapters, cables, and switches — to create logical paths between the server and the storage device. In the event that one or more of these components
fails, causing the path to fail, multipathing logic uses an alternate path for I/O so that applications can still access their data. Each network interface card (in the iSCSI case) or HBA should be connected by using redundant switch infrastructures to provide continued access to storage in the event of a failure in a storage fabric component.
Failover times vary by storage vendor, and can be configured by using timers in the Microsoft iSCSI Software
Initiator driver, or modifying the Fibre Channel host bus adapter driver parameter settings.
New MPIO features in Windows Server 2008 include a Device Specific Module (DSM) designed to work with storage arrays that support the asymmetric logical unit access (ALUA) controller model (as defined in SPC-3), as well as storage arrays that follow the Active/Active controller model.

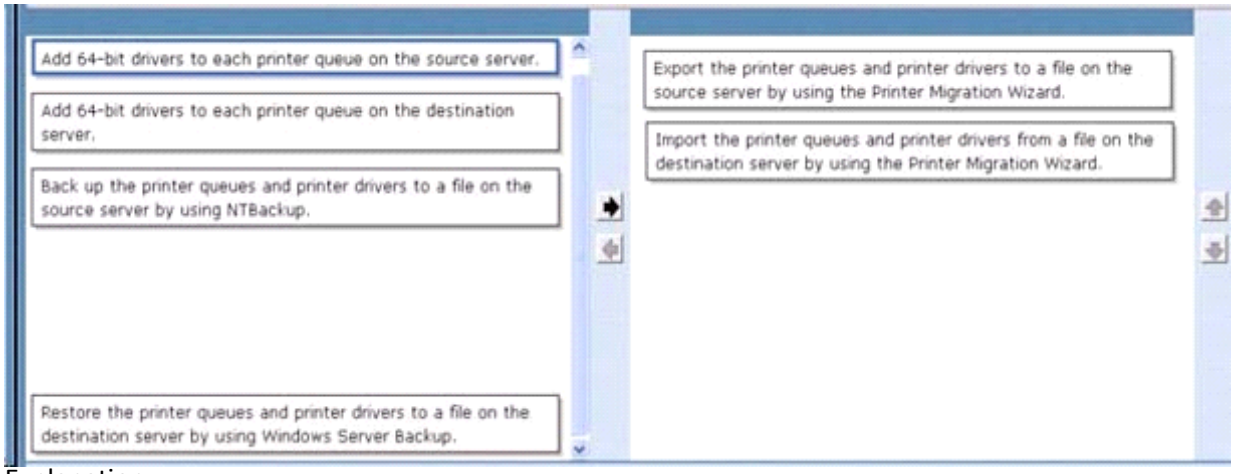
Question: 101

DRAG DROP

A company has a print server that runs Windows Server 2003 R2 Enterprise (x86). The print server is configured with 2S0 print queues. You are planning to migrate the print server to a new server that runs Windows Server 2008 R2 Enterprise. The destination server has the Print and Document Services role installed. You need to ensure that printer queues migrate successfully. 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.)



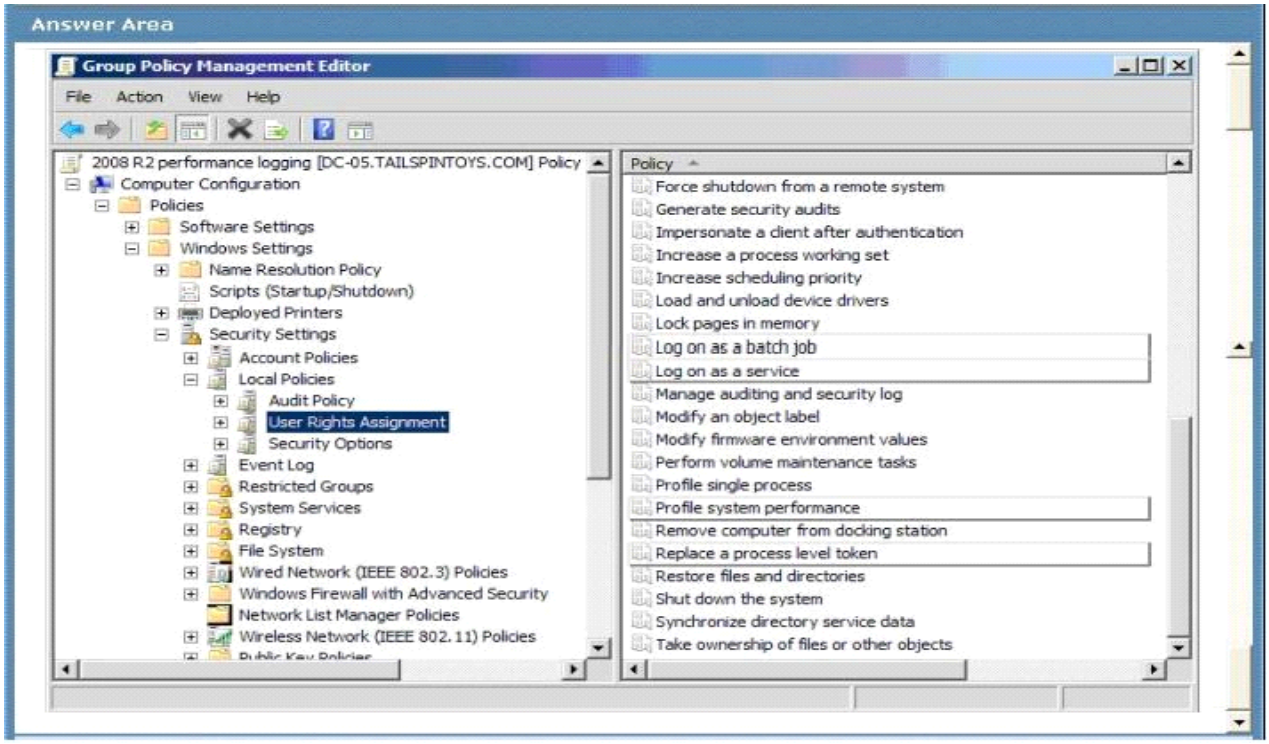
Answer:



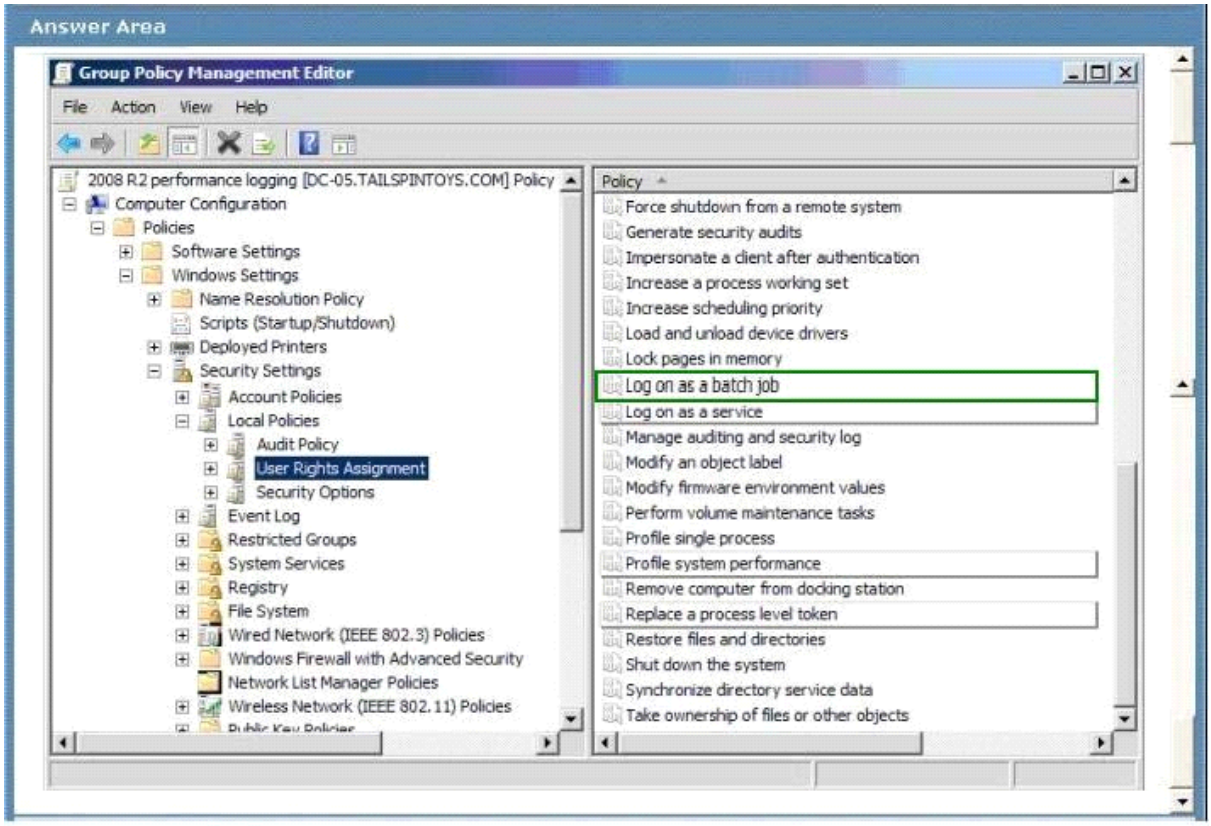
Explanation:
http://technet.microsoft.com/en-us/library/cc722360.aspx
Migrating print servers
Using the Windows interface
Using a command prompt
To migrate print servers by using Print Management
Open Print Management.
In left pane, click Print Servers, right-click the print server that contains the printer queues that you want to export, and then click Export printers to a file. This starts the Printer Migration Wizard.
On the Select the file location page, specify the location to save the printer settings, and then click Next to save the printers.
Right-click the destination computer on which you want to import the printers, and then click Import printers from a file. This launches the Printer Migration Wizard.
On the Select the file location page, specify the location of the printer settings file, and then click Next.
On the Select import options page, specify the following import options:
Import mode. Specifies what to do if a specific print queue already exists on the destination computer.
List in the directory. Specifies whether to publish the imported print queues in the Active Directory Domain Services.
Convert LPR Ports to Standard Port Monitors. Specifies whether to convert Line Printer Remote (LPR) printer ports in the printer settings file to the faster Standard Port Monitor when importing printers.
Click Next to import the printers.
To migrate print servers by using a command prompt
To open a Command Prompt window, click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.
Type:
CD %WINDIR%\System32\Spool\Tools Printbrm -s Error! Hyperlink reference not valid.> -b -f <filename>.printerExport
Type: Printbrm -s Error! Hyperlink reference not valid.> -r -f <filename>.printerExport

Question: 102
HOTSPOT

You are designing a monitoring solution to log performance for servers that run Windows Server 2008 R2. The monitoring solution must allow members of the Performance Log Users group to create and modify Data Collector Sets. You need to grant members of the Performance Log Users group the necessary permissions. Which User Rights Assignment policy should you configure?
To answer, select the appropriate User Rights Assignment policy in the answer area.



Answer:



Explanation:
Log on as a batch job
http://technet.microsoft.com/en-us/library/dd349804%28v=ws.10%29.aspx#BKMK_30
This policy setting determines which accounts can log on by using a batch-queue tool such as the Task Scheduler

service. When an administrator uses the Add Scheduled Task wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the Log on as a batch job user right. When the scheduled time arrives, the Task Scheduler service logs the user on as a batch job instead of as an interactive user, and the task runs in the user's security context.
Possible values:
User-defined list of accounts
Not Defined
Vulnerability
The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default setting of Not Defined is sufficient. Members of the local Administrators group have this right by default.
Countermeasure
You should allow the computer to manage this logon right automatically if you want to allow scheduled tasks to run for specific user accounts. If you do not want to use the Task Scheduler in this manner, configure the Log on as a batch job user right for only the Local Service account.
For IIS servers, you should configure this policy locally instead of through domain–based Group Policy settings so that you can ensure that the local IUSR_<ComputerName> and IWAM_<ComputerName> accounts have this logon right.
Potential impact
If you configure the Log on as a batch job setting by using domain-based Group Policy settings, the computer cannot assign the user right to accounts that are used for scheduled jobs in the Task Scheduler. If you install optional components such as ASP.NET or IIS, you may need to assign this user right to additional accounts that are required by those components. For example, IIS requires assignment of this user right to the IIS_WPG group and the IUSR_<ComputerName>, ASPNET, and IWAM_<ComputerName> accounts. If this user right is not assigned to this group and these accounts, IIS cannot run some COM objects that are necessary for proper functionality.

Question: 103

A company has a single Active Directory Domain Services (AD DS) domain. Each department within the company has its own organizational unit (OU). All client computers run Windows 7 Enterprise Edition and Microsoft Office 2010. The company wants to restrict access to some Office 2010 features. They develop a standard list of corporate restrictions. You have the following requirements:

- Apply the corporate restrictions to all existing and future departments.
- Ensure that specific restrictions can be added or removed for individual departments.
- Ensure that the corporate restrictions are not App1ied to users and computers in the built-in Active Directory containers.
- Minimize administrative effort for Applying restrictions to future departments.

You need to recommend a Group Policy object (GPO) deployment that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Create a GPO that contains the corporate restrictions and link it to the domain. Install the Office 2010 Group Policy Administrative Template settings. Create a separate GPO for each department that deploys and configures Office 2010.
B. Install the Office 2010 Group Policy Administrative Template settings. Create a Starter GPO that contains the corporate restrictions. Create a separate GPO based on the Starter GPO for each department that deploys and configures Office 2010.
C. Install the Office 2010 Resource Kit and create a custom transform (.mst) file for each department. Create a Starter GPO that contains the corporate restrictions. Create a separate GPO based on the Starter GPO for each department that deploys Office 2010 by using the transform file.
D. Install the Office 2010 Resource Kit and create custom installer files for each department. Create a GPO that contains the corporate restrictions and link it to the domain. Create a separate GPO for each department that deploys the installer files,

Answer: B

Explanation:
Starter GPOs are used as a base template to build other GPOs from. admin templates (ADMX & ADML files) need to be applied so that the settings specific to Office 2010 can be applied

Question: 104

You are designing a recovery solution for file servers that run Windows Server 2008 R2. File servers have the operating system and settings on volume C and shared data on other volumes. The recovery solution must meet the following requirements:

- Create restorable point-in-time copies of files stored in shared folders on the file servers.
- Provide users the ability to compare versions of an open file.

You need to design a recovery solution that meets the requirements. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Enable the windows Server Backup feature and schedule a backup of the shared folders on the file servers.
B. Enable Shadow Copies on all file server volumes.
C. Enable the Windows Server Backup feature and schedule a backup of the file server system state data.
D. Enable Shadow Copies on only file server volumes that contain shared folders.

Answer: D

Explanation:
Windows Server 2008 Volume Shadow Copy is a mechanism whereby the contents of shared folders can be automatically backed up at pre-determined intervals to a shadow volume. Once implemented, shadow copy will backup the previous 64 versions of each file in the shadowed volume and provide users with the ability to restore files from any of the previous 64 versions without administrator intervention, enabling users to independently restore deleted, damaged or overwritten files. In addition to restoring individual files to a previous version, shadow copy also provides the ability to restore an entire volume.
The requirement is to enable this on shared folders only so answer D meets this requirement best.

Question: 105

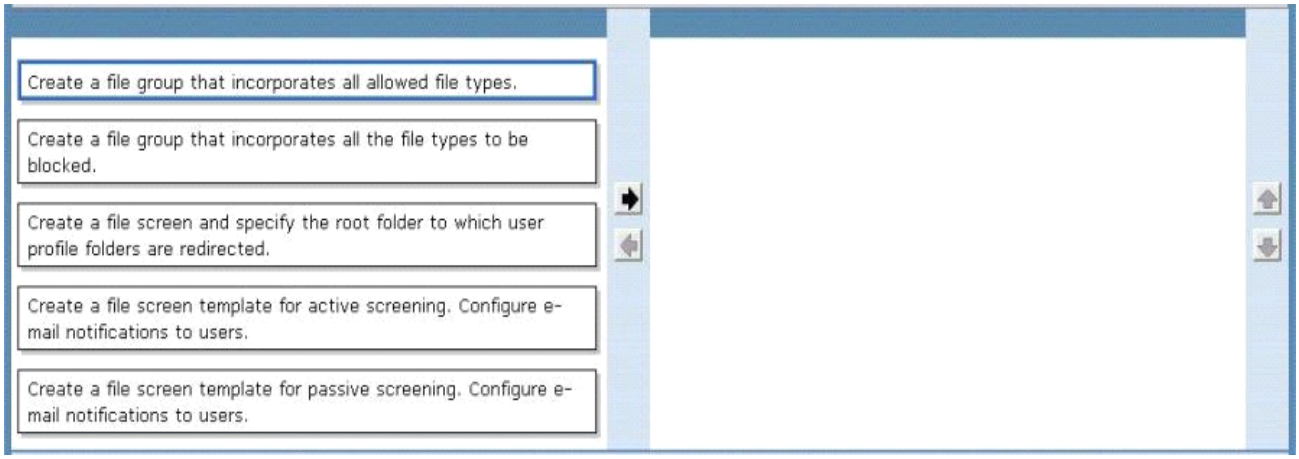
DRAG DROP
A company's file servers are running out of disk space. The company uses folder redirection policies to redirect user profile folders to 50 dedicated file servers. The files stored on the file servers include the following types of files that should not be stored in user profile folders:

- Audio and video files
- Files created by a computer-aided drafting (CAD) Application

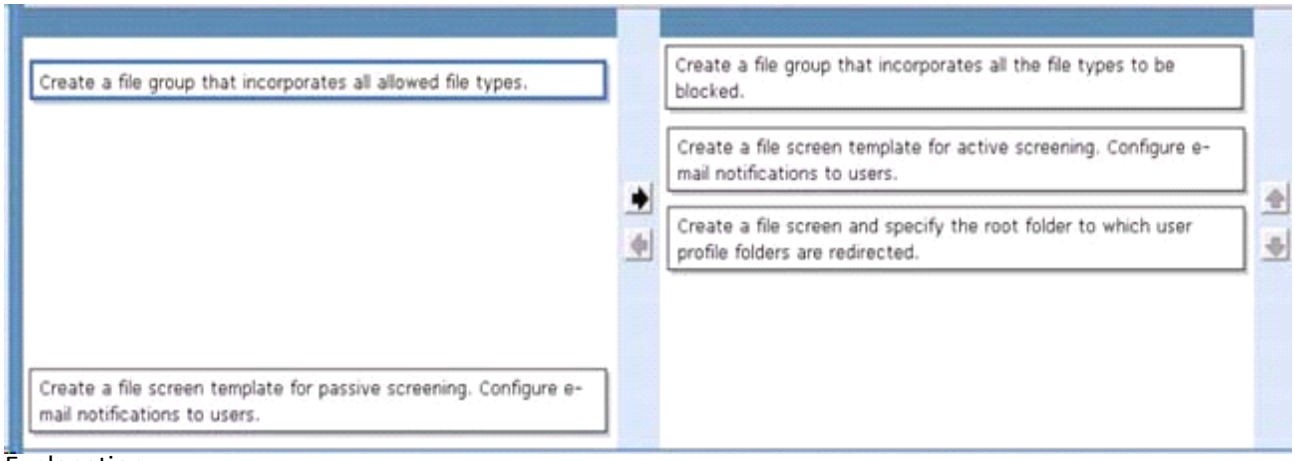
You decide to implement File Server Resource Manager (FSRM) on the dedicated file servers. You have the following requirements:

- 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.)



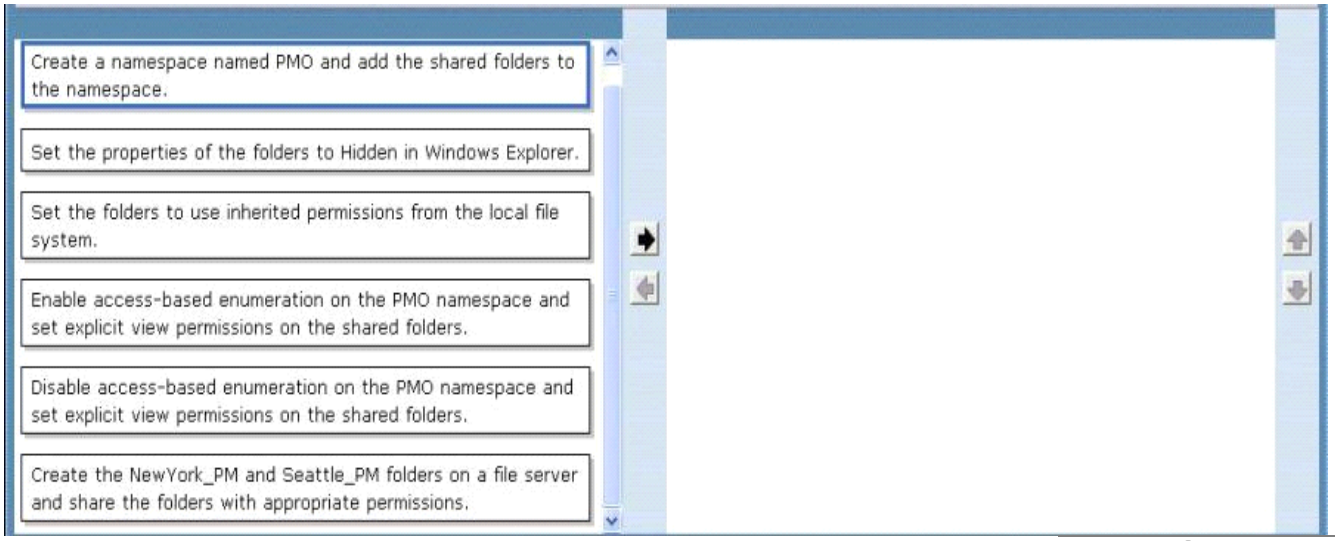
Answer:



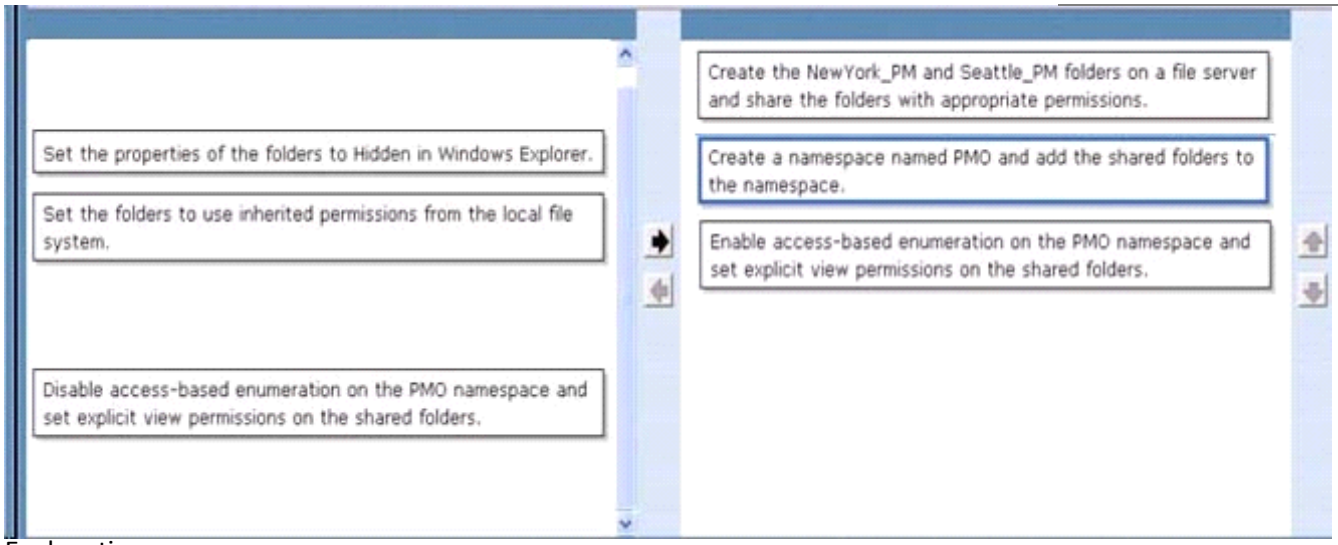
Explanation:
FSRM
File Server Resource Manager is a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. By using File Server Resource Manager, administrators can place quotas on folders and volumes, actively screen files, 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-fsrm-file-serverresource-manager.aspx

Question: 106 DRAG DROP

A company has offices in New York and Seattle. Project managers from each office are in the NewYork_PM and Seattle_PM Active Directory security groups, respectively. You are planning to store all active IT project resources for the Project Management Office in branch-specific folders in a namespace. You need to ensure that project managers from each branch can see only folders from that branch in the namespace. 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.)



Answer:

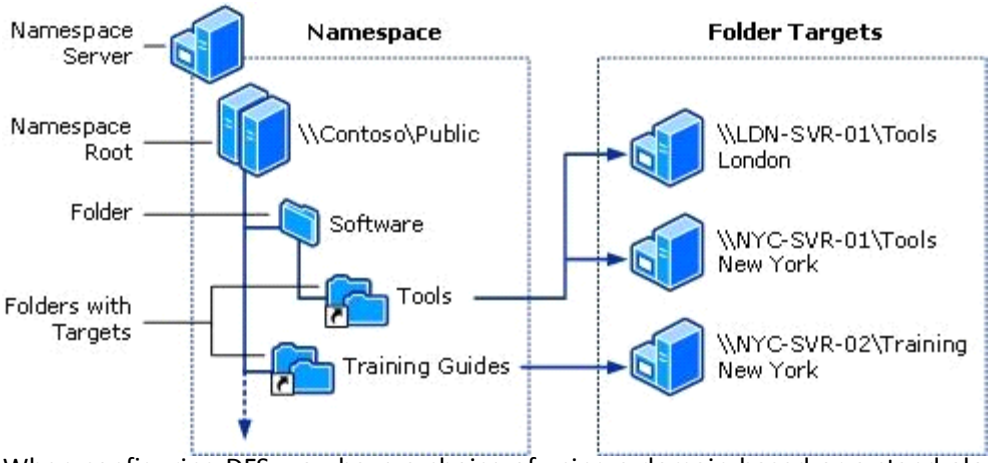


Explanation:

DFS Services are available on all currently supported versions of Windows Server, but there are significant improvements in the Windows Server 2008 editions. The DFS namespace client is available for all currently supported versions of Windows, both client and server. Domain-based DFS namespaces require the use of Active Directory.

DFS Namespaces

A DFS namespace is basically a place where you will have links to all your file shares. From an administrator point of view, you should think of it as a folder structure where you keep the list of target file shares. Your users will see it as a single share with many folders and they will have no idea that they are navigating across a set of servers to get to the subfolders and files.



When configuring DFS, you have a choice of using a domain-based or a stand-alone namespace. If you already have Active Directory deployed, you should consider using a domain-based namespace. If you're not using Active Directory, your only choice is a stand-alone one.

The main advantage of the domain-based namespaces is that your configuration will be stored in Active Directory and you won't have to rely on a single server to provide the namespace information to your clients.

The path users refer to uses the name of the domain and it will not need to change because your namespace server name changed (only if you change your domain name). With a stand-alone DFS, that server name becomes part of the main path to the namespace.

There are also two domain-based DFS modes: Windows Server 2008 mode and Windows Server 2000 mode.

Windows Server 2008 mode (which requires Windows Server 2003 forest functional level, Windows Server 2008 domain functional level and Windows Server 2008 running on all namespace servers) includes support for more than 5,000 folders with targets per namespace and access-based enumeration.

Adding Folders to the Namespace

After your create the namespace, you will add folders to it, specifying the associated folder target. This means pointing to the actual file shares, making each one appear to users as a folder under the namespace. Before you do that, you want to think long and hard about the folder structure you're creating. A basic goal of DFS is to create a stable infrastructure that will not constantly change on your users.

Multiple Targets

It's useful to have multiple copies of the same data stored in different file servers. One reason for that is faulttolerance (if one server is unavailable, you can still access the other one). The other reason is to choose the copy of the data that is closer to you. If you're in a branch office and you want to access a very large file, you would rather get a copy from a server in that branch.

It's actually quite simple to add more folder targets to an existing folder or create the folder with multiple targets initially. All you have to do is make sure that you provide the multiple targets for the same folder in that namespace when you configure it.

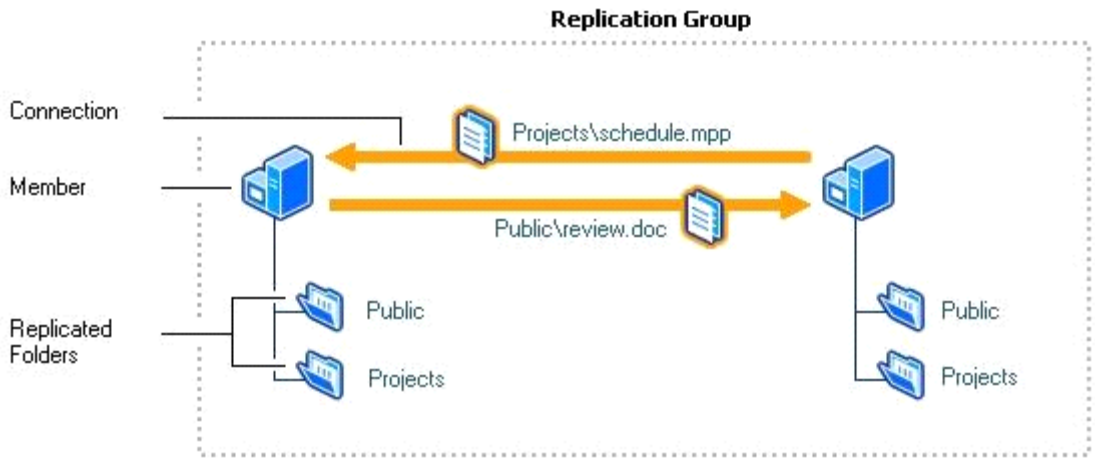
DFS Replication

At this point, you're probably thinking: How does the data get copied across multiple servers?

Well, Windows Server includes a component to replicate data between file servers in case you need that. It's called DFS-R (Distributed File System Replication). DFS-R was introduced with Windows Server 2003 R2 (replacing the old NTFRS with many advantages). DFS-R can be used for both domain-based and stand-alone DFS.

To replicate files between two (or more) shares, you need to create a replication group and specify a few things like which servers will replicate (members) and what they will replicate (replicated folders). DFS-R is aware of site topology. It also has options to control scheduling and the use of bandwidth (throttling). DFS-R uses

Remote Differential Compression (RDC), meaning that only changes in the files are sent over the network, not the entire file.



What does access-based enumeration do?

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

This feature is active only when viewing files and folders in a shared folder; it is not active when viewing files and folders in the local file system.

Access-based enumeration can be enabled or disabled by using Share and Storage Management Access-based enumeration can be manually enabled or disabled on individual shared folders and volumes by using Share and Storage Management. This snap-in is available after a folder or volume has been shared. You can access Share and Storage Management in the File Services server role in Server Manager, and in Administrative Tools. You can also install it manually in Server Manager by adding the File Server role service to File Services.

There are two ways to enable and disable access-based enumeration by using Share and Storage Management:

Share a folder or volume by using the Provision a Shared Folder Wizard. If you select the SMB protocol on the Share Protocols page of the Provision a Shared Folder Wizard, the advanced settings options on the SMB Settings page includes the option to enable access-based enumeration on the shared folder or volume. (To see the advanced settings options, on the SMB Settings page of the wizard, click Advanced).

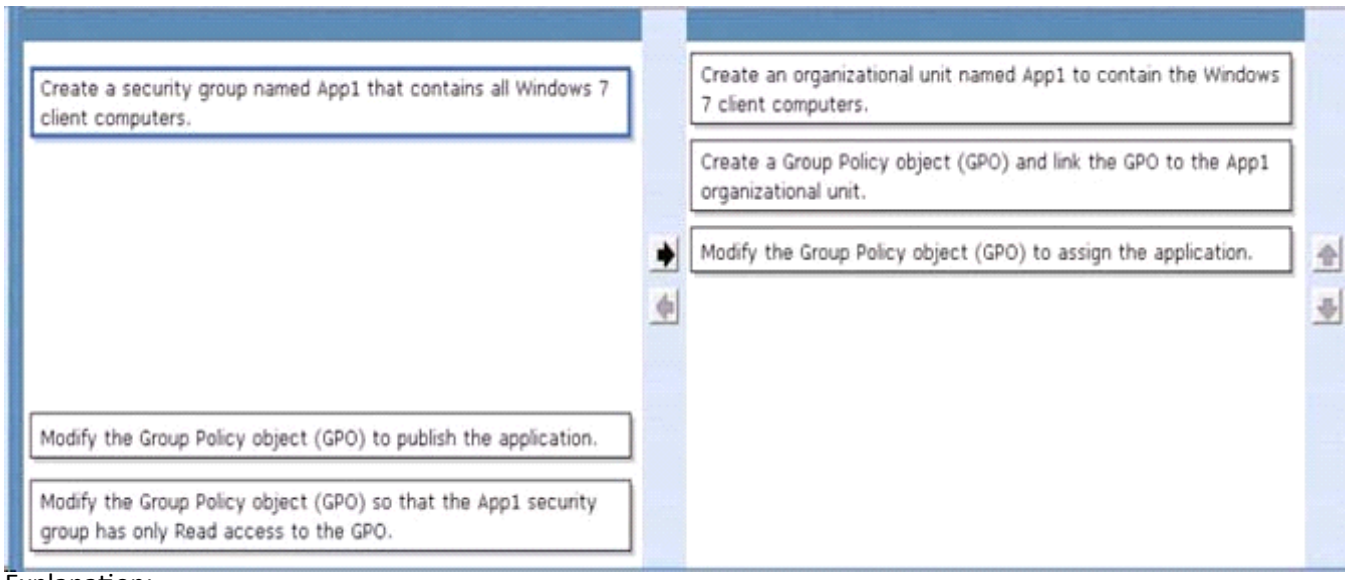
Change the properties of an existing shared folder or volume. To change the properties of an existing shared folder or volume, on the Shares tab of Share and Storage Management, click the shared folder or volume, and then click Properties in the Action pane. The information under Advanced settings displays whether accessbased enumeration is enabled. Click Advanced and then select or clear the Enable access-based enumeration check box.

Question: 107 DRAG DROP

A company has client computers that run Windows 7 and Windows Vista. The company has a single domain Active Directory Domain Services (AD DS) forest with domain controllers that run Windows Server 2008 R2. An Application must be installed on the windows 7 client computers when users log on to the computers. You need to design an Application deployment solution. 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.)

Answer:



Explanation:
http://support.microsoft.com/kb/816102
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: 108

A company has file servers that run a Server Core installation of Windows Server 2008. You are designing the migration of the file servers to Windows Server 2008 R2. After the migration, you will install the Remote Desktop Services server role on the file servers. You need to ensure that shared resources on the file servers are available after

the migration, and minimize administrative effort. What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Move the shared resources off of the existing file servers. Perform a clean installation of Windows Server 2008 R2 on the file servers. Move the shared resources back onto the file servers.
B. Upgrade the existing file servers to a Server Core installation of Windows Server 2008 R2, and then upgrade the file servers to a full installation of Windows Server 2008 R2.
C. Deploy new file servers with Windows Server 2008 R2 installed. Migrate the shared resources to the new file servers.
D. Deploy new file servers with a Server Core installation of Windows Server 2008 R2. Migrate the shared resources to the new file servers.

Answer: C

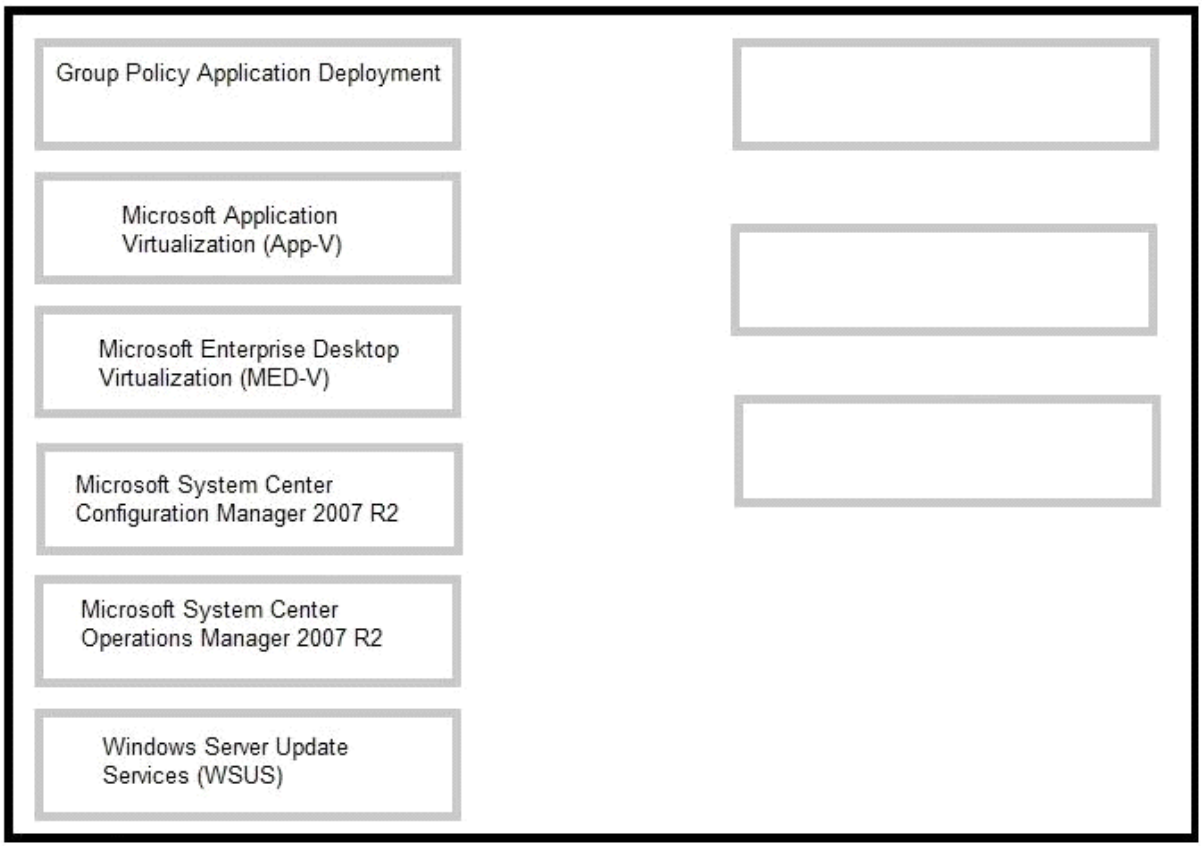
Explanation:
The key here is minimize effort & Remote Desktop Services.
Server Core wouldn't allow remote desktop services as it has no GUI so that would rule out answer A you also cant upgrade from Core to Full see http://www.windowsitpro.com/article/tips/can-i-upgrade-fromserver-core-2008-to-the-full-windows-server-2008- or http://serverfault.com/questions/92523/upgrade-fromwindows-2008-server-core-to-full-windows-2008-server upgrade considerations for Server Core installations of Windows Server 2008
You can use the Server Core installation option only by performing a clean installation.
You cannot upgrade from earlier versions of Windows to Server Core installations of Windows Server 2008.
You cannot upgrade from non-Server Core installations of Windows Server 2008 to Server Core installations of Windows Server 2008.
You cannot convert Server Core installations of Windows Server 2008 to non-Server Core installations of Windows Server 2008.
You can upgrade Server Core installations of Windows Server 2008 only to Windows Server Core R2 when it is released.
Answer C is possible but again you're asked to minimize effort so D would be 1 step less thus reducing your effort and possible down time.

Question: 109

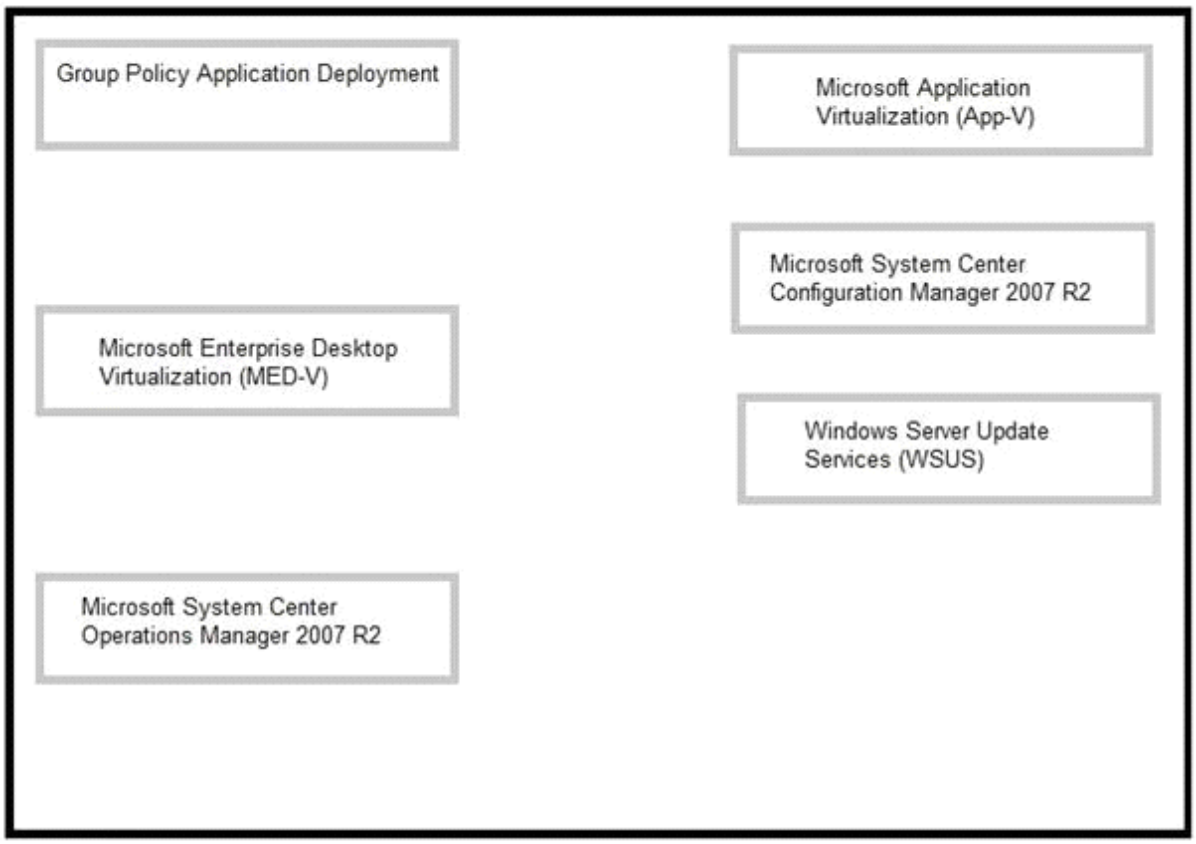
DRAG DROP
A company has client computers that run Windows 7. Each client computer is deployed with Microsoft Office 2010 pre-installed. The company is adding three line-of-business-Applications that require access to Office functionality. None of the line-of-business Applications can co-exist with the others on the same client computer. You are designing a solution that must meet the following requirements:

- Allow the use of all the line-of-business Applications on each client computer.
- Maintain a central inventory of all Applications.
- Centralize the process of deploying, streaming, updating and reporting on all Applications.

You need to recommend a solution that meets the requirements. Which technologies should you recommend to achieve the indicated goals?
To answer, drag the appropriate technologies in the correct location or locations in the answer area.



Answer:



Explanation:
CAREFUL - This answer May not be fully correct!

However
Given that App-V lets you resolve conflicts that arise between different applications or different versions of the same application. . Use App-V when the application you want to use runs on your host OS, but doesn't interact well with other applications on your host OS. Consider Office. Office 2010, 2007, 2003 and Office XP all run great on Windows 7, but you can't install all four versions of Office on the same OS at the same time. This is where App-V can really help. With App-V, I can use Office 2010, 2007, 2003 and Office XP on the same installation of Windows 7 at the same time! The line of Business Applications need access to Office which is installed locally so App-V would appear to be correct.
:
http://technet.microsoft.com/en-us/library/bb680651.aspx

Welcome to Microsoft System Center Configuration Manager 2007. Configuration Manager 2007 contributes to a more effective Information Technology (IT) department by enabling secure and scalable operating system and application deployment and desired configuration management, enhancing system security, and providing comprehensive asset management of servers, desktops, and mobile devices.
Post-Setup Configuration Tasks
After Setup has run, there are still a few tasks you must perform to have a functioning Configuration Manager 2007 site. For example, you might need to assign new site system roles and install clients. For more information, see Checklist for Required Post Setup Configuration Tasks.
Common Configuration Manager Tasks
For more information about how to do common Configuration Manager 2007 tasks, see the following topics.

- Planning and Deploying the Server Infrastructure for Configuration Manager 2007
- Planning and Deploying Clients for Configuration Manager 2007
- Collect hardware and software asset information
- Distribute software
- Deploy software updates
- Deploy operating systems
- Manage desired configurations
- Remotely administer a computer
- Restrict non-compliant computers from accessing the network
- Manage mobile devices like Smartphones and Pocket PCs

Case Study: 1
Humongous Insurance
Scenario:
COMPANY OVERVIEW
Humongous Insurance has a main office and 20 branch offices. The main office is located in New York. The branch offices are located throughout North America. The main office has 8,000 users. Each branch office has 2 to 250 users.
PLANNED CHANGES
Humongous Insurance plans to implement Windows BitLocker Drive Encryption (BitLocker) on all servers.
EXISTING ENVIRONMENT
The network contains servers that run either Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. All client computers run either Windows 7 Enterprise or Windows Vista Enterprise.
Business Goals
Humongous Insurance wants to minimize costs whenever possible.
Existing Active Directory/Directory Services
The network contains a single Active Directory forest named humongousinsurance.com. The forest contains

two child domains named north.humongousinsurance.com and south.humongousinsurance.com. The functional level of the forest is Windows Server 2008 R2.

Existing Network Infrastructure

Each child domain contains a Web server that has Internet Information Services (IIS) installed. The forest root domain contains three Web servers that have IIS installed. The Web servers in the forest root domain are configured in a Network Load Balancing (NLB) cluster. Currently, all of the Web servers use a single domain user account as a service account. Windows Server Update Services (WSUS) is used for company-wide patch management. The WSUS servers do not store updates locally. The network contains Remote Desktop servers that run Windows Server 2008 R2. Users in the sales department access a line-of-business Application by using Remote Desktop. Managers in the sales department use the Application to generate reports. Generating the reports is CPU intensive. The sales managers report that when many users are connected to the servers, the reports take a long time to process.

Humongous Insurance has the following standard server builds:

- Class 1 - Dual x64 CPUs, 4-GB RAM, Windows Web Server 2008 R2
- Class 2 - Dual x64 CPUs, 4-GB RAM, Windows Server 2008 R2 Standard
- Class 3 - Quad x64 CPUs, 8-GB RAM, Windows Server 2008 R2 Standard
- Class 4 - Quad x64 CPUs, 8-GB RAM, Windows Server 2008 R2 Enterprise

Current Administration Model

Humongous Insurance currently uses the following technologies to manage the network:

- Microsoft Desktop Optimization Pack
- Microsoft Forefront EndPoint Protection
- Microsoft System Center Operations Manager
- Microsoft System Center Configuration Manager

TECHNICAL REQUIREMENTS

Humongous Insurance must meet the following technical requirements:

- A certificate must be required to recover BitLocker-protected drives.
- Newly implemented technologies must minimize the impact on LAN traffic.
- Newly implemented technologies must minimize the storage requirements.
- The management of disk volumes and shared folders must be performed remotely whenever possible.
- Newly implemented technologies must minimize the amount of bandwidth used on Internet connections.
- All patches and updates must be tested in a non-production environment before they are App1ied to production servers.
- Multiple versions of a Group Policy object (GPO) must be maintained in a central archive to facilitate a rol required.

The management of passwords and service principal names (SPNs) for all service accounts must be automated whenever possible.

Question: 1

You need to recommend a BitLocker recovery method that meets the company's technical requirements. Which recovery method should you recommend?

A. a data recovery agent
B. a recovery key
C. a recovery password printed and stored in a secure location

D. a recovery password stored in Active Directory

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/dd875560%28WS.10%29.aspx
Data recovery agents are accounts that are able to decrypt BitLocker-protected drives by using their smart card certificates and public keys. Recovery of a BitLocker-protected drive can be accomplished by a data recovery agent that has been configured with the proper certificate. Before a data recovery agent can be configured for a drive, you must add the data recovery agent to Public Key Policies\BitLocker Drive Encryption in either the Group Policy Management Console (GPMC) or the Local Group Policy Editor. You must also enable and configure the Provide the unique identifiers for your organization policy setting to associate a unique identifier to a new drive that is enabled with BitLocker. An identification field is a string that is used to uniquely identify a business unit or organization. Identification fields are required for management of data recovery agents on BitLocker-protected drives. BitLocker will only manage and update data recovery agents when an identification field is present on a drive and is identical to the value configured on the computer.

Question: 2

You need to recommend a data management solution that meets the company's technical requirements. What should you include in the recommendation?

A. DFS Management
B. File Server Resource Manager (FSRM)
C. Share and Storage Management
D. Storage Explorer

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc753175.aspx
Share and Storage Management provides a centralized location for you to manage two important server resources:
Folders and volumes that are shared on the network
Volumes in disks and storage subsystems
Shared resources management
You can share the content of folders and volumes on your server over the network using the Provision a Shared Folder Wizard, which is available in Share and Storage Management. This wizard guides you through the necessary steps to share a folder or volume and assign all applicable properties to it. With the wizard, you can:
Specify the folder or volume that you want to share or create a new folder to share.
Specify the network sharing protocol used to access the shared resource.
Change the local NTFS permissions for the folder or volume you will be sharing.
Specify the share access permissions, user limits, and offline access to files in the shared resource.
Publish the shared resource to a Distributed File System (DFS) namespace.
If Services for Network File System (NFS) has been installed, specify NFS-based access permissions for the shared resource.
If File Server Resource Manager is installed on your server, apply storage quotas to the new shared resource, and create file screens to limit the type of files that can be stored in it.
Using Share and Storage Management, you can also monitor and modify important aspects of your new and existing shared resources. You can:
Stop the sharing of a folder or volume.

Change the local NTFS permissions for a folder or volume.
Change the share access permissions, offline availability, and other properties of a shared resource.
See which users are currently accessing a folder or a file and disconnect a user if necessary.
If Services for Network File System (NFS) has been installed, change the NFS-based access permissions for a shared resource.
For more information about using Share and Storage Management to manage shared resources, see Provisioning Shared Resources.
Storage management With Share and Storage Management, you can provision storage on disks that are available on your server, or on storage subsystems that support Virtual Disk Service (VDS). The Provision Storage Wizard guides you through the process of creating a volume on an existing disk, or on a storage subsystem attached to your server. If the volume is going to be created on a storage subsystem, the wizard will also guide you through the process of creating a logical unit number (LUN) to host that volume. You also have the option of only creating the LUN, and using Disk Management to create the volume later.
Share and Storage Management also helps you monitor and manage the volumes that you have created, as well as any other volumes that are available on your server. Using Share and Storage Management you can:
Extend the size of a volume.
Format a volume.
Delete a volume.
Change volume properties like compression, security, offline availability and indexing.
Access disk tools for error checking, defragmentation, and backup.

Question: 3

You need to recommend a server build for the Web servers. Which server build should you recommend?

A. Class 1
B. Class 2
C. Class 3
D. Class 4

Answer: A

Explanation:

Windows Web Server 2008

Windows Web Server 2008 is designed to function specifically as a Web applications server. Other roles, such as Windows Deployment Server and Active Directory Domain Services, are not supported on Windows Web Server 2008. You deploy this server role either on a screened subnet to support a Web site viewable to external hosts or as an intranet server. As appropriate given its stripped-down role, Windows Web Server 2008 does not support the high-powered hardware configurations that other editions of Windows Server 2008 do. Windows Web Server 2008 has the following properties:

- The 32-bit version (x86) supports a maximum of 4 GB of RAM and 4 processors in SMP configuration.
- The 64-bit version (x64) supports a maximum of 32 GB of RAM and 4 processors in SMP configuration.
- Supports Network Load Balancing clusters.

You should plan to deploy Windows Web Server 2008 in the Server Core configuration, which minimizes its attack surface, something that is very important on a server that interacts with hosts external to your network environment. You should only plan to deploy the full version of Windows Web Server 2008 if your organization's Web applications rely on features such as ASP.NET, because the .NET Framework is not included in a Server Core installation.

Question: 4

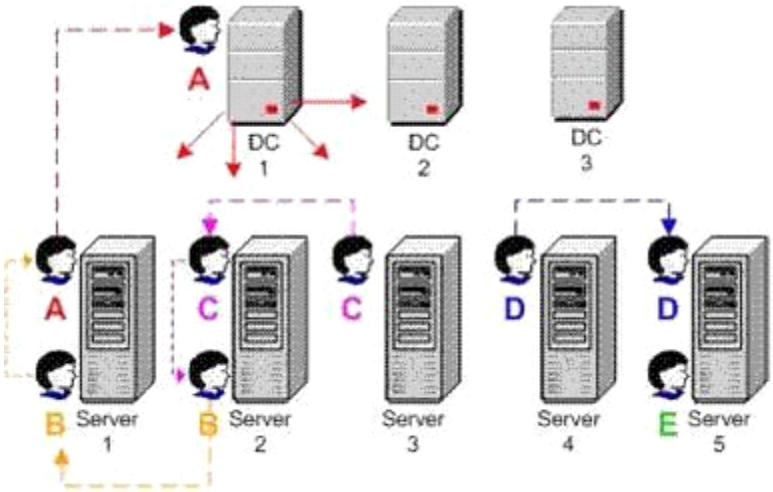
You need to recommend a strategy for using managed service accounts on the Web servers. How many managed service accounts should you recommend?

A. 1
B. 2
C. 3
D. 5

Answer: D

Explanation:
There are 5 web servers in total, 3 in the forest root domain and 1 in each child domain. Q 9 in this exam actually confirms the answer is 5 Service Account Vulnerability The practice of configuring services to use domain accounts for authentication leads to potential security exposure. The degree of risk exposure is dependent on various factors, including:
The number of servers that have services that are configured to use service accounts. The vulnerability profile of a network increases for every server that has domain account authenticated services that run on that server. The existence of each such server increases the odds that an attacker might compromise that server, which can be used to escalate privileges to other resources on a network.
The scope of privileges for any given domain account that services use. The larger the scope of privileges that a service account has, the greater the number of resources that can be compromised by that account.
Domain administrator level privileges are a particularly high risk, because the scope of vulnerability for such accounts includes any computer on the network, including the domain controllers. Because such accounts have administrative

privileges to all member servers, the compromise of such an account would be severe and all computers and data in the domain would be suspect.
The number of services configured to use domain accounts on any given server. Some services have unique vulnerabilities, which make them somewhat more susceptible to attacks. Attackers will usually attempt to exploit known vulnerabilities first. Use of a domain account by a vulnerable service presents an escalated risk to other systems, which could have otherwise been isolated to a single server.
The number of domain accounts that are used to run services in a domain. Monitoring and managing the security of service accounts requires more diligence than ordinary user accounts, and each additional domain account in use by services only complicates administration of those accounts. Given that administrators and security administrators need to know where each service account is used to detect suspicious activity highlights
The need to minimize the number of those accounts.
The preceding factors lead to several possible vulnerability scenarios that can exist, each with a different level of potential security risk. The following diagram and table describe these scenarios.
For these examples it is assumed that the service accounts are domain accounts and each account has at least one service on each server using it for authentication. The following information describes the domain accounts shown in the following figure.
Account A has Administrator-equivalent privileges to more than one domain controller.
Account B has administrator-equivalent privileges on all member servers.
Account C has Administrator-equivalent privileges on servers 2 and 3.
Account D has Administrator-equivalent privileges on servers 4 and 5.
Account E has Administrator-equivalent privileges on a single member server only.



Question: 5

You need to recommend a solution for managing GPOs. The solution must meet the company's technical requirements. What should you include in the recommendation?

A. Desktop Optimization Pack
B. Forefront EndPoint Protection
C. System Center Configuration Manager
D. System Center Operations Manager

Answer: A

Explanation:
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.

Microsoft Desktop Optimization Pack	
Application Virtualization	App-V turns applications into centrally managed services that are never installed, never conflict, and are streamed on demand to end users.
Enterprise Desktop Virtualization	MED-V provides deployment and management of virtual PC images to enable key enterprise scenarios, primarily application compatibility with Windows Vista and Windows 7.
Advanced Group Policy Management	AGPM provides governance and control over Group Policy through robust change management and role-based administration.
Asset Inventory Service	AIS is a hosted service that collects software inventory data and translates it into business intelligence.
Diagnostics and Recovery Toolset	DaRT reduces downtime by accelerating desktop repair, recovery, and troubleshooting of unbootable Windows-based desktops.
System Center Desktop Error Monitoring	DEM enables proactive problem management by analyzing and reporting on application and system crashes.

Microsoft Advanced Group Policy Management (AGPM) is the MDOP application that can help customers overcome the challenges that can affect Group Policy management in any organization, particularly those with complex information technology (IT) environments. A robust delegation model, role-based administration, and change-request approval provide granular administrative control. For example, you can delegate Reviewer, Editor, and Approver roles to other users—even users who do not typically have access to production GPOs. (Editors can edit GPOs but cannot deploy them; Approvers can deploy GPO changes.)

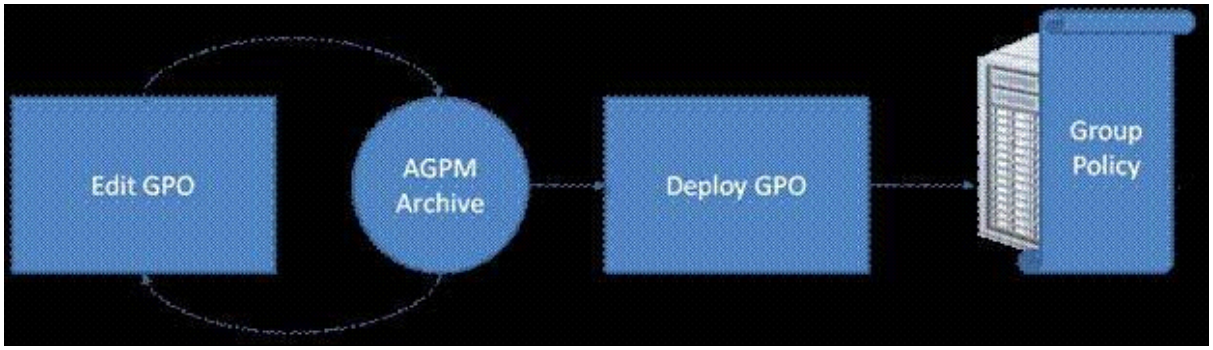
AGPM can also help reduce the risk of widespread failures. You can use AGPM to edit GPOs offline, outside of the production environment, and then audit changes and easily find differences between GPO versions. In addition, AGPM supports effective change control by providing version tracking, history capture, and quick rollback of deployed GPO changes. It even supports a management workflow by allowing you to create GPO template libraries and send GPO change e-mail notifications.

This white paper describes the key features of AGPM, such as change control and role-based delegation. The paper then describes how Software Assurance customers can begin evaluating AGPM today.

Offline Editing

The AGPM archive provides offline storage for GPOs. As Figure 2 shows, changes that you make to GPOs in the archive do not affect the production environment until you deploy the GPOs. By limiting changes to the archive, you can edit GPOs and test them in a safe environment, without affecting the production environment.

After reviewing and approving the changes, you can then deploy them with the knowledge that you can quickly roll them back if they have an undesired effect.

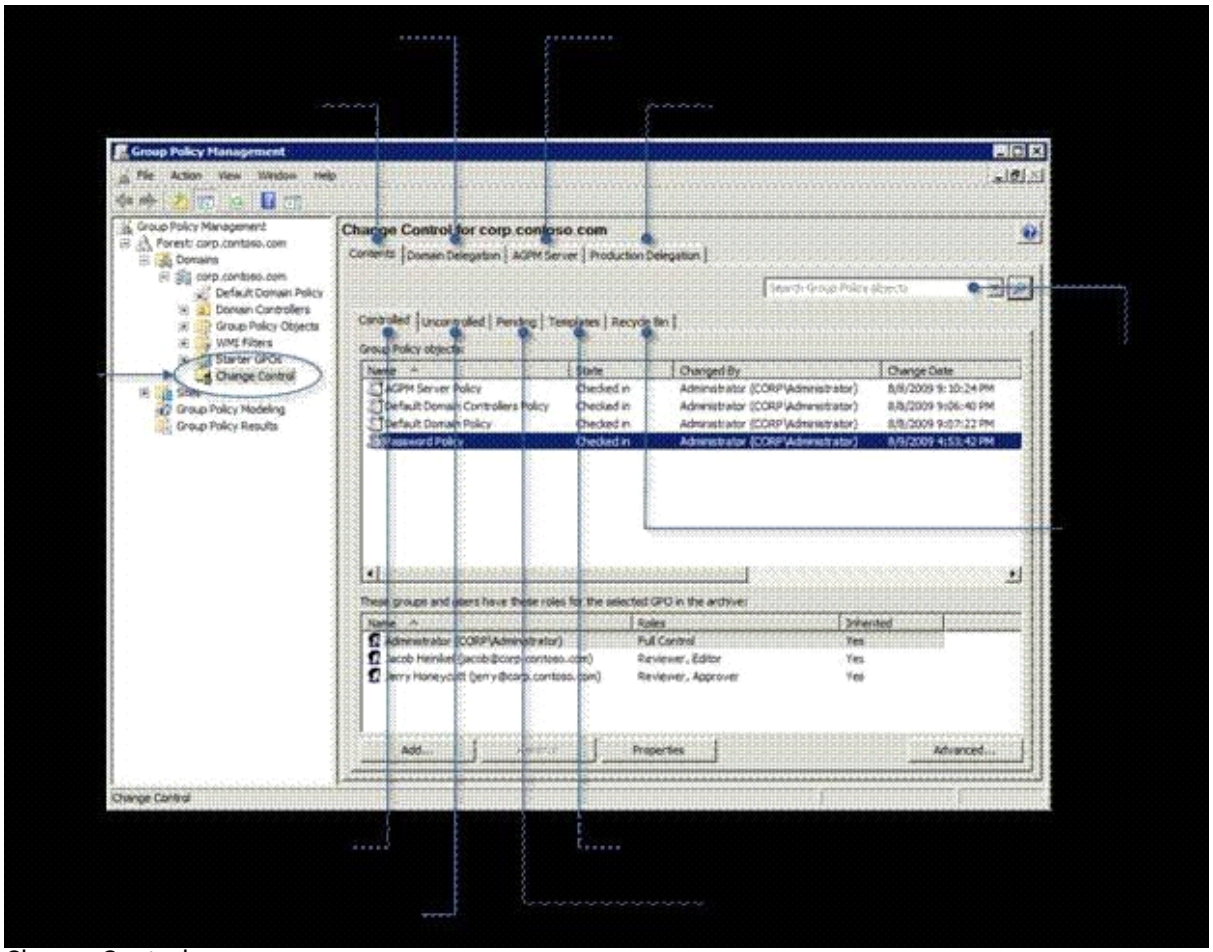


GPMC Integration

AGPM has a server component (the AGPM Service) and a client component (the AGPM snap-in), each of which you install separately. First, you install Microsoft Advanced Group Policy Management - Server on a system that has access to the policies that you want to manage. Then, you install the Microsoft Advanced Group Policy Management - Client on any system from which Group Policy administrators will review, edit, and deploy GPOs.

The AGPM snap-in integrates completely with the Group Policy Management Console (GPMC), as Figure 3 shows. Click Change Control in the console tree to open AGPM in the details pane and to manage the AGPM archive on the Contents tab. Here, you can review, edit, and deploy controlled GPOs (that is, GPOs in the archive). You can also take control of uncontrolled GPOs (that is, GPOs that are not in the archive), approve pending changes, and manage GPO templates. On the Domain Delegation tab, AGPM Administrators (Full

Control) delegate roles to AGPM users and configure e-mail notifications. Configure the AGPM Server connection on the AGPM Server tab. AGPM 3.0 introduced the Production Delegation tab, which AGPM Administrators can use to delegate permission to edit GPOs in the production environment.



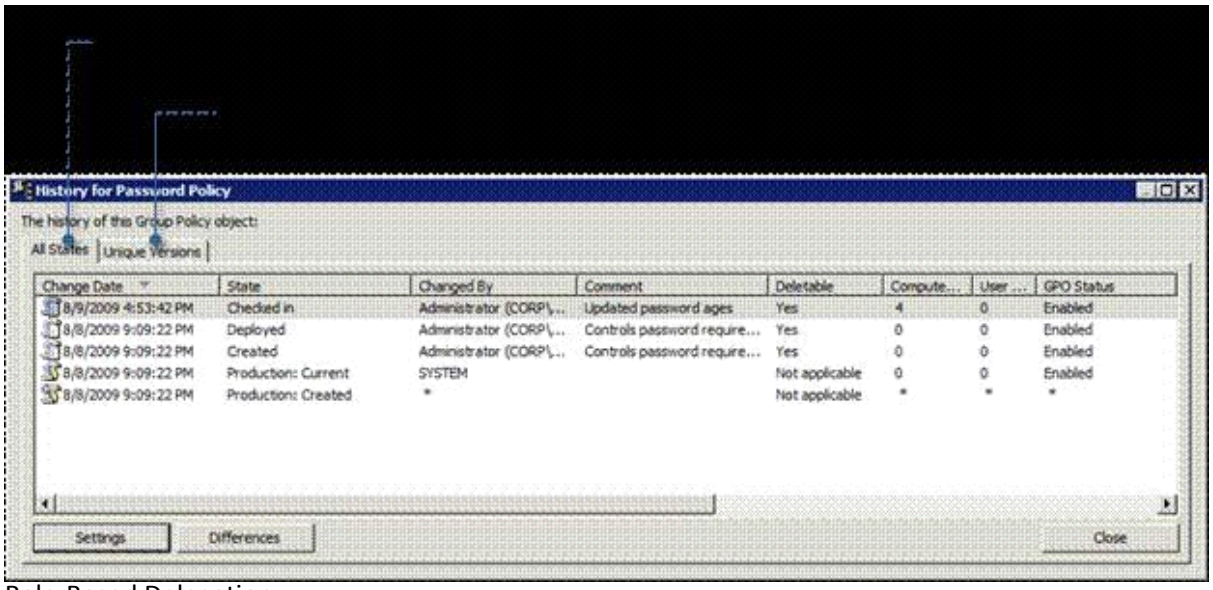
Change Control

AGPM provides advanced change control features that can help you manage the lifecycle of GPOs. Many of the AGPM change control concepts will be familiar to administrators who have experience using common version-control tools, such as the version control feature in Microsoft Office SharePoint® Server 2007. The following steps are necessary to change and deploy a GPO:

1. Check out the GPO from the archive.
2. Edit the GPO as necessary.
3. Check in the GPO to the archive.
4. Deploy the GPO to production.

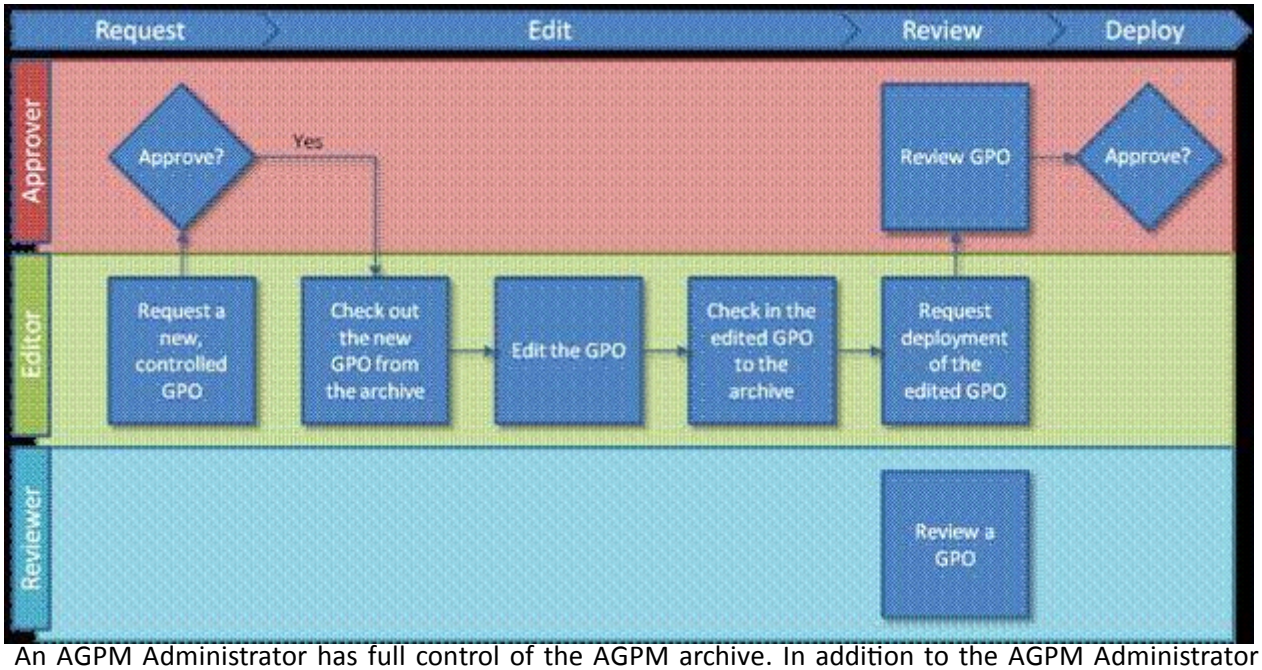
Change control means more than locking a GPO to prevent multiple users from changing it at the same time. AGPM keeps a history of changes for each GPO, as shown in Figure 4. You can deploy any version of a GPO to production, so you can quickly roll back a GPO to an earlier version if necessary. AGPM can also compare different versions of a GPO,

showing added, changed, or deleted settings. Therefore, you can easily review changes before approving and deploying them to the production environment. In addition, a complete history of each GPO enables you to audit not only changes but also all activities related to that GPO.



Role-Based Delegation

Group Policy already provides a rich delegation model that allows you to delegate administration to regional and task-oriented administrators. However, Group Policy also lets administrators approve their own changes. In contrast, AGPM provides a role-based delegation model that adds a review and approval step to the workflow, as shown in Figure 5.



An AGPM Administrator has full control of the AGPM archive. In addition to the AGPM Administrator role, AGPM defines three special roles to support its delegation model:

· Reviewer. Reviewers can view and compare GPOs. They cannot edit or deploy GPOs.

· Editor. Editors can view and compare GPOs. They can also check out GPOs from the archive, edit GPOs, and check in GPOs to the archive. Editors can request deployment of a GPO.

· Approver. Approvers can approve the creation and deployment of GPOs. (When Approvers create or deploy a GPO, approval is automatic.)

As an AGPM Administrator, you can delegate these roles to users and groups for all controlled GPOs within the domain (domain delegation). For example, you can delegate the Reviewer role to users, allowing them to review any controlled GPO in the domain. You can also delegate these roles to users for individual controlled GPOs. Rather than

allow users to edit any controlled GPO in the domain, for example, you can give them permission to edit a specific controlled GPO by delegating the Editor role for that GPO only.

Search and Filter

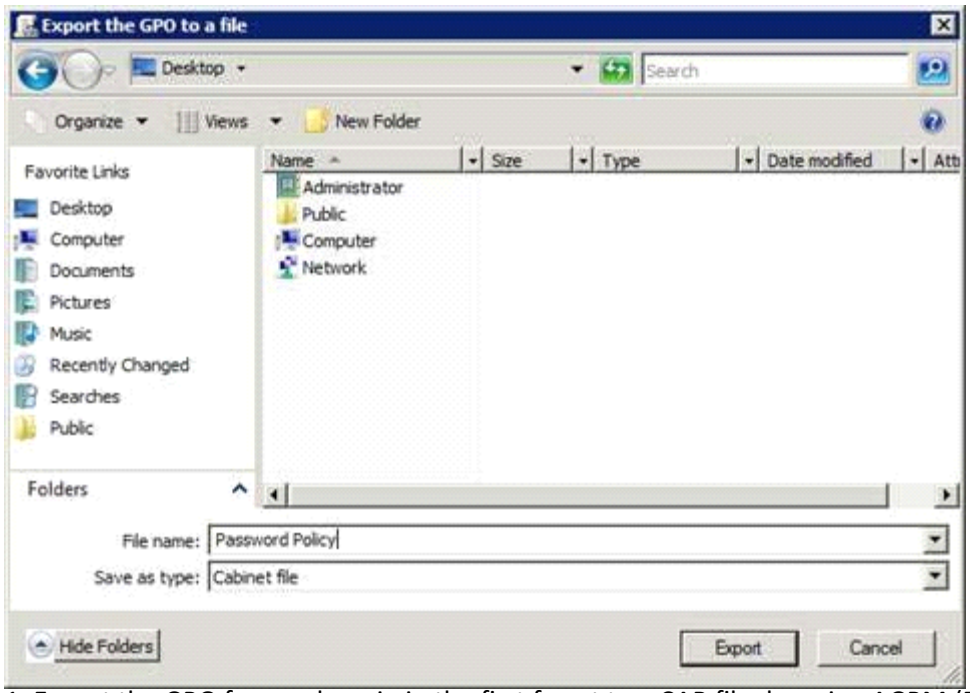
AGPM 4.0 introduces the ability to filter the list of GPOs that it displays. For example, you can filter the list by name, status, or comment. You can even filter the list to show GPOs that were changed by a particular user or on a specific date. AGPM displays partial matches, and searches are not case sensitive.

AGPM supports complex search strings using the format column: string, where column is the name of the column by which to search and string is the string to match. For example, to display GPOs that were checked in by Jerry, type state: "checked in" changed by: Jerry in the Search box. Figure 6 shows another example. You can also filter the list by GPO attributes by using the format attribute: string, where attribute is the name of the GPO attribute to match. To display all GPOs that use the Windows® Management Instrumentation (WMI) filter called MyWMIFilter, type wmi filter: mywmifilter in the Search box.

When searching for GPOs, you can use special terms to search by date, dynamically. These special terms are the same terms that you can use when using Windows Explorer to search for files. For example, you can filter the list to display GPOs that were changed today, yesterday, this week, last week, and so on.

Cross-Forest Management

In addition to filtering, AGPM 4.0 also introduces cross-forest management. You can use the following process to copy a controlled GPO from a domain in one forest to a domain in a second forest:



1. Export the GPO from a domain in the first forest to a CAB file, by using AGPM (Figure 7).
2. On a computer in a domain in the first forest, copy the CAB file to a portable storage device.
3. Insert the portable storage device into a computer in a domain in the second forest.
4. Import the GPO into the archive in a domain in the second forest, by using AGPM.

When you import the GPO into the second forest, you can import it as a new controlled GPO. You can also import it to replace the settings of an existing GPO that is checked out of the archive.

The obvious benefit of cross-forest management is testing. Combined with offline editing and change control, cross-forest management enables you to test GPOs in a controlled test environment (the first forest). After verifying the GPO, you can move it into the production environment (the second forest).

Windows Support

Three versions of AGPM are available: AGPM 2.5, AGPM 3.0, and AGPM 4.0. Each is incompatible with the others and supports different Windows operating systems. For more information about choosing the right version of AGPM for your environment and about the Windows operating systems that each supports, see Choosing Which Version of AGPM to Install.

AGPM 4.0 introduces support for Windows 7 and Windows Server® 2008 R2. Additionally, AGPM 4.0 still supports Windows Vista® with Service Pack 1 (SP1) and Windows Server 2008. Table 1 describes limitations in mixed environments that include newer and older Windows operating systems.

Question: 6

You are evaluating whether to use express installation files as an update distribution mechanism. Which technical requirement is met by using the express installation files?

A. Newly implemented technologies must minimize the impact on LAN traffic.
B. Newly implemented technologies must minimize the storage requirements.
C. Newly implemented technologies must minimize the amount of bandwidth used on Internet connections.
D. All patches and updates must be tested in a nonproduction environment before they are App1ied to production servers.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc708456%28v=ws.10%29.aspx
The express installation files feature is an update distribution mechanism. You can use express installation files to limit the bandwidth consumed on your local network, but at the cost of bandwidth consumption on your Internet connection. By default, WSUS does not use express installation files. To better understand the tradeoff, you first have to understand how WSUS updates client computers.
Updates typically consist of new versions of files that already exist on the computer being updated. On a binary level these existing files might not differ very much from updated versions. The express installation files feature is a way of identifying the exact bytes that change between different versions of files, creating and distributing updates that include just these differences, and then merging the original file with the update on the client computer. Sometimes this is called delta delivery because it downloads only the difference, or delta, between two versions of a file.
When you distribute updates by using this method, it requires an initial investment in bandwidth. Express installation files are larger than the updates they are meant to distribute. This is because the express installation file must contain all the possible variations of each file it is meant to update.
The upper part of the "Express Installation Files Feature" illustration depicts an update being distributed by using the express installation files feature; the lower part of the illustration depicts the same update being distributed without using the express installation files feature. Notice that with express installation files enabled, you incur an initial download three times the size of the update. However, this cost is mitigated by the reduced amount of bandwidth required to update client computers on the corporate network. With express installation files disabled, your initial download of updates is smaller, but whatever you download must then be distributed to each of the clients on your corporate network.
Important
Although there are some variables with express installation files, there are also some things you can count on.
For example, express installation files are always bigger in size than the updates they are meant to distribute.
As far as bandwidth goes, it is always less expensive to distribute updates using express installation files than to distribute updates without.
Not all updates are good candidates for distribution using express installation files. If you select this option, you obtain express installation files for any updates being distributed this way. If you are not storing updates locally, you cannot use the express installation files feature. By default, WSUS does not use express installation files.
To enable this option see http://technet.microsoft.com/en-us/library/cc708460%28v=ws.10%29.aspx
Update Storage Options
Use the Update Files section to determine if updates will be stored on WSUS or if client computers will connect to the Internet to get updates. There is a description of this feature in Determine Where to Store Updates earlier in this guide.

To specify where updates are stored
On the WSUS console toolbar, click Options, and then click Synchronization Options.
Under Update Files and Languages, click Advanced, then read the warning and click OK.
If you want to store updates in WSUS, in the Advanced Synchronization Options dialog box, under Update Files, click Store update files locally on this server. If you want clients to connect to the Internet to get updates, then click Do not store updates locally; clients install updates from Microsoft Update.
Deferred Downloads Options
Use the Update Files section to determine if updates should be downloaded during synchronization or when the update is approved. Find a description of this feature in "Deferring the Download of Updates," in Determine Bandwidth Options to Use for Your Deployment earlier in this guide.
To specify whether updates are downloaded during synchronization or when the update is approved On the WSUS console toolbar, click Options, and then click Synchronization Options.
Under Update Files and Languages, click Advanced, then read the warning and click OK.
If you want to download only metadata about the updates during synchronization, in the Advanced Synchronization Options dialog box, under Update Files, select the Download updates to this server only when updates are approved check box. If you want the update files and metadata during synchronization, clear the check box.
Express Installation Files Options
Use the Update Files section to determine if express installation files should be downloaded during synchronization. Find a description of this feature in “Using Express installation files,” in Determine Bandwidth Options to Use for Your Deployment earlier in this paper.
To specify whether express installation files are downloaded during synchronization
On the WSUS console toolbar, click Options, and then click Synchronization Options.
Under Update Files and Languages, click Advanced, then read the warning and click OK.
If you want to download express installation files, in the Advanced Synchronization Options dialog box, under Update Files, select the Download express installation files check box. If you do not want express installation files, clear the check box.
Filtering Updates Options
Use the Languages section to select the language of the updates to synchronize. There is a description of this feature in “Filtering updates,” in Determine Bandwidth Options to Use for Your Deployment earlier in this guide.
To specify language options
On the WSUS console toolbar, click Options, and then click Synchronization Options.
Under Update Files and Languages, click Advanced, then read the warning and click OK.
In the Advanced Synchronization Options dialog box, under Languages, select one of the following language options, and then click OK.
Download only those updates that match the locale of this server (Locale) where Locale is the name of the server locale. This means that only updates targeted to the locale of the server will be downloaded during synchronization.
Download updates in all languages, including new languages This means that all languages will be downloaded during synchronization. If a new language is added, it will be automatically downloaded.
Download updates only in the selected languages This means that only updates targeted to the languages you select will be downloaded during synchronization. If you choose this option, you must also choose each language you want from the list of those available.

Question: 7

You need to recommend a solution to decrease the amount of time it takes for the sales managers to generate reports. What should you include in the recommendation?

A. Desktop Optimization Pack
B. File Server Resource Manager (FSRM)
C. Remote Desktop Connection Broker (RD Connection Broker)
D. Windows System Resource Manager (WSRM)

Answer: D

Explanation:
Dedulas:
http://technet.microsoft.com/en-us/library/cc754150
You can use Windows System Resource Manager to allocate processor and memory resources to applications, users, Remote Desktop Services sessions, and Internet Information Services (IIS) application pools So based upon the information given in the exhibits: the reports are CPU INTENSIVE & when there are a lot of users connected the report take longer to process. you need to reduce the time it takes for reports to be generated a bottle neck on the CPU would increase the time it takes to generate reports so the required solution would need to allocate additional CPU resources to the sales managers or else limit the CPU resources used by the regular users.
If we look at http://technet.microsoft.com/en-us/library/cc753280
Windows System Resource Manager manages processor resources by adjusting the priority of processes. This guarantees a minimum percentage of available CPU bandwidth to process groups that are defined by process matching criteria. Resource management is not enforced unless the total CPU usage is greater than 70 percent....The simplest method of allocating processor resources is to assign a percent CPU target to each group of processes that are defined by a process matching criterion. This target is the percent of available CPU bandwidth that is guaranteed as a minimum to the process group.
So with that in mind I'd me inclined to say the answer is WSRM. because FSRM in a nutshell has nothing what so ever to do with CPU resources its only about disk management, applying disk quotas, blocking certain file types etc

Question: 8

You need to recommend a solution to decrease the amount of time it takes for the sales managers to generate reports. What should you include in the recommendation?

A. Implement Windows System Resource Manager (WSRM) on the Remote Desktop servers.
B. Implement File Server Resource Manager (FSRM) on the Remote Desktop servers.
C. Implement Windows System Resource Manager (WSRM) on the web servers.
D. Implement File Server Resource Manager (FSRM) on the web servers.

Answer: A

Explanation:
Dedulas:
http://technet.microsoft.com/en-us/library/cc754150
You can use Windows System Resource Manager to allocate processor and memory resources to applications, users, Remote Desktop Services sessions, and Internet Information Services (IIS) application pools So based upon the information given in the exhibits: the reports are CPU INTENSIVE & when there are a lot of users connected the report take longer to process.you need to reduce the time it takes for reports to be generated a bottle neck on the CPU would increase the time it takes to generate reports so the required solution would need to allocate additional CPU resources to the sales managers or else limit the CPU resources used by the regular users.

Question: 9

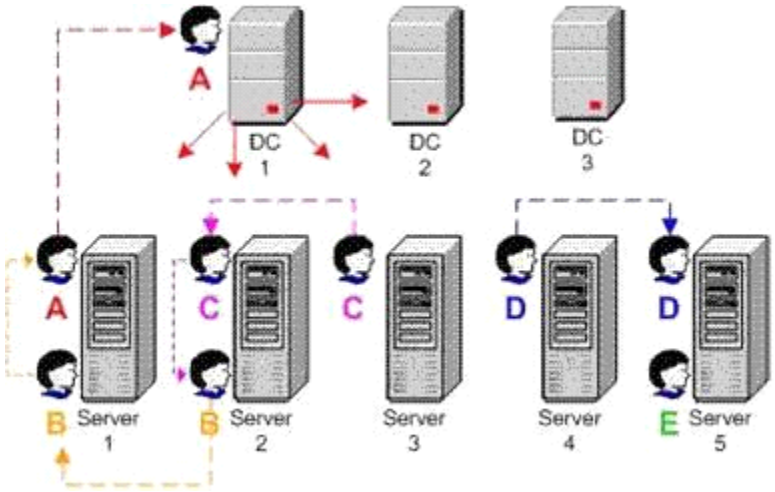
You need to recommend a strategy for using managed service accounts on the Web servers. Which managed service accounts should you recommend?

A. One account for all the web servers.

B. One account for each web server.
C. One account for the parent domain and one account for both child domains.
D. One account for the parent domain and one account for each child domain.

Answer: B

Explanation:
There are 5 web servers in total, 3 in the forest root domain and 1 in each child domain.
Service Account Vulnerability
The practice of configuring services to use domain accounts for authentication leads to potential security exposure. The degree of risk exposure is dependent on various factors, including:
The number of servers that have services that are configured to use service accounts. The vulnerability profile of a network increases for every server that has domain account authenticated services that run on that server. The existence of each such server increases the odds that an attacker might compromise that server, which can be used to escalate privileges to other resources on a network.
The scope of privileges for any given domain account that services use. The larger the scope of privileges that a service account has, the greater the number of resources that can be compromised by that account.
Domain administrator level privileges are a particularly high risk, because the scope of vulnerability for such accounts includes any computer on the network, including the domain controllers. Because such accounts have administrative privileges to all member servers, the compromise of such an account would be severe and all computers and data in the domain would be suspect.
The number of services configured to use domain accounts on any given server. Some services have unique vulnerabilities, which make them somewhat more susceptible to attacks. Attackers will usually attempt to exploit known vulnerabilities first. Use of a domain account by a vulnerable service presents an escalated risk to other systems, which could have otherwise been isolated to a single server.
The number of domain accounts that are used to run services in a domain. Monitoring and managing the security of service accounts requires more diligence than ordinary user accounts, and each additional domain account in use by services only complicates administration of those accounts. Given that administrators and security administrators need to know where each service account is used to detect suspicious activity highlights the need to minimize the number of those accounts.
The preceding factors lead to several possible vulnerability scenarios that can exist, each with a different level of potential security risk. The following diagram and table describe these scenarios.
For these examples it is assumed that the service accounts are domain accounts and each account has at least one service on each server using it for authentication. The following information describes the domain accounts shown in the following figure.
Account A has Administrator-equivalent privileges to more than one domain controller.
Account B has administrator-equivalent privileges on all member servers.
Account C has Administrator-equivalent privileges on servers 2 and 3.
Account D has Administrator-equivalent privileges on servers 4 and 5.
Account E has Administrator-equivalent privileges on a single member server only.



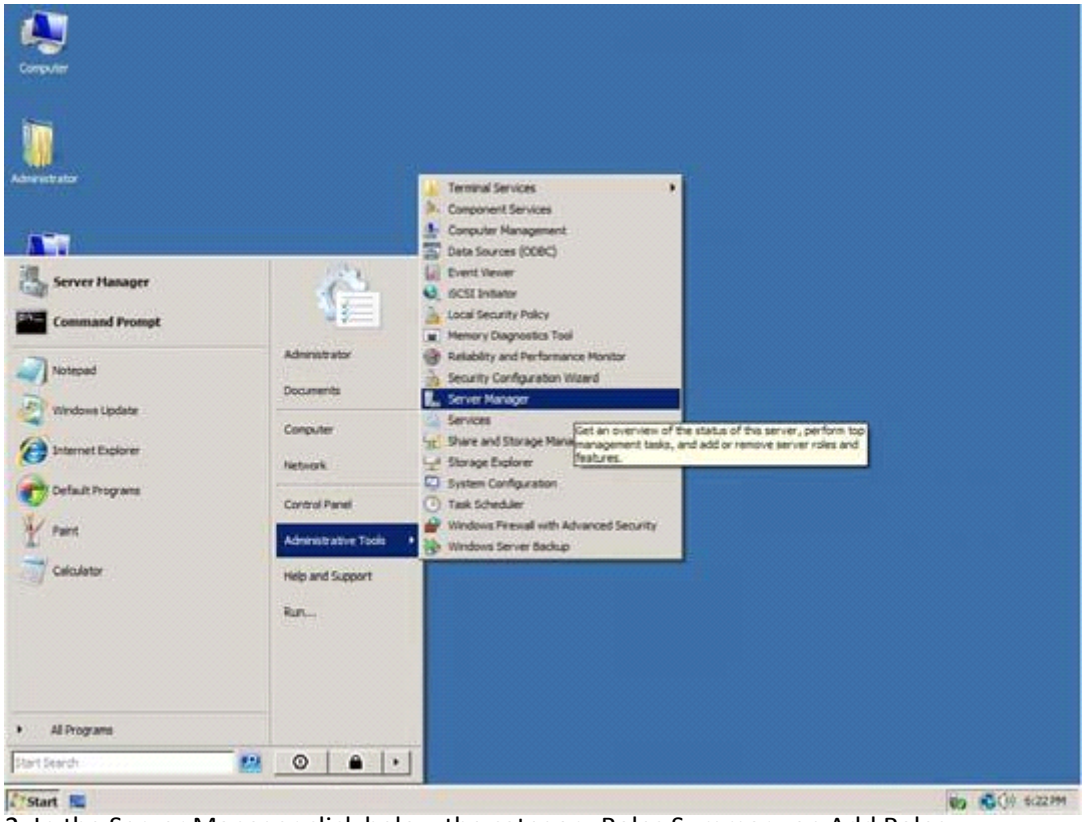
Question: 10

You need to recommend a solution to minimize the amount of time it takes for the legal department users to locate files in the Legal share. What should you include in the recommendation?

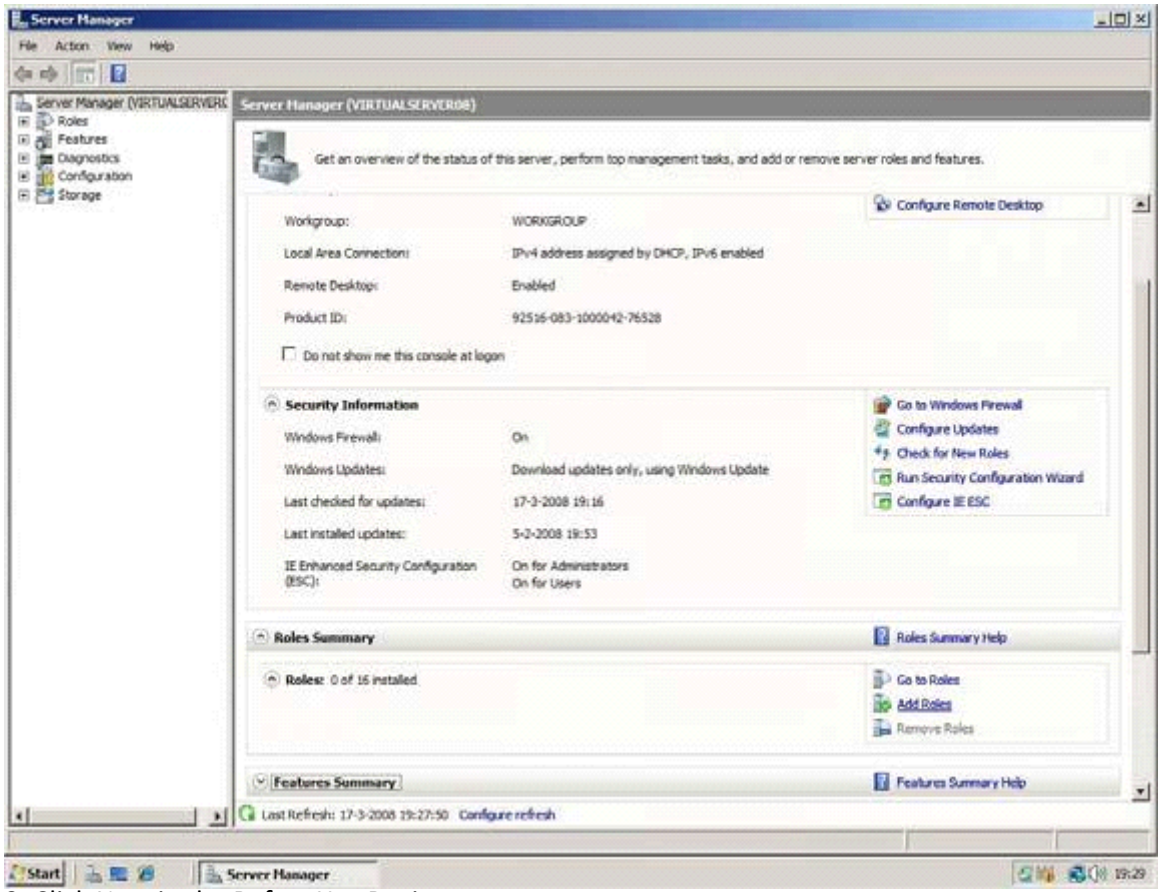
A. File Server Resource Manager (FSRM)
B. Print and Document Services
C. Services for Network File System (NFS)
D. Windows Search Service

Answer: D

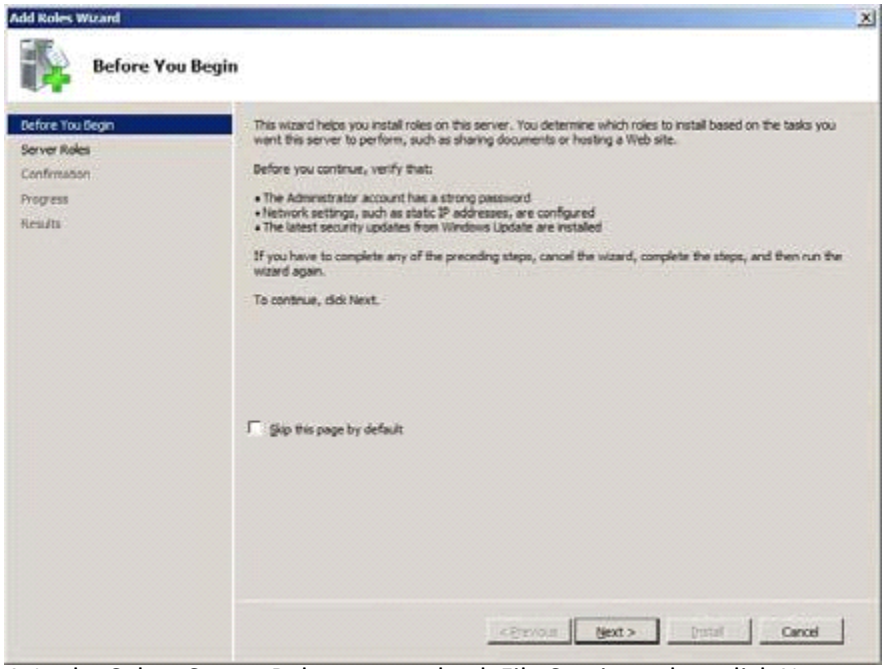
Explanation:
windows search is an optional component in server 2008. You have to enable the file server role to get it. The Windows Search Service is a file server role service that provides indexing of common files on Windows computers. By installing the Windows Search Service, clients can search more quickly for files, using an index that is stored on the file server to enable it follow these steps
http://www.win2008workstation.com/win2008/enable-windows-search-service
1. Start the Server Manager by clicking the Server Manager icon in the systray, or the
Server Manager shortcut in directly the Start menu or in the menu Administrative Tools.



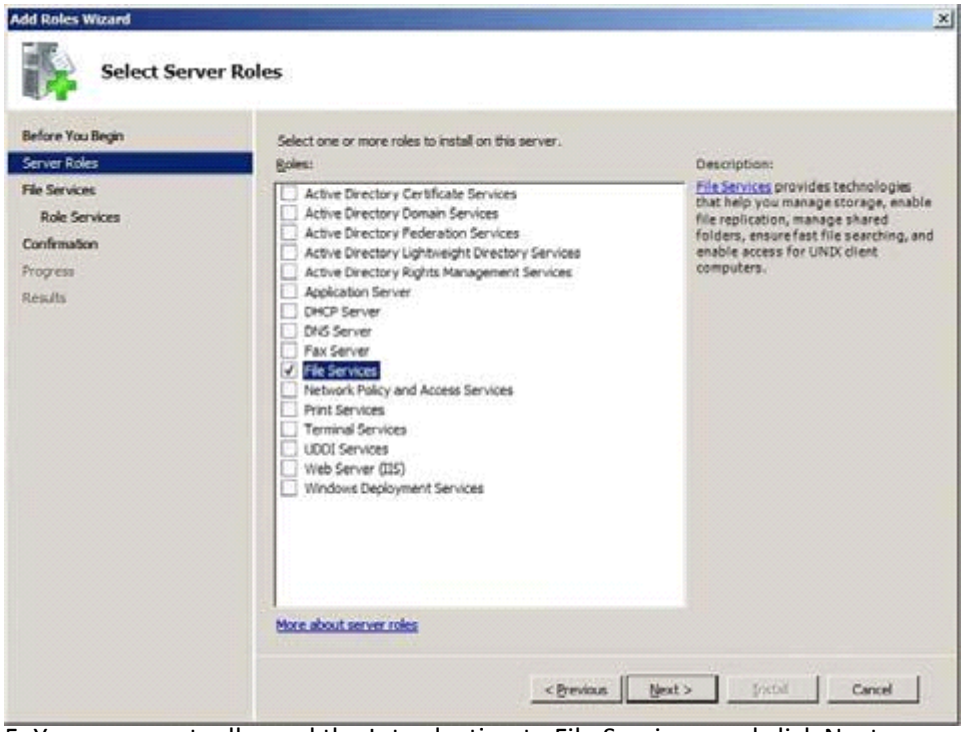
2. In the Server Manager click below the category Roles Summary on Add Roles.



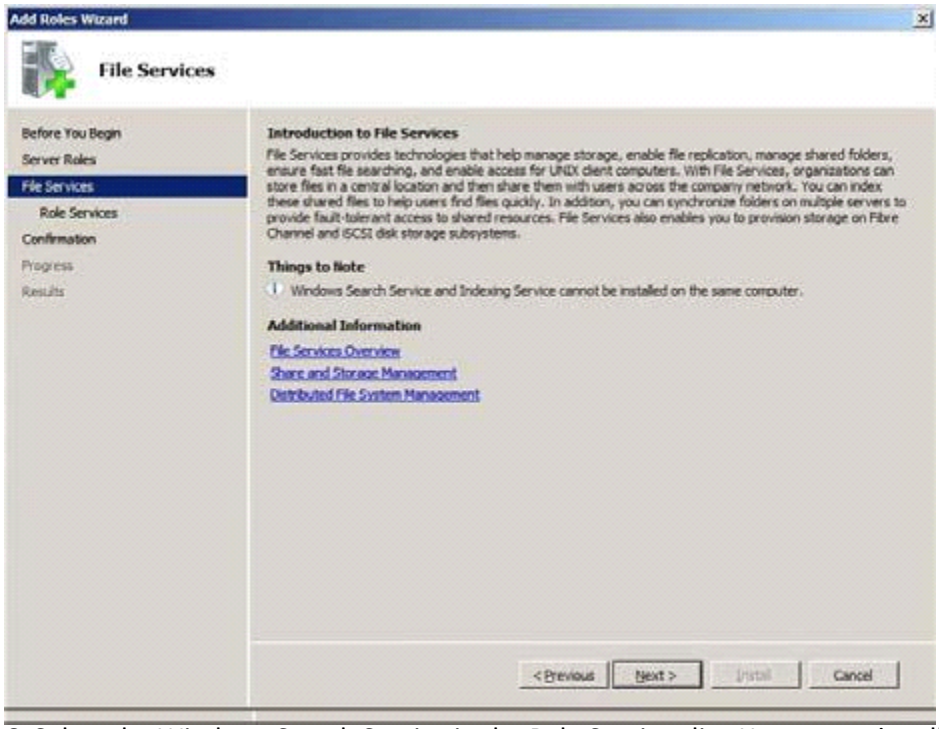
3. Click Next in the Before You Begin screen.



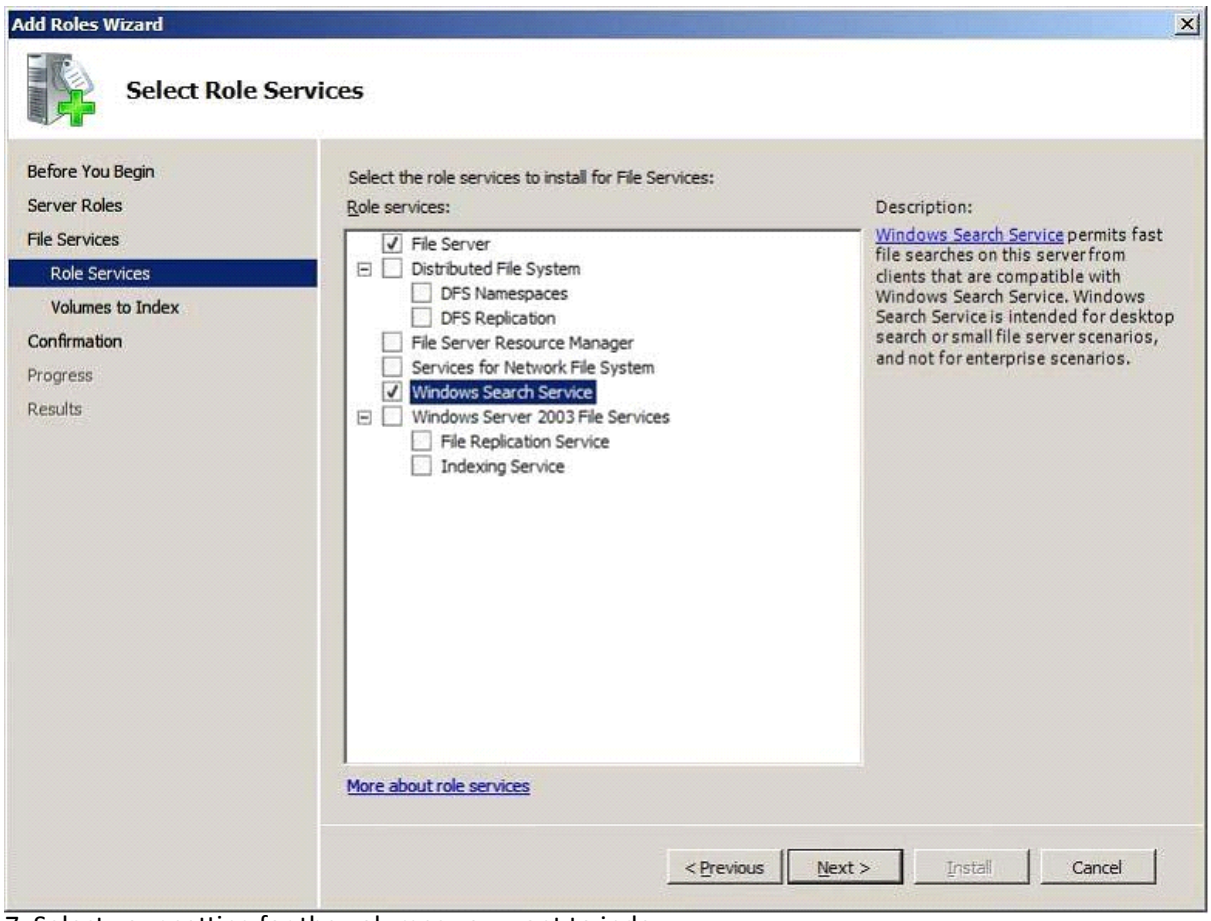
4. In the Select Server Roles screen check File Services, then click Next.



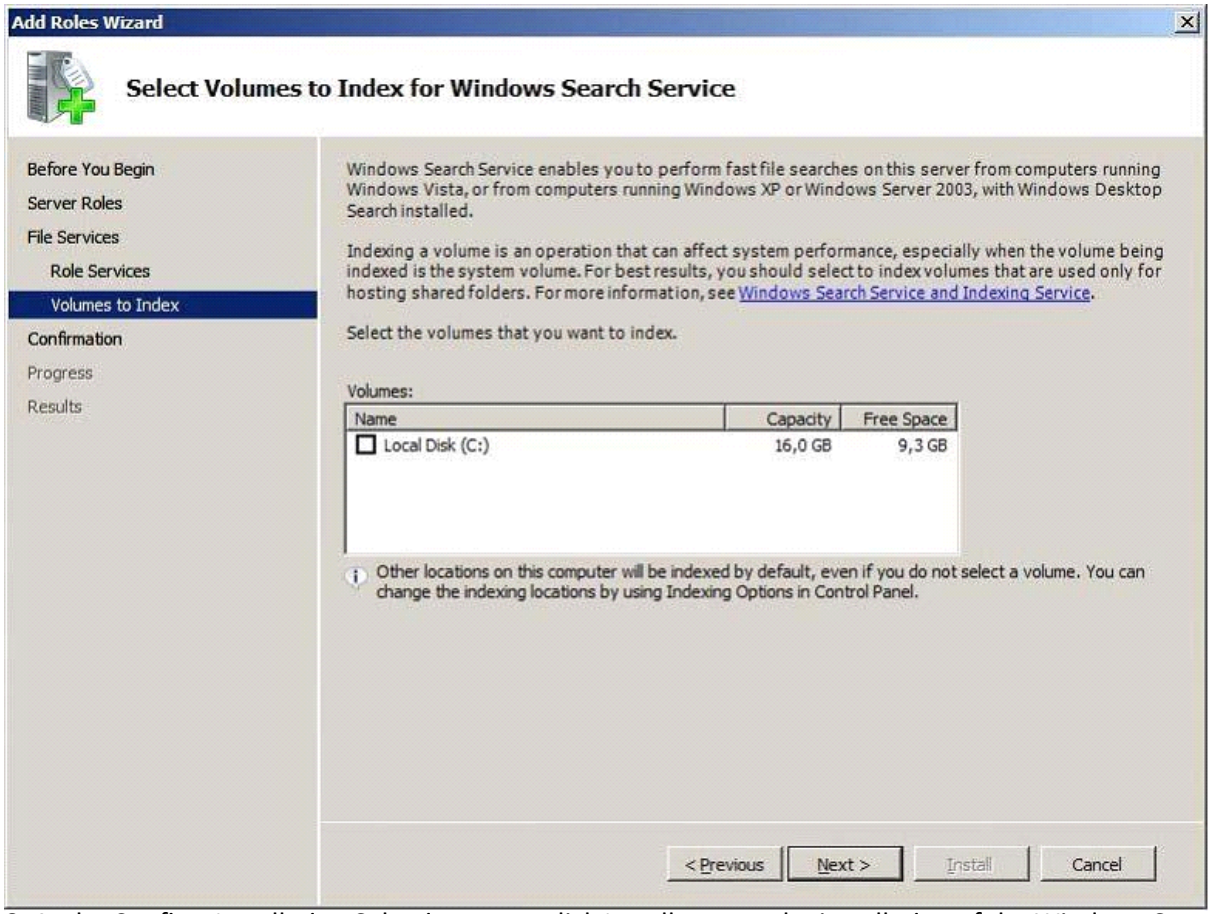
5. You can eventually read the Introduction to File Services, and click Next.



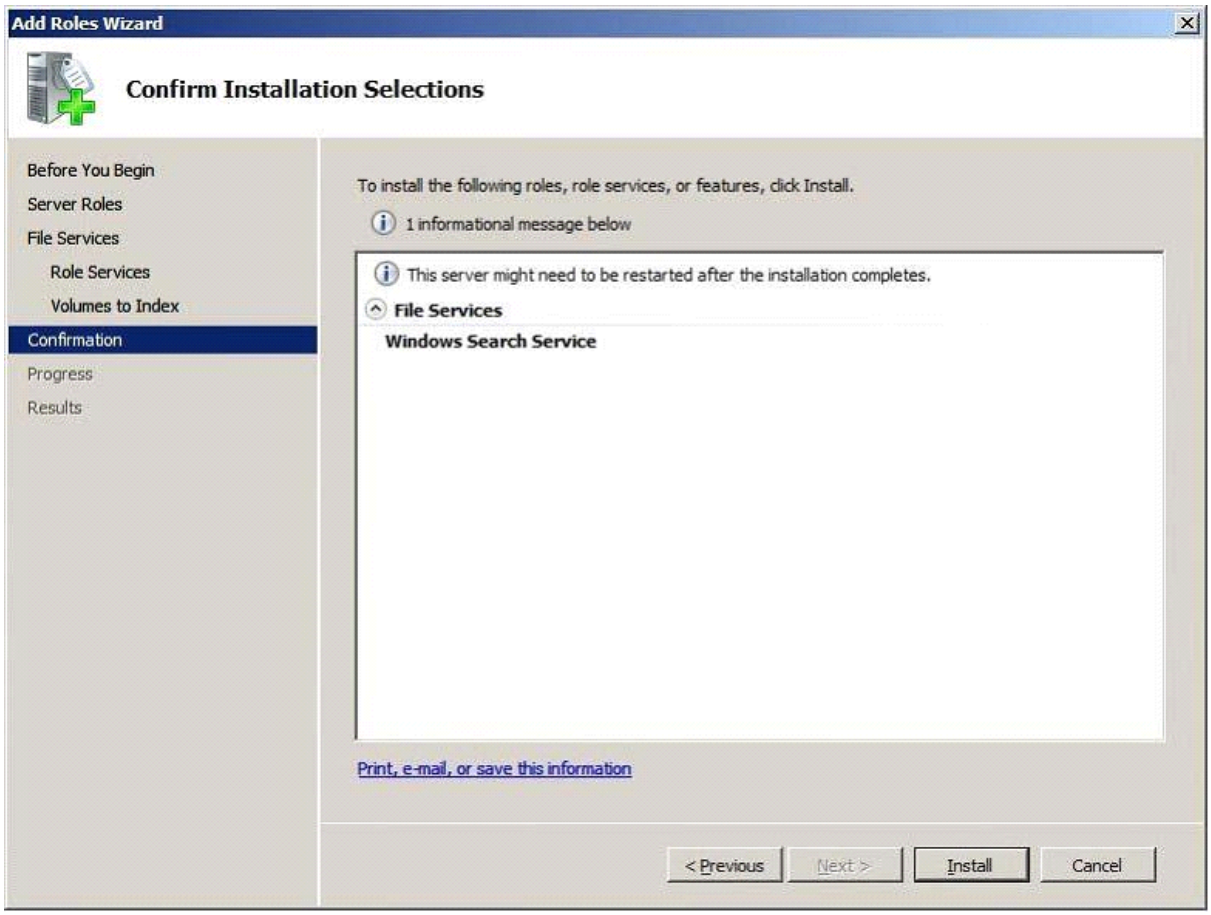
6. Select the Windows Search Service in the Role Services list. You can optionally uncheck the File Server role.



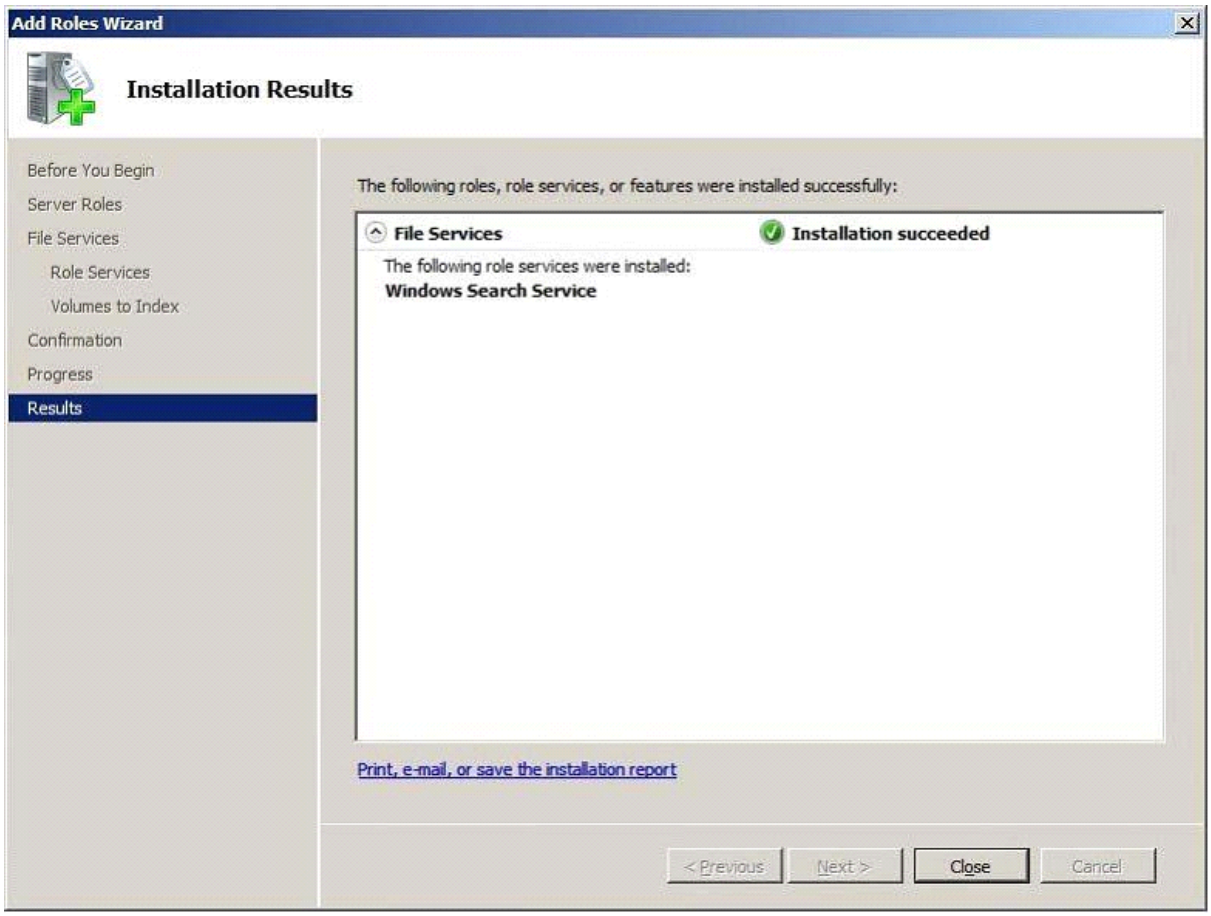
7. Select your setting for the volumes you want to index.



8. At the Confirm Installation Selections page click Install to start the installation of the Windows Search Service role.



9. After the installation has finished click Close. The Windows Search service has now automatically be started and will be indexing your system during idle time!



Case Study: 2
Contoso, Ltd.
Scenario:
COMPANY OVERVIEW
Contoso, Ltd. is a consulting company that has a main office and two branch offices. The main office is located in Johannesburg. The branch offices are located in Brisbane and Montreal. The Johannesburg office has 400 users. Each branch office has 100 users.
PLANNED CHANGES
Contoso plans to open a new branch office. The new office will have a 512-Kbps connection to the Montreal office and a 2-Mbps connection to the Internet. The new branch office will have a domain controller, a DirectAccess server, a file server, and a Web server. All branch office servers will be virtualized. Contoso plans to implement role-based access control for all new virtual machines (VMs) deployed on Hyper-V servers.
In the new branch office, a user named User1 must be permitted to perform only the following actions on the Hyper-V server:
- Start the VMs.
- View the configuration of the VMs.

EXISTING ENVIRONMENT
All servers run Windows Server 2008 R2. All client computers run Windows 7 Enterprise. The main office has multiple file servers. Each branch office has one file server. Each file server has two hard disks. One disk has the server' s operating system installed and the other disk stores data files. File server backups are performed regularly. The main office has a Windows Server Update Services (WSUS) server. All client

computers are configured to receive updates from the WSUS server. The main office connects to each branch office by using a 512-Kbps WAN link.

Existing Active Directory/Directory Services

The network contains a single Active Directory domain named contoso.com. An Active Directory site exists for each office. Each Active Directory site contains three subnets. Each subnet contains client computers. The main office has two domain controllers. Each branch office has one domain controller.

REQUIREMENTS

Storage Requirements

Contoso must meet the following storage requirements:

- Improve data availability on the file servers.
- Improve the performance of the file servers.
- Limit each user's storage space on the file servers to 2 GB.
- Prevent users from storing audio and video files on the file servers.
- Provide additional storage on the file servers without causing downtime.
- Enable users to access the previous versions of all the files stored on the file servers.

Technical Requirements

Contoso must meet the following technical requirements:

- Minimize the potential attack surface.
- Minimize WAN link utilization between the offices.
- Minimize the number of server licenses purchased.
- Minimize server downtime caused by Applying updates.
- Minimize the amount of administrative effort required to approve the updates.
- Minimize the amount of time it takes for users in the branch offices to access files on the file servers in the main office.

Problem Statements

Users in the accounting department use a custom Application named App1. The configurations for App1 can only be changed by editing the registry. Currently, a technician must visit each client computer in the accounting department to change the App1 configurations.

Question: 1

You need to recommend a solution for users in the branch office to access files in the main office. What should you include in the recommendation?

A. a BranchCache server that operates in Distributed Cache mode
B. a BranchCache server that operates in Hosted Cache mode
C. a domainbased Distributed File System (DFS) namespace and DFS Replication
D. a standalone Distributed File System (DFS) namespace and DFS Replication

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/dd755969%28WS.10%29.aspx
requirement = Minimize the amount of time it takes for users in the branch offices to access files on the file servers in the main office BranchCache™ is a feature in Windows® 7 and Windows Server® 2008 R2 that can reduce wide area network (WAN) utilization and enhance network application responsiveness when users access content in a central office from branch office locations. When you enable BranchCache, a copy of the content that is retrieved from the Web server or file server is cached within the branch office. If another client in the branch requests the same content, the client can download it directly from the local branch network without needing to retrieve the content by using the Wide Area Network (WAN).

This whitepaper provides an overview of BranchCache, explains the different modes in which BranchCache operates, and describes how BranchCache is configured. The paper also explains how BranchCache works with Web servers and file servers and the steps BranchCache takes to determine that the content is up-to-date.
Hosted Cache mode
The Hosted Cache is a central repository of data downloaded from BranchCache enabled servers into the branch office by BranchCache enabled clients. The configuration of Hosted Cache mode is described later in this document.
Hosted Cache mode does not require a dedicated server. The BranchCache feature can be enabled on a server that is running Windows Server 2008 R2, which is located in a branch that is also running other workloads. In addition, BranchCache can be set up as a virtual workload and run on a server with other workloads, such as File and Print.
Figure 2 illustrates Hosted Cache mode and provides a simplified illustration of the document caching and retrieval process.

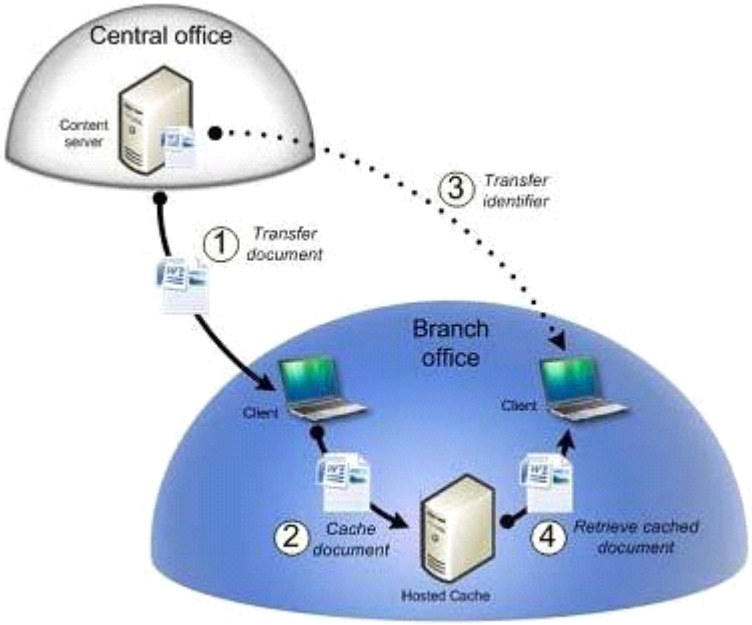


Figure 2 Hosted Cache mode

Question: 2

You need to recommend a solution for managing App1. The solution must require the minimum amount of administrative effort. What should you include in the recommendation?

A. Group Policy Administrative Templates
B. Group Policy Preferences
C. Group Policy Software Settings
D. Windows Remote Management (WinRM)

Answer: B

Explanation:
Could be A or B, its down to which takes the least effort
http://blogs.technet.com/b/askds/archive/2007/08/14/deploying-custom-registry-changes-throughgroup-policy.aspx
Group Policy Templates (ADMX Files)
Administrative templates provide Group Policy setting information for the items that appear under Administrative Templates. Group Policy tools use Administrative template files to populate policy settings in the user interface. This allows administrators to manage registry-based policy settings. Administrative templates provide Group Policy setting

information for the items that appear under Administrative Templates. Group Policy tools use Administrative template files to populate policy settings in the user interface. This allows administrators to manage registry-based policy settings. Administrative template files in Windows Server 2008
R2 and Windows 7 are divided into ADMX (language-neutral) and ADML (language-specific) files. ADML files are XML-based ADM language files that are stored in a language-specific folder. By default, the %Systemroot%\PolicyDefinitions folder on a local computer stores all ADMX files, and ADML files for all languages that are enabled on the computer.
Group Policy Preferences
http://technet.microsoft.com/en-us/library/cc731892%28WS.10%29.aspx
Group Policy preferences, new for the Windows Server 2008 operating system, include more than 20 new Group Policy extensions that expand the range of configurable settings within a Group Policy object (GPO).
These new extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC), under the new Preferences item. Examples of the new Group Policy preference extensions include folder options, mapped drives, printers, scheduled tasks, services, and Start menu settings.
http://support.microsoft.com/kb/943729
Examples of the new Group Policy preference extensions include the following:
Folder Options
Drive Maps
Printers
Scheduled Tasks
Services
Start Menu
The key difference between "Group Policy Preferences" and "Group Policies (settings)" is enforcement. "Group Policies" enforce policy settings and prevent users from changing them. Group Policy Preferences does not (necessarily) enforce settings to machines/users, but merely applies the settings as preferences.
"Group Policy Preferences" extend more than 20 Group Policy categories within a Group Policy Object (GPO) and enable IT professionals to configure, deploy, and manage operating system and application settings including mapped drives, scheduled tasks, power options, files and/or folders, printers, folder options and Start menu settings for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP systems.
White Paper: http://www.microsoft.com/downloads/info.aspx?
na=90&p=&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=42e30e3f-6f01-4610-9d6ef6e0fb7a0790&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2fd%2fc%2fe%2fdce0c60f-8c2e-40ad-94c3-020cd6d0db6d%2fGroup+Policy+Preferences.docx
GP Policy vs. Preference vs. GP preferences
worth a look:
http://blogs.technet.com/b/grouppolicy/archive/2008/03/04/gp-policy-vs-preference-vs-gp-preferences.aspx

Question: 3

You need to recommend a solution for the file servers in the branch offices that meets the storage Requirements. What should you include in the recommendation?

A. Distributed File System (DFS) and access-based enumeration (ABE)
B. File Server Resource Manager (FSRM) quotas and file screens
C. NTFS disk quotas and NTFS permissions
D. Services for Network File System (NFS) and offline files

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc732431.aspx

File Server Resource Manager is a suite of tools for Windows Server® 2008 that allows administrators to understand, control, and manage the quantity and type of data that is 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 efficiently monitor existing storage resources, but it also aids in the planning and implementation of future policy changes.

Setting File Server Resource Manager Options Information about configuring general notification and reporting options before working with File Server Resource Manager.

Quota Management Information about creating quotas that set a soft or hard space limit on a volume or folder tree.

File Screening Management Information about creating file screening rules that block files from a volume or a folder tree.

Storage Reports Management Information about generating storage reports that can be used to monitor disk usage patterns, identify duplicate files and dormant files, track quota usage, and audit file screening.

Classification Management Information about creating and applying file classification properties, which are used to categorize files.

File Management Tasks Information about performing file management tasks to automate the process of finding subsets of files on a server and applying simple commands.

Managing Remote Storage Resources Information about performing resource management tasks on a remote computer where File Server Resource Manager is also installed.

Troubleshooting File Server Resource Manager Instructions for problem solving.

Using File Server Resource Manager

Applies To: Windows Server 2008 R2

There are several navigational options in the File Server Resource Manager snap-in. The following tables detail the navigational options in the File Server Resource Manager nodes, which include:

Quotas

Quota Templates

File Screens

File Screen Templates

File Groups

Quotas

Item	Details
Filter	Opens the **Quota Filter** dialog box, where you can select options to limit the display of quotas in the Results pane. To restore the complete list of quota types and paths: in the **Quota Filter** dialog box, select **All**.
Create Quota	Opens the **Create Quota** dialog box. For more information about creating quotas, see Create a Quota.
Refresh	Refreshes the console details.
Create Template from Quota	Opens the **Create Quota Template** dialog box with the properties of the selected quota. For more information about creating quota templates, see Create a Quota Template.
View Quotas Affecting Folder	Displays only those quotas that affect the same folder as the selected quota.
Edit Quota Properties	Opens the **Quota Properties** dialog box for the selected quota. For more information about editing quota properties, see Quota Properties.
Delete Quotas	Prompts you for confirmation that you want to delete the selected quota. If the quota was derived from a template, that template will not be deleted.
Reset Peak Usage	Eliminates the current peak usage figure so that the peak usage recording starts over.
Enable Quotas	Enables the selected quota.
Disable Quotas	Disables the selected quota.

File Screens

Item	Details
Filter	Opens the **File Screen Filter** dialog box, where you can select options to limit the display of file screens in the Results pane. To complete list of file screen types and paths: in the **File Screen Filter** dialog box, select **All**.
Create File Screen	Opens the **Create File Screen** dialog box. For more information about creating file screens, see Create a File Screen.
Create File Screen Exception	Opens the **Create File Screen Exception** dialog box. For more information about creating file screen exceptions, see Create a Fi Exception.
Refresh	Refreshes the console details.
Create a Template from File Screen	Opens a **Create File Screen Template**dialog box that includes the properties of the selected file screen. For more information al file screen templates, see Create a File Screen Template.
Edit File Screen Properties	Opens the **File Screen Properties**(or **File Screen Exception Properties**) dialog box for the selected file screen (or file screen more information, see File Screen Properties and File Screen Exception Properties.
Delete File Screens	Prompts you for confirmation that you want to delete the selected file screen (or file screen exception). If the file screen was deri template, that template will not be deleted.

Question: 4

You are evaluating whether to add an additional hard disk drive to each file server and create a striped volume for the data files. Which storage requirement is met by adding the hard disk drive and creating the striped volume?

A. Improve data availability on the file servers.
B. Improve the performance of the file servers.
C. Provide additional storage on the file servers without causing downtime.
D. Enable users to access the previous versions of all the files stored on the file servers.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc732422.aspx
A striped volume is a dynamic volume that stores data in stripes on two or more physical disks. Data in a striped volume is allocated alternately and evenly (in stripes) across the disks. Striped volumes offer the best performance of all the volumes that are available in Windows, but they do not provide fault tolerance. If a disk in a striped volume fails, the data in the entire volume is lost.
You can create striped volumes only on dynamic disks. Striped volumes cannot be extended. You can create a striped volume onto a maximum of 32 dynamic disks.

Question: 5

You need to recommend a solution that enables User1 to perform the required actions on the HyperV server. What should you include in the recommendation?

A. Active Directory delegation
B. Authorization Manager role assignment
C. local security groups on the Hyper-V server
D. local security groups on the VMs

Answer: B

Explanation:

http://technet.microsoft.com/en-us/library/dd283030%28v=ws.10%29.aspx
You use Authorization Manager to provide role-based access control for Hyper-V. For instructions on implementing role-based access control.
Authorization Manager is comprised of the following:
Authorization Manager snap-in (AzMan.msc). You can use the Microsoft Management Console (MMC) snapin to select operations, group them into tasks, and then authorize roles to perform specific tasks. You also use it to manage tasks, operations, user roles, and permissions. To use the snap-in, you must first create an authorization store or open an existing store. For more information, see http://go.microsoft.com/fwlink/?
LinkId=134086.
Authorization Manager API. The API provides a simplified development model in which to manage flexible groups and business rules and store authorization policies. For more information, see Role-based Access
Control (http://go.microsoft.com/fwlink/?LinkId=134079).
Authorization Manager requires a data store for the policy that correlates roles, users, and access rights. This is called an authorization store. In Hyper-V, this data store can be maintained in an Active Directory database or in an XML file on the local server running the Hyper-V role. You can edit the store through the Authorization Manager snap-in or through the Authorization Manager API, which are available to scripting languages such as VBScript.
If an Active Directory database is used for the authorization store, Active Directory Domain Services (AD DS) must be at the Windows Server 2003 functional level.
The XML store does not support delegation of applications, stores, or scopes because access to the XML file is controlled by the discretionary access control list (DACL) on the file, which grants or restricts access to the entire contents of the file. (For more information about Authorization Manager delegation, see http://go.microsoft.com/fwlink/?LinkId=134075). Because of this, if an XML file is used for the authorization store, it is important that it is backed up regularly. The NTFS file system does not support applications issuing a sequence of separate write operations as a single logical write to a file when multiple applications write to the same file.
This means an Authorization Manager policy file (XML file) could be edited simultaneously by two administrative applications and could become corrupted. The Hyper-V VSS writer will back up the authorization store with the server running the Hyper-V role.
http://technet.microsoft.com/en-us/library/cc725995%28WS.10%29.aspx
A role assignment is a virtual container for application groups whose members are authorized for the role. A role assignment is based on a single role definition, and a single role definition can be the basis of many role assignments.
The most common procedure that administrators carry out is the assignment of application groups, or Windows users and groups, to a role. For step-by-step instructions, see Assign a Windows User or Group to a Role or
Assign an Application Group to a Role.

Question: 6

You need to identify which operating system must be installed on the HyperV server in the new branch office. Which operating system should you identify?

A. a Server Core installation of Windows Server 2008 R2 Enterprise
B. a Server Core installation of Windows Server 2008 R2 Standard
C. Windows Server 2008 R2 Enterprise
D. Windows Server 2008 R2 Standard

Answer: A

Explanation:
Hyper-V has specific requirements. Hyper-V requires an x64-based processor, hardware-assisted virtualization, and hardware data execution prevention (DEP). Hyper-V is available in x64-based versions of Windows Server 2008—specifically, the x64-based versions of Windows Server 2008 Standard, Windows Server 2008 Enterprise, and Windows Server 2008 Datacenter technical requirements include minimizing attach surface, Server Core achieves

this. so should you use Enterprise or Standard as Hyper V can be implemented on both x64 versions?
http://www.directionsonmicrosoft.com/sample/DOMIS/update/2008/02feb/0208ws2plp_ch.htm
1 Windows Server 2008 Standard, Enterprise, and Datacenter are also offered in "without Hyper-V" editions that do not include the hypervisor technology.
2 When customers exercise the maximum number of OS instances permitted by the server license, the physical OS instance may not be used to run any workload beyond hosting the virtual machines.
3 A single package contains both 32-bit and 64-bit versions. The server license grants the customer the option to use either the 32-bit version or the 64-bit version of the software.
4 Supports hot addition of memory, but not hot replacement of memory, nor hot add or replacement of processors.
5 Use of Windows Server 2008's new Terminal Services Gateway capability is limited to 250 connections.
6 Includes restrictions limiting scalability.
7 Volume licensing customers typically receive additional discounts of 10% to 30%.
8 Client Access Licenses (CALs) retail for US$40 apiece but are offered to volume customers for as much as 50% off. External Connectors are available only via volume licensing programs. Pricing for an External Connector starts at approximately US$1,800 in the least-discounted programs
Under the planned changes it states that each branch will have one DC, a DirectAccess Server a File Server and a Web Server and that all branches will be virtualised. therefore you will be running 4 VMs Windows server 2008 Enterprise allows the running of 4 VMS on one license
So the answer is A becase Server core reduces the surface attack area and virtualization on Enterprise server will meet the VM and licensing requirements

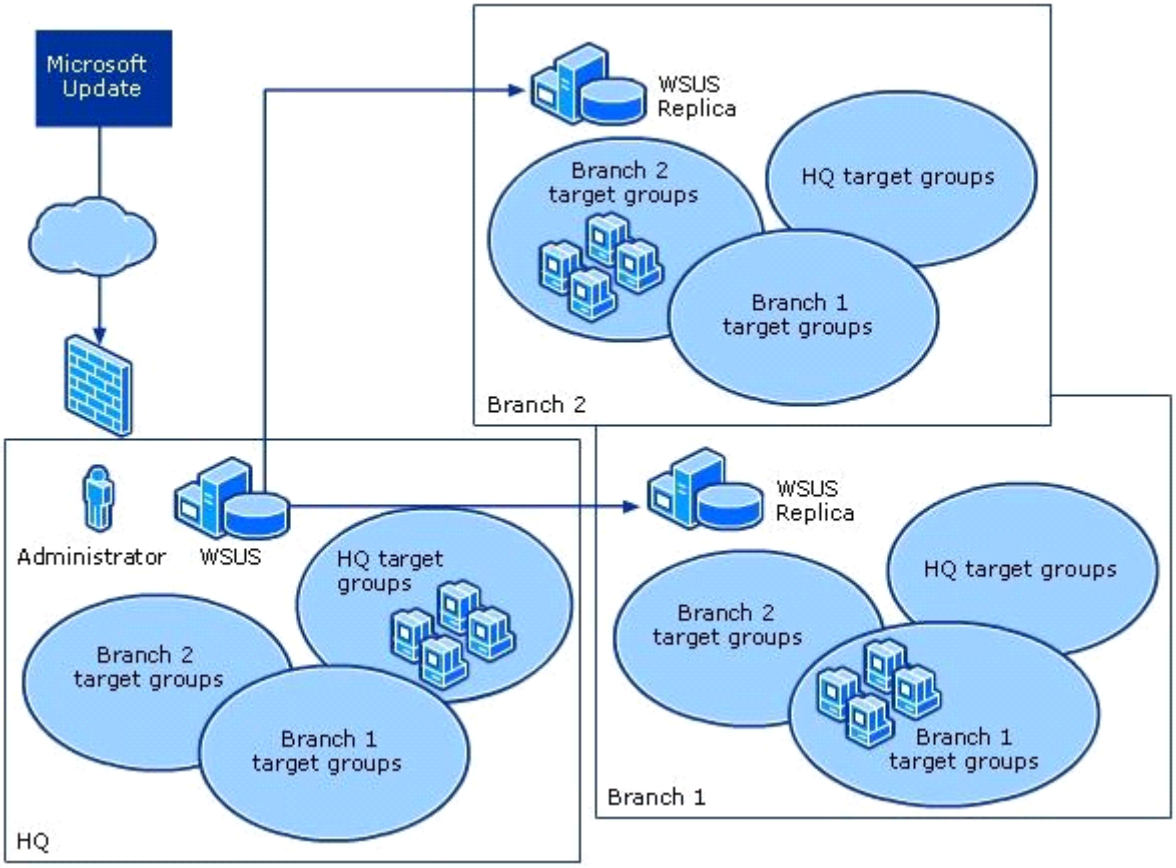
Question: 7

You need to recommend a Windows update strategy for the new branch office. What should you recommend doing in the new branch office?

A. Deploy WSUS in replica mode. Configure updates to be stored on the new WSUS server.
B. Deploy WSUS in autonomous mode. Configure updates to be stored on the new WSUS server.
C. Deploy WSUS in replica mode. Configure the WSUS clients to retrieve updates from Microsoft Update.
D. Deploy WSUS in autonomous mode. Configure the WSUS clients to retrieve updates from Microsoft Update.

Answer: C

Explanation:
New office has a 2MMbps link to the internet and only a 512Kbps link to HQ. so configuring WSUS to update from MS Update will meet the requirement to minimize WAN Link utalization. Making the WSUS server a replica will meet the requirement to minimize the administrative effort to approve updates as all updates would be approved in HQ and this approval would be replicated out to the branch offices.
http://technet.microsoft.com/en-us/library/dd939820%28WS.10%29.aspx
Replica mode (centralized administration)
In replica mode, an upstream WSUS server shares updates, approval status, and computer groups with downstream servers. Downstream replica servers inherit update approvals and are not administered separately from the upstream WSUS server.
The following image shows how you might deploy replica WSUS servers in a branch office environment.



Question: 8

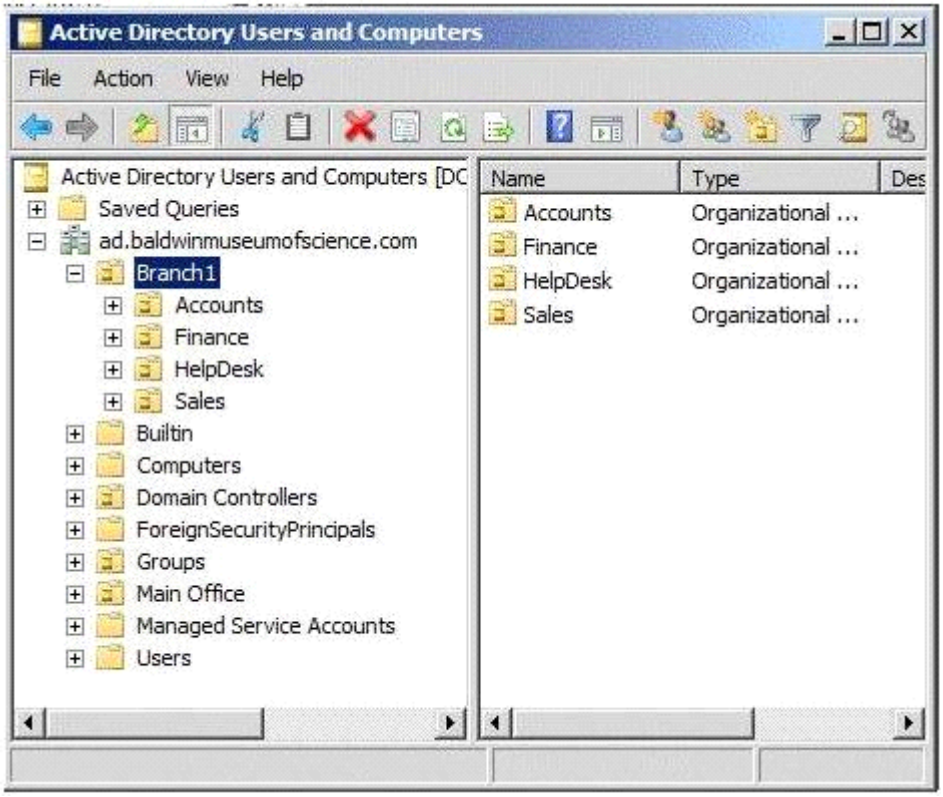
You need to recommend a solution that enables User1 to perform the required actions on the Hyper-V server. What should you include in the recommendation?

A. Authorization Manager role assignment
B. Group Policy object (GPO) assignment on the VMs
C. Group Policy object (GPO) assignment on the Hyper-V server
D. local security groups on the VMs

Answer: A

Case Study: 3
Baldwin Museum of Science
Scenario:
COMPANY OVERVIEW
The Baldwin Museum of Science is an internationally renowned museum of science history.
Physical Location
The museum has a main office and a branch office named Branch1. The main office has 5,000 users. Branch1 has 1,000 users. The main office connects to Branch1 by using a WAN link. The WAN link is highly saturated. The museum has a sales department. All of the users in the sales department have client computers that run Windows XP Service Pack 3 (SP3).
EXISTING ENVIRONMENT
Active Directory Environment

The network contains one Active Directory forest. The forest contains two domains named baldwinmuseumofscience.com and ad.baldwinmuseumofscience.com. All user accounts and computer accounts for all employees are in the ad.baldwinmuseumofscience.com domain. The organizational unit (OU) structure for ad.baldwinmuseumofscience.com is shown in the exhibit. (Click the Case Study **Exhibits** button.)



Network Infrastructure

The network contains the following servers and Applications:

• Application servers that run either Windows Server 2003 Service Pack 2 (SP2), Windows Server 2008 SP2, or Windows Server 2008 R2.

• A custom Application named App1 that runs on all of the Application servers. App1 writes events to the Application log.

• A line-of-business Application named App2 that requires Internet Explorer 6. All of the users in the sales department run App2.

• File servers that run Windows Server 2008 R2.

The main office has the following:

• A two-node failover cluster that runs Windows Server 2008 R2 and has the Hyper-V role installed and a Clustered Shared Volume. The failover cluster hosts four virtual machines (VM) that run Windows Server 2008 R2. The VMs are stored on the Clustered Shared Volume. Each VM runs Microsoft SQL Server 2008.

• A server named Server1 that hosts two shared folders named Sharel and Share2. Sharel hosts 50,000 research documents that are shared by multiple users. Share2 hosts documents that are created by users in the sales department.

Administration Model

All users in Branch 1 are members of global groups and universal groups. The groups are located in an OU named Groups in the ad.baldwinmuseumofscience.com domain.

REQUIREMENTS

Planned Changes

The Baldwin Museum of Science plans to implement a new branch office named Branch2. Branch2 wi and will be configured as a separate Active Directory site. Branch2 will be configured to meet the following

requirements:
• Minimize the cost of deploying new servers.
• Contain only client computers that run Windows 7.
• Connect to the main office by using a saturated WAN link.
• Contain only servers that run Windows Server 2008 R2. The servers will be configured as either file servers or Web servers. The file shares on the file servers must be available if a single file server fails.
In Branch2, if a single domain controller or a WAN link fails, users in the branch must be able to:
• Change their passwords.
• Log on to their client computers.

Technical Requirements

The Baldwin Museum of Science must meet the following technical requirements:
• Hardware and software costs must be minimized whenever possible.
• All VMs must be backed up twice a day.
• All VM backups must include the VM configuration information.
• Events generated by App1 must be stored in a central location.
• An administrator must be notified by e-mail when App1 generates an error.
• The number of permissions assigned to help desk technicians must be minimized.
• The help desk technicians must be able to reset the passwords and modify the membership of all users in Branch1.
• If a user overwrites another user's research document, the user must be able to recover a previous version of the document.
• When users in the sales department work remotely, they must be able to access the files in Share1 in the minimum amount of time.

Security

The Baldwin Museum of Science must meet the following security requirements:
- All scripts that run on production servers must be signed.
- Managers in Branch1 must be allowed to access the Internet at all times.
- Web site administrators must not be required to log on interactively to Web servers.
- Users in Branch1 must only be allowed to access the Internet between 12:00 and 13:00.
- Users and managers must be prevented from downloading executable files from the Internet.
- Administration of the corporate Web sites must support all bulk changes and scheduled content updates.

Question: 1

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.

Answer: A

Explanation:
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: 2

You need to recommend a highavailability solution for the file servers in Branch2 that supports the museum's planned changes. What should you include in the recommendation?

A. a standalone Distributed File System (DFS) namespace and DFS Replication
B. a domainbased Distributed File System (DFS) namespace and DFS Replication
C. Failover Clustering and Clustered Shared Volumes
D. Network Load Balancing (NLB) and Storage Manager

Answer: B

Explanation:
Distributed File System (DFS)
DFS is a method of both simplifying your organization’s shared folder structure and providing data redundancy through replication. DFS lets you collect shared folders located on different servers into one or more logically structured namespaces. Rather than having to remember which server hosts a specific shared folder, they can access the DFS namespace and find all shared folders.
You can replicate a DFS namespace and folders within a site and across WAN links. A user connecting to files within the shared folder structures contained in the DFS namespace will connect automatically to shared folders in the same Active Directory Directory Services (AD DS) site (when available) rather than across a WAN. You can have several DFS Namespace servers in a site and spread over several sites, so if one server goes down a user can still access files within the shared folder structure. The architecture of DFS ensures that a change to a file on a DFS share is replicated quickly and efficiently to all other replicas of that DFS share.
Creating a DFS Namespace
You can create a namespace when you install the DFS Management role service, as shown in Figure 10-2, or create it later.
You can add additional namespaces by right-clicking DFS Namespaces in the DFS Management console and selecting New Namespace. You can create namespaces on a member server or domain controller running Windows Server

2008. However, you cannot create more than one namespace on a server running Windows Server 2008 Standard edition. You can create multiple namespaces on servers running Windows Server 2008 Enterprise and Datacenter editions.
A namespace is a virtual view of shared folders in an organization, and it has a path to a namespace similar to a Universal Naming Convention (UNC) path to a shared folder. You can create two types of namespaces:
Domain-Based Namespaces
A domain namespace uses a domain as its namespace root, such as \\adatum.com\MyNameSpace. A domainbased namespace can be hosted on multiple namespace servers to increase its availability, and its metadata is stored in AD DS. Domain-based namespaces can be created on one or more member servers or domain controllers in the same domain, and metadata for a domain-based namespace is stored by AD DS. Each server must contain an NTFS volume to host the namespace. Multiple namespace servers increase the availability of the namespace. A domain-based namespace cannot be a clustered resource in a failover cluster. However, you can locate the namespace on a server that is also a node in a failover cluster provided that you configure the namespace to use only local resources on that server.
Standalone Namespaces
A stand-alone namespace uses a namespace server as its namespace root, such as \\ServerA\MyNameSpace.
A stand-alone namespace is hosted on only one server. You would choose a stand-alone namespace if your organization does not use AD DS, if you needed to create a single namespace with more than 5,000 DFS folders but your organization did not support Windows Server 2008 mode, or if you wanted to use a failover cluster to increase availability.

Question: 3

You need to recommend an administrative solution for the help desk technicians that meets the museum's technical requirements. What should you recommend?

A. Add the help desk technicians to the Domain Admins group.
B. Add the help desk technicians to the Accounts Operators group.
C. Assign permissions for the Groups OU and the Branch1 OU to the help desk technicians.
D. Assign permissions for the domain object and the Users container to the help desk technicians.

Answer: C

Explanation:
You can delegate administrative control to any level of a domain tree by creating organizational units within a domain and delegating administrative control for specific organizational units to particular users or groups. By giving permissions on the Groups OU they can modify group membership and create groups within that OU, by giving them permissions on the Branch1 OU they will be able to reset passwords within that OU.
http://www.windowsecurity.com/articles/Implementing-Active-Directory-Delegation-Administration.html
How to delegate password reset permissions for your IT staff
One of the most common tasks to delegate, usually to a service desk or Help desk, is the capacity to reset users' passwords when they forget them and unlock their accounts. To accomplish this, you'll need to perform a few delegations: You'll need to delegate the Reset Password Extended Right permission and the Write
Property permission for the pwdLastSet and lockoutTime attributes.
http://community.spiceworks.com/how_to/show/1464 well worth a look
To delegate group membership
http://www.scribd.com/doc/42818731/AD-Delegating-Control-of-Group-Membership

Question: 4

You are planning to upgrade the client computers of the users in the sales department to Windows 7. You need to recommend an upgrade solution to ensure that the client computers can run App2. What should you include in the recommendation?

A. Internet Explorer Administration Kit (IEAK)
B. Microsoft Application Compatibility Toolkit (ACT)
C. Microsoft Application Virtualization (AppV)
D. Microsoft Enterprise Desktop Virtualization (MEDV)

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/ff433573.aspx
MED-V uses Microsoft Virtual PC to provide an enterprise solution for desktop virtualization. With MED-V, you can easily create, deliver, and manage corporate Virtual PC images on any Windows®-based desktop.
MED-V is an integral component of the Microsoft Desktop Optimization Pack, a dynamic solution available to Software Assurance customers, which helps reduce application deployment costs, enables delivery of applications as services, and helps to better manage and control enterprise desktop environments.

Question: 5

You need to recommend a solution for controlling access to the Internet. The solution must meet the museum's security policy. What should you include in the recommendation?

A. File Server Resource Manager (FSRM) file screens and Group Policy objects (GPOs)
B. Microsoft Forefront Threat Management Gateway (TMG) 2010
C. Microsoft Forefront Unified Access Gateway (UAG) 2010
D. Windows Firewall with Advanced Security and Group Policy objects (GPOs)

Answer: B

Explanation: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=14238
Forefront Threat Management Gateway 2010 allows employees to safely and productively use the Internet without worrying about malware and other threats.
It provides multiple protection capabilities including URL filtering*, antimalware inspection*, intrusion prevention, application- and network-layer firewall, and HTTP/HTTPS inspection – that are integrated into a unified, easy to manage gateway, reducing the cost and complexity of Web security.
http://www.isaserver.org/tutorials/Creating-Web-Access-Policy-Forefront-Threat-Management-Gateway-TMGBeta-1-Part1.html

Question: 6

You need to recommend a management solution for the corporate Web sites that meets the museum's security policy. What should you include in the recommendation?

A. Internet Information Services (IIS) Manager
B. Remote Desktop Services (RDS)
C. Remote Server Administration Tools (RSAT)
D. Windows PowerShell 2.0

Answer: D

Explanation:
RSAT isnt right because that will give them access to other tools they do not need. the admins are not required login in so that takes care of RDS because that means they MUST log on interactively, that leaves IIS and Powershell. PowerShell meets the requirements of the security policy, IIs wont

Question: 7

You need to recommend an access solution for the users in the sales department that meets the museum's technical requirements. What should you include in the recommendation?

A. BranchCache in Distributed Cache mode
B. BranchCache in Hosted Cache mode
C. offline files
D. transparent caching

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/gg277982%28WS.10%29.aspx
Offline Files (Client Side Caching or CSC) and Folder Redirection are two features that are often used together to redirect the path of local folders such as the Documents folder to a network location, while caching the contents locally for increased speed and reliability.

Question: 8

You need to recommend a backup solution for the VMs that meets the museum's technical requirements. What should you include in the recommendation?

A. On each VM, perform a full server backup by using Windows Server Backup.
B. On each physical node, perform a full server backup by using Windows Server Backup.
C. Deploy Microsoft System Center Data Protection Manager 2010 and create a new protection group.
D. Deploy Microsoft System Center Virtual Machine Manager (VMM) 2008 R2 and schedule checkpoints

Answer: C

Explanation:
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 endusers.
What is a custom volume?
You can assign a custom volume to a protection group member, in place of the DPM storage pool. A custom volume is a volume that is not in the DPM storage pool and is specified to store the replica and recovery points for a protection group member.
Any volume that is attached to the DPM server can be selected as a custom volume, except the volume that contains

the system and program files. To use custom volumes for a protection group member, two custom volumes must be available: one volume to store the replica and one volume to store the recovery points

Question: 9

You need to recommend a monitoring solution for App1 that meets the museum's technical requirements. What should you include in the recommendation?

A. event subscriptions
B. Microsoft SharePoint Foundation 2010 alerts
C. Microsoft System Center Operations Manager 2007 R2 and the SMTP service
D. Resource Monitor

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc749183.aspx
Event Viewer enables you to view events on a single remote computer. However, troubleshooting an issue might require you to examine a set of events stored in multiple logs on multiple computers.
Windows Vista includes the ability to collect copies of events from multiple remote computers and store them locally. To specify which events to collect, you create an event subscription. Among other details, the subscription specifies exactly which events will be collected and in which log they will be stored locally. Once a subscription is active and events are being collected, you can view and manipulate these forwarded events as you would any other locally stored events.
Using the event collecting feature requires that you configure both the forwarding and the collecting computers.
The functionality depends on the Windows Remote Management (WinRM) service and the Windows Event Collector (Wecsvc) service. Both of these services must be running on computers participating in the forwarding and collecting process. To learn about the steps required to configure event collecting and forwarding computers, see Configure Computers to Forward and Collect Events.

Question: 10

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.

Answer: B

Explanation:
Possible answers are B & 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_2008

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.

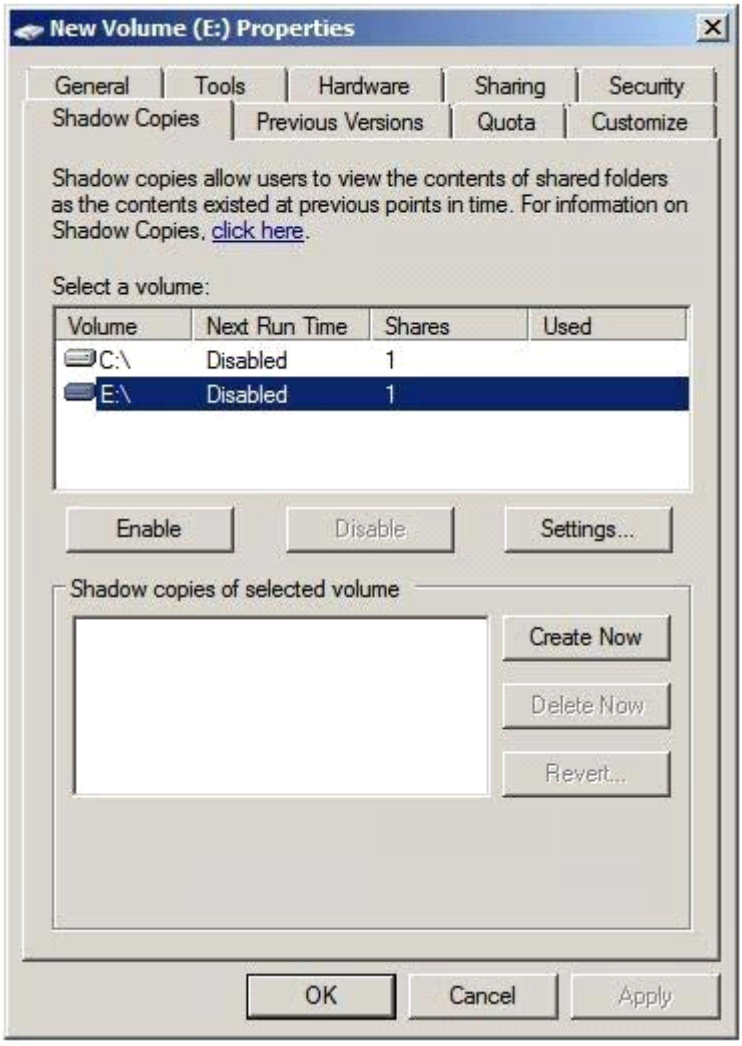
Once the Shadow Copy system has been configured the shadow copy client needs to be set up on the systems of any users that are likely to need to be able to restore files in shared folders.

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

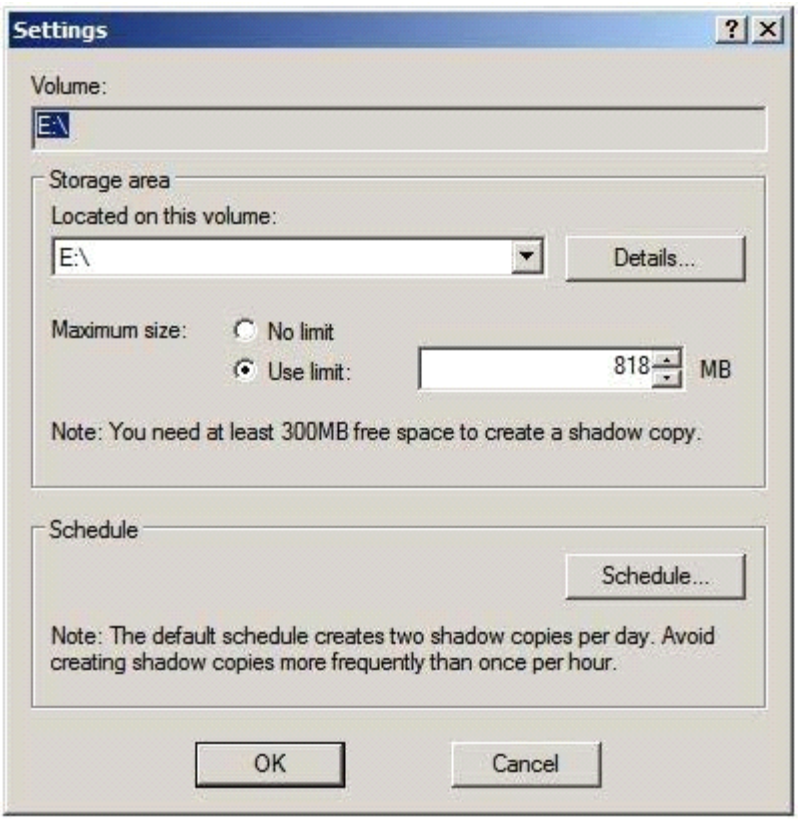
volume will automatically be shadowed. Shadow Copy can be configured either graphically using the Computer Management tool or via the command prompt. Command-line configuration of Shadow Copy will be covered in a later section of this chapter. This section will focus on Computer Management configuration.

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.

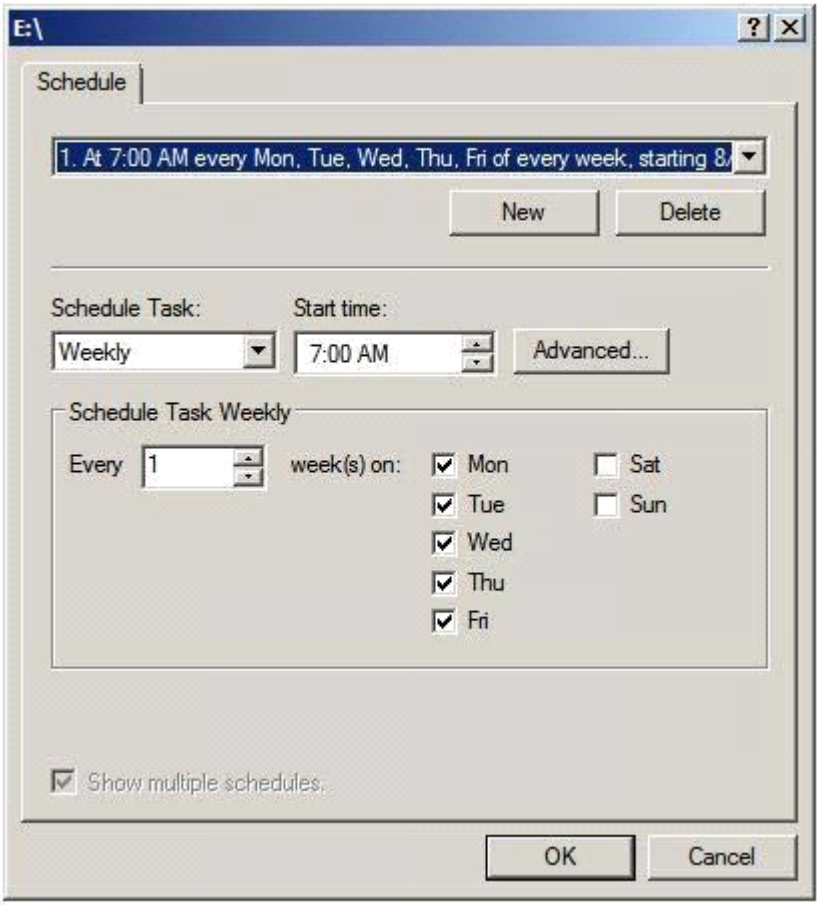
Schedule the shadow copy snapshots by clicking on the Schedule... button. By default, Windows configures two snapshots each day (at 7:00am and 12:00pm respectively). To remove a currently defined snapshot, select it from the drop down list and click on Delete. To modify a run, select it from the drop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



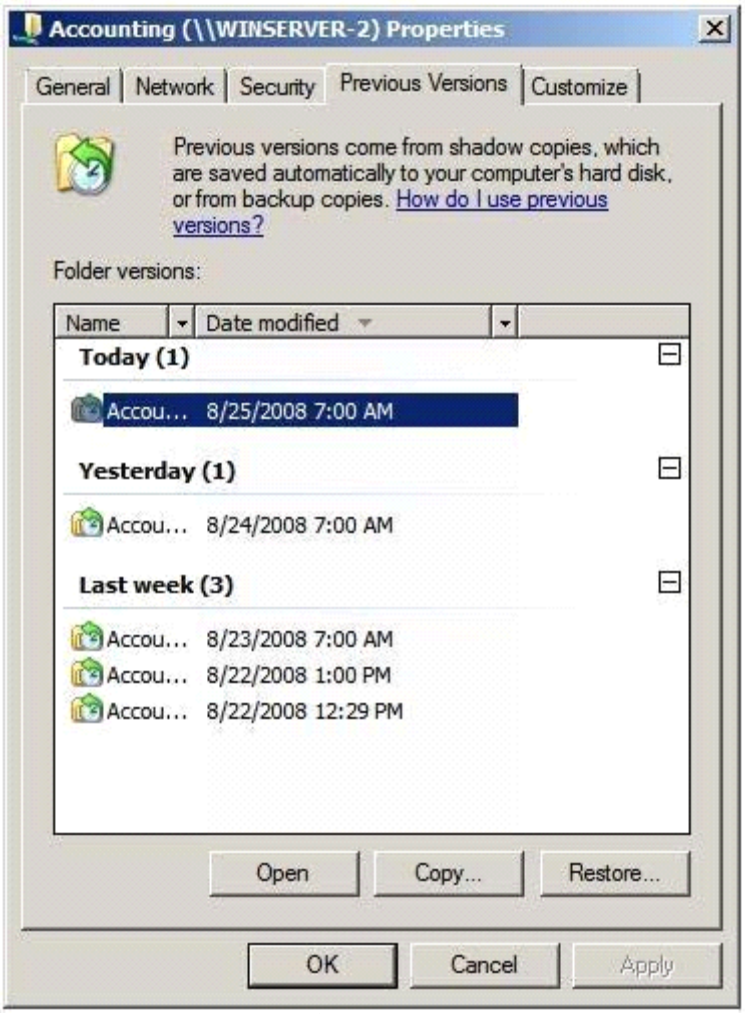
Once the schedules have been configured, click on OK to dismiss the scheduling dialog. Click OK once again in the Settings dialog to return to the Shadow Copy properties panel. At this point, the volume for which a schedule has been defined will have a small clock image superimposed over the volume icon 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.

Case Study: 4
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:
- One file server named Server1.
- Two domain controllers named DC10 and DC11 that are configured as DNS 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: 1

You need to recommend a solution for deploying App1. The solution must support the company's planned changes. What should you include in the recommendation?

A. Group Policy Software Installation
B. Microsoft Application Virtualization (App-V)
C. Microsoft Enterprise Desktop Virtualization (MED-V)
D. Microsoft System Center Configuration Manager

Answer: A

Requirements include minimize costs when possible
Using a GPO to install software is freely available in AD
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.
Create a Distribution Point
To publish or assign a computer program, you must create a distribution point on the publishing server:
Log on to the server computer as an administrator.
Create a shared network folder where you will put the Microsoft Windows Installer package (.msi file) that you want to distribute.
Set permissions on the share to allow access to the distribution package.
Copy or install the package to the distribution point. For example, to distribute Microsoft Office XP, run the administrative installation (setup.exe /a) to copy the files to the distribution point.
Create a Group Policy Object
To create a Group Policy object (GPO) to use to distribute the software package:
Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
In the console tree, right-click your domain, and then click Properties.
Click the Group Policy tab, and then click New.
Type a name for this new policy (for example, Office XP distribution), and then press ENTER.
Click Properties, and then click the Security tab.
Click to clear the Apply Group Policy check box for the security groups that you want to prevent from having this policy applied.
Click to select the Apply Group Policy check box for the groups that you want this policy to apply to.
When you are finished, click OK.
Assign a Package
To assign a program to computers that are running Windows Server 2003, Windows 2000, or Microsoft Windows XP Professional, or to users who are logging on to one of these workstations:
Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
In the console tree, right-click your domain, and then click Properties.
Click the Group Policy tab, select the group policy object that you want, and then click Edit.
Under Computer Configuration, expand Software Settings.

Right-click Software installation, point to New, and then click Package.
In the Open dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\file server\share\file name.msi.
Important Do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package.
Click Open.
Click Assigned, and then click OK. The package is listed in the right pane of the Group Policy window.
Close the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in.
When the client computer starts, the managed software package is automatically installed.
Publish a Package
To publish a package to computer users and make it available for installation from the Add or Remove Programs tool in Control Panel:
Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
In the console tree, right-click your domain, and then click Properties.
Click the Group Policy tab, click the group policy object that you want, and then click Edit.
Under User Configuration, expand Software Settings.
Right-click Software installation, point to New, and then click Package.
In the Open dialog box, type the full UNC path of the shared installer package that you want. For example, \\file server\share\file name.msi.
Important Do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package.
Click Open.
Click Publish, and then click OK.
The package is listed in the right pane of the Group Policy window.
Close the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in.
Test the package:
Note Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.
Log on to a workstation that is running Windows 2000 Professional or Windows XP Professional by using an account that you published the package to.
In Windows XP, click Start, and then click Control Panel.
Double-click Add or Remove Programs, and then click Add New Programs.
In the Add programs from your network list, click the program that you published, and then click Add. The program is installed.
Click OK, and then click Close.
Redeploy a Package
In some cases you may want to redeploy a software package. For example, if you upgrade or modify the package. To redeploy a package:
Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
In the console tree, right-click your domain, and then click Properties.
Click the Group Policy tab, click the Group Policy object that you used to deploy the package, and then click Edit.
Expand the Software Settings container that contains the software installation item that you used to deploy the package.
Click the software installation container that contains the package.
In the right pane of the Group Policy window, right-click the program, point to All Tasks, and then click
Redeploy application. You will receive the following message:
Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?
Click Yes.
Quit the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in.

Remove a Package
To remove a published or assigned package:
Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
In the console tree, right-click your domain, and then click Properties.
Click the Group Policy tab, click the Group Policy object that you used to deploy the package, and then click Edit.
Expand the Software Settings container that contains the software installation item that you used to deploy the package.
Click the software installation container that contains the package.
In the right pane of the Group Policy window, right-click the program, point to All Tasks, and then click Remove.
Do one of the following:
Click Immediately uninstall the software from users and computers, and then click OK.
Click Allow users to continue to use the software but prevent new installations, and then click OK.
Quit the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in.

Question: 2

You need to recommend a solution for managing the shared folders that meets the company's technical requirements. What should you include in the recommendation?

A. Computer Management
B. File Server Resource Manager (FSRM)
C. Share and Storage Management
D. Storage Explorer

Answer: A

Explanation:
Windows 2003 doesn't support Share and Storage Management, therefore changed to A again. Some of the servers run Windows 2003 if all servers were 2008 then Share And Storage Manager would be used

Question: 3

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.

Answer: C

Explanation:
To reduce replication traffic and the amount of data stored in the global catalog, you can use application directory partitions for Active Directory–integrated 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: 4

You need to recommend a monitoring solution for the file servers in the main office. The solution must meet the company's technical requirements. What should you include in the recommendation?

A. File Server Resource Manager (FSRM) active file screens
B. File Server Resource Manager (FSRM) passive file screens
C. Performance Monitor alerts
D. Performance Monitor logs

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc732349%28WS.10%29.aspx
Active = prevents the saving of restricted files
Passive = monitors for the saving of restricted files
Create file screens to block files that belong to particular file groups from being saved on a volume or in a folder tree. A file screen affects all folders in the designated path. For example, you might create a file screen to prevent users from storing audio and video files in their personal folders on the server.
You can configure File Server Resource Manager to generate e-mail or other notifications when a file screening event occurs.
A file screen can be either active or passive:
-Active screening prevents users from saving unauthorized file types on the server.
-Passive screening monitors users saving specific file types and generates any configured notifications, but does not prevent users from saving files.

Question: 5

You plan to implement a WSUS server in a branch office. You need to recommend a solution for deploying the WSUS server that meets the company's technical requirements. What should you include in the recommendation?

A. an autonomous WSUS server that is configured to download updates from Microsoft Update
B. an autonomous WSUS server that is configured to download updates from the WSUS server in the main office
C. a WSUS server running in replica mode that is configured to download updates from Microsoft Update
D. a WSUS server running in replica mode that is configured to download updates from the WSUS server in the main office

Answer: C

Explanation:
Each Office has a highspeed link and the WAN link to the main office is saturated as one of the requirements is to minimize traffic between branch and main offices then C offers the best solution.
http://technet.microsoft.com/en-us/library/dd939820%28WS.10%29.aspx
Replica mode (centralized administration)
In replica mode, an upstream WSUS server shares updates, approval status, and computer groups with downstream

servers. Downstream replica servers inherit update approvals and are not administered separately from the upstream WSUS server.
The following image shows how you might deploy replica WSUS servers in a branch office environment. says the branch sites have a dedicated high speed link so utalise that instead of the wan link

Question: 6

You need to recommend a file recovery solution that meets the company's technical requirements. What should you include in the recommendation?

A. Distributed File System (DFS) Replication
B. File Server Resource Manager (FSRM) active file screens
C. shadow copies
D. Windows Storage Server 2008

Answer: C

Explanation:
Windows Server 2008 Volume Shadow Copy is a mechanism whereby the contents of shared folders can be automatically backed up at pre-determined intervals to a shadow volume. Once implemented, shadow copy will backup the previous 64 versions of each file in the shadowed volume and provide users with the ability to restore files from any of the previous 64 versions without administrator intervention, enabling users to independently restore deleted, damaged or overwritten files. In addition to restoring individual files to a previous version, shadow copy also provides the ability to restore an entire volume.
http://www.techotopia.com/index.php/Configuring_Volume_Shadow_Copy_on_Windows_Server_2008

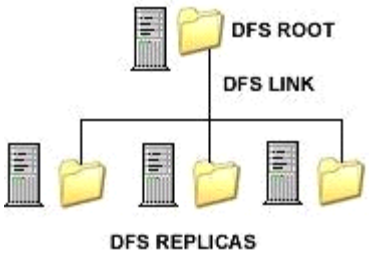
Question: 7

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.

Answer: D

Explanation:
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: 8

You need to recommend changes to the DFS infrastructure that meet the company's security requirements. What should you recommend?

A. Modify the NTFS permissions and the share permissions of the DFS targets.
B. Modify the referrals settings of the DFS namespace and the NTFS permissions of the DFS targets.
C. Migrate the namespace to Windows Server 2008 mode and modify the referrals settings.
D. Migrate the namespace to Windows Server 2008 mode and enable accessbased enumeration (ABE).

Answer: D

Explanation:
ABE is enabled by default and lets you hide files and folders from users who do not have access to them.

Question: 9

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

A. Microsoft Baseline Security Analyzer (MBSA)
B. Microsoft Security Assessment Tool (MSAT)
C. Resultant Set of Policy (RSoP)
D. Security Configuration Wizard (SCW)

Answer: A

Explanation:
http://technet.microsoft.com/en-us/security/cc184924
Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems.

Question: 10

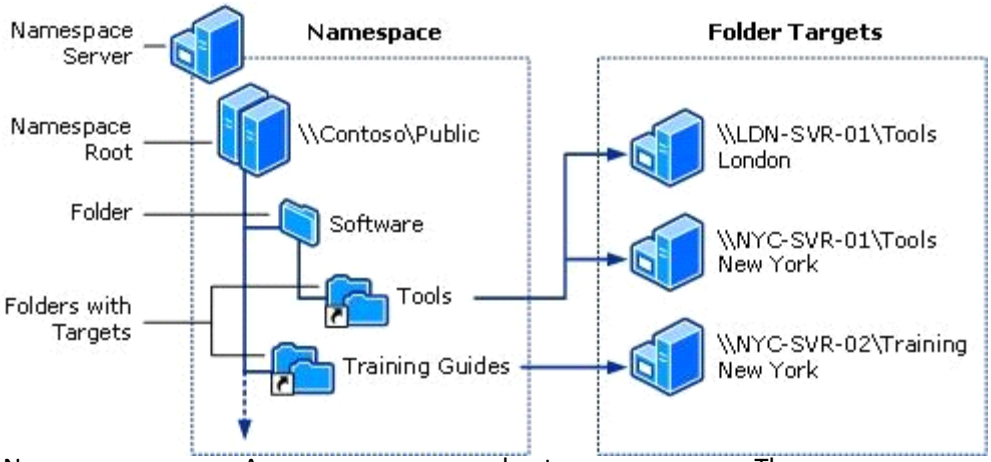
You need to recommend changes to the DFS infrastructure that meet the company's technical requirements. What should you recommend implementing in each branch office? (Each correct answer presents part of the solution. Choose two.)

A. a DFS namespace server

B. a DFS replica
C. a standalone DFS namespace
D. BranchCache in Distributed Cache mode
E. BranchCache in Hosted Cache mode

Answer: A, B

Explanation:
When deploying domain-based namespaces, you can add additional namespace servers to host a namespace.
This has several advantages:
If one namespace server hosting the namespace goes down, the namespace will still be available to users who need to access shared resources on your network. Adding another namespace thus increases the availability of your namespace.
If you have a namespace that must be available to users all across your organization but your Active Directory network has more than one site, then each site should have a namespace server hosting your namespace. That way, when users in a site need to contact a namespace server for referrals, they can do so locally instead of sending traffic requests to other sites. This improves performance and reduces unnecessary WAN traffic.
Note that adding additional namespace servers is only supported for domain-based namespaces, not standalone namespaces.
http://technet.microsoft.com/en-us/library/cc732863%28v=ws.10%29.aspx
DFS Namespaces enables you to group shared folders located on different servers by transparently connecting them to one or more namespaces. A namespace is a virtual view of shared folders in an organization. When you create a namespace, you select which shared folders to add to the namespace, design the hierarchy in which those folders appear, and determine the names that the shared folders show in the namespace. When a user views the namespace, the folders appear to reside on a single, high-capacity hard disk. Users can navigate the namespace without needing to know the server names or shared folders hosting the data.
The path to a namespace is similar to a Universal Naming Convention (UNC) path of a shared folder, such as \\Server1\Public\Software\Tools. If you are familiar with UNC paths, you know that in this example the shared folder, Public, and its subfolders, Software and Tools, are all hosted on Server1. Now, assume you want to give users a single place to locate data, but you want to host data on different servers for availability and performance purposes. To do this, you can deploy a namespace similar to the one shown in the following figure. The elements of this namespace are described after the figure.



Namespace server. A namespace server hosts a namespace. The namespace server can be a member server or a domain controller.
Namespace root. The root is the starting point of the namespace. In the previous figure, the name of the root is Public, and the namespace path is \\Contoso\Public. This type of namespace is known as a domain-based namespace, because it begins with a domain name (for example, Contoso) and its metadata is stored in AD DS. Although a single namespace server is shown in the previous figure, a domain-based namespace can be hosted on multiple namespace

servers.
Folder. Folders help build the namespace hierarchy. Folders can optionally have folder targets. When users browse a folder with targets in the namespace, the client computer receives a referral that directs the client computer to one of the folder targets.
Folder targets. A folder target is a UNC path of a shared folder or another namespace that is associated with a folder in a namespace. In the previous figure, the folder named Tools has two folder targets, one in London and one in New York, and the folder named Training Guides has a single folder target in New York. A user who browses to \\Contoso\Public\Software\Tools is transparently redirected to the shared folder \\LDN-SVR-01\Tools or \\NYC-SVR-01\Tools, depending on which site the user is in.

Question: 11

You need to recommend a solution for managing the address information of the user accounts. The solution must meet the company's security requirements. What should you include in the recommendation?

A. Active Directory delegation
B. Authorization Manager
C. built-in security groups
D. user rights assignments

Answer: A

Explanation:
Delegation of control means you can give fine grained rights to specific tasks to specific users or groups within AD.
So a single user or group can be delegated permissions to create new user accounts within a specific OU or Site within your AD forest or domain

Case Study: 5
City Power & Light
Scenario:
COMPANY OVERVIEW
Overview
City Power & Light is an international utilities company. The company has a sales department, a finance department, and a production department.
Physical Location
The company has a main office and a branch office.
EXISTING ENVIRONMENT
Network Infrastructure
The network contains the following servers:

- A server named Server1 that runs Windows Server 2008 R2 Enterprise and has the Hyper-V role installed. Server1 hosts three virtual machines (VMs) that run Windows Server 2008 R2 Enterprise. The VMs always run.
- A Windows Server Update Services (WSUS) server in the main office. The WSUS server manages updates for the client computers in the main office only.
- Several file servers that store data on an iSCSI Storage Area Network (SAN). The file servers have multiple network cards.
- An enterprise root certification authority (CA) named CA1 that runs Windows Server 2008 R2.

The branch office connects to the main office by using a WAN link. The WAN link is highly saturated. All

client computers on the network connect to the Internet by using a single Internet connection at the main office.

Problem Statements

All client computers run Microsoft Office 2003. The client computers for the users in the sales department run a 64-bit version of Windows 7. Sales users must be able to run a 64-bit version of Office 2010 and Office 2003 concurrently when they work offline. Office 2010 must be deployed by using the minimum amount of administrative effort.

REQUIREMENTS

Business Goal

City Power & Light has the following business goals:

- Software and hardware costs must be minimized, whenever possible.
- Due to power restrictions at the data center in the main office, all new servers must be deployed on VMs, whenever possible.

Planned Changes

City Power & Light plans to implement the following changes in their network:

- A WSUS server in the branch office.
- A robotic-based tape library for the file servers.
- A document management system that supports the following requirements:
    - o Retains multiple versions of a document
    - o Automatically App1ies access policies to documents
- A solution for managing Group Policy objects (GPOs) that supports the following:
    - o Version tracking
    - o Offline modification
    - o Role-based access control
- Nine VMs that run Windows Server 2008 R2 Enterprise. Only five VMs will run concurrently.
- Two Microsoft SQL Server 2008 Enterprise servers in a failover cluster. The cluster will be attached to a hardware RAID-5 array that has five 2-terabyte drives.
- Five additional physical servers for the finance department. The new servers will use native-boot virtual hard disks (VHDs). The VHD images will contain a single partition.

Technical Requirements

City Power & Light must meet the following technical requirements:

- The file servers must maintain their connection to the SAN if a network card fails.
- The bandwidth utilization between the main office and the branch office must be minimized.
- Administrators in the main office must approve or reject updates for all of the client computers in all of the offices.

Security Requirements

City Power & Light must meet the following security requirements:

- All help desk technicians must be able to approve certificate requests and revoke certificates. The help desk technicians must be prevented from modifying the properties of the CA.
- All telecommunications technicians must be able to manage the virtual networks of Server1. The telecommunications technicians must be prevented from performing all other Hyper-V management task.

All of the documents created by users in the finance department must be shared with all of the managers in the company. After 30 days, only those who created the documents must be able to access the documents.

Question: 1

You need to recommend a disk configuration for the planned SQL Server deployment. The solution must ensure that the servers can fail over automatically. What should you include in the recommendation?

A. GPT disks and basic disks
B. GPT disks and dynamic disks
C. MBR disks and basic disks
D. MBR disks and dynamic disks

Answer: A

Explanation:
Tnx SoK for the edditional material
Server 2008 introduces support for GPT disks in cluster storage
http://technet.microsoft.com/en-us/library/cc770625%28v=ws.10%29.aspx
n Windows Server® 2008 Enterprise and Windows Server® 2008 Datacenter, the improvements to failover clusters (formerly known as server clusters) are aimed at simplifying clusters, making them more secure, and enhancing cluster stability. Cluster setup and management are easier. Security and networking in clusters have been improved, as has the way a failover cluster communicates with storage
What new functionality does failover clustering provide?
New validation feature. With this feature, you can check that your system, storage, and network configuration is suitable for a cluster.
Support for GUID partition table (GPT) disks in cluster storage. GPT disks can have partitions larger than two terabytes and have built-in redundancy in the way partition information is stored, unlike master boot record (MBR) disks.
http://technet.microsoft.com/en-us/library/cc770625%28WS.10%29.aspx
Support for GPT disks in cluster storage
GUID partition table (GPT) disks are supported in failover cluster storage. GPT disks provide increased disk size and robustness. Specifically, GPT disks can have partitions larger than two terabytes and have built-in redundancy in the way partition information is stored, unlike master boot record (MBR) disks. With failover clusters, you can use either type of disk.
Why Basic disks over Dynamic?
Only Basic discs can be used in a failover cluster
http://technet.microsoft.com/en-us/library/cc733046.aspx

Question: 2

You need to recommend a management solution for Server1 that meets the company's security requirements. What should you include in the recommendation?

A. accessbased enumeration (ABE)
B. Authentication Mechanism Assurance
C. Authorization Manager
D. HyperV Manager

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc732290%28WS.10%29.aspx
What does Authorization Manager do?

Authorization Manager is a role-based security architecture for Windows that can be used in any application that needs role-based authorization, including ASP.NET Web applications, ASP.NET Web services, and client/server systems based on .NET Remoting. The role-based management model enables you to assign users to roles and gives you a central place to record permissions assigned to each role. This model is often called rolebased access control.

Question: 3

You need to recommend a solution for the file servers that meets the company's technical requirements. What should you include in the recommendation?

A. Storage Manager for SANs
B. Network Load Balancing (NLB)
C. TCP/IP offload services
D. the Multipath I/O feature

Answer: D

Explanation:
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.

Question: 4

You need to recommend a solution for the new VMs that supports the company's planned changes. What should you recommend doing before the new VMs are deployed?

A. Purchase one additional Enterprise license.
B. Purchase two additional Enterprise licenses.
C. Deploy an additional physical server that runs Microsoft HyperV Server 2008 R2.
D. Deploy an additional physical server that runs Windows Server 2008 R2 Enterprise.

Answer: A

Explanation:
Best I could come up with was the following:
Enterprise release includes the license for 4 virtual servers on one physical Server if that physical server is only running hyper V. as it stands the existing server has only 3 VMs leaving on license free, you need a total of 5 VMs running concurrently so you can utilize the one spare that you have.

Question: 5

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

Answer: C

Explanation:
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: 6

You need to recommend a security solution for the documents in the finance department. The solution must meet the company's security requirements. What should you include in the recommendation?

A. accessbased enumeration (ABE) and Encrypted File System (EFS)
B. accessbased enumeration (ABE) and Windows BitLocker Drive Encryption (BitLocker)
C. Active Directory Rights Management Services (AD RMS)
D. File Server Resource Manager (FSRM) file screens

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd996658%28WS.10%29.aspx
Rights policy templates are used to control the rights that a user or group has on a particular piece of rightsprotected content. Active Directory Rights Management Services (AD RMS) stores rights policy templates in the configuration database. Optionally, it may maintain a copy of all rights policy templates in a shared folder that you specify.

Question: 7

You need to recommend a delegation solution for CA1 that meets the company's security requirements. What should you include in the recommendation?

A. accessbased enumeration (ABE)
B. Active Directory delegation
C. Authorization Manager
D. role separation

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/cc732590(v=ws.10).aspx
You can use role-based administration to organize certification authority (CA) administrators into separate, predefined CA roles, each with its own set of tasks. Roles are assigned by using each user's security settings.
You assign a role to a user by assigning that user the specific security settings that are associated with the role. A user that has one type of permission, such as Manage CA permission, can perform specific CA tasks that a user with another type of permission, such as Issue and Manage Certificates permission, cannot perform.

Question: 8

You need to recommend a deployment solution for Office 2010 to address the problem statements. What should you include in the recommendation?

A. Microsoft Application Virtualization (App-V)
B. Microsoft Enterprise Desktop Virtualization (MED-V)
C. Microsoft HyperV Server 2008 R2
D. Windows XP Mode

Answer: A

Explanation:
The users need to be able to run both Office 2003 & 2007 at the same time. so they need to run in isolation to each other. App-V provides this service
http://technet.microsoft.com/en-us/library/ee958112.aspx
Microsoft Application Virtualization (App-V) can make applications available to end user computers without having to install the applications directly on those computers. This is made possible through a process known as sequencing the application, which enables each application to run in its own self-contained virtual environment on the client computer. The sequenced applications are isolated from each other. This eliminates application conflicts, but the applications can still interact with the client computer.

Question: 9

You need to recommend an automated deployment solution for the new servers in the finance department. What should you include in the recommendation?

A. Microsoft Hyper-V Server 2008 R2
B. Microsoft System Center Virtual Machine Manager (VMM)
C. Windows Deployment Services (WDS)
D. Windows Server Migration Tools

Answer: C

Explanation:
Windows Deployment Services is a server role that was included with Windows Server 2008 and now includes various updates for Windows Server 2008 R2. The information in this section is specific to the Windows Server 2008 R2 release and does not apply to the initial release of Windows Server 2008.
In Windows Server 2008 R2, you can deploy virtual hard disk (.vhd) images of Windows Server 2008 R2 to a physical (not virtual) computer using Windows Deployment Services. In general, you deploy .vhd images in the same way that you deploy .wim images. However, using WDSUTIL at the command line is the only supported method of adding and configuring the images

Question: 10

You need to recommend a backup solution for the file servers that supports the company's planned changes. What should you include in the recommendation?

A. File Server Resource Manager (FSRM)
B. Microsoft System Center Data Protection Manager
C. Windows Server Backup
D. Windows Storage Server 2008

Answer: B

Explanation:
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 endusers.

Question: 11

You need to deploy a WSUS server in the branch office that meets the company's technical requirements. What should you deploy?

A. an autonomous WSUS server that is configured to download updates from Microsoft Update
B. an autonomous WSUS server that is configured to download updates from the WSUS server in the main office
C. a WSUS server running in replica mode that is configured to download updates from Microsoft Update
D. a WSUS server running in replica mode that is configured to download updates from the WSUS server in the main office

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/dd939820%28WS.10%29.aspx
All clients computers on the network connect to the main office via a highly saturated link, they don't have an independant link so updates must come from HQ
Replica mode (centralized administration)
In replica mode, an upstream WSUS server shares updates, approval status, and computer groups with downstream servers. Downstream replica servers inherit update approvals and are not administered separately from the upstream WSUS server.
The following image shows how you might deploy replica WSUS servers in a branch office environment.
It says that all branch PCs on the network connect to the internet by using a single internet connection at the main office.
To me that implies that all traffic to the branch travels thorugh the main office so if the branch updated from MS it has to come through the main office so you'd be downloading the same patches twice, that is wasting bandwidth and one requirement is to minimize bandwidth usage

Question: 12

You need to recommend a document management solution that supports the company's planned changes. What should you include in the recommendation?

A. Active Directory Rights Management Services (AD RMS) and File Server Resource Manager (FSRM)
B. Active Directory Rights Management Services (AD RMS) and Microsoft SharePoint Foundation 2010
C. Authorization Manager and Microsoft SharePoint Foundation 2010
D. File Server Resource Manager (FSRM) and Share and Storage Management

Answer: B

Explanation:
AD RMS meets the requirement for Role Based Access Control, Sharepoint meets the requirements for multiple versions
Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications to help safeguard digital information from unauthorized use. Content owners can define who can open, modify, print, forward, or take other actions with the information.
http://www.plusconsulting.com/WhitePapers/SharePoint%202010%20Business%20Value%20WhitePaper.pdf

Case Study: 6
Lucerne Publishing
Scenario:
COMPANY OVERVIEW
Overview
Lucerne Publishing is a large publishing company that produces both traditional books and e-books.
Physical Location
The company has a main office and a branch office. The main office is located in New York. The branch office is located in San Francisco. The main office has a satellite office located in Boston. The company has 7,500 users.
EXISTING ENVIRONMENT
Active Directory Environment
The network contains an Active Directory forest. The forest contains a single domain named lucernepublishing.com.
Network Infrastructure
Client computers in the New York office and the San Francisco office run either Windows Vista or Windows XP. All client computers in the Boston office run Windows 7.
The company has a finance department. All of the client computers in the finance department run Windows XP. The finance department uses an Application named App1. App1 only runs on Windows XP.
The relevant servers in the New York office are configured as shown in the following table.

Server name	Operating System	Server role
New York Office		
DC1	Windows Server 2003 R2	Domain controller
DC2	Windows Server 2008 R2	Domain controller
DFS1	Windows Server 2008 R2	Distributed File System (DFS)
SQL1	Windows Server 2008 R2	Microsoft SQL Server 2008
SQL2	Windows Server 2008 R2	Microsoft SQL Server 2008 R2
Server1	Windows Server 2003 R2	File server
San Francisco Office		
DFS2	Windows Server 2008	Distributed File System (DFS)
DC3	Windows Server 2003 R2	Domain controller

The servers have the following configurations:

- Remote Desktop is enabled on all servers.
- The passwords for all service accounts are set to never expire.
- Server1 stores roaming user profiles for users in the Boston office.
- SQL1 and SQL2 are deployed in a two-node failover cluster named Clusterl.
- All servers have Pre-Boot Execution Environment (PXE)-compliant network adapters.
- The servers in the San Francisco office contain neither a recovery partition nor optical media drives.

DFSl and DFS2 are members of the same DFS Replication group. The DFS namespace is configured to use Windows 2000 Server mode.

The Boston office has no servers. The Boston office connects to the New York office by using a dedicated hardware VPN device.

The finance department publishes monthly forecast reports that are stored in DFS.

REQUIREMENTS

Business Goals

Lucerne Publishing must minimize administrative costs, hardware costs, software costs, and development costs, whenever possible.

Planned Changes

All client computers will be upgraded to Windows 7.

A VPN server will be deployed in the main office. All VPN clients must have the latest Windows updates before they can access the internal network.

You plan to deploy a server that has the Remote Desktop Gateway (RD Gateway) role service installed.

Technical Requirements

Lucerne Publishing must meet the following technical requirements:

- Upgrade all client computers to Windows 7.
- Minimize Group Policy-related replication traffic.
- Ensure that App1 can be used from client computers that run Windows 7.
- Ensure that users can use App1 when they are disconnected from the network.
- Ensure that you can perform a bare metal recovery of the servers in the San Francisco office.
- Minimize the amount of time it takes users in the Boston office to log on to their client computers.
- Ensure that domain administrators can connect remotely to all computers in the domain through RD Gateway.

- Ensure that file server administrators can access DFS servers and file servers through the RD Gateway.
- Prevent file server administrators from accessing other servers through the RD Gateway

Security Requirements

Lucerne Publishing must meet the following security requirements:

- USB storage devices must not be used on any servers.
- The passwords for all user accounts must be changed every 60 days.
- Users must only be able to modify the financial forecast reports on DFSl. DFS2 must contain a read-only copy of the financial forecast reports.
- All operating system drives on client computers that run Windows 7 must be encrypted.
- Only approved USB storaqe devices must be used on client computers that run Windows 7.

Question: 1

You need to recommend a solution for managing Group Policy that meets the company's technical requirements. What should you recommend?

A. Implement a central store.
B. Upgrade DC3 to Windows Server 2008 R2.
C. Create starter Group Policy objects (GPOs).
D. Deploy Advanced Group Policy Management (AGPM).

Answer: A

Explanation:
http://msdn.microsoft.com/en-us/library/bb530196.aspx
Create a Central Store
The central store is a folder structure created in the sysvol directory on the domain controllers in each domain in your organization. You will need to create the central store only once on a single domain controller for each domain in your organization. The File Replication service then replicates the central store to all domain controllers. It is recommended that you create the central store on the primary domain controller because the Group Policy Management Console and Group Policy Object Editor connect to the primary domain controller by default.
The central store consists of a root-level folder containing all language-neutral ADMX files and subfolders containing the language-specific ADMX resource files.

Question: 2

You need to recommend which role services must be deployed to support the company's planned changes. Which two role services should you recommend? (Each correct answer presents part of the solution. Choose two.)

A. Health Registration Authority (HRA)
B. Host Credential Authorization Protocol (HCAP)
C. Network Policy Server (NPS)
D. Routing and Remote Access service (RRAS)

Answer: C, D

Explanation:

Network Policy Server
NPS is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy. You can use NPS to centrally manage network access through a variety of network access servers, including 802.1X authenticating switches and wireless access points, VPN servers, and dial-up servers. In addition, NPS is configurable as a Network Access Protection (NAP) policy server.
Routing and Remote Access
Using Routing and Remote Access, you can deploy Point-to-Point Tunneling Protocol (PPTP), Secure Socket
Tunneling Protocol (SSTP), or Later Two Tunneling Protocol (L2TP) with Internet Protocol security (IPsec) VPN connections to provide end users with remote access to your organization's network. You can also create a site-to-site VPN connection between two servers at different locations.
Health Registration Authority (HRA)
HRA is a Network Access Protection (NAP) component that issues health certificates to clients that pass the health policy verification that is performed by NPS using the client statement of health (SoH). HRA is used only with the NAP IPsec enforcement method.
Host Credential Authorization Protocol (HCAP)
HCAP allows you to integrate your Microsoft NAP solution with Cisco Network Access Control Server. When you deploy HCAP with NPS and NAP, NPS can perform client health evaluation and the authorization of Cisco 802.1X access clients.

Question: 3

You need to recommend a solution for the USB storage devices on the client computers. The solution must meet the company's security requirements. What should you include in the recommendation?

A. Encrypted File System (EFS)
B. the App1ocker Group Policy settings
C. the Enhanced Storage Access settings
D. Windows BitLocker Drive Encryption (BitLocker)

Answer: C

Explanation:
What is Enhanced Storage?
http://windows.microsoft.com/en-us/windows7/What-is-Enhanced-Storage
There are different types of storage devices, such as USB flash drives or external hard drives. Some have no particular security enhancements, while others have built-in safety features. Enhanced Storage devices have built-in safety features that let you control who can access the data on the device by using a password or a certificate (if the device is being used in a workplace). Once someone has access to the device, they have access to the data because the data on the device is not encrypted. Some device manufacturers might offer encryption on Enhanced Storage devices. Check the device packaging or documentation to see if the device includes encryption.
An Enhanced Storage device can be an external USB hard drive or a USB flash drive. When you purchase a USB hard drive or flash drive, the packaging might indicate that it's an Enhanced Storage device.
The first time that you plug the device into your computer, you'll be prompted to create a password or use a certificate with the device. Once the password is entered or the certificate is retrieved, the data on the device is accessible. It's important to use a strong password to help keep your data secure.
n addition to the device access password, you can set a recovery password, which you can use to reset the device access password. You can create the recovery password when you create the device access password or by right-clicking the device in the Computer folder, and then selecting Set password.
You can also use the recovery password as an administrator password. Administrators can choose to set a device password for the user of the device, and then use the recovery password as an administrator password.
This way, the administrator can unlock the storage device if the person using it forgets their password.

Enhanced Storage Access settings
http://technet.microsoft.com/en-us/library/dd560657%28WS.10%29.aspx
Enhanced Storage devices are devices that support the IEEE 1667 protocol to provide functions such as authentication at the hardware level of the storage device. These devices can be very small, such as USB flash drives, to provide a convenient way to store and carry data. At the same time, the small size makes it very easy for the device to be lost, stolen, or misplaced.

Question: 4

You need to recommend a solution for managing the service accounts for SQL1 and SQL2. The solution must meet the company's security requirements. What should you include in the recommendation?

A. a custom password filter
B. a Password Settings object (PSO)
C. managed service accounts
D. manual password changes

Answer: D

Explanation:
req - passwords to change every 60 days.
Service account passwords are set to never expire so can not meet the above requirement, so manual intervention is required.

Question: 5

You need to recommend a solution to minimize the amount of time it takes for users in the Boston office to log on to their client computers. What should you include in the recommendation?

A. access based enumeration (ABE)
B. folder redirection
C. the Active Directory site link cost
D. universal group membership caching

Answer: B

Explanation: http://technet.microsoft.com/en-us/library/cc732275.aspx
Folder Redirection User settings and user files are typically stored in the local user profile, under the Users folder. The files in local user profiles can be accessed only from the current computer, which makes it difficult for users who use more than one computer to work with their data and synchronize settings between multiple computers. Two technologies exist to address this problem: Roaming Profiles and Folder Redirection. Both technologies have their advantages, and they can be used separately or together to create a seamless user experience from one computer to another. They also provide additional options for administrators managing user data.
When a user logs in their profile is loaded as part of the login process. the My Documents folder is part of the user profiel, by redirecting this folder to a file server it means that it does not needed to be loaded at login thus reducing the login time. while having the added benifit of enabling the company to back up these files.

Question: 6

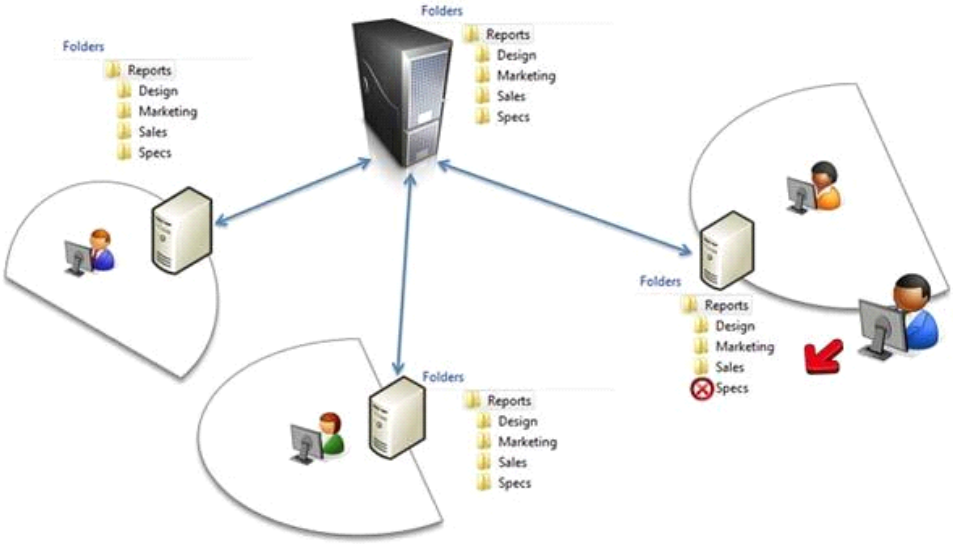
You need to recommend changes to the infrastructure to ensure that DFS meets the company's security requirements.

What should you include in the recommendation?

A. Upgrade DFS2 to Windows Server 2008 R2.
B. Implement accessbased enumeration (ABE).
C. Implement Authentication Mechanism Assurance.
D. Configure the DFS namespace to use Windows Server 2008 mode.

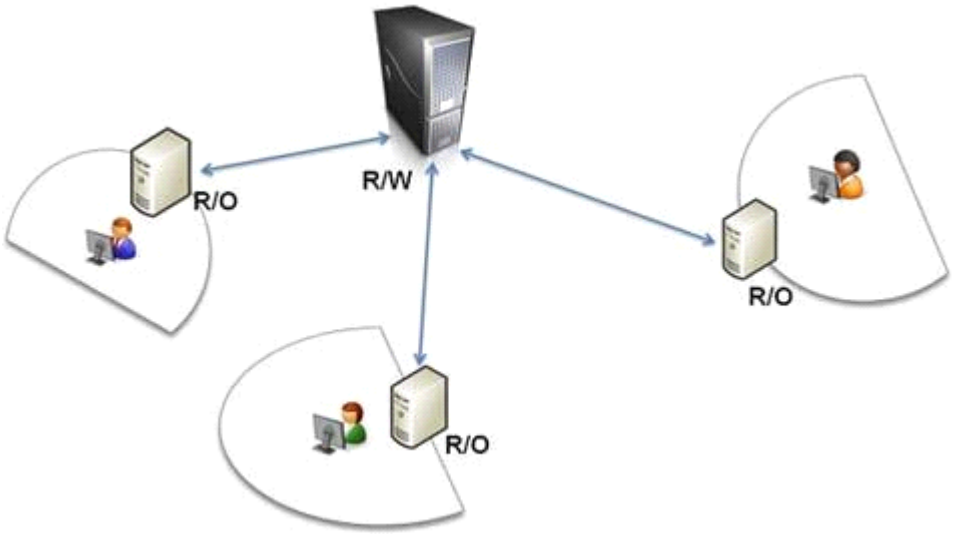
Answer: A

Explanation:
Users must only be able to modify the financial forecast reports on DFSl. DFS2 must contain a read-only copy of the financial forecast reports.
Both servers are part of the same replication group and it is in Windows 2000 server mode
http://blogs.technet.com/b/filecab/archive/2009/04/01/configuring-a-read-only-replicated-folder.aspx
Please read the following notes carefully before deploying the read-only replicated folders feature.
a) Feature applicability: The read-only replicated folders feature is available only on replication member servers which are running Windows Server 2008 R2. In other words, it is not possible to configure a replicated folder to be read-only on a member server running either Windows Server 2003 R2 or Windows Server 2008.
b) Backwards compatibility: Only the server hosting read-only replicated folders needs to be running Windows Server 2008 R2. The member server that hosts a read-only replicated folder can replicate with partners that are on Windows Server 2003 or Windows Server 2008. However, to configure and administer a replication group that has a read-only replicated folder, you need to use the DFS Management MMC snap-in on Windows Server 2008 R2.
c) Administration of read-only replicated folders: In order to configure a replicated folder as read-only replicated folder, you need to use the DFS Management MMC snap-in on Windows Server 2008 R2. Older versions of the snap-in (available on Windows Server 2003 R2 or Windows Server 2008) cannot configure or manage a read-only replicated folder. In other words, these snap-ins will not display the option to mark a replicated folder 'read-only'.
d) Schema updates: If you have an older version of the schema (pre-Windows Server 2008), you will need to update your Active Directory schema to include the DFS Replication schema extensions for Windows Server 2008.
http://blogs.technet.com/b/filecab/archive/2009/01/21/read-only-replicated-folders-on-windows-server-2008-r2.aspx
Why deploy read-only replicated folders?
Consider the following scenario. Contoso Corporation has a replication infrastructure similar to that depicted in the diagram below. Reports are published to the datacenter server and these need to be distributed to Contoso's branch offices. DFS Replication is configured to replicate a folder containing these published reports between the datacenter server and branch office servers.
The DFS Replication service is a multi-master file replication engine – meaning that changes can be made to replicated data on any of the servers taking part in replication. The service then ensures that these changes are replicated out to all other members in that replication group and that conflicts are resolved using 'last-writerwins' semantics.



Now, a Contoso employee working in a branch office accidentally deletes the 'Specs' sub-folder from the replicated folder stored on that branch office's file server. This accidental deletion is replicated by the DFS Replication service, first to the datacenter server and then via that server to the other branch offices. Soon, the 'Specs' folder gets deleted on all of the servers participating in replication. Contoso's file server administrator now needs to restore the folder from a previously taken backup and ensure that the restored contents of the folder once again replicate to all branch office file servers.

Administrators need to monitor their replication infrastructure very closely in order to prevent such situations from arising or to recover lost data if needed. Strict ACLs are a way of preventing these accidental modifications from happening, but managing ACLs across many branch office servers and for large amounts of replicated data quickly degenerates into an administrative nightmare. In case of accidental deletions, administrators need to scramble to recover data from backups (often up-to-date backups are unavailable) and in the meantime, end-users face outages leading to loss of productivity.



This situation can be prevented by configuring read-only replicated folders on branch office file servers. A readonly replicated folder ensures that no local modifications can take place and the replica is kept in sync with a read-write enabled copy by the DFS Replication service. Therefore, read-only replicated folders enable easyto-deploy and low-administrative-overhead data publication solutions especially for branch office scenarios.

How does all this work?

For a read-only replicated folder, the DFS Replication service intercepts and inspects every file system operation. This is done by virtue of a file system filter driver that layers above every replicated folder that is configured to be read-only. Volumes that do not host read-only replicated folders or volumes hosting only readwrite replicated folders are ignored by the filter driver.

Only modifications initiated by the service itself are allowed – these modifications are typically caused by the service installing updates from its replication partners. This ensures that the read-only replicated folder is maintained in sync with a read-write enabled replicated folder on another replication partner (presumably located at the datacenter server).
All other modification attempts are blocked – this ensures that the contents of the read-only replicated folder cannot be modified locally. As shown in the below figure, end-users are unable to modify the contents of the replicated folder on servers where it has been configured to be read-only. The behavior is similar to that of a read-only SMB share – contents can be read and attributes can be queried for all files, however, modifications are not possible.

Question: 7

You need to recommend a solution for starting the servers in the San Francisco office from Windows Recovery Environment (Windows RE). The solution must meet the company's security requirements. What should you include in the recommendation?

A. an iSCSI initiator
B. the Multipath I/O feature
C. Wake On LAN
D. Windows Deployment Services (WDS)

Answer: D

Explanation:
All Servers are PXE enabled

Question: 8

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

Answer: B

Explanation:
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: 9

You are planning to upgrade the operating systems of the client computers in the finance department. You need to recommend a solution for App1 that meets the company's technical requirements. What should you include in the

recommendation?

A. Microsoft Application Virtualization (AppV)
B. RemoteApp and Desktop Connection
C. RD Gateway
D. Windows XP Mode

Answer: D

Explanation:
http://www.microsoft.com/oem/en/products/windows/pages/windows_xp_mode.aspx
Windows XP Mode: Providing Flexibility For You and Your Customers
We're committed to providing a smooth transition as your customers move to the Windows 7 operating system.
Many of them will upgrade from Windows XP and will require the flexibility to run their current Windows XP applications.
We're focused on providing you with the right tools to help customers achieve their goals to:
Maximize productivity.
Manage their technology infrastructure and total cost of ownership.
Designed for Small Business
Windows XP Mode is a new feature of Windows 7 Professional, Ultimate, and Enterprise. Many applications designed for Windows XP will run in Windows 7, but some legacy applications may not be compatible.
Windows XP Mode allows many of these applications to run right from the Windows 7 desktop. Benefits include:
Ease of use: Time is precious for small-business customers. Windows XP Mode utilizes Windows Virtual PC to launch Windows XP applications with a single click directly from the Windows 7 desktop.
Business continuity: In addition to enabling customers to run Windows XP applications virtually on a Windows 7-based PC, Windows XP Mode also supports many Windows XP devices—for instance, those connected to USB ports.
Cost management: Windows XP Mode extends the life of existing Windows XP applications and devices, and reduces the learning curve by using many familiar applications and devices.
Windows XP Mode Now Supported on PCs Without Virtualization-Enabled Processors
Microsoft has removed the virtualization-enabled processor requirement for Windows XP Mode on Windows 7 Professional and Ultimate. Windows XP Mode continues to use hardware virtualization such as Intel Virtualization Technology (Intel® VT) or the AMD-V™ chipset when available but it no longer requires them.
Microsoft has released an update that enables PCs without hardware virtualization to also take advantage of Windows XP Mode.

Question: 10

You need to recommend an RD Gateway configuration that meets the company's technical requirements. What should you recommend?

A. Create two Remote Desktop connection authorization policies (RD CAPs) and one Remote Desktop resource authorization policy (RD RAP).
B. Create one Remote Desktop connection authorization policy (RD CAP) and two Remote Desktop resource authorization policies (RD RAPs).
C. Create one Remote Desktop resource authorization policy (RD RAP) and deploy the Remote Desktop Connection Broker (RD Connection Broker) role service.
D. Create one Remote Desktop connection authorization policy (RD CAP) and deploy the Remote Desktop Connection Broker (RD Connection Broker) role service.

Answer: B

Explanation:
CAP=who can connect RAP=what resources are available
Connection Authorization Policies (CAP)
Terminal Services connection authorization policies (TS-CAPs) specify which users are allowed to connect through the TS Gateway Server to resources located on your organization's internal network. This is usually done by specifying a local group on the TS Gateway Server or a group within Active Directory. Groups can include user or computer accounts. You can also use TS-CAPs to specify whether remote clients use password or smart-card authentication to access internal network resources through the TS Gateway Server. You can use TS-CAPs in conjunction with NAP; this scenario is covered in more detail by the next lesson.
Resource Authorization Policies (RAP)
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: 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 App1ocker Group Policy settings
C. the IPSec enforcement method
D. Windows BitLocker Drive Encryption (BitLocker)

Answer: D

Explanation:
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

You need to recommend a solution for managing the service accounts for SQL1 and SQL2. The solution must meet the company's security requirements. What should you include in the recommendation?

A. Configure the service accounts as standard user accounts and perform manual password changes as required.
B. Configure the service accounts as managed service accounts.
C. Configure the service accounts as standard user accounts and use a Password Settings object (PSO) to allow different password settings.
D. Configure the service accounts as virtual accounts.

Answer: A

Explanation:
req - passwords to change every 60 days.
Service account passwords are set to never expire so can not meet the above requirement, so manual intervention is required.

Case Study: 7
A. Datum
Scenario
COMPANY OVERVIEW
A. Datum Corporation is a manufacturing company that has a main office and two branch offices. The main office is located in Denver. The branch offices are located in New York and Montreal. The main office has 10,000 users. Each branch office has approximately 200 users.
PLANNED CHANGES
A. Datum plans to deploy a new intranet site named Sitel in the main office. Two servers that run a Server Core installation of Windows Server 2008 R2 *are* requisitioned for the deployment of Site1. You plan to deploy a domain controller in each office. You have a new server named Backup1. All servers will be backed up remotely by using Windows Server Backup on Backup1.
BUSINESS GOALS
A. Datum has the following business goals:
- Changes to the environment must minimize costs.
- Changes to the environment must optimize the use of new hardware.
- The costs to manage the network infrastructure and the servers must be minimized.

EXISTING ENVIRONMENT
All servers run Windows Server 2008 R2. All client computers run Windows 7 Enterprise. The network contains a Web server named Web1. Web1 is located in the perimeter network and is accessible from the internal network and the Internet. Web1 runs a Server Core installation of Windows Server 2008 R2 Standard.
Existing Active Directory/Directory Services
The network contains a single Active Directory domain named adatum.com. The main office has two domain controllers.
Existing Network Infrastructure
Each office has a file server. The main office connects to each branch office by using a WAN link. Users in the branch offices frequently access the file server in the main office.
Current Administration Model
All domain administrators work in the main office and remotely manage the servers by using their Windows 7 computers. A group named Branch Admins has the rights to manage all of the client computers in the branch offices. You have several ADMX files that contain custom Application settings.
REQUIREMENTS
Security Requirements
The BranchAdmins group members must be able to install updates and drivers on the domain controllers in the branch offices. Passwords must not be stored by using reversible encryption. All authentication traffic on the network must be encrypted.
Application Requirements
A new Application named WebApp2 must be deployed on Web1. The WebApp2 deployment must meet the following requirements:
- Users must be authenticated to access WebApp2.
- WebApp2 must support Web browsers from various vendors.
- WebApp2 must be accessible to internal users and Internet users.

- A failure of WebApp2 must not cause other Web Applications to fail.
- Internet users must be required to configure the minimum number of changes on their client computers to access WebApp2.

Site1 must be configured to meet the following requirements:

- Site1 must support the most user connections possible.
- Site1 must be backed up every day by a remote server,
- If a single Web server fails, users must be able to access Site1.
- If a single Web server fails, users must not receive an error message when they access Site1.

Technical Requirements

You must ensure that domain administrators can access the ADMX files from any client computer that they use to manage Group Policies. You must ensure that the domain administrators are notified by e-mail each time a user copies video files to the file servers.

Question: 1

You need to recommend a solution for Group Policy that meets the company's technical requirements. What should you recommend?

A. Create a Central Store.
B. Enable folder redirection.
C. Modify the File Replication Service (FRS) settings for SYSVOL.
D. Configure SYSVOL to use Distributed File System (DFS) Replication.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc709647%28WS.10%29.aspx
Microsoft Windows Vista® and Windows Server 2008 introduce a new format for displaying registry-based policy settings. Registry-based policy settings (located under the Administrative Templates category in the Group Policy Object Editor) are defined using a standards-based, XML file format known as ADMX files. These new files replace ADM files, which used their own markup language. The Group Policy tools —Group Policy Object Editor and Group Policy Management Console—remain largely unchanged. In the majority of situations, you will not notice the presence of ADMX files during your day-to-day Group Policy administration tasks.

Question: 2

You need to recommend a strategy for the file servers that meets the company's technical requirements. What should you recommend?

A. Implement active file screens.
B. Implement passive file screens.
C. Configure classification rules.
D. Configure File Server Resource Manager (FSRM) quotas

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc732349%28WS.10%29.aspx
Create file screens to block files that belong to particular file groups from being saved on a volume or in a folder tree.

A file screen affects all folders in the designated path. For example, you might create a file screen to prevent users from storing audio and video files in their personal folders on the server.
You can configure File Server Resource Manager to generate e-mail or other notifications when a file screening event occurs.
A file screen can be either active or passive:
-Active screening prevents users from saving unauthorized file types on the server.
-Passive screening monitors users saving specific file types and generates any configured notifications, but does not prevent users from saving files.

Question: 3

You need to recommend an availability solution for Site1 that meets the company's Application requirements and business goals. What should you include in the recommendation?

A. hardware load balancing
B. Network Load Balancing (NLB)
C. round robin DNS
D. Windows Failover Clustering

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc725691.aspx
The Network Load Balancing (NLB) feature in Windows Server 2008 R2 enhances the availability and scalability of Internet server applications such as those used on Web, FTP, firewall, proxy, virtual private network (VPN), and other mission-critical servers. A single computer running Windows Server 2008 R2 provides a limited level of server reliability and scalable performance. However, by combining the resources of two or more computers running one of the products in Windows Server 2008 R2 into a single virtual cluster, NLB can deliver the reliability and performance that Web servers and other mission-critical servers need.

Question: 4

You need to recommend changes to Web1 that meet the company's Application requirements for the WebApp2 deployment. What should you recommend?

A. Add a second IP address.
B. Configure request filtering.
C. Create separate Application pools.
D. Add worker processes to the DefaultAppPool.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc753449%28WS.10%29.aspx
An application pool is a group of one or more URLs that are served by a worker process or a set of worker processes. Application pools set boundaries for the applications they contain, which means that any applications that are running outside a given application pool cannot affect the applications in the application pool.
Application pools offer the following benefits:
Improved server and application performance. You can assign resource-intensive applications to their own application pools so that the performance of other applications does not decrease.

Improved application availability. If an application in one application pool fails, applications in other application pools are not affected.
Improved security. By isolating applications, you reduce the chance that one application will access the resources of another application.
In IIS 7, application pools run in one of two modes: integrated mode and classic mode. The application pool mode affects how the server processes requests for managed code. If a managed application runs in an application pool with integrated mode, the server will use the integrated, request-processing pipelines of IIS and ASP.NET to process the request. However, if a managed application runs in an application pool with classic mode, the server will continue to route requests for managed code through Aspnet_isapi.dll, processing requests the same as if the application was running in IIS 6.0.
Most managed applications should run successfully in application pools with integrated mode, but you may have to run in classic mode for compatibility reasons. Test the applications that are running in integrated mode first to determine whether you really need classic mode.

Question: 5

You need to recommend a strategy for managing the domain controllers in the branch offices that meets the company security requirements. What should you include in the recommendation?

A. Configure Administration Role Separation.
B. Add the BranchAdmins group to the Domains Admins group.
C. Add the BranchAdmins group to the Server Operators group.
D. Assign the permission for the domain controller computer objects to the BranchAdmins group.

Answer: B

Question: 6

You need to recommend a security strategy for WebApp2 that meets the company's Application requirements. What should you include in the recommendation?

A. Basic authentication and SSL
B. Digest authentication and SSL
C. Digest authentication and SSL VPN
D. Basic authentication and SSL VPN

Answer: A

Explanation:
You must support multiple browsers and one advantage of the basic access authentication is all web browsers support it. But due to the fact that the username and password are passed in cleartext, it is rarely used by itself on publicly accessible Internet web sites. However, it is somewhat commonly found on publicly accessible sites if combined with SSL/TLS (HTTPS). The use of SSL/TLS to encrypt the entire connection mitigates the fact that the Basic passwords themselves are not encrypted. Most browsers will actually display an alert of some kind if a site uses Basic Auth without SSL/TLS, but will not display an alert when Basic Auth is used on a connection that has SSL/TLS enabled.

Question: 7

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.

Answer: B, C

Question: 8

You need to recommend a security strategy for WebApp2 that meets the company's application requirements. What should you include in the recommendation?

A. Basic authentication and connection security rules
B. Basic authentication and SSL
C. Digest authentication and connection security rules
D. Digest authentication and SSL

Answer: B

Explanation:
You must support multiple browsers and one advantage of the basic access authentication is all web browsers support it. But due to the fact that the username and password are passed in cleartext, it is rarely used by itself on publicly accessible Internet web sites. However, it is somewhat commonly found on publicly accessible sites if combined with SSL/TLS (HTTPS). The use of SSL/TLS to encrypt the entire connection mitigates the fact that the Basic passwords themselves are not encrypted. Most browsers will actually display an alert of some kind if a site uses Basic Auth without SSL/TLS, but will not display an alert when Basic Auth is used on a connection that has SSL/TLS enabled.

Case Study: 8
Graphic Design Institute, Case A
Scenario
COMPANY OVERVIEW
Graphic Design Institute is a training company that has a main office and 10 branch offices. The main office is located in Bangalore.
PLANNED CHANGES
Graphic Design Institute plans to implement the following changes:
- Deploy a new two-node failover cluster that runs the Hyper-V server role on each node.
- Ensure that intra-cluster network traffic is isolated from all other network traffic.
- Implement Network Access Protection (NAP) for all of the client computers on the internal network and for all of the client computers that connect remotely.

EXISTING ENVIRONMENT
The relevant servers in the main office are configured as shown in the following table.

Server name	Operating system	Server role or role service
Web1	Windows Server 2008 R2	Web Server (IIS)
Web2	Windows Server 2008 R2	Web Server (IIS)
Web3	Windows Server 2008 R2	Web Server (IIS)
WSUS1	Windows Server 2008 R2	Windows Server Update Services (WSUS)
NPAS1	Windows Server 2008 R2	Network Policy and Access Services (NPAS)

The server has the following configurations:

- NPAS1 contains a static IP address pool,
- Web1, Web2, and Web3host a copy of the corporate Web site.
- Web1, Web2, and Web3 are located in the perimeter network and belong to a workgroup.

All client computers run Windows XP Professional, Windows Vista Enterprise, or Windows 7 Enterprise, All client computers *are* members of the domain.

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

Existing Active Directors/Directory Services

The network contains a single-domain Active Directory forest named graphicdesigninstitute.com. The Active Directory Recycle Bin is enabled.

Existing Network Infrastructure

Graphic Design Institute has an internal network and a perimeter network.

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

TECHNICAL REQUIREMENTS

All of the accounts used for administration must be assigned the minimum amount of permissions.

Web1, Web2, and Web3 must have the identical configurations for the corporate Web site. The Web servers must contain a local copy of all the Web pages in the Web site. When a Web page is modified on any of the Web servers, the modifications must be copied automatically to all of the Web servers.

A user named Admin1 must be responsible for performing the following tasks:

- Restarting all of the Web servers.
- Backing up and restoring the files on all of the Web servers.

A user named Admin2 must be responsible for performing the following tasks:

- Backing up the Active Directory database.
- Recovering deleted objects from the Active Directory Recycle Bin.

Question: 1

You need to recommend a solution for configuring the Web servers. The solution must meet the company's technical requirements. What should you include in the recommendations?

A. Active Directory Lightweight Directory Services (AD LDS)
B. Failover Clustering
C. HTTP redirection
D. IIS Shared Configuration

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/cc731992%28WS.10%29.aspx
The Shared Configuration feature enables you to do the following actions:
Configure the Web server to use configuration files and encryption keys from a central location.
Export the configuration files and encryption keys from your Web server to a central location that can be shared with other servers or used to store a backup copy of configuration files and encryption keys.
This is useful when you have a Web farm and want each Web server in the farm to use the same configuration files and encryption keys.

Question: 2

You need to ensure that Web1, Web2, and Web3 download updates from WSUS1. What should you do?

A. Modify the Default Domain Policy Group Policy object (GPO).
B. Modify the local computer policy on Web1, Web2, and Web3.
C. Import a security policy template toWeb1, Web2, and Web3.
D. Create a service location (SRV) record in the _msdcs.graphicsdesigninstitute.com DNS zone.

Answer: B

Explanation:
Servers belong to a work group so WSUS policy cant be applied using AD GPO. but the local security policy can be modified to point to the WSUS server

Question: 3

Which NAP enforcement method should you recommend?

A. 802.1x
B. DHCP
C. IPSec
D. VPN

Answer: C

Explanation:
Requirements/information:
Implement Network Access Protection (NAP) for all of the client computers on the internal network and for all of the client computers that connect remotely
Some users work remotely. To access the company's internal resources, the remote users use a VPN connection to NPAS1.
The network contains network switches and wireless access points (WAPs) from multiple vendors Some of the network devices are more than 10 years old and do not support portbased authentication.
Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer's identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.
NAP Enforcement Methods
When a computer is found to be noncompliant with the enforced health policy, NAPenforces limited network access.

This is done through an Enforcement Client (EC). Windows Vista, Windows XP Service Pack 3, and Windows Server 2008 include NAPEC support for IPsec, IEEE 802.1X, Remote Access VPN, and DHCP enforcement methods. Windows Vista and Windows Server 2008 also support NAP enforcement for Terminal Server Gateway connections.
NAP enforcement methods can either be used individually or can be used in conjunction with each other to limit the network access of computers that are found not to be in compliance with configured health policies. Hence you can apply the remote access VPN and IPsec enforcement methods to ensure that internal clients and clients coming in from the Internet are only granted access to resources if they meet the appropriate client health benchmarks.
802.1X step-by-step guide.
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8a0925ee-ee06-4dfbbba2-07605eff0608&displaylang=en
802. 802.1X Enforcement
When 802.1X is used—over either wired or wireless networks—the client device's access is restricted by network infrastructure devices such as wireless connection points and switches. Until the device has demonstrated its compliance, client access is restricted.
Restriction is enforced on the network access device using an access control list (ACL) or by placing the client device on restricted virtual local area networks (VLANs). The 802.1X standard is more complex to deploy than DHCP, but it provides a high degree of protection.
as a requirement of 802.1 is port authentication and some of the devices ate 10+ years old and do not support this then then this rules out this method
IPSEC ENFORCEMENT
IPsec enforcement works by applying IPsec rules. Only computers that meet health compliance requirements are able to communicate with each other. IPsec enforcement can be applied on a per-IP address, per-TCP port number, or per-UDP port number basis. For example: You can use IPsec enforcement to block RDP access to a web server so that only computers that are healthy can connect to manage that server but allow clients that do not meet health requirements to connect to view Web pages hosted by the same web server.
IPsec is the strongest method of limiting network access communication through NAP. Where it might be possible to subvert other methods by applying static addresses or switching ports, the IPsec certificate used for encryption can be obtained by a host only when it passes the health check. No IPsec certificate means that communication with other hosts that encrypt their communications using a certificate issued from the same CA is impossible.
VPN Enforcemement
VPN enforcement is used on connecting VPN clients as a method of ensuring that clients granted access to the internal network meet system health compliance requirements. VPN enforcement works by restricting network access to noncompliant clients through the use of packet filters. Rather than being able to access the entire network, incoming VPN clients that are noncompliant have access only to the remediation server group.
As is the case with 802.1X enforcement, the health status of a connected client is monitored continuously. If a client becomes noncompliant, packet filters restricting network access will be applied. If a noncompliant client becomes compliant, packet filters restricting network access will be removed. VPN enforcement requires an existing remote access infrastructure and an NPS server. The enforcement method uses the VPN EC, which is included with Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.
DHCP NAP Enforcement
DHCP NAP enforcement works by providing unlimited-access IPv4 address information to compliant computers and limited-access IPv4 address information to noncompliant computers. Unlike VPN and 802.1X enforcement methods, DHCP NAP enforcement is applied only when a client lease is obtained or renewed. Organizations using this method of NAP enforcement should avoid configuring long DHCP leases because this will reduce the
frequency at which compliance checks are made.
To deploy DHCP NAP enforcement, you must use a DHCP server running Windows Server 2008 or Windows Server 2008 R2 because this includes the DHCP Enforcement Service (ES). The DHCP EC is included in the DHCP Client service on Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.
The drawback of DHCP NAP enforcement is that you can get around it by configuring a client's IP address statically. Only users with local administrator access can configure a manual IP, but if your organization gives users local administrator access, DHCP NAP enforcement may not be the most effective method of keeping these computers off

the network until they are compliant.

Question: 4

You need to recommend the server configurations for the new failover cluster. The configurations must support the company's planned changes. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

A. From HyperV Manager on each node, configure one virtual network.
B. From HyperV Manager on one node, configure two virtual networks.
C. Install one network adapter on each node. Configure the network adapters to use multiple IP addresses.
D. Install two network adapters on each node. Configure the network adapters to communicate on separate subnets.

Answer: A, D

Explanation:
There's only a need for one virtual network because a virtual network is the same as a virtual switch and there is no requirement for a separate switch your requirement is to have inter cluster network traffic isolated from other network traffic by creating separate subnets you can ensure that cluster related traffic remains on one subnet while regular network traffic is carried on the other subnet

Question: 5

You need to ensure that Admin2 can administer Active Directory to meet the company's technical requirements. What should you do?

A. Add Admin2 to the Domain Admins global group.
B. Add Admin2 to the Backup Operators domain local group.
C. Delegate full control ofall objects in graphicdesigninstitute.com to Admin2.
D. Delegate full control of all objects in the Domain Controllers organizational unit (OU) to Admin2.

Answer: A

Explanation:
You can enable Active Directory Recycle Bin only if the forest functional level of your environment is set to Windows Server 2008 R2. Membership in Domain Admins, or equivalent, is the minimum required to use AD recycle bin

Question: 6

You need to recommend a solution for the Web server content that meets the company's technical requirements. What should you include in the recommendation?

A. Distributed File System (DFS) Replication
B. folder redirection
C. HTTP redirection
D. IIS Shared Configuration

Answer: A

Explanation:
AD is a prerequisite for DFS and we have workgroup in the perimeter network
By using Shared Configuration, you can share your IIS configuration across multiple servers. Please note that this article is focused on the back end configuration of the web servers and not the front end task of load balancing the servers.
Shared Configuration allows you to set up Internet Information Services (IIS) quickly and easily on multiple servers so that the sites, application pools and IIS server settings are consistent across two or more servers.
You only have to configure a server one time and then you can replicate the IIS settings. Shared Configuration is not for individual sites on a server but for the entire IIS configuration on a server.

Question: 7

You need to ensure that Admin1 can administer the Web servers to meet the company's technical requirements. To which group should you add Admin1?

A. the Administrators local group on each Web server
B. the Backup Operators domain local group
C. the Backup Operators local group on each Web server
D. the Domain Admins global group

Answer: C

Explanation:
The requirements are:
Restarting all of the Web servers.
Backing up and restoring the files on all of the Web servers
Backup Operators
Members of this group can back up and restore files on a computer, regardless of any permissions that protect those files. This is because the right to perform a backup takes precedence over all file permissions. Members of this group cannot change security settings.
1. Access this computer from the network
2. Allow logon locally
3. Back up files and directories
4. Bypass traverse checking
5. Log on as a batch job
6. Restore files and directories
7. Shut down the system

Case Study: 9
Litware, Inc
Scenario
COMPANY OVERVIEW
Litware, Inc. is a manufacturing company that has a main office and two branch office. The main office is located in Montreal. The branch offices *are* located in Seattle and New York. The main office has 4,000 users. The branch offices each have 500 users.
PLANNED CHANGES
Litware plans to open a new sales office. The sales office will have a direct connection to the Internet. The sales office will have a single server. The sales office requires a connection to the Montreal office. The connection to the Montreal office must use either TCP port 80 or TCP port 443. The network currently

contains a Fibre Channel Storage Area Network (SAN). A new iSCSI SAN will be implemented during the next month. The current SAN and the new SAN are from different manufacturers. Both SANs use a virtual disk service (VDS) interface.

EXISTING ENVIRONMENT

All servers run Windows Server 2008 R2. All client computers run Windows 7 Enterprise. The main office has a single DHCP server. The IP addresses for all of the client computers must be assigned from the DHCP server. All software is installed from a central software distribution point in the main office. Software deployments for the branch offices frequently fail due to bandwidth limitations.

Existing Active Directory/Directory Services

The network contains a single Active Directory domain named litwareinc.com. Each office has two domain controllers.

Current Administration Model

Currently, all help desk users have full administrator rights to the servers. The help desk users use Remote Desktop to log on to the servers and perform tasks such as managing Active Directory user accounts and creating DHCP reservations.

TECHNICAL REQUIREMENTS

Windows Firewall must be managed by using the minimum amount of administrative effort. Windows Firewall configurations must be duplicated easily between servers that have the same server role. Litware must centralize the monitoring of critical system events. The monitoring solution must use the existing infrastructure. Litware plans to prevent help desk users from interactively logging on to servers. Help desk users must not have full administrator rights to the servers.

The software deployment process must be updated to meet the following requirements:

- Application source files must be centrally managed.
- Software deployments to the offices in Seattle and New York must remain unaffected if a WAN link fails.

The SANs must be administered by using a single tool.

Question: 1

You need to recommend changes to the software deployment process that meet the company's technical requirements. What should you include in the recommendation?

A. BranchCache in Distributed Cache mode
B. BranchCache in Hosted Cache mode
C. domain-based Distributed File System (DFS)
D. standalone Distributed File System (DFS)

Answer: C

Explanation:
Software is installed and managed from a central location, so regardless of where a user is in the network the share for the installation files should appear to be the same, this is done using DFS Namespaces. There is one AD Domain and each Office also has 2 DCs so you can add the updated files in the HQ and then use DFS replication to replicate the new files to the branch namespace servers Distributed File System (DFS) Namespaces and DFS Replication offer simplified, highly-available access to files, load sharing, and WAN-friendly replication. In the Windows Server® 2003 R2 operating system, Microsoft revised and renamed DFS Namespaces (formerly called DFS), replaced the Distributed File System snap-in with the DFS Management snap-in, and introduced the new DFS Replication feature. In the Windows Server® 2008 operating system, Microsoft added the Windows Server 2008 mode of domain-based namespaces and added a number of usability and performance improvements.

What does Distributed File System (DFS) do?
The Distributed File System (DFS) technologies offer wide area network (WAN)-friendly replication as well as simplified, highly-available access to geographically dispersed files. The two technologies in DFS are the following:
DFS Namespaces. Enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. This structure increases availability and automatically connects users to shared folders in the same Active Directory Domain Services site, when available, instead of routing them over WAN connections.
DFS Replication. DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the AD DS SYSVOL folder in domains that use the Windows Server 2008 domain functional level.
in respect to answers A or B these may possibly work but this test http://www.sustainableit.co.za/wp-content/uploads/downloads/2010/09/Is_BranchCache_right_for_software_distribution.pdf would suggest its not the most efficient solution.

Question: 2

You need to recommend a tool to manage the SANs. The tool must support the company's planned changes and technical requirements. Which tool should you recommend?

A. Disk Management
B. Share and Storage Management
C. Storage Explorer
D. Storage Manager for SANs

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc754551%28WS.10%29.aspx
Storage Manager for SANs is a Microsoft Management Console (MMC) snap-in that helps you create and manage logical unit numbers (LUNs) on Fibre Channel and Internet SCSI (iSCSI) disk drive subsystems that support Virtual Disk Service (VDS) in your storage area network (SAN).

Question: 3

You need to recommend a VPN solution for the new sales office. The solution must support the company's planned changes. What should you include in the recommendation?

A. Internet Key Exchange version 2 (IKEv2)
B. Layer 2 Tunneling Protocol (L2TP)
C. PointtoPoint Tunneling Protocol (PPTP)
D. Secure Socket Tunneling Protocol (SSTP)

Answer: D

Explanation:
http://support.microsoft.com/kb/947032
SSTP is a new kind of Virtual Private Networking (VPN) tunnel that is available in the Routing and Remote Access Server role in Windows Server 2008. SSTP allows for Point-to-Point Protocol (PPP) packets to be encapsulated over HTTP. This allows for a VPN connection to be more easily established through a firewall or through a Network Address

Translation (NAT) device. Also, this allows for a VPN connection to be established through an HTTP proxy device.
The information is this article is more likely to apply to a small-sized or medium-sized organization. For these kinds of organizations, it is common to have one public IP address that is assigned to the external interface of a NAT router or of a gateway device. This article describes the following scenario:
You have a Windows Server 2008-based Secure Socket Tunneling Protocol (SSTP)-based VPN server.
The server is assigned a private IP address.
The server is located on an internal network behind a NAT device.

Question: 4

You need to recommend a solution for managing all of the servers. The solution must meet the company's technical requirements. What should you include in the recommendation?

A. Remote Server Administration Tools (RSAT)
B. the Administration Tools Pack (adminpak.msi)
C. the Remote Desktop Gateway (RD Gateway) role service
D. the Remote Desktop Web Access (RD Web Access) role service

Answer: A

Explanation:
http://support.microsoft.com/kb/941314
Microsoft Remote Server Administration Tools (RSAT) enables IT administrators to remotely manage roles and features in Windows Server 2008 from a computer that is running Windows Vista with Service Pack 1 (SP1). It includes support for remote management of computers that are running either a Server Core installation option or a full installation option of Windows Server 2008. It provides similar functionality to the Windows Server 2003 Administration Tools Pack.

Question: 5

You need to recommend an IP addressing strategy for the client computers in the new sales office. What should you recommend implementing in the new sales office?

A. DHCP server roles
B. the DirectAccess feature
C. the Network Policy Server (NPS) role service
D. the Remote Access Service role service

Answer: D

Explanation:
The Routing and Remote Access service in Windows Server® 2008 supports remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections. Routing and Remote Access consists of the following components:
Remote Access
The remote access feature provides VPN services so that users can access corporate networks over the Internet as if they were directly connected. Remote access also enables remote or mobile workers who use dial-up communication links to access corporate networks.
Routing
Routing and Remote Access is a full-featured software router and an open platform for routing and networking.

It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments or over the Internet by using secure VPN connections. Routing is used for multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services.

Routing

A router is a device that manages the flow of data between network segments, or subnets. A router directs incoming and outgoing packets based on the information it holds about the state of its own network interfaces and a list of possible sources and destinations for network traffic. By projecting network traffic and routing needs based on the number and types of hardware devices and applications used in your environment, you can better decide whether to use a dedicated hardware router, a software-based router, or a combination of both. Generally, dedicated hardware routers handle heavier routing demands best, and less expensive software-based routers are sufficient to handle lighter routing loads.

A software-based routing solution, such as the Routing and Remote Access service in Windows Server® 2008, can be ideal on a small, segmented network with relatively light traffic between subnets. Conversely, enterprise network environments that have a large number of network segments and a wide range of performance requirements might need a variety of hardware-based routers to perform different roles throughout the network.

Remote access

By configuring Routing and Remote Access to act as a remote access server, you can connect remote or mobile workers to your organization's networks. Remote users can work as if their computers are physically connected to the network.

All services typically available to a LAN-connected user (including file and print sharing, Web server access, and messaging) are enabled by means of the remote access connection. For example, on a server running Routing and Remote Access, clients can use Windows Explorer to make drive connections and to connect to printers. Because drive letters and universal naming convention (UNC) names are fully supported by remote access, most commercial and custom applications work without modification.

A server running Routing and Remote Access provides two different types of remote access connectivity:

Virtual private networking (VPN) VPN is the creation of secured, point-to-point connections across a private network or a public network such as the Internet. A VPN client uses special TCP/IP-based protocols called tunneling protocols to make a virtual call to a virtual port on a VPN server. The best example of virtual private networking is that of a VPN client that makes a VPN connection to a remote access server that is connected to the Internet. The remote access server answers the virtual call, authenticates the caller, and transfers data between the VPN client and the corporate network.

In contrast to dial-up networking, VPN is always a logical, indirect connection between the VPN client and the VPN server over a public network, such as the Internet. To ensure privacy, you must encrypt data sent over the connection.

Dial-up networking In dial-up networking, a remote access client makes a nonpermanent, dial-up connection to a physical port on a remote access server by using the service of a telecommunications provider, such as analog phone or ISDN. The best example of dial-up networking is that of a dial-up networking client that dials the phone number of one of the ports of a remote access server.

Dial-up networking over an analog phone or ISDN is a direct physical connection between the dial-up networking client and the dial-up networking server. You can encrypt data sent over the connection, but it is not required.

Question: 6

You need to recommend a process for monitoring the servers. The process must meet the company's technical requirements. What should you include in the recommendation?

A. event subscriptions
B. Data Collector Sets (DCSs)
C. Resource Monitor
D. Microsoft System Center Operations Manager

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc749183.aspx
Event Viewer enables you to view events on a single remote computer. However, troubleshooting an issue might require you to examine a set of events stored in multiple logs on multiple computers.
Windows Vista includes the ability to collect copies of events from multiple remote computers and store them locally. To specify which events to collect, you create an event subscription. Among other details, the subscription specifies exactly which events will be collected and in which log they will be stored locally. Once a subscription is active and events are being collected, you can view and manipulate these forwarded events as
You would any other locally stored events.
Using the event collecting feature requires that you configure both the forwarding and the collecting computers.
The functionality depends on the Windows Remote Management (WinRM) service and the Windows Event Collector (Wecsvc) service. Both of these services must be running on computers participating in the forwarding and collecting process. To learn about the steps required to configure event collecting and forwarding computers, see Configure Computers to Forward and Collect Events.

Question: 7

You need to recommend a strategy for managing Windows Firewall that meets the company's technical requirements. What should you include in the recommendation?

A. domainbased Group Policy objects (GPOs)
B. local Group Policy objects (GPOs)
C. Starter Group Policy objects (GPOs)
D. System Starter Group Policy objects (GPOs)

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/ee461027.aspx
The Windows PowerShell command-line and scripting language can be used to automate many Group Policy tasks, including configuring registry-based policy settings and various Group Policy Management Console (GPMC) tasks. To help you perform these tasks, the Group Policy module for Windows PowerShell provides the cmdlets covered in this section.
You can use these Group Policy cmdlets to perform the following tasks for domain-based Group Policy objects (GPOs):
Maintain GPOs: GPO creation, removal, backup, reporting, and import.
Associate GPOs with Active Directory Directory Services (AD DS) containers: Group Policy link creation, update, and removal.
Set inheritance and permissions on AD DS organizational units (OUs) and domains.
Configure registry-based policy settings and Group Policy Preferences Registry settings.

Case Study: 10
Fabrikam Inc
Scenario
COMPANY OVERVIEW
Fabrikam Inc. is a manufacturing company that has a main office and a branch office.
PLANNED CHANGES
You plan to deploy a failover cluster named Cluster1 in the branch office. Cluster1 will be configured to meet the following requirements:
- The cluster will host eight virtual machines (VMs).

- The cluster will consist of two nodes named Node1 and Node2.
- The quorum mode for the cluster will be set to Node and Disk Majority.
- A user named Admin1 will configure the virtual switch configuration of the VMs.
- The cluster nodes will use shared storage on an iSCSI Storage Area Network (SAN).

You plan to configure a VM named File2 as a file server. Users will store confidential files on File2. You plan to deploy a Microsoft Forefront Threat Management Gateway (TMG) server in each site. The Forefront TMG server will be configured as a Web proxy.

EXISTING ENVIRONMENT

The research department is located in the branch office. Research users frequently travel to the main office.

Existing Active Directory/Directory Services

The network contains a single-domain Active Directory forest named fabrikam.com. The functional level of the forest is Windows Server 2008. The relevant organizational units (OUs) for the domain are configured as shown in the following table.

OU name	OU description
Main Office Users	Users in the main office
Main Office Computers	Computers in the main office
Main Office Servers	Servers in the main office
Branch Office Users	Users in the branch office
Branch Office Computers	Computers in the branch office
Branch Office Servers	Servers in the branch office
Domain Controllers	Domain controllers

The relevant sites for the network are configured shown in the following table.

Active Directory site name	Site description
MainOfficeSite	Main office
BranchOfficeSite	Branch office

The relevant group policy objects (GPOs) are configured as shown in the following table.

GPO name	Linked to
Default Domain Policy	Fabrikam.com domain
Default Domain Controllers Policy	Domain Controllers OU
GPO1	Fabrikam.com domain
GPO2	Main Office Computers OU
GPO3	Branch Office Computers OU
GPO4	MainOfficeSite site
GPO5	BranchOfficeSite site

Existing Network Infrastructure

All users run windows server 2008 R2. The relevant servers are configured as shown in following table.

Server name	Role service	Server site
File1	File Services	MainOfficeSite
DC1	Active Directory Domain Services (AD DS)	MainOfficeSite
DC2	Active Directory Domain Services (AD DS)	MainOfficeSite
WSUS1	Windows Server Update Services (WSUS)	MainOfficeSite
WSUS2	Windows Server Update Services (WSUS)	MainOfficeSite

WSUS2 is configured as a downstream replica server. File1 contains a share named Templates. Users access the Templates share by using the path \\fabrikam.com\dfs\templates. File1 has the Distributed File System (DFS) Replication role service and the DFS Namespaces role service installed.

TECHNICAL REQUIREMENTS

- Fabrikam must meet the following requirements:

- Minimize the cost of IT purchases.
- Minimize the potential attack surface on the servers.
- Minimize the number of rights assigned to administrators.
- Minimize the number of updates that must be installed on the servers.
- Ensure that Internet Explorer uses the local ForeFront TMG server to connect to the Internet.
- Ensure that all client computers continue to receive updates from WSUS if a WSUS server fails.
- Prevent unauthorized users from accessing the data stored on the VMs by making offline copies of the VM files.

Fabrikam must meet the following requirements for the Templates share:

- Ensure that users access the files in the Templates share from a server in their local site.
- Ensure that users always use the same UNC path to access the Templates share, regardless of the site in which the users are located.

Question: 1

You need to configure Internet Explorer to meet the company's technical requirements. Which GPO or GPOs should you modify?

A. Default Domain Policy
B. GPO1
C. GPO2 and GPO3
D. GPO4 and GPO5

Answer: D

Explanation:
The company has 2 sites
He following list contains example applications of policy:
A GPO linked to a site applies to all users and computers in the site.
A GPO applied to a domain applies to all users and computers in the domain and, by inheritance, to all users and computers in child organizational units. Be aware that policy is not inherited across domains.
A GPO applied to an organizational unit applies directly to all users and computers in the organizational unit and, by inheritance, to all users and computers in child organizational units.

Question: 2

You need to recommend the minimum number of logical unit numbers (LUNs) that must be provisioned for Cluster1. The recommendation must support the company's planned changes.
Which number should you recommend?

A. 1
B. 2
C. 8
D. 9

Answer: B

Explanation:

LUN Stands for "Logical Unit Number." LUNs are used to identify SCSI devices, such as external hard drives, connected to a computer. Each device is assigned a LUN, from 0 to 7, which serves as the device's unique address.
LUNs can also be used for identifying virtual hard disk partitions, which are used in RAID configurations. For example, a single hard drive may be partitioned into multiple volumes. Each volume can then be assigned a unique LUN.
A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover).
Users experience a minimum of disruptions in service.
In simple terms, the quorum for a cluster is the number of elements that must be online for that cluster to continue running. In effect, each element can cast one “vote” to determine whether the cluster continues running. The voting elements are nodes or, in some cases, a disk witness or file share witness. Each voting element (with the exception of a file share witness) contains a copy of the cluster configuration, and the Cluster service works to keep all copies synchronized at all times.
There are four quorum modes:
Node Majority: Each node that is available and in communication can vote. The cluster functions only with a majority of the votes, that is, more than half.
Node and Disk Majority: Each node plus a designated disk in the cluster storage (the “disk witness”) can vote, whenever they are available and in communication. The cluster functions only with a majority of the votes, that is, more than half.
Node and File Share Majority: Each node plus a designated file share created by the administrator (the “file share witness”) can vote, whenever they are available and in communication. The cluster functions only with a majority of the votes, that is, more than half.
No Majority: Disk Only: The cluster has quorum if one node is available and in communication with a specific disk in the cluster storage.
Choosing the quorum mode for a particular cluster
The following table describes clusters based on the number of nodes and other cluster characteristics, and lists the quorum mode that is recommended in most cases.
A “multi-site” cluster is a cluster in which an investment has been made to place sets of nodes and storage in physically separate locations, providing a disaster recovery solution.

Description of cluster
Odd number of nodes
Even number of nodes (but not a multi-site cluster)
Even number of nodes, multi-site cluster
Even number of nodes, no shared storage

as the Quorum will be set to Node And Disk Majority this means we need an even number of nodes which we have (node1 & node2)

Question: 3

You need to recommend a strategy for delegating administrative rights to Admin1. The strategy must support the company's planned changes. What should you include in the recommendation?

A. the Authorization Manager snapin on Node1 and Node2
B. the Authorization Manager snapin on the VMs
C. the Network Configuration Operators local group on each VM

D. the Network Configuration Operators local group on Node1 and Node2

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc731364.aspx
An authorization store can contain authorization policy information for many applications in a single policy store. All applications in one authorization store can access all of the groups defined at the store level.
You must be assigned to the Authorization Manager Administrator user role to complete this procedure. By default, Administrators is the minimum Windows group membership assigned to this role. Review the details in "Additional considerations" in this topic

Question: 4

You need to configure Windows Update to meet the company's technical requirements. What should you do?

A. Configure WSUS2 as an autonomous server.
B. Create a Network Load Balancing (NLB) cluster.
C. Create multiple Host (A) records and use round robin DNS.
D. Configure multiple service location (SRV) records and use round robin DNS.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/dd939896%28WS.10%29.aspx
Network load balancing (NLB) is an optional feature of Windows Server that load balances network traffic for high availability. You can install Windows Server Update Services (WSUS) 3.0 SP2 in a network that uses NLB, but this configuration requires that you perform additional steps during WSUS setup.

Question: 5

You need to protect the confidential data files on File2 against unauthorized offline access. What should you use?

A. Encrypting File System (EFS) on File2
B. file screens on Node1 and Node2
C. NTFS permissions on File2
D. Windows BitLocker Drive Encryption (BitLocker) on Node1 and Node2

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc749610%28WS.10%29.aspx
Per-user encryption of offline files Offline copies of files from remote servers can also be encrypted by using EFS. When this option is enabled, each file in the offline cache is encrypted with a public key from the user who cached the file. Thus, only that user has access to the file, and even local administrators cannot read the file without having access to the user's private keys.

Question: 6

You need to recommend a file access solution for the Templates share. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

A. Add File2 as a namespace server for \\fabrikam.com\dfs.
B. Add \\File2\templates as a folder target for \\fabrikam.com\dfs\templates.
C. In the Group Policy preferences of GPO2 and GPO3, add new mapped drives.
D. Create a DFS Replication group that contains \\File1\templates and \\File2\templates.

Answer: B, D

Explanation:
http://technet.microsoft.com/en-us/library/cc753479%28WS.10%29.aspx
Distributed File System (DFS) Namespaces and DFS Replication offer simplified, highly-available access to files, load sharing, and WAN-friendly replication. In the Windows Server® 2003 R2 operating system, Microsoft revised and renamed DFS Namespaces (formerly called DFS), replaced the Distributed File System snap-in with the DFS Management snap-in, and introduced the new DFS Replication feature. In the Windows Server® 2008 operating system, Microsoft added the Windows Server 2008 mode of domain-based namespaces and added a number of usability and performance improvements.
What does Distributed File System (DFS) do?
The Distributed File System (DFS) technologies offer wide area network (WAN)-friendly replication as well as simplified, highly-available access to geographically dispersed files. The two technologies in DFS are the following:
DFS Namespaces. Enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. This structure increases availability and automatically connects users to shared folders in the same Active Directory Domain Services site, when available, instead of routing them over WAN connections.
DFS Replication. DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the AD DS SYSVOL folder in domains that use the Windows Server 2008 domain functional level.

Question: 7

You need to recommend an operating system for Node1 and Node2. The recommendation must meet the company's technical requirements. Which operating system image should you install?

A. a full installation of Windows Server 2008 R2 Enterprise
B. a full installation of Windows Server 2008 R2 Standard
C. a Server Core installation of Windows Server 2008 R2 Enterprise
D. a Server Core installation of Windows Server 2008 R2 Standard

Answer: C

Explanation:
By using server core you minimize the surface attack area

Case Study: 11
Nothwind Traders
Scenario
COMPANY OVERVIEW
Northwind Traders is an import/export company that has a main office and two branch offices. The main

office is located in Toronto. The branch offices are located in Vancouver and Seattle. The main office has 2,000 users. Each branch office has 500 users.

EXISTING ENVIRONMENT

All client computers run Windows 7 Enterprise. All servers run Windows Server 2008 R2. All new servers are deployed by using Windows Deployment Services (WDS).

Northwind Traders has multiple Hyper-V servers. The Hyper-V servers *are* managed by using Microsoft System Center Virtual Machine Manager (VMM).

The perimeter network contains a standalone server. The server has the Active Directory Lightweight Directory Service (AD LDS) service role installed. AD LDS is administered on the server by using the Active Directory module for Windows PowerShell.

All virtual machines (VMs) access iSCSI-based storage by using a Microsoft iSCSI Initiator installed on the VM.

Existing Active Directory/Directory Services

The network contains a single Active Directory forest named northwindtraders.com. The forest contains five Remote Desktop servers. All Remote Desktop servers are in an organizational unit (OU) named RD Servers.

TECHNICAL REQUIREMENTS

Northwind Traders must meet the following technical requirements:

- Minimize server downtime.
- Ensure that you can recover all of the data hosted on the VMs.
- Ensure that you can perform bare metal restores of the Hyper-V servers.
- Minimize the number of times a server restarts when it is deployed.
- Monitor the CPU utilization, memory utilization, and disk utilization of all the servers to analyze performance trends.
- Ensure that a specific set of Group Policy settings are App1ied to users who use Remote Desktop to connect to the Remote Desktop servers. The settings must differ from those App1ied when the users log on locally to their own computers.
- Copy a custom Microsoft Office Word dictionary to the computers in the legal department. Update the custom dictionary on a regular basis. Copy the updated version of the dictionary as soon as possible to the legal department computers.

Question: 1

You need to recommend a strategy to ensure that the administration of AD LDS is encrypted. What should you include in the recommendation?

A. a server authentication certificate
B. client authentication certificates
C. Digest authentication
D. Windows Integrated authentication

Answer: A

Explanation:

http://technet.microsoft.com/en-us/library/cc725767%28WS.10%29.aspx

The Lightweight Directory Access Protocol (LDAP) is used to read from and write to Active Directory Lightweight Directory Services (AD LDS). By default, LDAP traffic is not transmitted securely. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology.

To enable SSL-based encrypted connections to AD LDS, you must request and obtain a server authentication certificate

from a trusted certification authority (CA) in your organization or from a trusted third-party CA. For more information about installing and using a CA, see Certificate Services (http://go.microsoft.com/fwlink/?LinkID=48952).

Question: 2

You need to recommend a solution for monitoring the servers. The solution must meet the company's technical requirements. What should you include in the recommendation?

A. Data Collector Sets (DCSs)
B. event subscriptions
C. Reliability Monitor
D. Windows System Resource Manager (WSRM)

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc771692%28WS.10%29.aspx
Data Collector Sets An important new feature in Windows Reliability and Performance Monitor is the Data Collector Set, which groups data collectors into reusable elements for use with different performance monitoring scenarios. Once a group of data collectors is stored as a Data Collector Set, operations such as scheduling can be applied to the entire set through a single property change. You can schedule repeated collection of a Data Collector Set to create logs, load it in Performance Monitor to see the data in real time, and save it as a template to use on other computers. Windows Reliability and Performance Monitor also includes default Data Collector Set templates to help you begin collecting performance data immediately.

Question: 3

You need to recommend a solution for improving the automated deployment of servers. The solution must meet the company's technical requirements. What should you include in the recommendation?

A. an offline domain join
B. native-boot virtual hard disks (VHDs)
C. the Offline servicing of images
D. the Online servicing of images

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/offline-domain-join-djoin-step-by-step%28WS.10%29.aspx
Offline domain join is a new process that computers that run Windows® 7 or Windows Server® 2008 R2 can use to join a domain without contacting a domain controller. This makes it possible to join computers to a domain in locations where there is no connectivity to a corporate network.

Question: 4

You need to recommend a Group Policy strategy for the Remote Desktop servers. What should you include in the recommendation?

A. block inheritance
B. loopback processing

C. security filtering
D. WMI filtering

Answer: B

Explanation:
http://support.microsoft.com/?id=231287
Group Policy applies to the user or computer in a manner that depends on where both the user and the computer objects are located in Active Directory. However, in some cases, users may need policy applied to them based on the location of the computer object alone. You can use the Group Policy loopback feature to apply Group Policy Objects (GPOs) that depend only on which computer the user logs on to.
http://technet.microsoft.com/en-us/windowsserver/cc817587
Managing Terminal Services
What is loopback processing?
Group Policy loopback processing can be used to alter the application of GPOs to a user by including GPOs based on the location of the computer object. The typical way to use loopback processing is to apply GPOs that depend on the computer to which the user logs on.

Question: 5

You need to recommend a solution for deploying the custom Word dictionary. What should you include in the recommendation?

A. Distributed File System (DFS)
B. Group Policy preferences
C. Offline servicing
D. WDS

Answer: B

Explanation:
http://support.microsoft.com/kb/943729
This article discusses the Group Policy preferences that are new in Windows Server 2008 and how to enable down-level computers to process these new items. Group Policy preferences are made up of more than 20 new Group Policy client-side extensions (CSEs) that expand the range of configurable settings in a Group Policy object (GPO). These new preference extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC). The kinds of preference items that can be created by using each extension are listed when New is selected for the extension. Examples of the new Group Policy preference extensions include the following:
Folder Options
Drive Maps
Printers
Scheduled Tasks
Services
Start Menu

Question: 6

You need to recommend a backup strategy for HyperV. What should you recommend?

A. Take a snapshot of each VM, and then run a full backup of the HyperV hosts by using Windows Server Backup.

B. Shut down the VMs, and then run a full backup of the HyperV hosts by using Windows Server Backup. Restart the VMs when the backup is complete.
C. From each VM, run a full backup by using Windows Server Backup, and then run a full backup of the HyperV hosts by using Windows Server Backup.
D. From each VM, run a full backup by using Windows Server Backup. Shut down the VMs, and then run a full backup of the HyperV hosts by using Windows Server Backup. Restart the VMs when the backup is complete.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd252619%28WS.10%29.aspx
There are two basic methods you can use to perform a backup. You can:
Perform a backup from the server running Hyper-V. We recommend that you use this method to perform a full server backup because it captures more data than the other method. If the backup application is compatible with Hyper-V and the Hyper-V VSS writer, you can perform a full server backup that helps protect all of the data required to fully restore the server, except the virtual networks. The data included in such a backup includes the configuration of virtual machines, snapshots associated with the virtual machines, and virtual hard disks used by the virtual machines. As a result, using this method can make it easier to recover the server if you need to, because you do not have to recreate virtual machines or reinstall Hyper-V. However, virtual networks are not included in a full server backup. You will need to reconfigure the virtual networking by recreating the virtual networks and then reattaching the virtual network adapters in each virtual machine to the appropriate virtual network. As part of your backup planning, make sure you document the configuration and all relevant settings of your virtual network if you want to be able to recreate it.
Perform a backup from within the guest operating system of a virtual machine. Use this method when you need to back up data from storage that is not supported by the Hyper-V VSS writer. When you use this method, you run a backup application from the guest operating system of the virtual machine. If you need to use this method, you should use it in addition to a full server backup and not as an alternative to a full server backup.
Perform a backup from within the guest operating system before you perform a full backup of the server running Hyper-V. For more information about storage considerations, see the following section.

Case Study: 12
Wingtip Toys
Scenario
COMPANY OVERVIEW
Wingtip Toys is an international company that has a main office and several branch offices. The main office is located in Moscow. The branch offices are located throughout Europe. The main office has 500 users. Each branch office has 4 to 70 users.
PLANNED CHANGES
Wingtip Toys opens a new branch office that contains a file server. You plan to promote the file server to a Read-only Domain Controller (RODC). Wingtip Toys plans to hire a consulting firm to manage its Web site. The consulting firm must only be permitted to manage the Web site and must be prevented from accessing to all other server resources. Wingtip Toys plans to purchase a high-resolution printer that will be connected to a print server in the main office. Users must be charged for each page that they print on the printer. You plan to present additional storage to a two node failover cluster in the main office. The storage will be used by the file server instance.
EXISTING ENVIRONMENT
All servers run either Windows Server 2008 or Windows Server 2008 R2. All client computers run either Windows Vista Enterprise or Windows 7 Enterprise.
Existing Network Infrastructure
The network contains an internal network and a perimeter network. The company Web site is hosted on a

standalone server in the perimeter network. The main office connects to each branch office by using a 1-Mbps WAN link.

Existing Active Directory Environment

The network contains a single Active Directory domain named wingtiptoys.com. An Active Directory site exists for each office. Each Active Directory site contains a single subnet. The main office has two domain controllers. Each branch office has a single domain controller.

REQUIREMENTS

Technical Requirements

Wingtip Toys must meet the following technical requirements:

- Minimize network utilization.
- Minimize WAN link utilization.
- Ensure that the file servers can access additional storage as a local drive.
- Ensure that changes to the network are transparent to users whenever possible.
- Ensure that new storage solutions are supported by Windows Failover Clustering.
- Ensure that each user can access his Documents folder from any client computer.
- Automatically organize the files on the file servers according to the contents of the files.
- Ensure that storage can be provisioned without causing any downtime of the file servers.
- Ensure that the data on the file servers is protected by using Windows BitLocker Drive Encryption (BitLocker).

Problem Statements

All users store their documents and other data in the Documents folder on their respective client computers. The users report that when they log on to a computer that is not their own, their documents *are* unavailable.

Question: 1

You need to recommend a solution for storing user documents. What should you include in the recommendation?

A. folder redirection
B. home folders
C. mandatory user profiles
D. roaming user profiles

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc732275.aspx
Folder Redirection User settings and user files are typically stored in the local user profile, under the Users folder. The files in local user profiles can be accessed only from the current computer, which makes it difficult for users who use more than one computer to work with their data and synchronize settings between multiple computers. Two technologies exist to address this problem: Roaming Profiles and Folder Redirection. Both technologies have their advantages, and they can be used separately or together to create a seamless user experience from one computer to another. They also provide additional options for administrators managing user data.

Question: 2

You need to recommend a monitoring solution for the new printer. What should you include in the recommendation?

A. Data Collector Sets (DCSs)
B. event subscriptions

C. object access auditing
D. Print Management filters

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc766468%28WS.10%29.aspx
Establishing audit policy is an important facet of security. Monitoring the creation or modification of objects gives you a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach.
There are nine different kinds of events you can audit. If you audit any of these kinds of events, Windows® records the events in the Security log, which you can find in Event Viewer. Account logon events. Audit this to see each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. Account logon events are generated in the domain controller's Security log when a domain user account is authenticated on a domain controller. These events are separate from Logon events, which are generated in the local Security log when a local user is authenticated on a local computer. Account logoff events are not tracked on the domain controller.
Account management. Audit this to see when someone has changed an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group.
Directory service access. Audit this to see when someone accesses an Active Directory® directory service object that has its own system access control list (SACL).
Logon events. Audit this to see when someone has logged on or off your computer (either while physically at your computer or by trying to log on over a network).
Object access. Audit this to see when someone has used a file, folder, printer, or other object. While you can also audit registry keys, we don't recommend that unless you have advanced computer knowledge and know how to use the registry.
Policy change. Audit this to see attempts to change local security policies and to see if someone has changed user rights assignments, auditing policies, or trust policies.
Privilege use. Audit this to see when someone performs a user right.
Process tracking. Audit this to see when events such as program activation or a process exiting occur.
System events. Audit this to see when someone has shut down or restarted the computer, or when a process or program tries to do something that it does not have permission to do. For example, if malicious software tried to change a setting on your computer without your permission, system event auditing would record it.

Question: 3

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).

Answer: C

Explanation:
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: 4

You need to recommend a solution for promoting the RODC in the new branch office. What should you include in the recommendations?

A. Implement the Windows Search service and implement a custom iFilter.
B. Implement File Server Resource Manager (FSRM) and configure file classifications.
C. Implement Microsoft SharePoint Foundation 2010 and create a custom workflow.
D. Implement a Distributed File System (DFS) namespace and configure folder targets.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/ee344836%28WS.10%29.aspx
What is the File Classification Infrastructure?
The Windows Server 2008 R2 File Classification Infrastructure (FCI) automates classification processes so that you can manage your data more effectively. You can save money and reduce risk by storing and retaining files based on their business value or impact. The built-in solution for file classification provides expiration, custom tasks, and reporting. The extensible infrastructure enables you to meet additional customer classification needs
by building rich end-to-end classification solutions that are built on the classification foundation of Windows Server in a consistent and supported way and within the existing Windows file serving platforms.

Question: 5

You are evaluating whether to add an iSCSI target in the main office to add storage to the file servers. Which technical requirement cannot be met when using an iSCSI target?

A. Ensure that the data on the file servers is protected by using BitLocker.
B. Ensure that the file servers can access additional storage as a local drive.
C. Ensure that new storage solutions are supported by Windows Failover Clustering.
D. Ensure that storage can be provisioned without causing any downtime of the file servers.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/ee449438%28WS.10%29.aspx

Drive configuration	Supported	Not supported
Network	None	Network file system (NFS) Distributed File System (DFS)
Optical media	None	CD file system (CDFS) Live File System Universal Disk Format (UDF)
Software	Basic volumes	Software-based RAID systems Bootable and non-bootable virtual hard disks (VHDs) Dynamic volumes RAM disks
File system	NTFS FAT16 FAT32 ExFAT	CD File system
Drive connection	USB Firewire SATA SAS ATA	iSCSI Fiber Channel eSATA Bluetooth

Question: 6

You need to recommend a solution for promoting the RODC in the new branch office. What should you include in the recommendation?

A. Active Directory snapshots
B. an unattended answer file
C. Install From Media (IFM)
D. Answer ID D

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc816722%28WS.10%29.aspx
When you install Active Directory Domain Services (AD DS) by using the install from media (IFM) method, you can reduce the replication traffic that is initiated during the installation of an additional domain controller in an Active Directory domain. Reducing the replication traffic reduces the time that is necessary to install the additional domain controller.

Case Study: 13
Blue Yonder Airlines

Scenario

COMPANY OVERVIEW

Blue Yonder Airlines has a main office and four branch offices. Each branch office has six satellite offices. The main office is located in Sydney. The branch offices are located in London, New York, Bangkok, and Istanbul. The main office has 1,000 users. Each branch office has 500 users. Each satellite office has 50 to 100 users.

PLANNED CHANGES

Each satellite office will have a single server deployed. The servers will have the following server roles installed:

- File server
- Print server
- Read-only Domain Controller (RODC)

Each satellite office will have a local support technician who performs the following tasks:

- Manages printers.
- Manages server backups.
- Manages updates on the server.

Each support technician will only be permitted to manage the server located in his office. You plan to implement a backup and recovery solution to restore deleted Active Directory objects. The solution must ensure that the attributes of the deleted objects are restored to the same state they were in before they were deleted. You plan to deploy a custom sales Application named App2 to the portable computers of all company sales consultants. The setup program of App2 requires local administrative privileges. App2 will be updated monthly.

BUSINESS GOALS

Blue Yonder Airlines has the following business goals:

- Minimize server downtime.
- Minimize administrative effort.

Minimize interruptions to users caused by WAN link failures.

EXISTING ENVIRONMENT

The network contains servers that run either Windows Server 2008 R2 or Windows Server 2008. All client computers were recently replaced with new computers that run Windows 7 Enterprise.

Users do not have local administrator rights on the client computers.

Existing Active Directory/Directory Services

The network contains a single Active Directory domain named blueyonderairlines.com. The functional level of the domain is Windows Server 2008. All domain controllers run Windows Server 2008.

Existing Network Infrastructure

All offices have wired and wireless networks.

The main office has a file server that stores large graphics files. The files are used by all of the users in all of the offices.

A Group Policy is used to assign an Application named App1 to all of the users in the domain.

The branch offices contain public computers on which temporary employees can browse the Internet and view electronic brochures. When the employees log on to the public computers, they must all receive the same user settings. App1 must not be installed on the public computers. The computer accounts for all of the public computers are in an organizational unit (OU) name Public.

REQUIREMENTS

Security Requirements

All computers in the domain must have a domain-level security Group Policy object (GPO) App1ied.

You plan to implement Network Access Protection (NAP) by using switches and wireless access points (WAPs) as NAP enforcement points.

The public computers must meet the following security requirements:

• Only authorized Applications must be run.
• Automatic updates must be enabled and App1ied automatically.
Users must be denied access to the local hard disk drives and the network shares from the public computers.

Technical Requirements

The file server in each branch office is configured as shown in the following table.

Share name	File path
Data	E:\data
Users	E:\users
Apps	E:\apps

Each user is allocated 1 GB of storage on the Users share in their local office. Each user must be prevented from storing files larger than 500 MB on the Data share in their local office.
Blue Yonder Airlines must meet the following requirements for managing App2:
• Sales consultants must use the latest version of the Application.
• When a new version of App2 is installed, the previous version must be uninstalled. Sales consultants must be able to run App2 when they are disconnected from the network.

Question: 1

You need to recommend a strategy for recovering objects deleted from Active Directory that supports the planned changes. What should you include in the recommendation? (Each correct answer presents part of the solution. Choose two.)

A. Active Directory Recycle Bin
B. Active Directory snapshots
C. non-authoritative restores
D. tombstone reanimation

Answer: B, D

Explanation:
The domain level is only server 2008 so recycle bin isn't available.
http://technet.microsoft.com/en-us/library/cc753609%28WS.10%29.aspx
This guide shows how you can use an improved version of Ntdsutil and a new Active Directory® database mounting tool in Windows Server® 2008 to create and view snapshots of data that is stored in Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS), without restarting the domain controller or AD LDS server. A snapshot is a shadow copy—created by the Volume Shadow Copy Service (VSS)—of the volumes that contain the Active Directory database and log files.
The Active Directory database mounting tool (Dsamain.exe) can improve recovery processes for your organization by providing a means to compare data as it exists in snapshots that are taken at different times so that you can better decide which data to restore after data loss. This eliminates the need to restore multiple backups to compare the Active Directory data that they contain.
This guide provides step-by-step instructions for using the Active Directory database mounting tool, including creating, listing, and mounting snapshots of AD DS; preparing them for viewing as a Lightweight Directory Access Protocol (LDAP) server; and viewing the data itself.
If you have some idea which organizational unit (OU) or objects were deleted, you can look up the deleted objects in the snapshots and record the attributes and back-links that belonged to the deleted objects. You can reanimate these objects by using the tombstone reanimation feature on a domain controller in your production environment. Then, you must manually repopulate these objects with the stripped attributes and back-links as identified in the snapshots.
For more information about tombstone reanimation, see Reanimating Active
Directory Tombstone Objects (http://go.microsoft.com/fwlink/?LinkID=116204).

Question: 2

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.

Answer: C

Explanation:
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: 3

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

Answer: A

Explanation:
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.

Question: 4

You need to recommend a solution for managing the public computers in the branch offices. What should you recommend?

A. Create a GPO that is linked to the domain and configure security filtering for the GPO.
B. Create a GPO that is linked to the Public OU and configure security filtering for the GPO.
C. Create a GPO that is linked to the Public OU and enable loopback processing in the GPO.
D. Create a GPO that is linked to the domain and enable block inheritance on the Public OU.

Answer: C

Explanation:
http://support.microsoft.com/?id=231287
Group Policy applies to the user or computer in a manner that depends on where both the user and the computer objects are located in Active Directory. However, in some cases, users may need policy applied to them based on the location of the computer object alone. You can use the Group Policy loopback feature to apply Group Policy Objects (GPOs) that depend only on which computer the user logs on to.
http://technet.microsoft.com/en-us/windowsserver/cc817587
Managing Terminal Services
What is loopback processing?
Group Policy loopback processing can be used to alter the application of GPOs to a user by including GPOs based on the location of the computer object. The typical way to use loopback processing is to apply GPOs that depend on the computer to which the user logs on.

Question: 5

You need to recommend an administrative solution for the local support technicians in the satellite offices. The solution must meet the company's security requirements. What should you include in the recommendation?

A. Active Directory delegation
B. Administrator Role Separation
C. managed service accounts

D. Restricted Groups

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc753170%28WS.10%29.aspx
This topic explains how you can use Administrator Role Separation (ARS) on a read-only domain controller (RODC) to delegate RODC administration to a user who is not a member of the Domain Admins group.
One problem encountered by administrators of domain controllers in perimeter networks is that domain controllers typically have to be set up and administered by domain administrators. Administrative operations, such as applying software updates, performing an offline defragmentation, or backing up the system, cannot be delegated.
With the introduction of RODCs, domain administrators can delegate both the installation and the administration of RODCs to any domain user, without granting them any additional rights in the domain. The ability to perform this delegation is called ARS.

Question: 6

You need to recommend a solution to ensure that users in the London office can access the graphics files in the main office. The solution must meet the company's business goals. What should you recommend?

A. Configure the client computers to use BranchCache in Distributed Cache mode.
B. Deploy a standalone Distributed File System (DFS) namespace. Configure a DFS Replication group.
C. Deploy a domainbased Distributed File System (DFS) namespace. Configure a DFS Replication group.
D. Deploy a BranchCache server that operates in Hosted Cache mode. Configure the client computers to use the BranchCache server.

Answer: C

Explanation:
BranchCach is a Server 2008 R2 feature
http://technet.microsoft.com/en-us/library/cc731545.aspx
Review Requirements for DFS Replication
Applies To: Windows Server 2008 R2
Before you can deploy DFS Replication, you must configure your servers as follows:
Extend (or update) the Active Directory Domain Services (AD DS) schema to include Windows Server 2003 R2, Windows Server 2008, or Windows Server 2008 R2 schema additions. To use read-only replicated folders, the schema must include the Windows Server 2008 or newer schema additions. For information about extending the AD DS schema, see the Microsoft Web site at (http://go.microsoft.com/fwlink/?LinkId=93051).
Ensure that all servers in a replication group are located in the same forest. You cannot enable replication across servers in different forests.
Verify that all members of the replication group are running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 R2. DFS Replication is supported on all x64 editions of Windows Server 2008 R2 and all x64 and x86 editions of Windows Server 2008. DFS Replication is not available for Itanium-Based Systems.
Install DFS Replication on all servers that will act as members of a replication group.
Install the DFS Management snap-in on a server to manage replication. This server cannot run a Server Core installation of the Windows Server 2008 operating system.
Contact your antivirus software vendor to check that your antivirus software is compatible with DFS Replication.
Store replicated folders on NTFS volumes.
To include a failover cluster in a replication group, the failover cluster must be running Windows Server 2008 R2. Install and configure the failover cluster feature and then use the High Availability Wizard to create a clustered File

Server instance before adding the instance as a replication group member. For more information, see Add a Failover Cluster to a Replication Group.
On a server that is running a version of Windows older than Windows Server 2008 R2, locate replicated folders for failover clusters in the local storage of a node. Versions of the DFS Replication service older than Windows Server 2008 R2 are not designed to coordinate with cluster components, and the service will not fail over to another node.

Question: 7

You need to implement a solution for the branch office file servers that meets the company's technical requirements. What should you implement on the branch office file servers?

A. File Server Resource Manager (FSRM) quotas
B. Network Policy Server (NPS) connection request policies
C. NTFS disk quotas
D. Windows System Resource Manager (WSRM) resource allocation policies

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/cc766468%28WS.10%29.aspx
Establishing audit policy is an important facet of security. Monitoring the creation or modification of objects gives you a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach.
There are nine different kinds of events you can audit. If you audit any of these kinds of events, Windows® records the events in the Security log, which you can find in Event Viewer.
Account logon events. Audit this to see each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. Account logon events are generated in the domain controller's Security log when a domain user account is authenticated on a domain controller. These events are separate from Logon events, which are generated in the local Security log when a local user is authenticated on a local computer. Account logoff events are not tracked on the domain controller.
Account management. Audit this to see when someone has changed an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group.
Directory service access. Audit this to see when someone accesses an Active Directory® directory service object that has its own system access control list (SACL).
Logon events. Audit this to see when someone has logged on or off your computer (either while physically at your computer or by trying to log on over a network).
Object access. Audit this to see when someone has used a file, folder, printer, or other object. While you can also audit registry keys, we don't recommend that unless you have advanced computer knowledge and know how to use the registry.
Policy change. Audit this to see attempts to change local security policies and to see if someone has changed user rights assignments, auditing policies, or trust policies.
Privilege use. Audit this to see when someone performs a user right.
Process tracking. Audit this to see when events such as program activation or a process exiting occur.
System events. Audit this to see when someone has shut down or restarted the computer, or when a process or program tries to do something that it does not have permission to do. For example, if malicious software tried to change a setting on your computer without your permission, system event auditing would record it.

Case Study: 14
School of Fine Art
Scenario

COMPANY OVERVIEW

School of Fine Art is an educational institution that has a main campus and two satellite campuses. The main campus is located in New York. The satellite campuses are located in Los Angeles and Chicago. The main campus has approximately 4,000 users made up of students, faculty, and employees. Each satellite campus has approximately 1,000 users made up of students, faculty, and employees.

EXISTING ENVIRONMENT

The network contains a single Active Directory domain named fineartschool.net. All servers run Windows Server 2008 R2. All client computers run either Windows XP or Windows 7. The network contains Microsoft Application Virtualization (App-V) and Microsoft Enterprise Desktop Virtualization (MED-V).

Existing Network Infrastructure

The main campus has the following servers:

- A file server that contains confidential files
- A print server that has several printers installed
- A server that has the Windows Server Update Services (WSUS) server role installed

All client computers are updated by using the WSUS server. The main campus has a computer lab. The lab has 50 client computers that run Windows 7 Enterprise. The computer accounts for the lab computers are located in an organizational unit (OU) named LabOU. The user accounts and computer accounts for all of the students are located in an OU named StudentsOU. Both OUs are child objects in the fineartschool.net domain. The relevant Group Policy objects (GPOs) are configured as shown in the following table.

GPO name	Linked to
GPO1	Fineartschool.net domain
GPO2	LabOU
GPO3	StudentsOU

REQUIREMENTS

Technical Requirements

The computer lab must meet the following requirements:

• Ensure that the user settings in all domain-level GPOs are App1ied to each student.

• Prevent the settings in all domain-level GPOs from being App1ied to the client computers in the computer lab.

The update management infrastructure must meet the following requirements:

• Each campus must control the updates for its respective campus.

• Update status reports must be sent weekly to the Enterprise Administrator on the main campus.

Application Requirements

All client computers will be upgraded to Windows 7 Enterprise. An Application named App1 runs on every client computer. App1 is only compatible with Windows XP. App1 must remain available after all of the operating system upgrades are complete.

App1 must meet the following requirements:

• App1 must be available from the Start menu.

• The management of App1 must be centralized.

• Each user must have a unique instance of App1.

Security Requirements

Security for the file server on the main campus must meet the following requirements:

• Unauthorized users must be prevented from printing sensitive files stored on the server.

• The contents of the server* s hard disks must remain secure if the physical security of the server is compromised.

Problem Statements

Users report that they receive a different desktop environment every time they log on to a client computer in the computer lab. The print server on the main campus has reliability issues. A malfunction on a single printer often causes other printers to malfunction.

Question: 1

You need to increase the reliability of the print server on the main campus. What should you do?

A. Create printer pools.
B. Configure printer redirection.
C. Configure printer driver isolation.
D. Change the location of the Spool folder.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/dd878502%28WS.10%29.aspx
Printer driver isolation
Prior to Windows Server 2008 R2, the failure of printer driver components has been a main print server support issue—the failure of a printer driver loaded onto the print spooler process would cause the process to fail, which would lead to an outage of the entire printing system. The impact of a spooler failure on a print server is particularly significant because of the number of users and printers that are typically affected.
In Windows Server 2008 R2, you can now configure printer driver components to run in an isolated process separate from the printer spooler process. By isolating the printer driver, you can prevent a faulty printer driver from stopping all print operations on a print server, which results in a significant increase in server reliability.
In addition to the benefit of improving overall printing system stability, this new feature provides a means to isolate new drivers for testing and debugging, and to identify which printer drivers have been causing spooler failures.

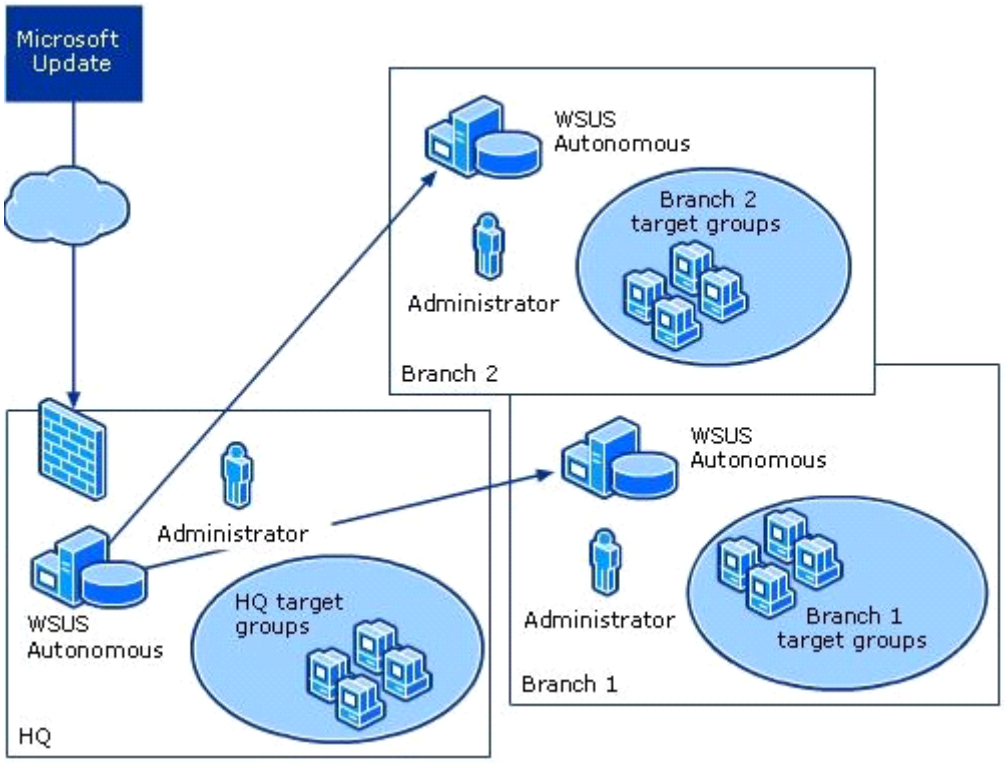
Question: 2

You need to recommend an update management strategy for the Chicago campus that meets the company's technical requirements. What should you recommend?

A. Deploy a WSUS server in replica mode, and then configure the server's reporting rollup settings.
B. Deploy a WSUS server in replica mode, and then configure the server's email notification settings.
C. Deploy a WSUS server in autonomous mode, and then configure the server's reporting rollup settings.
D. Deploy a WSUS server in autonomous mode, and then configure the server's email notification settings.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/dd939820%28WS.10%29.aspx
Autonomous mode (distributed administration)
Distributed management by using autonomous mode is the default installation option for WSUS. In autonomous mode, an upstream WSUS server shares updates with downstream servers during synchronization. Downstream WSUS servers are administered separately and they do not receive update approval status or computer group information from the upstream server. By using the distributed management model, each WSUS server administrator selects update languages, creates computer groups, assigns computers to groups, tests and approves updates, and makes sure that the correct updates are installed to the appropriate computer groups.
The following image shows how you might deploy autonomous WSUS servers in a branch office environment:



Question: 3

You need to recommend a strategy for the computer lab that meet the company's technical requirements. What should you recommend?

A. Enable the loopback setting in GPO2. Enable the Enforced option in GPO1.
B. Enable the Block Inheritance option on Lab OU. Enable the Enforced option in GPO1.
C. Enable the loopback setting in GPO2. Disable the user configuration settings in GPO3.
D. Enable the Block Inheritance option on Lab OU. Disable the user configuration settings in GPO3.

Answer: D

Explanation:
To apply the settings of a Group Policy object (GPO) to the users and computers of a domain, site, or organizational unit, you can link that domain site or organizational unit to that GPO. You can add one or more GPO links to each domain, site, and organizational unit in Group Policy Management Console. The settings deployed by GPOs linked to higher containers (parent container) in Active Directory are inherited by default to child containers and combine with any settings deployed in GPOs linked to child containers. If multiple GPOs attempt to set a setting to conflicting values, the GPO with the highest precedence sets the setting. GPO processing is based on a last writer wins model, and GPOs that are processed later have precedence over GPOs that are processed sooner. Group Policy objects are processed according to the following order:
The local Group Policy object (LPGO) is applied.
GPOs linked to sites.
GPOs linked to domains
GPOs linked to organizational units. In the case of nested organizational units, GPOs associated with parent organizational units are processed prior to GPOs associated with child organizational units.
Changing the link order
Within each domain, site, and organizational unit, the link order controls when links are applied. To change the

precedence of a link, you can change the link order, moving each link up or down in the list to the appropriate location. The link with the higher order (with 1 being the highest order) has the higher precedence for a given site, domain, or organizational unit. For example, if you add six GPO links and later decide that you want the last one that you added to have highest precedence, you can move the GPO link to the top of the list.
Blocking Group Policy inheritance
You can block policy inheritance for a domain or organizational unit. Using block inheritance prevents GPOs linked to higher sites, domains, or organizational units from being automatically inherited by the child-level. By default, children inherit all GPOs from the parent, but it is sometimes useful to block inheritance. For example, if you want to apply a single set of policies to an entire domain except for one organizational unit, you can link the required GPOs at the domain level (from which all organizational units inherit policies by default), and then block inheritance only on the organizational unit to which the policies should not be applied.
Enforcing a GPO link
You can specify that the settings in a GPO link should take precedence over the settings of any child object by setting that link to Enforced. GPO-links that are enforced cannot be blocked from the parent container. Without enforcement from above, the settings of the GPO links at the higher level (parent) are overwritten by settings in GPOs linked to child organizational units, if the GPOs contain conflicting settings. With enforcement, the parent
GPO link always has precedence. By default, GPO links are not enforced. In tools prior to GPMC, "enforced" was known as "No override."
Disabling a GPO link
By default, processing is enabled for all GPO links. You can completely block the application of a GPO for a given site, domain, or organizational unit by disabling the GPO link for that domain, site, or organizational unit.
Note that this does not disable the GPO itself, and if the GPO is linked to other sites, domains or organizational units, they will continue to process the GPO, if their links are enabled.
PO links set to enforce (no override) cannot be blocked.
The enforce and block inheritance options should be used sparingly. Casual use of these advanced features complicates troubleshooting.

Question: 4

You need to recommend changes to the file server on the main campus that meet the company's technical requirements. What should you include in the recommendation?

A. Encrypting File System (EFS)
B. NTFS permissions
C. Syskey
D. Windows BitLocker Drive Encryption (BitLocker)

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc731549%28WS.10%29.aspx
BitLocker Drive Encryption allows you to encrypt all data stored on the Windows operating system volume and configured data volumes, and by using a Trusted Platform Module (TPM), it can also help ensure the integrity of early startup components. BitLocker was first introduced with Windows Vista and Windows Server 2008 and subsequently updated with the release of Windows 7 and Windows Server 2008 R2.

Question: 5

You need to recommend changes to the existing environment that meet the company's security requirements for the file server on the main campus. What should you recommend?

A. Deploy Network Policy Server (NPS) and create a network policy.
B. Deploy Print and Document Services and create a custom printer filter.
C. Deploy File Server Resource Manager (FSRM) and create a file classification rule.
D. Deploy Active Directory Rights Management Services (AD RMS) and create an AD RMS rights policy template.

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/dd996658%28WS.10%29.aspx
Rights policy templates are used to control the rights that a user or group has on a particular piece of rightsprotected content. Active Directory Rights Management Services (AD RMS) stores rights policy templates in the configuration database. Optionally, it may maintain a copy of all rights policy templates in a shared folder that you specify.

Question: 6

You need to recommend a solution that meets the company's Application compatibility and provisioning requirements. What should you recommend?

A. Create a MED-V workspace.
B. Publish a RemoteApp program.
C. Package an Application by using the App-V Sequencer.
D. Create an Application compatibility shim by using the Application Compatibility Toolkit (ACT)

Answer: A

Explanation:
MED-V Usage Scenarios
The key usage scenario for MED-V is resolving application-to-operating system Incompatibility to accelerate the upgrade path to a new operating system. Businesses that need to continue to run legacy line-of business applications on users' desktop computers can do so by using Virtual PC. Incompatibility between legacy applications and newer versions of Microsoft Windows can often be a primary blocking issue preventing an enterprise from upgrading to the latest version of Windows, such as Windows Vista, to take advantage of the many new features and enhancements offered by this version. By delivering those applications in a Virtual PC that runs a previous version of the operating system (for example, Windows XP or Windows 2000), MED-V allows administrators to break the tight dependency between a computer's underlying hardware and the operating system, and it can help remove such blocking issues so that your users can benefit from having the latest version of Windows deployed on their desktop computers. From the user's perspective, with MED-V, these applications are accessible from the Start menu and appear side by side with regular applications—so there is minimal change to the user experience.
http://technet.microsoft.com/en-us/library/gg699692.aspx
Microsoft Enterprise Desktop Virtualization (MED-V), a core component of the Microsoft Desktop Optimization Pack (MDOP) for Microsoft Software Assurance, is the most robust and scalable solution for virtualizing Internet Explorer 7 and Internet Explorer 6. It provides a centrally managed solution that is intended for enterprise customers. If you use MED-V for virtualization, you can run Windows® 7 and still run older applications seamlessly, directly from a Windows 7 desktop. Users continue to work as they always have and as they launch their browser, MED-V determines whether to leave the URL in Internet Explorer 8 or whether it should redirect and display it in Internet Explorer 6 or Internet Explorer 7 on the MED-V workspace. The MEDV policy that is created and managed by the administrator determines the who, what, and how of applications from the MED-V workspace. By using MED-V, you retain the productivity benefits of the newest operating system, yet you can use older applications that might be best suited for your work.

Question: 7

You need to recommend a solution that meets the company's Application provisioning requirements. What should you recommend?

A. Create a new MEDV workspace.
B. Publish a new RemoteApp program.
C. Create an Application compatibility shim.
D. Package a new Application by using the AppV Sequencer.

Answer: A

Explanation:
MED-V Benefits
The key benefit of MED-V is that it helps enterprises deal with incompatibility between applications and the operating system. For instance, if a user needs to run an early version of Internet Explorer and that version of Internet Explorer is not supported on Windows Vista, the administrator can use MED-V 1.0 to deploy this early version of Internet Explorer to the user as part of a Windows XP virtual image. (And when MED-V 1.0 SP1 becomes available in Q1 of 2010, the user will be able to do the same thing on computers running Windows 7.) The user can then have two copies of Internet Explorer running simultaneously on his desktop—the most recent version (running on the host computer) and the earlier version (running in the MED-V workspace). From the user's perspective, both copies of Internet Explorer appear as if they were running on the local computer. MED-V does this by allowing users to run legacy applications within a virtual machine that has an earlier version of Microsoft Windows installed. The user can then access these applications either from a virtual desktop (as with Virtual PC 2007 running natively on a system) or by using application windows that are seamlessly integrated into the local desktop of the user's computer (similar to RemoteApp in Remote Desktop Services).
MED-V Usage Scenarios
The key usage scenario for MED-V is resolving application-to-operating system Incompatibility to accelerate the upgrade path to a new operating system. Businesses that need to continue to run legacy line-of-business applications on users' desktop computers can do so by using Virtual PC. Incompatibility between legacy applications and newer versions of Microsoft Windows can often be a primary blocking issue preventing an enterprise from upgrading to the latest version of Windows, such as Windows Vista, to take advantage of the many new features and enhancements offered by this version. By delivering those applications in a Virtual PC that runs a previous version of the operating system (for example, Windows XP or Windows 2000), MED-V allows administrators to break the tight dependency between a computer's underlying hardware and the operating system, and it can help remove such blocking issues so that your users can benefit from having the latest version of Windows deployed on their desktop computers. From the user's perspective, with MED-V, these applications are accessible from the Start menu and appear side by side with regular applications—so there is minimal change to the user experience.
App1 is only xp compatible but needs to be available on win7 clients, it also needs to be centrally managed. So Med-V fits the needed requirements

Case Study: 15
Proseware, Inc
Scenario
COMPANY OVERVIEW
Proseware, Inc. is a publishing company that has a main office and a branch office. The main office is located in New York. The branch office is located in Sydney. The main office has 5,000 users. The branch office has 1,000 users.
PLANNED CHANGES
Proseware plans to deploy a new 64-bit Application named App2 to 10 users in the branch office. Only

members of the local Administrators group can run App2. Proseware is evaluating whether to deploy virtual desktop pools. The virtual desktop pools must meet the following requirements:

- Apply the settings in GPO1 to the virtual machines (VMs).
- Prevent the VMs from receiving the Automatic Updates settings from GP02,
- Ensure that only the host VM is affected if a virtual hard disk (VHD) file becomes corrupt.
- Minimize the amount of storage used to support the VMs.
- Minimize the amount of memory and CPU resources used by the VMs.
- Minimize administrative effort.

EXISTING ENVIRONMENT

All servers run either Windows Server 2008 or Windows Server 2008 R2. All of the client computers in the main office run Windows 7. All of the client computers in the branch office run Windows XP (x86) with Service Pack 3 (SP3). All of the client computers in the main office are configured as Microsoft Enterprise Desktop Visualization (MED-V) and Microsoft Application Virtualization (App-V) clients. A two-node Hyper-V cluster is deployed in the main office. The cluster uses Clustered Shared Volumes.

Existing Active Directory/Directory Services

The network contains a single Active Directory domain named proseware.com. The functional level of the forest is Windows Server 2008. The relevant organizational units (OUs) for the domain are configured as shown in the following table.

OU name	OU description
NYC	User accounts and computer accounts in the main office
SYD	User accounts and computer accounts in the branch office

A custom Group Policy object (GPO) named GPO1 is linked to the domain, GPO1 contains corporate computer security settings. A custom GPO named GP02 is linked to both office OUs. GP02 contains Windows Server Update Services (WSUS) settings.

Existing Network Infrastructure

Each office has servers that have the following server roles or role services installed:

- WSUS
- Hyper-V
- File Services
- Remote Desktop Web Access (RD Web Access)
- Remote Desktop Session Host (RD Session Host)
- Remote Desktop Virtualization Host (RD Virtualization Host)
- Remote Desktop Connection Broker (RD Connection Broker)

REQUIREMENTS

Technical Requirements

When users interactively logs on to any of the client computers in the branch office, they must automatically receive the local administrator rights to that computer. When users logs off, they must lose the administrator rights. The disk space on all file servers must be monitored. If any file server has less than 20% free disk space on a volume, a script must run that deletes temporary files.

Problem Statements

The main office has a shared folder named Legal. The Legal share is only accessed by users in the legal department. Legal department users report that it takes a long time to locate files in the Legal share by using keyword searches.

Question: 1

You need to recommend a monitoring solution for the file server that meets the technical requirements. What should

you include in the recommendation?

A. Data Collector Sets
B. File Server Resource Manger quotas
C. File Server Resource Manger storage reports
D. NTFS disk quotas

Answer: A

Explanation:
There's some debate about the answer to this one. is it A or B? concensus is pointng to A: data collector sets Probably the most relevant info is that we must run a script when running out of free space.NTFS quota doesn't have this service., FSRM Storage reports are just that reports so that leaves us with A or B
Microsoft Self Paced Handbook:
You can also add performance counter alerts to DCSs. This enables you to monitor a counter and detect an alert, which you can then use to start a batch file, send you an email, or call you on a pager. For example, if you configured an alert to trigger when free space on a logical volume falls below 30 percent, you could add this to a DCS and use it to trigger a batch file that archives the data on the volume.
Data Collector Sets
http://technet.microsoft.com/en-us/library/cc771692%28WS.10%29.aspx
An important new feature in Windows Reliability and Performance Monitor is the Data Collector Set, which groups data collectors into reusable elements for use with different performance monitoring scenarios. Once a group of data collectors is stored as a Data Collector Set, operations such as scheduling can be applied to the entire set through a single property change. You can schedule repeated collection of a Data Collector Set to create logs, load it in Performance Monitor to see the data in real time, and save it as a template to use on other computers.
Windows Reliability and Performance Monitor also includes default Data Collector Set templates to help you begin collecting performance data immediately.

Question: 2

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

A. Deploy a new AppV package that contains App2. Stream the package to the client computers of the 10 users.
B. Deploy a new MEDV workspace that contains App2. Deploy the workspace to the client computers of the 10 users.
C. On an RD Session Host server in the branch office, install and publish App2 by using RemoteApp. Deploy the RemoteApp program as an MSI file.
D. On an RD Virtualization Host server in the branch office, create 10 Windows 7 VMs that contain App2. Configure the new VMs as personal virtual desktops.

Answer: D

Question: 3

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

Answer: B

Explanation:
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 2) critical data is stored on volumes outside the dynamically expanding VHD.

Question: 4

You need to recommend a solution to provision new Applications on the VMs for the planned virtual desktop pool deployment. What should you recommend?

A. Deploy the Applications to the VMs by using AppV streaming.
B. Deploy the Applications to the VMs by using Group Policy Software Installation.
C. Deploy a MEDV workspace to each VM. Deploy the Applications to the workspace.
D. Deploy the Applications by using RemoteApp. Create a RemoteApp and Desktop Connection for each VM.

Answer: D

Explanation:
The client PCs are using Windows XP which are x86 architecture and the app is x64

Question: 5

You need to recommend a solution for configuring the Automatic Updates settings on the VMs. What should you include in the recommendation?

A. block inheritance
B. loopback processing
C. security filtering
D. WMI filtering

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/cc947846%28WS.10%29.aspx
To make sure that each GPO associated with a group can only be applied to computers running the correct version of Windows, use the Group Policy Management MMC snap-in to create and assign WMI filters to the GPO. Although you can create a separate membership group for each GPO, you would then have to manage the memberships of the different groups. Instead, use only a single membership group, and let WMI filters automatically ensure the correct GPO is applied to each computer.

Question: 6

You need to recommend a solution for managing administrative rights for the branch office client computers. The solution must meet the company's technical requirements. What should you recommend configuring?

A. Account Policies by using GPOs
B. Local Users and Groups by using Group Policy preferences
C. Restricted Groups by using GPOs
D. Security Options by using Group Policy preferences

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc731892%28WS.10%29.aspx
Group Policy preferences, new for the Windows Server 2008 operating system, include more than 20 new Group Policy extensions that expand the range of configurable settings within a Group Policy object (GPO).
These new extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC), under the new Preferences item. Examples of the new Group Policy preference extensions include folder options, mapped drives, printers, scheduled tasks, services, and Start menu settings.
http://support.microsoft.com/kb/943729
Examples of the new Group Policy preference extensions include the following:
Folder Options
Drive Maps
Printers
Scheduled Tasks
Services
Start Menu

Question: 7

Users frequently search for documents from the Start menu or in Windows Explorer. You need to recommend a solution to minimize the amount of time it takes for users in the Legal department to locate tiles stored on the Legal share. What should you include in the recommendation?

A. Configure Windows Search Service on the client computers in the Legal department and add the Legal share to the file server library.
B. Configure Windows Search Service on the file server and add the Legal share to the file server library.
C. Configure Windows Search Service on the file server and add the Legal share to the client computers in the legal department.
D. Configure Windows Search Service on the client computers in the Legal department and add the Legal share to the client library.

Answer: C

Explanation:
Windows search can speed up searching through file shares by using indexing

Case Study: 16
Trey Research
Scenario
COMPANY OVERVIEW
Trey Research is a pharmaceutical company that has a main office and two branch offices. The main office is located in Denver. The branch offices are located in New York and Seattle. The main office has 10,000 users. Each branch office has approximately 200 users.
PLANNED CHANGES
You plan to deploy a new Application named App1. App1 is developed in-house. The binary executables and support files for App1 contain sensitive intellectual property. Users must access App1 through document invocation. The users must be prevented from directly copying or accessing the App1 program files.
EXISTING ENVIRONMENT
The network contains a single Active Directory domain named treyresearch.com. All servers run Windows Server 2008 R2. All client computers run Windows 7 Enterprise. The network contains a Web server named Web1 that hosts an intranet site. All users use Web1. Users report that access to the content on Web1 is slow. You discover that the CPU utilization of Web1 is approximately 90 percent during peak hours. Microsoft System Center Configuration Manager is used to deploy updates to all of the client computers.
Existing Network Infrastructure
Each office has several file servers. The file servers have a limited amount of storage space. Users access the data on all of the file servers. Each branch office has a WAN link to the main office. Users in the branch office frequently access the file server in the main office.
Current Administration Model
All servers are currently administered remotely by using Remote Desktop. Help desk users perform the following administrative tasks in the domain:
- Manage printers.
- Create shared folders.
- Manage Active Directory users.
- Modify file permissions and share permissions.

All of the help desk users are members of a global group named HelpDesk. Business Goals. Trey Research has the following business goals:
- Minimize the cost of making changes to the environment.
- Minimize the cost of managing the network infrastructure and the servers

REQUIREMENTS
Technical Requirements
Trey Research plans to Virtualize all of the servers during the next three years. Trey Research must meet the following technical requirements for virtualization:
- Simplify the management of all hardware.
- Allocate CPU resources between virtual machines (VMs).
- Ensure that the VMs can connect to multiple virtual local area networks (VLANs).
- Minimize the amount of administrative effort required to convert physical servers to VMs.

Trey Research must ensure that users can access content in the shared folders if a single server fails. The solution must also reduce the amount of bandwidth used to access the shared folders from the branch offices. Trey Research must meet the following technical requirements for the intranet site:
- Improve response time for users.
- Provide redundancy if a single server fails.

Security Requirements
A new corporate security policy states that only Enterprise Administrators are allowed to interactively log on to servers.
User Requirements
Users report that it is difficult to locate files in the shared folders across the network. The users want a single point of access for all of the shared folders in the company.

Question: 1

You need to recommend changes to the intranet site that meet the company's technical requirements. What should you include in the recommendation?

A. additional Application pools
B. additional worker processes
C. Failover Clustering
D. Network Load Balancing (NLB)

Answer: D

Explanation:
http://technet.microsoft.com/en-us/library/cc725691.aspx
The Network Load Balancing (NLB) feature in Windows Server 2008 R2 enhances the availability and scalability of Internet server applications such as those used on Web, FTP, firewall, proxy, virtual private network (VPN), and other mission-critical servers. A single computer running Windows Server 2008 R2 provides a limited level of server reliability and scalable performance. However, by combining the resources of two or more computers running one of the products in Windows Server 2008 R2 into a single virtual cluster,
NLB can deliver the reliability and performance that Web servers and other mission-critical servers need.

Question: 2

You need to recommend a deployment strategy for App1. What should you recommend?

A. Assign App1 to users by using a Group Policy.
B. Publish App1 to users by using a Group Policy.
C. Deploy App1 as a RemoteApp program by using an MSI file.
D. Deploy App1 as a RemoteApp program by using an RDP file.

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc753844%28WS.10%29.aspx
USERS SHOLD NOT BE ALLOWED ACCESS ANY EXE FILES ETC so A &B are out
What does TS RemoteApp do?
RemoteApp programs are programs that are accessed remotely through Terminal Services and appear as if they are running on the end user's local computer. Users can run RemoteApp programs side by side with their local programs. A user can minimize, maximize, and resize the program window, and can easily start multiple programs at the same time. If a user is running more than one RemoteApp program on the same terminal server, the RemoteApp programs will share the same Terminal Services session.
Users can run RemoteApp programs in a number of ways. They can:
Double-click a Remote Desktop Protocol (.rdp) file that has been created and distributed by their administrator.

Double-click a program icon on their desktop or Start menu that has been created and distributed by their administrator with a Windows Installer (.msi) package.
Double-click a file whose extension is associated with a RemoteApp program. (This can be configured by their administrator with a Windows Installer package.)
Access a link to the RemoteApp program on a Web site by using TS Web Access.
The .rdp files and Windows Installer packages contain the settings needed to run RemoteApp programs. After opening the RemoteApp program on a local computer, the user can interact with the program that is running on the terminal server as if it were running locally.

Question: 3

You are evaluating whether to deploy Hyper-V. Which technical requirement is NOT met by a HyperV deployment?

A. Allocate CPU resources between VMs.
B. Simplify the management of all hardware.
C. Ensure that the VMs can connect to multiple VLANs.
D. Minimize the amount of administrative effort required to convert physical servers to VMs.

Answer: D

Question: 4

You need to identify each help desk user who bypasses the new corporate security policy. What should you do?

A. Configure Audit Special Logon and define Special Groups.
B. Configure Audit Other Privilege Use Events and define Special Groups.
C. Configure Audit Sensitive Privilege Use and configure auditing for the HelpDesk group.
D. Configure Audit Object Access and modify the auditing settings for the HelpDesk group.

Answer: A

Explanation:
http://technet.microsoft.com/en-us/library/dd772635%28WS.10%29.aspx
This security policy setting determines whether the operating system generates audit events when:
A special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level.
http://support.microsoft.com/kb/947223
Special Groups is a new feature in Windows Vista and in Windows Server 2008. The Special Groups feature lets the administrator find out when a member of a certain group logs on to the computer. The Special Groups feature lets an administrator set a list of group security identifiers (SIDs) in the registry. An audit event is logged in the Security log if the following conditions are true:
Any of the group SIDs is added to an access token when a group member logs on.
Note An access token contains the security information for a logon session. Also, the token identifies the user, the user's groups, and the user's rights.
In the audit policy settings, the Special Logon feature is enabled.

Question: 5

You need to identify which tool the help desk users must use to perform administrative tasks. Which tool should you identify?

A. RemoteApp
B. Remote Assistance
C. Remote Desktop
D. Remote Server Administration Tools (RSAT)

Answer: D

Explanation:
http://support.microsoft.com/kb/941314
Microsoft Remote Server Administration Tools (RSAT) enables IT administrators to remotely manage roles and features in Windows Server 2008 from a computer that is running Windows Vista with Service Pack 1 (SP1). It includes support for remote management of computers that are running either a Server Core installation option or a full installation option of Windows Server 2008. It provides similar functionality to the Windows Server 2003 Administration Tools Pack.

Question: 6

You need to recommend changes to the environment that meet the company's user requirements. What should you include in the recommendation?

A. failover clustering
B. Network Load Balancing (NLB)
C. Distributed File System (DFS) Replication
D. a BranchCache in Hosted Cache mode

Answer: C

Explanation:
http://technet.microsoft.com/en-us/library/cc753479%28WS.10%29.aspx
Distributed File System (DFS) Namespaces and DFS Replication offer simplified, highly-available access to files, load sharing, and WAN-friendly replication. In the Windows Server® 2003 R2 operating system, Microsoft revised and renamed DFS Namespaces (formerly called DFS), replaced the Distributed File System snap-in with the DFS Management snap-in, and introduced the new DFS Replication feature. In the Windows Server® 2008 operating system, Microsoft added the Windows Server 2008 mode of domain-based namespaces and added a number of usability and performance improvements.
What does Distributed File System (DFS) do?
The Distributed File System (DFS) technologies offer wide area network (WAN)-friendly replication as well as simplified, highly-available access to geographically dispersed files. The two technologies in DFS are the following:
DFS Namespaces. Enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. This structure increases availability and automatically connects users to shared folders in the same Active Directory Domain Services site, when available, instead of routing them over WAN connections.
DFS Replication. DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the AD DS SYSVOL folder in domains that use the Windows Server 2008 domain functional level.

Question: 7

You need to recommend changes to the environment that meet the company's user requirements. What should you include in the recommendation?

A. a BranchCache in Distributed Cache mode
B. a BranchCache in Hosted Cache mode
C. Distributed File System (DFS) namespaces
D. Distributed File System (DFS) Replication

Answer: C

Explanation:
Users want a single point of access for all shares, a DFS Namespace will provide this. it will also meet the fail over requirement for is one server is unavailable

Case Study: 17
Graphic Design Institute, Case B
General Background
You are the systems administrator for the Graphic Design Institute (GDI). GDI is a private liberal arts and technical college with campuses in multiple cities.
Technical Background
The campus locations, users, client computers, and servers are described in the following table.

Location	Users	Client computers		Servers	
		Qty	Operating system	Qty	Operating system
Austin	2000	400	Windows XP Professional SP3	10	Windows Server 2003 R2 Standard
Boston	3000	600	Windows 7 Enterprise SP1	10 30 4	Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Data Center Windows Web Server 2008
Buffalo	1500	300	Windows XP Professional SP3	10	Windows Server 2003 R2 Standard
Charlotte	1500	300	Windows XP Professional SP3	10	Windows Server 2003 R2 Standard
Minneapolis	2100	420	Windows XP Professional SP3	10	Windows Server 2003 R2 Standard
New Haven	2000	400	Windows 7 Enterprise SP1	10	Windows Server 2008 R2 Standard
Northridge	2100	420	Windows XP Professional SP3	10	Windows Server 2003 R2 Standard
Tacoma	800	160	Windows XP Professional SP3	5 1	Windows Server 2008 R2 Standard Server Core Windows Web Server 2008 R2

The campuses are connected by a fully meshed WAN.
The corporate network includes Active Directory Domain Services (AD DS). Domain controllers are located on each campus.
GDI uses Microsoft Windows Deployment Server (WDS) to distribute images by using Preboot Execution Environment (PXE). GDI builds images by using the Windows Automated Installation Kit (WAIK).
GDI uses Microsoft Windows Server Update Services (WSUS) to distribute and manage Windows security updates and software updates. All private client computers and portable computers used by faculty and staff are members of the WSUS computer group named Staff. All shared client computers are members of the WSUS computer group named LabComputers. All faculty and staff users are members of the global security group named GDI_Staff. All students are members of the global security group named GDI_Students.
Specific servers are configured as shown in the following table.

Location	Server names	Roles
Austin	AUDC01 AUDC02	Domain controllers
Austin	AUDATA01	WSUS Replica Server, file server
Boston	BODC01 BODC02	Domain controllers
Boston	BODATA03	WSUS Parent Server, file server
Buffalo	BUDC01 BUDC02	Domain controllers
Buffalo	BUDATA01	WSUS Replica Server, file server
Charlotte	CHDC01 CHDC02	Domain controllers
Charlotte	CHDATA01	WSUS Replica Server, file server
Charlotte	CHDATA02 CHDATA03 CHDATA04	File servers
Minneapolis	MNDC01 MNDC02	Domain controllers
Minneapolis	MNDATA01	WSUS Replica Server, file server
New Haven	NEDC01 NEDC02	Domain controllers
New Haven	NEDATA01	WSUS Replica Server, file server
Northridge	NODC01 NODC02	Domain controllers
Northridge	NODATA01	WSUS Replica Server, file server
Tacoma	TADC01	
Tacoma	TADATA01	WSUS Replica Server, file server

The main data center is located on the Boston campus. ADMX and ADML files are centrally stored on BODC01.

All Charlotte servers reside in the CH_Servers organizational unit (OU). CHDATA01, CHDATA02, CHDATA03, and CHDATA04 reside in the CH_FileServers OU.

CH_FileServers is a child OU of CH_Servers.

A Group Policy object (GPO) named ServerSettings App1ies Windows Internet Explorer settings to all servers.

Business Requirements

After successful migrations to Windows Server 2008 R2 in Boston, New Haven, and Tacoma, GDI plans to migrate its other campuses to Windows Server 2008 R2 in advance of a full Windows 7 client computer deployment. Server deployment on the Austin campus must be performed on weekends by using scheduled deployments. The post-migration environment must meet the following business requirements:

- Maximize security
- Maximize data protection
- Maximize existing resources
- Minimize downtime

Technical Requirements

The post-migration environment must meet the following security requirements:

- All updates must be distributed by using WSUS.
- All critical updates must be installed as soon as possible.
- All drives on the Minneapolis campus servers must have Windows BitLocker Drive Encryption

enabled.
The post-migration environment must meet the following data protection requirements:

- All servers must have automated backup routines.
- All backups must be replicated to the Boston data center at the end of each business week.
- The post-migration environment must meet the following resource requirements:
- Installations and recovery must be performed remotely.
- All department volumes on file servers must have NTFS quotas.
- Minimize download time for users who open Microsoft Office documents over the WAN.
- Ensure that users' files are always opened from the closest file server when available.
- Users' files must be accessible by the same path from all campuses.

Question: 1

You need to configure the role services on all file servers that are necessary to meet the technical requirements. Which role services should you configure? (Choose all that Apply.)

A. File Server Resource Manager
B. BranchCache for network files
C. Windows Search Service
D. Distributed File System
E. Services for Network File System

Answer: B, D

Explanation:
Requirements:
Minimize downtime for users accessing across a WAN = Branch Cache
Files Always opened from the nearest Server =DFS
Files at same path = DFS
Department volumes have Quotas
There is some debat if FSRM is needed. the original answer from Pass4Sure says that A FSRM is required.
However if you look at the exhibit it clearly says Departmental Volumes and not departmental shares so the question is do you need FSRM to apply quotas to a Volume? the answer is No you dont. NTFS Quota will apply quota by right clicking on the volume then selecting properties then selecting quotas. The differences between NTFS and FSRM quotas are basically NTFS is a disk quota, so the accounts cannot use more than the allowed space on the complete disk. With FSRM you can use folder quotas and differentiate it for your needs. so with NTFS if you set the quotas to 3 GB on one volume then all users that save data to that volume can only have up to 3GB of data on the whole volume, with FSRM quotas you can set it at the volume OR folder level.
A basic disk is a physical disk that contains primary partitions, extended partitions, or logical drives. Partitions and logical drives on basic disks are known as basic volumes. You can only create basic volumes on basic disks.
BranchCache
BranchCache is a wide area network (WAN) bandwidth optimization technology that is included in the Windows Server® 2008 R2 and Windows® 7 operating systems.
To optimize WAN bandwidth, BranchCache copies content from your main office content servers and caches the content at branch office locations, allowing client computers at branch offices to access the content locally rather than over the WAN.
At branch offices, content is cached either on servers that are running the BranchCache feature of Windows Server 2008 R2 or, when no server is available in the branch office, on computers running Windows 7. After a client computer requests and receives content from the main office and the content is cached at the branch office, other computers at

the same branch office can obtain the content locally rather than contacting the main office over the WAN link.
BranchCache helps improve content query response times for clients and servers in branch offices, and can also help improve network performance by reducing traffic over WAN links.
The BranchCache for network files role service is part of the File Services server role. BranchCache for network files is deeply integrated with file services and allows you to deploy a BranchCache-enabled file server.
When you deploy a BranchCache-enabled file server, BranchCache creates content information for every file in every shared folder where BranchCache is enabled.
Distributed File System (DFS) Namespaces and DFS Replication offer simplified, highly-available access to files, load sharing, and WAN-friendly replication. In the Windows Server® 2003 R2 operating system, Microsoft revised and renamed DFS Namespaces (formerly called DFS), replaced the Distributed File System snap-in with the DFS Management snap-in, and introduced the new DFS Replication feature. In the Windows Server® 2008 operating system, Microsoft added the Windows Server 2008 mode of domain-based namespaces and added a number of usability and performance improvements.
What does Distributed File System (DFS) do?
The Distributed File System (DFS) technologies offer wide area network (WAN)-friendly replication as well as simplified, highly-available access to geographically dispersed files. The two technologies in DFS are the following:
DFS Namespaces. Enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. This structure increases availability and automatically connects users to shared folders in the same Active Directory Domain Services site, when available, instead of routing them over WAN connections.
DFS Replication. DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the AD DS SYSVOL folder in domains that use the Windows Server 2008 domain functional level.
For completion I've included details on FSRM
FSRM
With the increasing demand on storage resources, as organizations rely more heavily on data than ever before, IT administrators face the challenge of overseeing a larger and more complex storage infrastructure, while at the same time, tracking the kind of information available in it. Managing storage resources not only includes data size and availability any more but also the enforcement of company policies and a very good understanding of how existing storage is utilized, allowing for sound strategic planning and proper response to organizational changes.
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.

Question: 2

You are designing a Windows Server 2008 R2 deployment strategy for the Minneapolis campus servers. Which deployment strategy should you recommend?

A. install from media.
B. Use a discover image in WDS.
C. Deploy a VHD image.
D. Deploy a WIM image.

Answer: D

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

VHD Image
- according to the official MS courseware book 6433A - a VHD can not contain more than one partition. so if true that rules VHD Images out because you need bitlocker and bitlocker requires 2 partitions. so if this is true then answer C is wrong.also
http://technet.microsoft.com/en-us/library/dd363560.aspx
A supported .vhd image. The only supported operating systems are Windows Server 2008 R2, Windows 7 Enterprise, and Windows 7 Ultimate. Fixed, dynamic, and differencing .vhd images are supported. However, note that a supported image cannot contain the following:
More than one operating system.
More than one partition.
Applications or data (instead of an operating system).
A 64-bit operating system that is partitioned with a GUID partition table (GPT).
So again further evidence that C is not the right answer as Bit locker needs 2 partitions.
I'm leaning toward Answer B because
WDS Images
WDS uses two different types of images: install images and boot images. Install images are the operating system images that will be deployed to computers running Windows Server 2008 R2, Windows Server 2008, Windows 7, or Windows Vista. A default installation image named Install.wim is located in the \Sources directory of the installation DVD. If you are using WDS to deploy Windows 7 to computers with different processor architectures, it will be necessary to add separate installation images for each architecture to the WDS server.
Architecture-specific images can be found on the architecture-specific installation media; for example, the Itanium image is located on the Itanium installation media, and the x64 default installation image is located on the x64 installation media. Although it is possible to create custom images, it is necessary to have only one image per processor architecture. For example, deploying Windows Server 2008 R2 Enterprise edition x64 to a computer with two x64 processors and to a computer with eight x64 processors in SMP configuration only requires access to the default x64 installation image. Boot images are used to start a client computer prior to the installation of the operating system image. When a computer starts off a boot image over the network, a menu is presented that displays the possible images that can be deployed to the computer from the WDS server. The Windows Server 2008 R2 Boot.wim file allows for advanced deployment options, and this file should be used instead of the Boot.wim file that is available from other sources.
In addition to the basic boot image, there are two separate types of additional boot images that can be configured for use with WDS. The capture image is a boot image that starts the WDS capture utility. This utility is used with a reference computer, prepared with the Sysprep utility, as a method of capturing the reference computer's image for deployment with WDS. The second type of additional boot image is the discover image. Discover images are used to deploy images to computers that are not PXE-enabled or on networks that don't allow PXE. These images are written to CD, DVD, or USB media and the computer is started off the media rather than off the PXE network card, which is the traditional method of using WDS.
I'm gonna make a huge assumption that the Minneapolis servers are on a different subnet, which makes sense because they are all different campuses for a college. but if there is a DHCP Server or IP Helper is enabled then that wont be a problem. So B may not be the answer
Media Install
It specifically says they use WDS for deployment. WDS is all about using images so would that not rule out media install? you can do media installs that are unattended but it requires sending a DVD and corresponding USB key with an answer file to the site and it being inserted into the server. but GDI uses PXE enabled network
cards so that would imply media is not used as images would be stored centrally. so I'd rule out A so that just leaves D

Question: 3

You need to plan for the installation of critical updates to only shared client computers. What should you recommend?

A. Configure all WSUS servers as upstream servers.
B. Create an Automatic Approval rule that App1ies to the GDI_Students group.
C. Create an Automatic Approval rule that App1ies to the LabComputers group.
D. Configure the shared client computers to synchronize hourly from Microsoft Update.

Answer: C

Question: 4

You are planning the deployment of Windows Server 2008 R2 to CHDATA03 and CHDATA04. You have the following requirements:

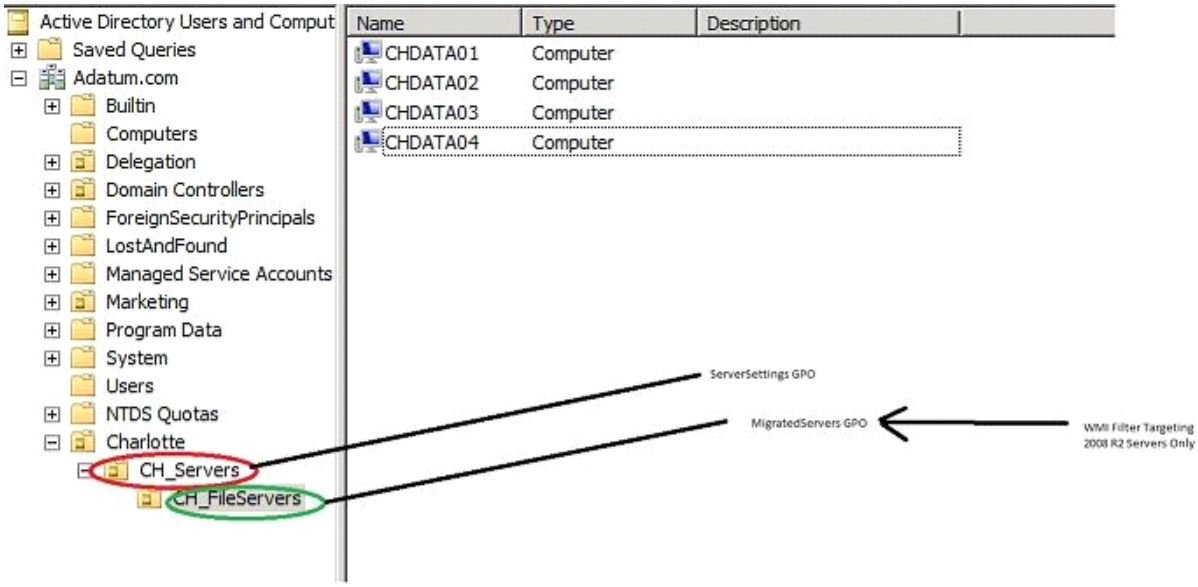
- Do not impact settings for CHDATA01 and CHDATA02.
- Apply Windows Server 2008 R2-specific settings to CHDATA03 and CHDATA04 after migration.
- Ensure that the ServerSettings GPO does not apply to CHDATA03 and CHDATA04 after migration.

You need to plan a strategy that meets the requirements. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create a GPO named MigratedServers that contains the Windows Server 2008 R2 settings. Create a WMI filter that targets Windows Server 2003 and link it to the MigratedServers GPO,
B. Block inheritance on the CH_FileServers OU.
C. Create a WMI filter that targets Windows Server 2003 and link it to the ServerSettings GPO.
D. Enable loopback processing on the MigratedServers GPO.
E. Link the MigratedServers GPO to the CH_FileServers OU.
F. Create a GPO named MigratedServers that contains the Windows Server 2008 R2 settings. Create a WMI filter that targets Windows Server 2008 R2 and link it to the MigratedServers GPO.

Answer: E, F

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



It on the second page of the exhibit it says that the ServerSettings GPO applies to all servers not all file servers. So that means one of two things, its linked to the CH_Servers OU OR its linked higher like at a domain level because then it applies to ALL servers in all regions. as the full AD structure is not clear I'll assume its applied on all CH servers only, but either way if its applied at a domain level it shouldn't matter.
If you first carry out step F you create the MigratedServers GPO, then you create the Server 2008 R2 WMI filter and apply that to the GPO you just created, then you carry out step E which links the MigratedServers GPO which has a Server 2008 R2 WMI filter to the CH_FileServers OU.
NOTE: possible issue
Thanks to SoK for highlighting this.
the question states what 2 steps
But requirement 3 says Ensure that the ServerSettings GPO does not apply to CHDATA03 and CHDATA04 after migration.
So ServerSettings GPO applies IE settings to servers in the CH_Servers ou and will also be applied to any Child OUs of that and on page 2 it says that CH_FileServers is a child of CH_servers so the ServerSettings GPO will be applied to all file servers by default regardless of their OS. the settings are IE settings and as its stands those settings would apply to CHDATA03 & CHDATA04 because of the ServerSettings GPO so unless you block that GPO somehow reaching the two 2008 file servers, answer B wont work because it then blocks them for CHDATA01 & CHDATA02 which you don't want. A wont work at it is an incorrect "replacement" for F because its applying 2008 settings to 2003 servers which is as useful as tits on a bull. D is pointless in this specific case so it a[[ears that C may be required. I'm going to leave C out for the moment because the question clearly states 2 answers

Question: 5

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.

Answer: B

Explanation:
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: 6

You are planning a recovery strategy in the event that a file server is unable to boot into Windows. You need to ensure that file servers can be restored from backups. What should the recovery strategy include?

A. Deploy backups by using WDS.
B. Boot from the Windows Server 2008 R2 DVD into the Recovery Environment, then restore from file server backups by using WBAdmin.
C. Reinstall Windows Server 2008 R2 from DVD, then restore from file server backups by using Windows Server Backup.
D. Restore from file server backups by using NTBackup.

Answer: A

Explanation:
Thanks to Testy for highlighting this one.
NTBackup is not compatible with Server 2008 R2.
Your requirements are for remote backup and remote restore.
The network has WDS installed and uses PXE boot on the servers so WDS could be used to deploy a backup.
Windows Recovery Environment (Windows RE) is an extensible recovery platform based on Windows Preinstallation Environment (Windows PE). When the computer fails to start, Windows automatically fails over into this environment, and the Startup Repair tool in Windows RE automates the diagnosis and repair of an unbootable Windows Vista installation. Furthermore, Windows RE is a starting point for various tools for manual system recovery. The primary audience of this technology includes original equipment manufacturers (OEMs), original device manufacturers (ODMs), and corporate IT professionals.
Image-based Recovery from Windows RE In the event that the Windows installation cannot be repaired with Startup Repair or other manual repair steps, Windows RE can be used to launch an image-based recovery tool.
User-created Recovery Image
Windows Vista provides end users with the ability to create a backup image of their entire operating system.
End users can do this by using the Backup tool. The system image can be stored on an external hard disk, on a hard disk partition other than those imaged, or on a DVD. To restore the computer by using this system image, users must launch the restore interface from the list of Windows RE manual tools.
Factory-created Recovery Image
To facilitate restoring a computer to its factory state, a recovery image can be placed on the Windows RE partition. This eliminates the need for a separate recovery media in most cases.
If the Windows image format is used in the manufacturing process, the same operating system image can be used for recovery as well. A computer manufacturer can develop an application by using the Imaging APIs for Windows and the Windows image to restore the operating system volume. This application can be launched from the Windows RE user interface (UI) by using customizations provided by the ODM.

Question: 7

You need to plan a scheduled daily backup of all files on TADC01. Which tools could you use? (Choose all that Apply.)

A. NTBackup
B. BITSAdmin
C. Windows Server Backup
D. Windows Backup
E. WBAdmin
F. Ntdsutil

Answer: C, E

Question: 8

You are testing a file replication strategy for the IT Budget folders on BODATA01, NEDATA01, and TADATA01. The IT Budget folder on TADATA01 is the primary member. You need to force replication of files to the Boston campus as soon as possible. Which command should you execute?

A. dfsrdiag.exe PollAO /Member:GD!\BODC01
B. dfsrdiag.exe PollAD /Member:GDI\TADC01
C. dfsrdiag.exe PollAD /Member:GDI\TADATA01
D. dfsrdiag.exe PollAD /Member:GDI\BODATA01

Answer: B

Explanation:
You are testing a file replication strategy on BODATA01. if you look at http://technet.microsoft.com/en-us/library/cc771488.aspx its says
You can use DFS Replication to keep the contents of folder targets in sync so that users see the same files regardless of which folder target the client computer is referred to. if you look to the Note on the bottom of the page its says:
To poll immediately for configuration changes, open a command prompt window and then type the following command once for each member of the replication group: dfsrdiag.exe PollAD /Member:DOMAINServer1.
so the question is do you poll the server holding the files or the DC in the location where the primary member is located? I'm pretty sure DFS-Replication uses AD DS replication so to me anyway I'd poll the DC.

Question: 8

You are designing a Windows Server 2008 R2 deployment strategy for the Minneapolis campus servers. Which deployment strategy should you recommend?

A. install from media.
B. Use a discover image in WDS.
C. Auto Add From Policy
D. Use multicast image deployment

Answer: D

Explanation:

Requirements - Bitlocker is needed on all disks in Minneapolis and installations must be done remotely it specifically says they use WDS for deployment. WDS is all about using images so would that not rule out media install? you can do media installs that are unattended but it requirese sending a DVD and corresponding USB key with an answer file to the site and it being inserted into the server. but GDI uses PXE enabled network cards so that would emply media is not used as images would be stored centrally.
I'm leaning toward Answer B because
http://technet.microsoft.com/en-us/library/dd637996%28v=ws.10%29.aspx
- "A client is on a different subnet and you do not have method of getting PXE to the client (for example, IP helper tables or Dynamic Host Control Protocol (DHCP))."
I'm gonna make a huge assumption that the Minneapolis servers are on a different subnet, which makes sense because they are all different campuses for a college
Multicasting. Provides the ability to transmit install images using multicasting. This includes the ability to automatically disconnect slow clients and the ability to transfer images using multiple streams of varying speeds. To locate these settings, right-click the server in the MMC snap-in, click Properties, and click the Multicast tab.
Multicast allows organizations to use their network bandwidth more efficiently, allowing an operating system image to be transmitted over the network once to multiple installation clients. For example, if you are deploying 20 computers running Windows Server 2008 R2, you save significant bandwidth in transmitting one installation image across the network (approximately 1.5 GB of data) compared to transmitting all 20 (approximately 60 GB of data). Multicast deployment is supported only in network environments where the routers support multicast transmissions.
The site in question has 10 servers so Multicast would be a possibility

Question: 9

You are designing a Windows Server 2008 R2 deployment strategy for the Austin campus servers. Which deployment strategy should you recommend?

A. Enable an Auto-Add Policy in WDS.
B. Create a discover image in WDS.
C. Deploy the images by using multicast transmission in WDS.
D. Deploy the images by using unicast transmission in WDS.

Answer: C

Question: 10

You are planning the migration of client computers on the Northridge campus to Windows 7. Due to compatibility concerns, the Northridge campus servers will not be migrated to Windows Server 2008 R2. The Northridge campus uses customized options in the inters.adm and system.adm administrative templates to handle key security restrictions. You need to ensure that the security restrictions will be applied to the migrated client computers. What should you recommend?
A. Copy the ADM files to \\BODC01\C$\Windows\SYSVOL\domain\policies\PolicyDefinitions and apply them to the Northridge GPOs.
B. Re-create the settings from the ADM files in the ADMX files on NODC01 and apply them to the Northridge GPOs.
C. Copy the ADM files to \\NODC01\CS\Windows\inf and apply them to the Northridge GPOs.
D. Re-create the settings from the ADM files in the ADMX files on BODC01 and apply them to the Northridge GPOs.

Answer: D

Case Study: 18
Tailspin Toys

Scenario

General Background

You are the Windows server administrator for Tailspin Toys. Tailspin Toys has a main office and a manufacturing office. Tailspin Toys recently acquired Wingtip Toys and is in the beginning stages of merging the IT environments. Wingtip Toys has a main office and a sales office.

Technical Background

The companies use the network subnets indicated in the following table.

Company	Office	Subnet
Tailspin Toys	Main office	10.10.10.0/24
Tailspin Toys	Manufacturing office	10.5.1.0/24
Wingtip Toys	Main office	172.16.10.0/24
Wingtip Toys	Sales office	192.168.1.0/24

The Tailspin Toys network and the Wingtip Toys network are connected by a point-to-point dedicated 45 Mbps circuit that terminates in the main offices.

Tailspin toys

The current Tailspin Toys server topology is shown in the following table.

Server name	IP address	Current role(s)	Operating system	Notes
TT-DC01	10.10.10.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DC02	10.10.10.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-APP01	10.10.10.20	Certification Authority (AD CS)	Windows Server 2008 R2 Enterprise	
TT-PRINT01	10.10.10.21	Print server, file server	Windows Server 2008 R2 Standard	
TT-DC03	10.5.1.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DC04	10.5.1.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-HOST05	10.10.10.30	Hyper-V host for developers	Windows Server 2008 R2 Enterprise	Hosts development VMs
TT-FILE01	10.10.10.40	File server	Windows Server 2008 R2 Standard	
TT-FILE02	10.10.10.50	File server	Windows Server 2008 Standard	

The Tailspin Toys environment has the following characteristics:

- All servers are joined to the tailspintoys.com domain.
- In the Default Domain Policy, the Retain old events Group Policy setting is enabled.
- An Active Directory security group named "Windows system administrators" is used to control all files and folders on TT-PRINT01.
- A Tailspin Toys administrator named Marc has been delegated rights to multiple organizational units (OUs) and object in the tailspintoys.com domain.
- Tailspin Toys developers use Hyper-V virtual machines (VMs) for development. There are 20 development VMs named TT-DEV01 through TT-DEV20.

Wingtip Toys

The current Wingtip Toys server topology is shown in the following table.

Server name	IP address	Current role(s)	Operating system	Notes
WT-DC01	172.16.10.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
WT-DC02	172.16.10.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
WT-APP01	172.16.10.20		Windows Server 2008 R2 Enterprise	
WT-PRINT01	172.16.10.21	Print server	Windows Server 2003 Standard x64	Some 64-bit print drivers
WT-DC03	192.168.1.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
WT-DC04	192.168.1.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones

All servers in the Wingtip Toys environment are joined to the wingtiptoys.com domain.

Infrastructure Services

You must ensure that the following infrastructure services requirements are met:

- All domain zones must be stored as Active Directory-integrated zones.
- Only DNS servers located in the Tailspin Toys main office may communicate with DNS servers at Wingtip Toys.
- Only DNS servers located in the Wingtip Toys main office may communicate with DNS servers at Tailspin Toys.
- All tailspintoys.com resources must be resolved from the Wingtip Toys offices.
- All wingtiptoys.com resources must be resolved from the Tailspin Toys offices.
- Certificates must be distributed automatically to all Tailspin Toys and Wingtip Toys computers.

Delegated Administration

You must ensure that the following delegated administration requirements are met:

- Tailspin Toys IT security administrators must be able to create, modify, and delete user objects in the wingtiptoys.com domain.
- Members of the Domain Admins group in the tailspintoys.com domain must have full access to the wingtiptoys.com Active Directory environment.
- A delegation policy must grant minimum access rights and simplify the process of delegating rights.
- Minimum permissions must always be delegated to ensure that the least privilege is granted for a job or task.
- Members of the TAILSPINTOYS\HeIpdesk group must be able to update drivers and add printer ports on TT-PRINT01.
- Members of the TAILSPINTOYS\Helpdesk group must not be able to cancel a print job on TT-PRINT01.
- Tailspin Toys developers must be able to start, stop, and Apply snapshots to their development VMs.

IT Security

You must ensure that the following IT security requirements are met:

- Server security must be automated to ensure that newly deployed servers automatically have the same security configuration as existing servers.
- Auditing must be configured to ensure that the deletion of user objects and OUs is logged.
- Microsoft Word and Microsoft Excel files must be automatically encrypted when uploaded to the Confidential document library on the Tailspin Toys Microsoft SharePoint site.
- Multifactor authentication must control access to Tailspin Toys domain controllers.
- All file and folder auditing must capture the reason for access.
- All folder auditing must capture all delete actions for all existing folders and newly created folders.
- New events must be written to the Security event log in the tailspintoys.com domain and retained indefinitely.
- Drive X:\ on TT-FILE01 must be encrypted by using Windows BitLocker Drive Encryption and must automatically unlock.

Question: 1

You need to recommend a solution to migrate shared printers from the print server at Wingtip Toys to the print server at Tailspin Toys. What should you recommend?

A. On the TT-PRINT01 server, run the printmig.exe command-line tool
B. On the WT-PRINT01 server, run the printbrm.exe command-line tool
C. On the WT-PRINT01 server, run the printmig.exe command-line tool
D. On the TT-PRINT01 server, run the printbrm.exe command-line tool

Answer: D

Explanation:
you are moving from a 2003 to a 2008 server so option B wont work coz WT-print01 is the 2003 server you can export print queues, printer settings, printer ports, and language monitors, and then import them on another print server running a Windows operating system. This is an efficient way to consolidate multiple print servers or replace an older print server.

The following table describes the supported and unsupported migration scenarios for the Printer Migration Wizard and Print Migrator 3.1, whether x64-base

Tool	Supported migration scenarios	Unsupported migration scenarios
Printer Migration Wizard, Printbrm.exe command-line tool	**Windows Vista** - Supports all migrations to Windows Vista. **Windows Server 2008 R2** - You cannot migrate directly from older operating systems (Windows NT Server 4.0, Windows 2000 Server) to **Windows Server 2008 R2**. Instead, you must migrate from the older operating system to a computer running Windows Vista, then migrate from Windows Vista to Windows Server 2008 R2.	Does not support migrati from Windows 2000 Serve and older systems.
Print Migrator 3.1	Supports migration to Windows Server 2003 from all previous Windows operating systems.	Does not support migrati Windows Vista and later operating systems.

Print Migrator 3.1 is no longer supported by Microsoft. The Printer Migration Wizard and the Printbrm.exe command-line tool were introduced in Windows 7 to replace it. For more information about this decision, see the blog Ask the Performance Team (http://blogs.technet.com/askperf/archive/2008/10/17/why-printmig-3-1-isretired.aspx).

Question: 2

You are planning for the IT integration of Tailspin Toys and Wingtip Toys. The company has decided on the following name resolution requirements:

- Name resolution for Internet-based resources must continue to operate by using the same DNS servers as prior to the merger.
- The existing connectivity between Tailspin Toys and Wingtip Toys must be used for all network communication.
- The documented name resolution goals must be met.

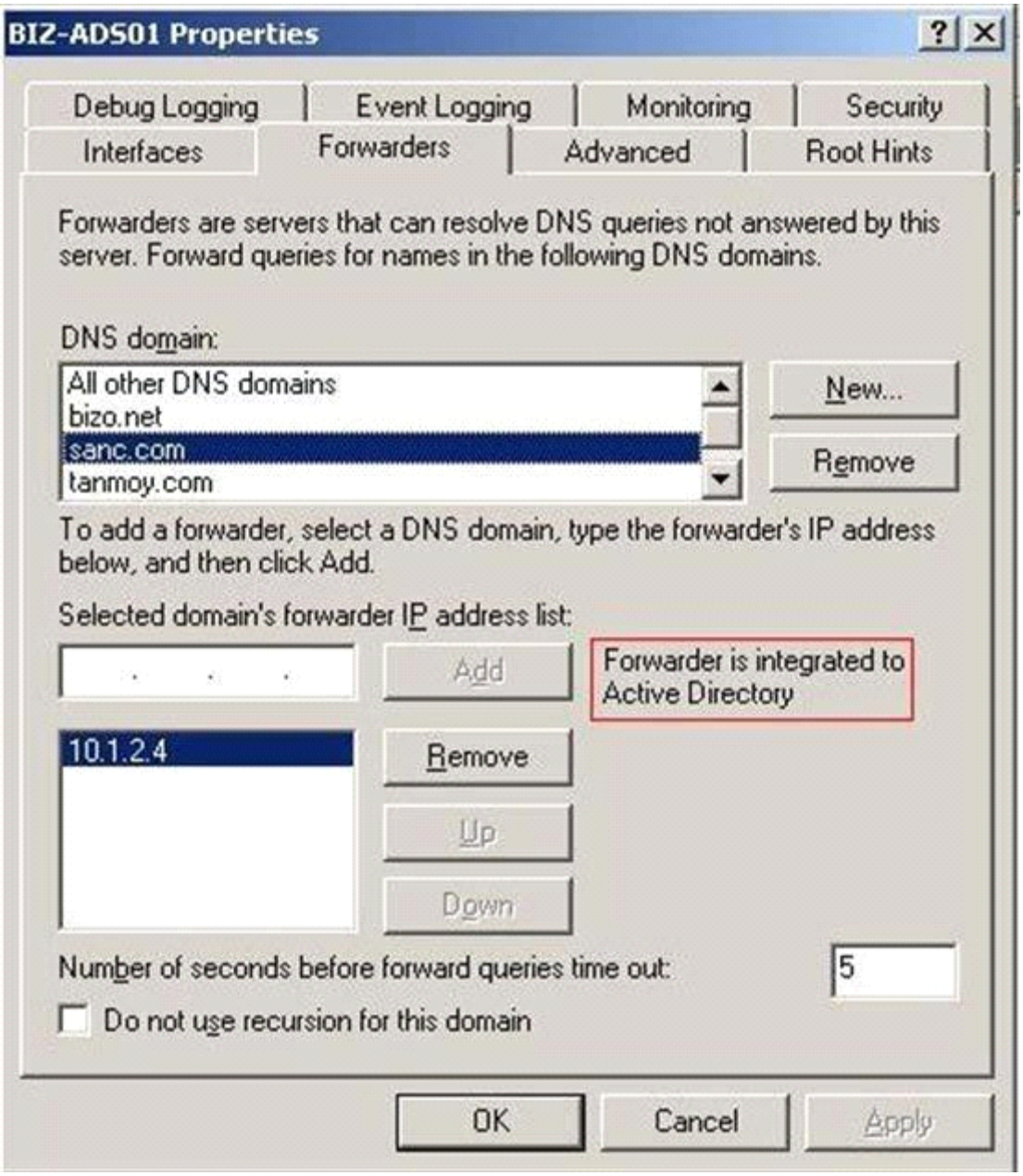
You need to provide a name resolution solution that meets the requirements. What should you recommend? (Choose all that Apply.)

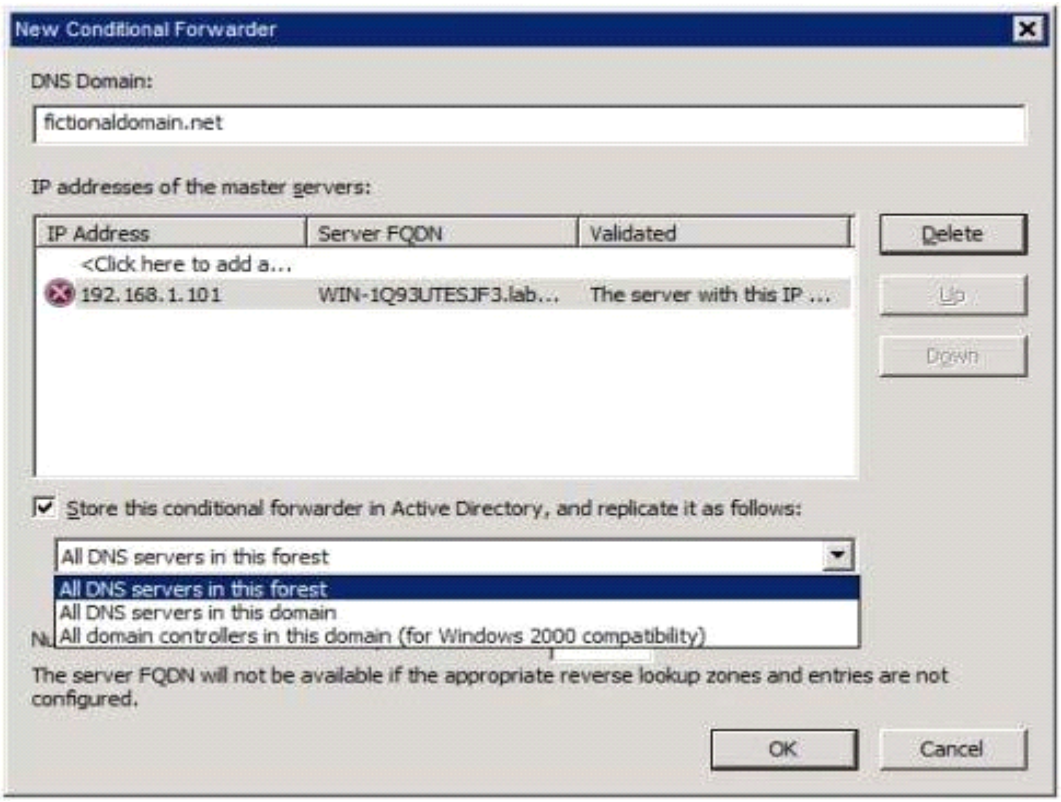
A. On TT-DC01, TT-DC02, TT-DC03, and TT-DC04, add forwarders with the IP addresses of 172.16.10.10 and 172.16.10.11.
B. On TT-DC01, add a conditional forwarder for wingtiptoys.com, use 172.16.10.10 and 172.16.10.11 as the IP addresses, and then configure it to replicate to all DNS servers in the tailspintoys.com domain.
C. On TT-DC01, TT-DC02, TT-DC03, and TT-DC04, add a secondary DNS zone for wingtiptoys.com and specify 172.16.10.10 and 172.16.10.11 as the master DNS servers.
D. On WT-DC01 and WT-DC02, add a secondary DNS zone for tailspintoys.com and specify 10.10.10.10 and 10.10.10.11 as the master DNS servers.
E. On WT-DC01, WT-DC02, WT-DC03, and WT-DC04, add forwarders with the IP addresses of 10.10.10.10 and 10.10.10.11.

F. On WT-DC01, add a conditional forwarder for tailspintoys.com, use 10.10.10.10 and 10.10.10.11 as the IP addresses, and configure it to replicate to all DNS servers in the wingtiptoys.com domain.

Answer: B, F

Explanation:
Conditional forwarding is used to control where a DNS server forwards queries for a specific domain. A DNS server on one network can be configured to forward queries to a DNS server on another network without having to query DNS servers on the Internet. They can also be used to help companies resolve each other's namespace in a situation where companies collaborate a merger is underway.
Forwarders and Forwarding
When a name server is queried in DNS, the way it responds depends on the type of query issued, which can be either iterative or recursive. In an iterative query, the client asks the name server for the best possible answer to its query. The name server checks its cache and the zones for which it is authoritative and returns the best possible answer to the client, which could be either a full answer like "here is the IP address of the host you are looking for" or a partial answer like "try this other name server instead, it might know the answer."
In a recursive query, things work a little different for here the client demands either a full answer (the IP address of the target host) or an error message like "sorry, name not found." In Windows DNS, client machines always send recursive queries to name servers, and name servers usually send iterative queries to other name servers.
What Conditional Forwarding Does
A conditional forwarder is one that handles name resolution only for a specific domain. For example, you could configure your name server to forward any requests for hosts in the domain google.com directly to a specific name server that is authoritative for the google.com domain. What this does is speed up the name resolution process by eliminating the need to go up to root to find this authoritative server.
So in our question above we would create a conditional forwarder in Wingtiptoys.com for tailspintoys.com and then create a conditional forwarder in tailspintoys.com for windtiptoys.com. additionally in Server 2008 there is a separate node in DNS Manager to configure Conditional Forwarders, previously if you wanted to configure Forwarding for a certain DNS domain, and you wanted to do this on all DNS Servers, you had to do this for all the DNS servers separately.
Forwarders can be configured centrally and can be configured as ‘Active Directory’ integrated
What does this mean: well this means they are stored in Active Directory and you can configure a replication scope, in the same way you can with AD Integrated DNS Zones, they can be replicated using following scopes:
- All DNS servers in this forest (through the ForestDNSZones Application Partition)
- All DNS servers in this domain (through the DomainDNSZones Application Partition)
-All Domain Controllers in this domain (for Windows 2000 compatibility), stored in the Domain Partition
- In a custom Application Partition of your liking, if you want to replicate only to certain Domain Controllers (that are probably your DNS servers)


BIZ-ADS01 Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Forwarders are servers that can resolve DNS queries not answered by this server. Forward queries for names in the following DNS domains.
DNS domain:
All other DNS domains
bizo.net
sanc.com
tanmoy.com
New...
Remove
To add a forwarder, select a DNS domain, type the forwarder's IP address below, and then click Add.
Selected domain's forwarder IP address list:
Add
Forwarder is integrated to Active Directory
10.1.2.4
Remove
Up
Down
Number of seconds before forward queries time out:
5
Do not use recursion for this domain
OK
Cancel
Apply



Question: 3

You need to recommend a solution to meet the IT security requirements and data encryption requirements for TT-FILE01 with the minimum administrative effort. What should you recommend? (Choose all that Apply.)

A. Turn on BitLocker on drive X:\ and select the Automatically unlock this drive on this computer option.
B. Migrate TT-FILE01 to Windows Server 2008 R2 Enterprise.
C. Store BitLocker recovery information in the tailspintoys.com domain.
D. Turn on BitLocker on the system drive.

Answer: A, C

Explanation:
Backing up recovery passwords for a BitLocker-protected disk volume allows administrators to recover the volume if it is locked. This ensures that encrypted data belonging to the enterprise can always be accessed by authorized users.
Storage of BitLocker recovery information in Active Directory
Backed up BitLocker recovery information is stored in a child object of the Computer object. That is, the Computer object is the container for a BitLocker recovery object.
Each BitLocker recovery object includes the recovery password and other recovery information. More than one BitLocker recovery object can exist under each Computer object, because there can be more than one recovery password associated with a BitLocker-enabled volume.
The name of the BitLocker recovery object incorporates a globally unique identifier (GUID) and date and time information, for a fixed length of 63 characters. The form is:
<Object Creation Date and Time><Recovery GUID>
For example:
2005-09-30T17:08:23-08:00{063EA4E1-220C-4293-BA01-4754620A96E7}

Question: 4

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?

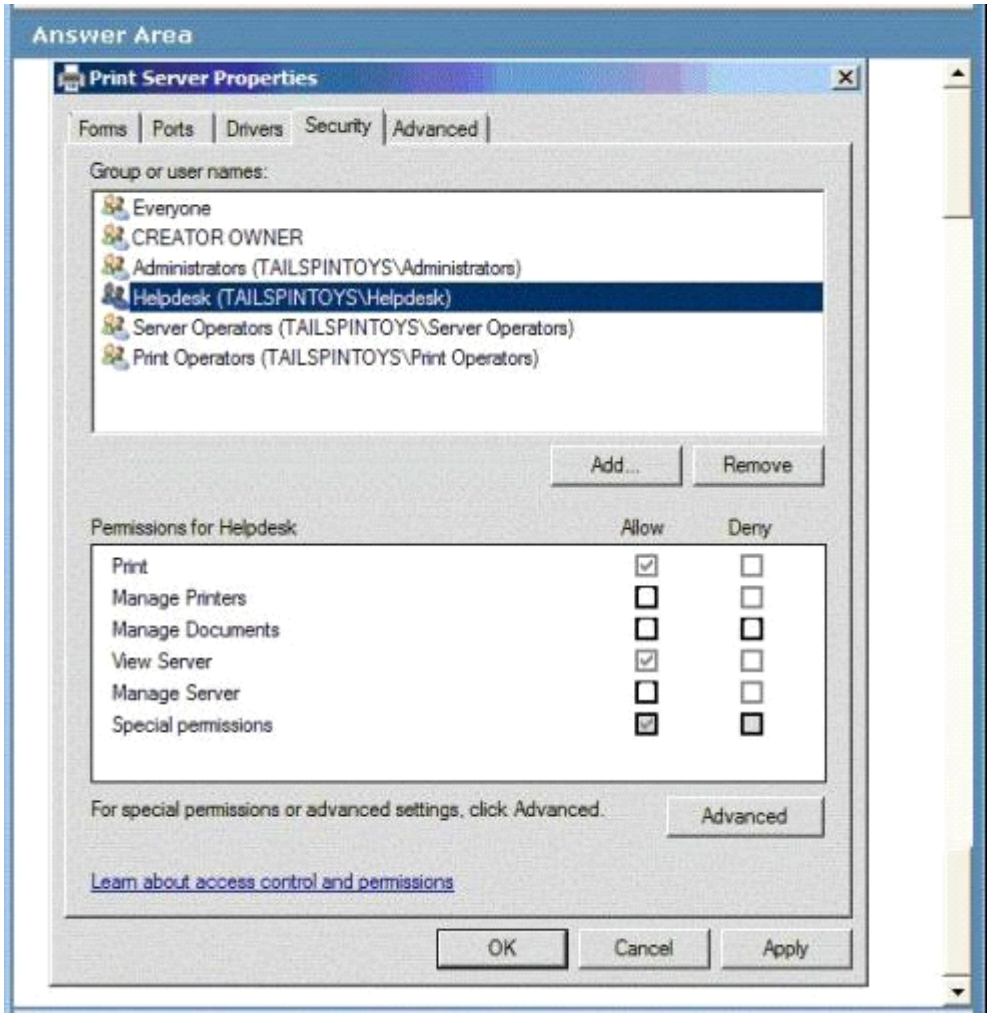
A. Upgrade TT-FILE02 to Windows Server 2008 Enterprise and use Application control policies in Group Policy.
B. Add the Connection Manager Administration Kit feature on TT-FILE02.
C. Upgrade TT-FILE02 to Windows Server 2008 R2 Standard and use Advanced Audit Policy Configuration settings in Group Policy.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

Answer: C

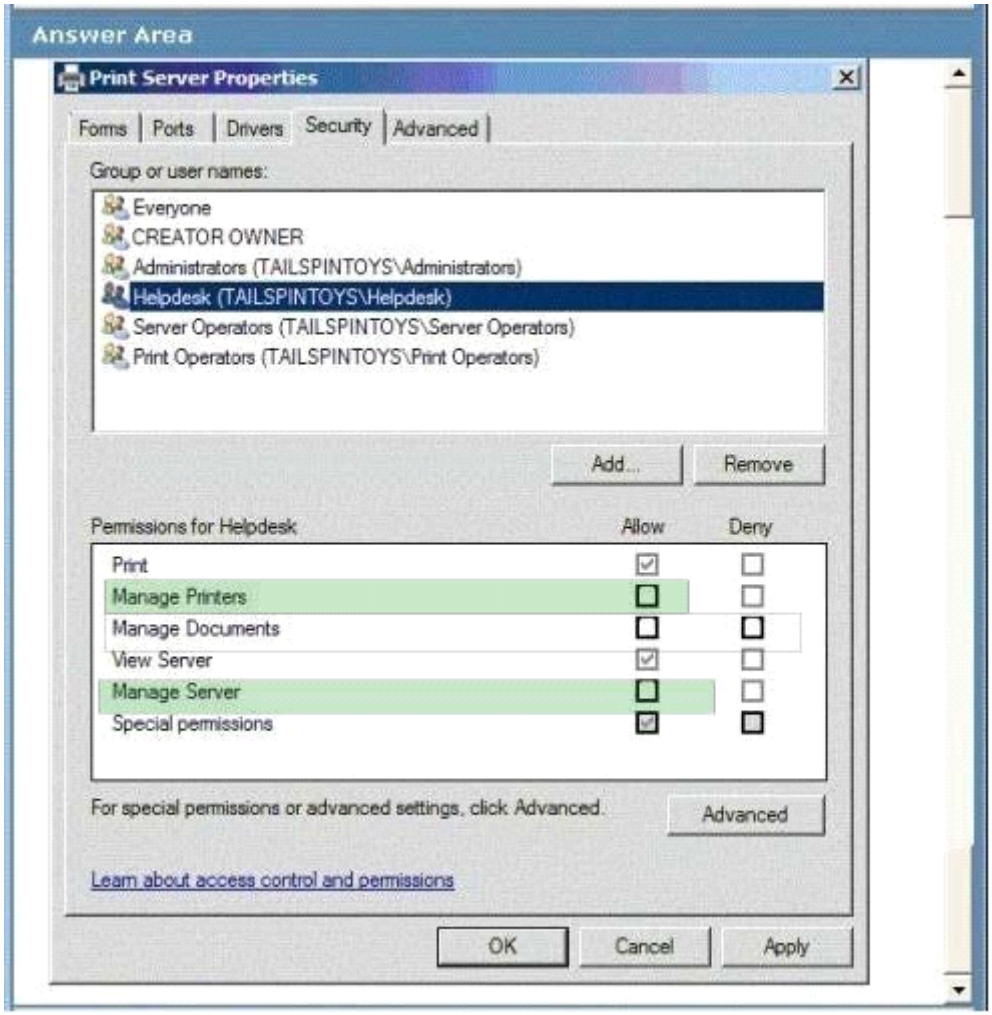
Explanation:
Security auditing enhancements in Windows Server 2008 R2 and Windows 7 can help your organization audit compliance with important business-related and security-related rules by tracking precisely defined activities, such as:
A group administrator has modified settings or data on servers 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: 5 HOTSPOT

You need to delegate print administration to meet the company requirements. What should you do?
To answer, select the appropriate check boxes in the dialog box.


Answer Area
Print Server Properties
Forms
Ports
Drivers
Security
Advanced
Group or user names:
Everyone
CREATOR OWNER
Administrators (TAILSPINTOYS\Administrators)
Helpdesk (TAILSPINTOYS\Helpdesk)
Server Operators (TAILSPINTOYS\Server Operators)
Print Operators (TAILSPINTOYS\Print Operators)
Add...
Remove
Permissions for Helpdesk
Allow
Deny
Print
Manage Printers
Manage Documents
View Server
Manage Server
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced
Learn about access control and permissions
OK
Cancel
Apply

Answer:



Explanation:

The two levels of print server permissions are:

View Server

The View Server permission assigns the ability to view the print server. Without the View Server permission, users cannot see the printers that are managed by the server. By default, this permission is given to members of the Everyone group.

Manage Server

The Manage Server permission assigns the ability to create and delete print queues (with already installed drivers), add or delete ports, and add or delete forms. A standard user with this permission is called a "delegated print administrator."

The three levels of printer permissions are:

Print

The Print permission assigns the ability for users to connect to printers and to print, pause, resume, start, and cancel their own documents. By default, this permission is given to members of the Everyone group when a print queue is created.

Manage Documents

The Manage Documents permission assigns the ability to control job settings for all documents and to pause, restart, and delete all documents.

Manage Printers

The Manage Printer permission assigns the ability to pause and restart the printer, change spooler settings, share a printer, adjust printer permissions, and change printer properties.

To create a full delegated print administrator Click Start, click Administrative Tools, right-click Print Management, and then click Run as administrator.

In the left pane, click Print Servers, right-click the applicable print server, and then click Properties.
In Print Server Properties, click the Security tab.
To configure permissions for a new group or user, click Add. Type the name of the group or user that you want to set permissions for by using the following format: domain name\username. Click OK to close the dialog box.
highlight the user or group name that you just added, and in Permissions for <user or group name>, click Allow for the Manage Server permission. (The View Server permission is assigned too.)
Select the Allow check boxes for the Print, Manage Documents, and Manage Printers permissions.
To create a partial delegated print administrator
To enable an administrator to add printers:
Follow the previous instructions, but select the Allow check boxes for the Manage Server and Print permissions. (View Server permission is assigned automatically too.)
To enable an administrator to manage existing print queues:
Follow the previous instructions, but select the Allow check boxes for the View Server, Print, Manage Documents, and Manage Printer permissions.
Print-related permissions and the tasks they enable

Question: 6

You need to recommend a solution to meet the certificate distribution requirements. What should you recommend?

A. Upgrade the Wingtip Toys client computers that run Windows XP to Windows 7.
B. Create a one-way trust from wingtiptoys.com to tailspintoys.com.
C. Create a two-way trust between tailspintoys.com and wingtiptoys.com.
D. Upgrade the Wingtip Toys servers that run Windows Server 2003 to Windows Server 2008 R2.
E. Create a one-way trust from tailspintoys.com to wingtiptoys.com.

Answer: C

Explanation:
Trusts
A trust is a relationship, which you establish between domains, that makes it possible for users in one domain to be authenticated by a domain controller in the other domain.
All Active Directory trusts between domains within a forest are transitive, two-way trusts. Therefore, both domains in a trust relationship are trusted. As shown in the following illustration, this means that if Domain A trusts Domain B and Domain B trusts Domain C, users from Domain C can access resources in Domain A (when they are assigned the proper permissions). Only members of the Domain Admins group can manage trust relationships.
Two-way trust
All domain trusts in an Active Directory forest are two-way, transitive trusts. When a new child domain is created, a two-way, transitive trust is automatically created between the new child domain and the parent domain. In a two-way trust, Domain A trusts Domain B and Domain B trusts Domain A. This means that authentication requests can be passed between the two domains in both directions. Some two-way relationships can be either nontransitive or transitive, depending on the type of trust that is created.
The Automatic Enrollment Method
Auto-enrollment makes it possible for an organization to configure the CA to automatically issue certificates to users and computers. Auto-enrollment can be defined as the process by which certificates can be obtained, updated, and stored for users and computers, without administrator and end user intervention.
The auto-enrollment feature also enables the centralized management of certificates, including:
Certificate enrollment
Certificate renewal
Modifying certificates
Superseding certificates

Question: 7

You need to remove Marc's delegated rights. What would you recommend?

A. Use the Delegation of Control Wizard.
B. Run the Resultant Set of Policy (RSoP) tool.
C. Run the dsacls command-line utility.
D. Run the xcalcs command-line utility.

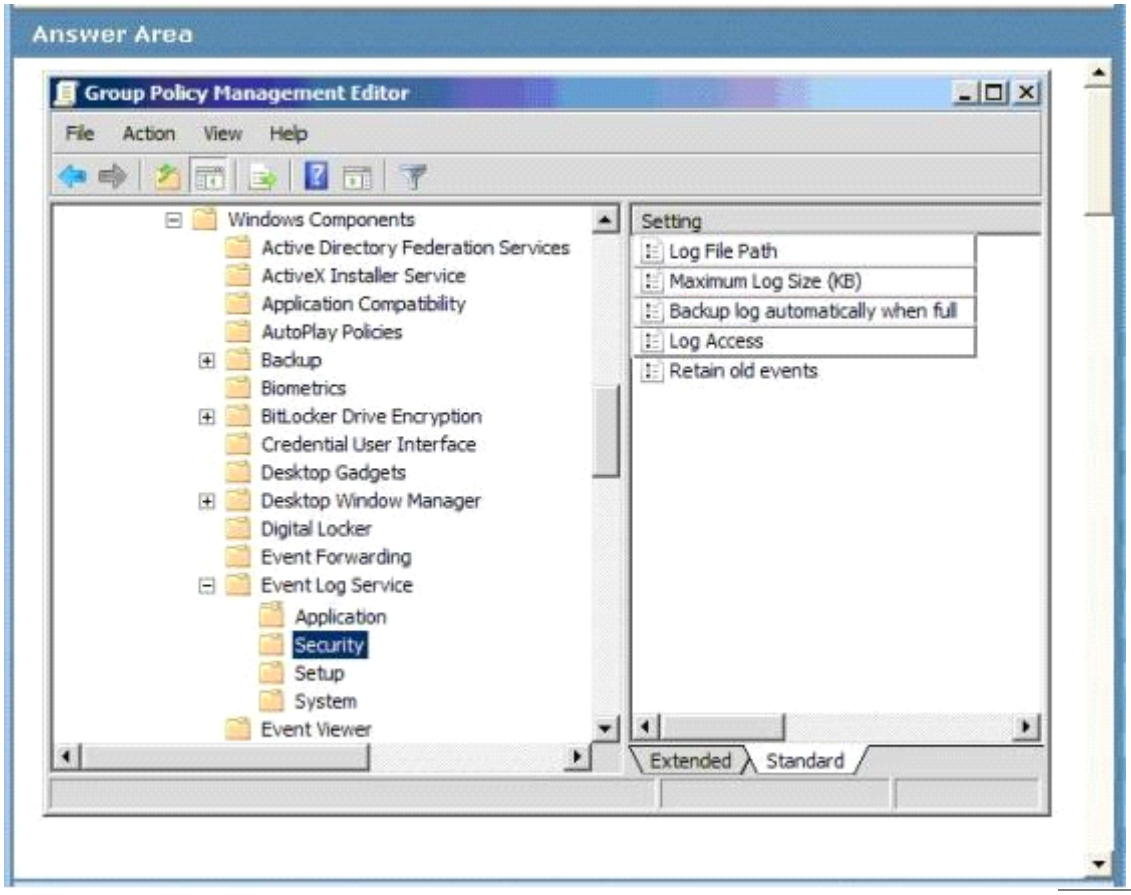
Answer: C

Explanation:
http://support.microsoft.com/kb/281146
DSACLS is used to View or Edit ACLs (access control entries) for objects in Active Directory.
Overview of Dsacls.exe
DsAcls uses the following syntax:
dsacls object [/a] [/d {user | group}:permissions [...]] [/g {user | group}:permissions [...]] [/i:{p | s | t}] [/n] [/p:{y | n}] [/r {user | group} [...]] [/s [/t]]
You can use the following parameters with Dsacls.exe:
object: This is the path to the directory services object on which to display or change the ACLs. This path must be a distinguished name (also known as RFC 1779 or x.500 format). For example:
CN=Someone,OU=Software,OU=Engineering,DC=Microsoft,DC=Com
To specify a server, add \\Servername\ before the object. For example:
\\MyServer\CN=Someone,OU=Software,OU=Engineering,DC=Microsoft,DC=Com
When you run the dsacls command with only the object parameter (dsacls object), the security information about the object is displayed.
/a : Use this parameter to display the ownership and auditing information with the permissions. /d {user | group}:permissions: Use this parameter to deny specified permissions to a user or group. User must use either user@domain or domain\user format, and group must use either group@domain or domain\group format. You can specify more than one user or group in a command. For more information about the correct syntax to use for permissions, see the <Permissions> Syntax section later in this article.
/g {user | group}:permissions: Use this parameter to grant specified permissions to a user or group. User must use either user@domain or domain\user format, and group must use either group@domain or domain \group format. You can specify more than one user or group in a command. For more information about the correct syntax to use for permissions, see the <Permissions> Syntax section later in this article.
/i:{p | s | t} : Use this parameter to specify one of the following inheritance flags:
p: Use this option to propagate inheritable permissions one level only.
s: Use this option to propagate inheritable permissions to subobjects only.
t: Use this option to propagate inheritable permissions to this object and subobjects.
/n : Use this parameter to replace the current access on the object, instead of editing it.
/p:{y | n}: This parameter determines whether the object can inherit permissions from its parent objects. If you omit this parameter, the inheritance properties of the object are not changed. Use this parameter to mark the object as protected (y = yes) or not protected (n = no).
Note This parameter changes a property of the object, not of an Access Control Entry (ACE). To determine whether an ACE is inheritable, use the /I parameter.
/r {user | group}: Use this parameter to remove all permissions for the specified user or group. You can specify more than one user or group in a command. User must use either user@domain or domain\user format, and group must use either group@domain or domain\group format.
/s: Use this parameter to restore the security on the object to the default security for that object class, as defined in the Active Directory schema.

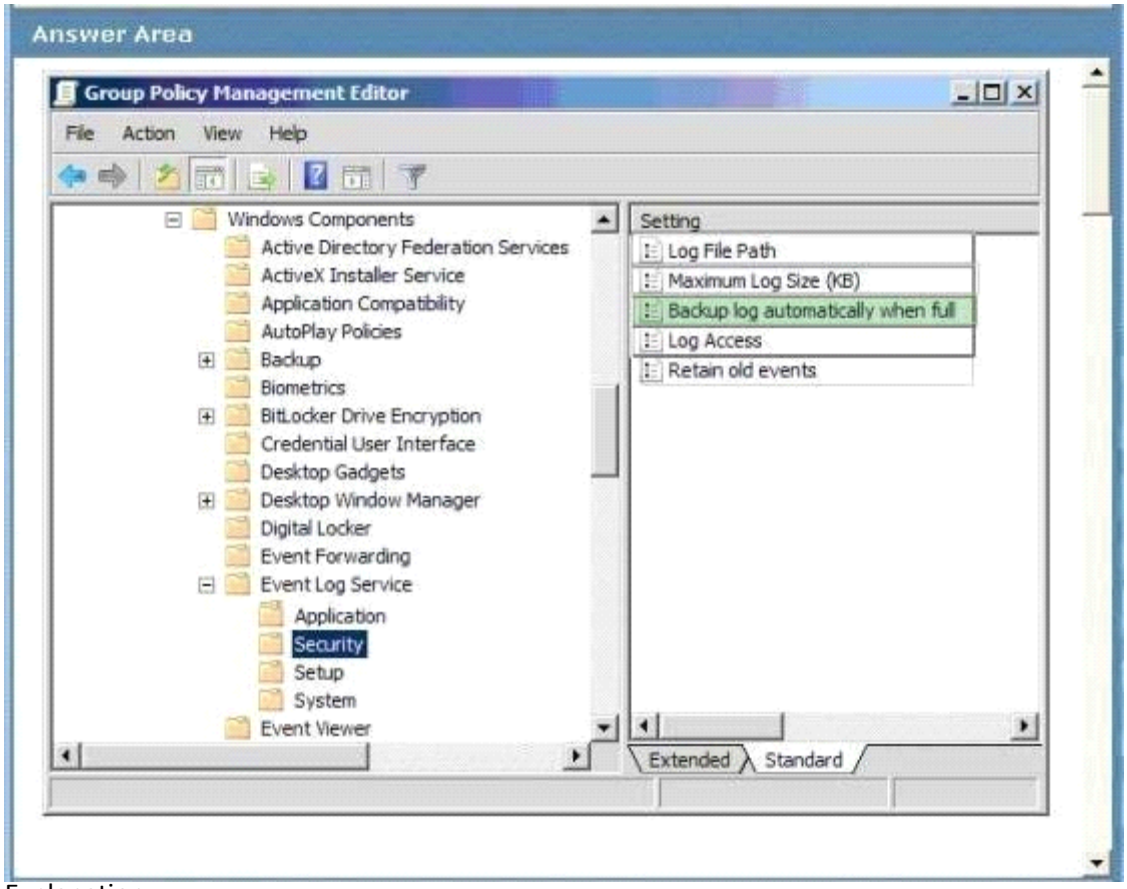
/t : Use this parameter to restore the security on the tree of objects to the default for each object class. This switch is valid only when you also use the /s parameter.

Question: 8 HOTSPOT

New security events are not being written to the current Security event log in the tailspintoys.com domain. However, old security events are still being maintained in the log. You need to meet the security event log requirements for the tailspintoys.com domain. Which Group Policy setting or settings should you select?
To answer, select the appropriate setting or settings in the Group Policy Management Editor.



Answer:



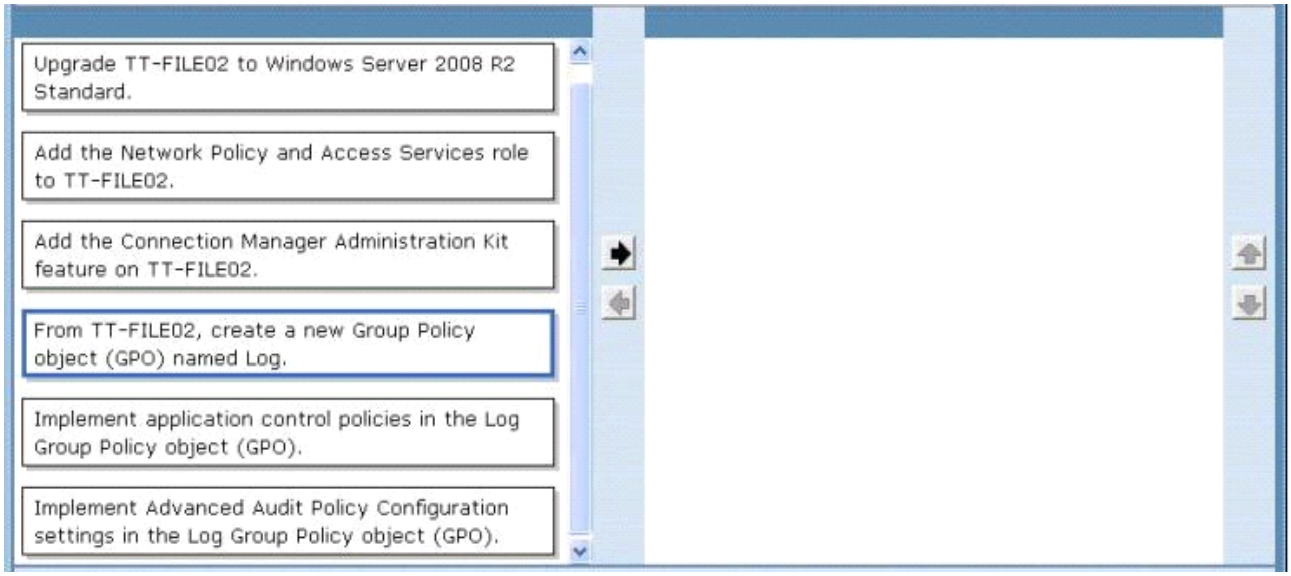
Explanation:
Backup log automatically when full
This policy setting controls Event Log behavior when the log file reaches its maximum size and takes effect only if the Retain old events policy setting is enabled. If you enable this policy setting and the Retain old events policy setting is enabled, the Event Log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the Retain old events policy setting is enabled, new events are discarded and the old events are retained. When this policy setting is not configured and the Retain old events policy setting is enabled, new events are discarded and the old events are retained.
Possible values:
Enabled
Disabled
Not Configured
normally you need RETAIN OLD EVENTS enabled also But this is already set in the default domain policy per the exhibit for the testlet

Question: 9 DRAG DROP

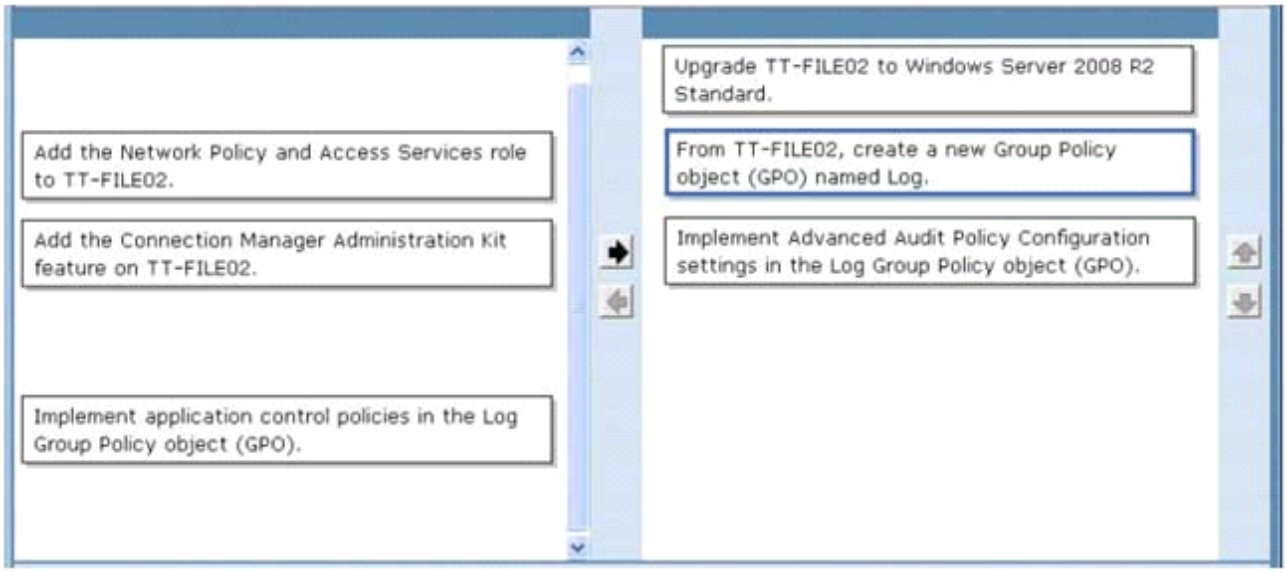
You need to recommend a solution that meets the following requirements:

- 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.

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.)



Answer:



Question: 10

You need to recommend a solution to meet the following requirements:

- Meet the company auditing requirements.
- Ensure that further administrative action is not required when new folders are added to the file server.

What should you recommend? (Choose all that Apply.)

A. Enable the Audit File System Group Policy setting for Success.
B. Enable the Audit object access Group Policy setting for Success.
C. Enable the Audit File System Group Policy setting for Failure.
D. Enable the Audit Handle Manipulation Group Policy setting for Success.
E. Enable the File system option of the Global Object Access Auditing Group Policy setting.
F. Enable the Audit Handle Manipulation Group Policy setting for Failure.

Answer: B, D, E

Explanation:
Security auditing allows you to track the effectiveness of your network defenses and identify attempts to circumvent them. There are a number of auditing enhancements in Windows Server 2008 R2 and Windows 7 that increase the level of detail in security auditing logs and simplify the deployment and management of auditing policies.
Auditing policy
Before you implement auditing policy, you must decide which event categories you want to audit. The auditing settings that you choose for the event categories define your auditing policy. On member servers and workstations that are joined to a domain, auditing settings for the event categories are undefined by default. On domain controllers, auditing is turned on by default. By defining auditing settings for specific event categories, you can create an auditing policy that suits the security needs of your organization.
Audit Object Access
This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.
If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.
To set this value to No auditing, in the Properties dialog box for this policy setting, select the Define these policy settings check box and clear the Success and Failure check boxes.
Note that you can set a SACL on a file system object using the Security tab in that object's Properties dialog box.
http://technet.microsoft.com/en-us/library/cc776774%28v=ws.10%29.aspx
Audit Handle Manipulation Group Policy setting
This policy setting determines whether the operating system generates audit events when a handle to an object is opened or closed. Only objects with configured SACLs generate these events, and only if the attempted handle operation matches the SACL. Event volume can be high, depending on how SACLs are configured.
When used together with the Audit File System or Audit Registry policy settings, the Audit Handle Manipulation policy setting can provide an administrator with useful "reason for access," audit data detailing the precise permissions on which the audit event is based. For example, if a file is configured as a read-only resource but a user attempts to save changes to the file, the audit event will log not just the event itself but the permissions that were used, or attempted to be used, to save the file changes.
Global Object Access Auditing Group Policy setting.
Global Object Access Auditing. In Windows Server 2008 R2 and Windows 7, administrators can define computer-wide system access control lists (SACLs) for either the file system or registry. The specified SACL is then automatically applied to every single object of that type. This can be useful both for verifying that all critical files, folders, and registry settings on a computer are protected, and for identifying when an issue with a system resource occurs.

Question: 11

Your network contains an Active Directory domain. You have a server that runs Windows Server 2008 R2 and has the Remote Desktop Services server role enabled. All client computers run Windows 7. You need to plan the deployment of a new line of business application to all client computers.
The deployment must meet the following requirements:
- Users must access the application from an icon on their desktops.
- Users must have access to the application when they are not connected to the network.
What should you do?

A. Publish the application as a RemoteApp.
B. Publish the application by using Remote Desktop Web Access (RD Web Access).
C. Assign the application to the Remote Desktop Services server by using a Group Policy object (GPO).
D. Assign the application to all client computers by using a Group Policy object (GPO).

Answer: D

Explanation:
Section: Exam B Mixed Q&A
Explanation:
http://support.microsoft.com/kb/816102
Assign a Package
To assign a program to computers that are running Windows Server 2003, Windows 2000, or Microsoft Windows XP Professional, or to users who are logging on to one of these workstations:
1. Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
2. In the console tree, right-click your domain, and then click Properties.
3. Click the Group Policy tab, select the group policy object that you want, and then click Edit.
4. Under Computer Configuration, expand Software Settings.
5. Right-click Software installation, point to New, and then click Package.
6. In the Open dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\file server\share\file name.msi.
Important Do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package.
7. Click Open.
8. Click Assigned, and then click OK. The package is listed in the right pane of the Group Policy window.
9. Close the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in.
10. When the client computer starts, the managed software package is automatically installed.

Question: 12

Your network contains an Active Directory domain. The domain contains a Remote Desktop Services server that runs Windows Server 2008 R2. All client computers run Windows 7. You need to deploy a new line of business application. The deployment must meet the following requirements:
- Users must have access to the application from the company portal.
- Users must always have access to the latest version of the application.
- You must minimize the number of applications installed on the client computers.
What should you do?

A. Publish the application to the users by using a Group Policy object (GPO).
B. Publish the application as a RemoteApp. Enable Remote Desktop Web Access (RD Web Access).
C. Assign the application to the client computers by using a Group Policy object (GPO).
D. Deploy the application by using Microsoft System Center Configuration Manager (SCCM) 2007 R2.

Answer: B

Explanation:
http://technet.microsoft.com/en-us/library/cc753844%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc730673%28WS.10%29.aspx
Terminal Services RemoteApp (TS RemoteApp)
Terminal Services RemoteApp (TSRemoteApp) enables organizations to provide access to standard Windows®-based programs from virtually any location to users with computers running WindowsVista®, WindowsServer®2008, or WindowsXP with Service Pack3 (SP3). TSRemoteApp is also available to users with computers running WindowsXP with Service Pack2 (SP2), Windows Server2003 with Service Pack1 (SP1), or Windows Server2003 with SP2 that have

the new Remote Desktop Connection (RDC) client installed.
What does TSRemoteApp do?
RemoteApp programs are programs that are accessed remotely through Terminal Services and appear as if they are running on the end user's local computer. Users can run RemoteApp programs side by side with their local programs. A user can minimize, maximize, and resize the program window, and can easily start multiple programs at the same time. If a user is running more than one RemoteApp program on the same terminal server, the RemoteApp programs will share the same Terminal Services session.
Users can run RemoteApp programs in a number of ways. They can:
Double-click a Remote Desktop Protocol (.rdp) file that has been created and distributed by their administrator.
Double-click a program icon on their desktop or Start menu that has been created and distributed by their administrator with a Windows Installer (.msi) package.
Double-click a file whose extension is associated with a RemoteApp program. (This can be configured by their administrator with a Windows Installer package.)
Access a link to the RemoteApp program on a Web site by using TSWeb Access.
The .rdp files and Windows Installer packages contain the settings needed to run RemoteApp programs. After opening the RemoteApp program on a local computer, the user can interact with the program that is running on the terminal server as if it were running locally.
Key scenarios for TSRemoteApp
TSRemoteApp is especially useful in scenarios such as the following:
Remote users. Users often need to access programs from remote locations, such as while working from home or while traveling. If you want users to access RemoteApp programs over an Internet connection, you can allow access through a Virtual Private Network (VPN), or you can deploy TSRemoteApp together with Terminal Services Gateway (TSGateway) to help secure remote access to the programs.
Branch offices. In a branch office environment, there may be limited local IT support and limited network bandwidth. By using TSRemoteApp, you can centralize the management of your applications and improve remote program performance in limited bandwidth scenarios.
Line-of-business (LOB) applications deployment. Companies often need to run consistent
LOB applications on computers that are running different Windows versions and configurations. Instead of deploying the LOB applications to all the computers in the company, which can be expensive in terms of time and cost, you can install the LOB applications on a terminal server and make them available through TSRemoteApp.
Application deployment. With TSRemoteApp you do not have to deploy and maintain different versions of the same program for individual computers. If employees need to use multiple versions of a program, you can install those versions on one or more terminal servers, and users can access them through TSRemoteApp.
Roaming users. In a company with a flexible desk policy, users can work from different computers. In some cases, the computer where a user is working may not have the necessary programs installed locally.
By using TSRemoteApp, you can install the programs on a terminal server and make them available to users as if those programs were installed locally.

Question: 13

You want to deploy web site with less attack surface, high available solution with minimal cost. Which one would you recommend? There are more than one correct answers but chose the best option.

A. Windows server 2008 R2 Enterprise full installation
B. Windows server 2008 R2 standard full installation.
C. Windows web server 2008 R2 with IIS 7.5 Server core.
D. Windows web server 2008 R2 with IIS 7.5 full installation.

Answer: C