Exam : **70-647**

Title : PRO: Windows Server 2008, Enterprise Administrator

Version : V15.02

Topic 1, Mixed Questions

1.Your network consists of one Active directory domain. The functional level of the domain is Windows Server 2008 R2. Your company has three departments named Sales, Marketing, and Engineering. All users in the domain are in an organizational unit (OU) named All Users. You have three custom applications. You deploy all custom applications by using a Group Policy object (GPO) named AppInstall. The Sales department purchases a new application that is only licensed for use by the Sales department. You need to recommend a solution to simplify the distribution of the new application.
The solution must meet the following requirements:
- The application must only be distributed to licensed users.
- The amount of administrative effort required to manage the users must remain unaffected.
- The three custom applications must be distributed to all existing and new users on the network.
What should you recommend?
A. Create a new child domain for each department and link the AppInstall GPO to each child domain. Create a new GPO. Link the new GPO to the Sales domain.
B. Create a new child OU for each department. Link the AppInstall GPO to the Marketing OU and the Engineering OU. Create a new GPO. Link the new GPO to the Sales OU.
C. Create a new group for each department and filter the AppInstall GPO to each group. Create a new GPO. Link the new GPO to the domain. Filter the new GPO to the Sales group.
D. Create a new group for each department. Filter the AppInstall GPO to the Marketing group and the Engineering group. Create a new GPO. Link the new GPO to the domain. Filter the new GPO to the Sales group.
Answer: C
Explanation:
To ensure that the other applications are distributed to all existing and new users on the network, you need to create a new group for each department and filter the InstallApp GPO to each group. Filtering allows you to target only specific computers or users. You can create and modify multiple preference items within each GPO, and you can filter each preference item to target only specific computers or users. Finally to simplify the distribution of the licensed application to the users of the sales department, you need to create and link a new GPO to the domain and filter the new GPO to the Sales group.
You should not filter the InstallApp GPO to the Marketing group and the Development groups only because all the other applications beside the licensed application need to be installed to the Sales department also.
Reference: Group Policy/ Preferences
http://technet2.microsoft.com/windowsserver2008/en/library/3b4568bc-9d3c-4477-807d-2ea149ff06491033.mspx?mfr=true

2.Your network contains servers that run Windows Server 2008 R2 and client computers that run Windows 7. All network routers support IPsec connections. Client computers and servers use IPsec to connect through network routers. You have two servers named Server1 and Server2. Server1 has Active Directory Certificate Services (AD CS) installed and is configured as a certification authority (CA). Server2 runs Internet Information Services (IIS). You need to recommend a certificate solution for the network routers.
The solution must meet the following requirements:

- Use the Simple Certificate Enrollment Protocol (SCEP).
- Enable the routers to automatically request certificates.
What should you recommend implementing?
A. Certification authority Web enrollment services on Server2
B. Network Device Enrollment Service on Server2
C. Online Responder service on Server1
D. Subordinate CA on Server1
Answer: B
Explanation:
To recommend a certificate solution for the network routers that would enable the routers to automatically request certificates and that would use Simple Certificate Enrollment Protocol (SCEP), you need to implement Network Device Enrollment Service on Server2.
The Network Device Enrollment Service allows routers and other network devices to obtain certificates based on the Simple Certificate Enrollment Protocol (SCEP) from Cisco Systems Inc.
Reference: Windows Server Active Directory Certificate Services Step-by-Step Guide/ AD CS Technology Review
http://technet2.microsoft.com/windowsserver2008/en/library/f7dfccc0-4f65-4d6f-a801-ae6a87fd174c1033.mspx?mfr=true

3.Your network consists of one Active Directory domain. Your company uses a firewall to connect to the Internet. Inbound TCP/IP port 443 is allowed on the firewall. You have terminal servers on the internal network. You have one server on the internal network that has Terminal Services Gateway (TS Gateway) deployed. All servers run Windows Server 2008. You need to recommend a solution that enables remote users to access network resources by using TS Gateway.
What should you recommend?
A. Change the firewall rules to permit traffic through port 3389 from the Internet.
B. Install the Terminal Services server role with the Terminal Services Web Access (TS Web Access) services role.
C. Install the Terminal Services server role with the Terminal Services Session Broker (TS Session Broker) services role.
D. Create a Terminal Services connection authorization policy (TS CAP) and a Terminal Services resource authorization policy (TS RAP).
Answer: D
Explanation:
To implement a solution that enables remote users to access network resources by using TS Gateway, you need to create a Terminal Services connection authorization policy (TS CAP) and a Terminal Services resource authorization policy (TS RAP).
TS CAPs allow you to specify who can connect to a TS Gateway server. Users are granted access to a TS Gateway server if they meet the conditions specified in the TS CAP. You must also create a Terminal Services resource authorization policy (TS RAP). A TS RAP allows you to specify the internal network resources that users can connect to through TS Gateway. Until you create both a TS CAP and a TS RAP, users cannot connect to internal network resources through this TS Gateway server.
Reference: Terminal Services Gateway (TS Gateway) / Why are TS CAPs important?
http://technet2.microsoft.com/windowsserver2008/en/library/9da3742f-699d-4476-b050-c50aa14aaf0810

33.mspx?mfr=true

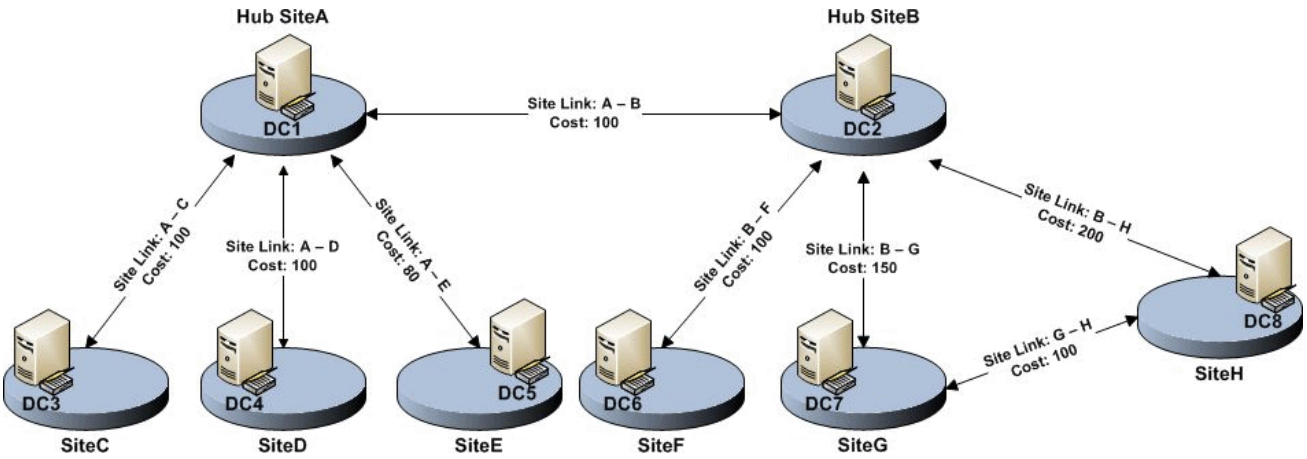
4.Your network consists of one Active Directory forest that contains one root domain and 22 child domains. All domain controllers run Windows Server 2003. All domain controllers run the DNS Server service and host Active Directory-integrated zones. Administrators report that it takes more than one hour to restart the DNS servers. You need to reduce the time it takes to restart the DNS servers.
What should you do?
A. Upgrade all domain controllers to Windows Server 2008.
B. Upgrade all domain controllers in the root domain to Windows Server 2008, and then set the functional level for the root domain to Windows Server 2008.
C. Deploy new secondary zones on additional servers in each child domain.
D. Change the Active Directory-integrated DNS zones to standard primary zones.
Answer: A
Explanation:
Sometime DNS server can take an hour or more in companies that have extremely large zones and the DNS data of the company is stored in AD DS. The result is that the DNS server is effectively unavailable to service client requests for the entire time that it takes to load AD DS-based zones. The problem can be solved by upgrading the domain controllers to Windows Server 2008.
This is because a DNS server running Windows Server 2008 now loads zone data from AD DS in the background while it restarts so that it can respond to requests for data from other zones.
Reference: DNS Server Role/ Background zone loading
http://technet2.microsoft.com/windowsserver2008/en/library/533a1cfc-5173-4248-914c-433bd018f66d1033.mspx?mfr=true

5.Your network consists of one Active Directory domain. All domain controllers run Windows Server 2008. You have file servers that run Windows Server 2008. Client computers run Windows Vista and UNIX-based operating systems. All users have both Active Directory user accounts and UNIX realm user accounts. Both environments follow identical user naming conventions. You need to provide the UNIX-based client computers access to the file servers.
The solution must meet the following requirements:
- Users must only log on once to access all resources.
- No additional client software must be installed on UNIX-based client computers.
What should you do?
A. Create a realm trust so that the Active Directory domain trusts the UNIX realm.
B. Install an Active Directory Federation Services (AD FS) server that runs Windows Server 2008 R2
C. Enable the subsystem for UNIX-based applications on the file servers. Enable a Network File System (NFS) component on the client computers.
D. Enable the User Name Mapping component and configure simple mapping. Enable a Network File System (NFS) component on the servers.
Answer: D
Explanation:
To provide the UNIX-based client computers access to the file servers, you need to enable the User Name Mapping component and configure simple mapping and also enable a Network File System (NFS) component on the servers.

User Name Mapping (UNM) bridges the gap between the different user identification used in Windows and UNIX worlds. When UNM is used it in conjunction with Server for NFS, UNM authenticates the incoming NFS access requests. With Client for NFS, it determines the effective UID and GID to be sent with the NFS requests to UNIX NFS servers.
Reference: Configuring User Name Mapping - Part 2 (Simple Mapping)
http://blogs.msdn.com/sfu/archive/2007/10/02/configuring-user-name-mapping-part-2-simple-mapping.aspx

6.Your Company has a main office and 10 branch offices. The network consists of one Active Directory domain. All domain controllers run Windows Server 2008 R2 and are located in the main office. Each branch office contains one member server. Branch office administrators in each branch office are assigned the necessary rights to administer only their member servers. You deploy one read-only domain controller (RODC) in each branch office. You need to recommend a security solution for the branch office Windows Server 2008 R2 domain controllers.
The solution must meet the following requirements:
- Branch office administrators must be granted rights on their local domain controller only.
- Branch office administrators must be able to administer the domain controller in their branch office. This includes changing device drivers and running Windows updates.
What should you recommend?
A. Add each branch office administrator to the Administrators group of the domain.
B. Add each branch office administrator to the local Administrators group of their respective domain controller.
C. Grant each branch office administrator Full Control permission on their domain controller computer object in Active Directory.
D. Move each branch office domain controller computer object to a new organizational unit (OU). Grant each local administrator Full Control permission on the new OU.
Answer: B
Explanation:
To allow branch office administrators to manage their local domain controller only, change device drivers, and run Windows updates, you need to add each branch office administrator to the local Administrators group of their respective domain controller. The users of Local administrator group have administrative rights on their local domain controllers to manage several machines to perform all necessary administrative tasks but they have restricted rights as compared to domain administrators.
Reference: Adding a group to the local administrators group
http://blogcastrepository.com/blogs/kim_oppalfenss_systems_management_ideas/archive/2007/04/23/adding-a-group-to-the-local-administrators-group.aspx

7.Your network consists of one Active Directory domain. The functional level of the forest is Windows Server 2003. All domain controllers run Windows Server 2003.
The relevant portion of the network is configured as shown in the exhibit. (Click the Exhibit button.)



The Bridge all site links option is enabled. You need to ensure that domain controllers in the spoke sites can replicate with domain controllers in only the hub sites. The solution must ensure that domain controllers can replicate if a server fails in one of the hub sites.

What should you do?

A. Lower the site link costs between the spoke sites and the hub sites.

B. Disable the Bridge all site links option. Create site link bridges that include the site links between each spoke site and the hub sites.

C. Disable the Bridge all site links option. Install a writable domain controller that runs Windows Server 2008 in each hub site.

D. Enable the global catalog server attribute for all domain controllers in the hub sites. Upgrade all domain controllers in the spoke sites to Windows Server 2008.

Answer: B

Explanation:

By default, all site links are bridged so that all the sites that are not connected by an explicit site link can communicate directly, through a chain of intermediary site links and sites.

However, if you want to ensure that domain controllers in the spoke sites do not replicate with other spoke sites when a server fails in one of the hub sites, you need to disable the Bridge all site links option.

You need to then create site link bridges to create the site links between each spoke site and the hub sites to ensure that domain controllers in the spoke sites can replicate with domain controllers in the hub sites.

Reference: Configuring site link bridges

http://technet2.microsoft.com/windowsserver/en/library/b42bb443-c5cd-4539-8dfa-917dbddb087a1033.mspx?mfr=true

8.Your company has 5,000 users. The network contains servers that run Windows Server 2008.

You need to recommend a collaboration solution for the users to meet the following requirements:

- Support tracking of document version history.
- Enable shared access to documents created in Microsoft Office.
- Enable shared access to documents created by using Web pages.

The solution must be achieved without requiring any additional costs.

What should you recommend?

A. Install servers that run the Web Server role.

B. Install servers that run the Application Server role.

C. Install servers that run Microsoft Windows SharePoint Services (WSS) 3.0.

D. Install servers that run Microsoft Office SharePoint Server (MOSS) 2007.
Answer: C
Explanation:
To achieve the desired results without requiring any additional cost, you need to use Microsoft Windows SharePoint Services (WSS) 3.0.
Reference: Microsoft Windows SharePoint Services 3.0 and the Mobile Workplace
http://download.microsoft.com/download/b/b/6/bb6672dd-252c-4a21-89de-78cfc8e0b69e/WSS%20Mobile%20Workplace.doc

9.Your Company has 10 offices. Each office has 10 domain controllers that run Windows Server 2008. The network consists of one Active directory domain. Each office has a local administrator. You use domain-level Group Policy objects (GPO). Office administrators have the necessary permissions to create and link domain-level Group Policy objects. You create custom Administrative Template (.admx) files locally on a computer that runs Windows Vista. You need to implement a GPO management strategy to ensure that the administrators can access the .admx files and any future updates to the .admx files from each office. The solution must ensure that .admx files remain identical across the company.
What should you do?
A. In the domain, create a central store. Copy the custom .admx files to the central store.
B. In each office, create a central store on a file server. Copy the custom .admx files to the central store.
C. Create a GPO and link it to the domain. Add the .admx files to the GPO.
D. Create a GPO and link it to the Domain Controllers organizational unit (OU). Add the custom .admx files to the GPO.
Answer: A
Explanation:
To implement a GPO management strategy to ensure that the administrators can access the .admx files and any future updates to these files from each office and to ensure that the .admx files remain identical across the company, you need to create a central store in the domain and copy the custom .admx files to the central store.
The central store for ADMX files allows all local administrators to edit domain-based GPOs to access the same set of ADMX files. When a central store is created, the Group Policy tools will use the ADMX files only in the central store, ignoring the locally stored versions. You need to copy the custom .admx files to the central store and not add them because there need to be only one ADMX file and not multiple versions of the same file in the central store.
Reference: Scenario 2: Editing Domain-Based GPOs Using ADMX Files
http://technet2.microsoft.com/WindowsVista/en/library/1494d791-72e1-484b-a67a-22f66fbf9d171033.mspx?mfr=true

10.Your network consists of one Active Directory domain. The network contains one Active Directory site. All domain controllers run Windows Server 2008. You create a second Active Directory site and plan to install a domain controller that runs Windows Server 2008 in the new site. You also plan to deploy a new firewall to connect the two sites. You need to enable the domain controllers to replicate between the two sites.
Which traffic should you permit through the firewall?
A. LDAP

B. NetBIOS
C. RPC
D. SMTP
Answer: C
Explanation:
You should permit RPC traffic through the firewall to enable the domain controllers to replicate between the two sites because the Active Directory relies on remote procedure call (RPC) for replication between domain controllers. You can open the firewall wide to permit RPC's native dynamic behavior.
Reference: Active Directory Replication over Firewalls
http://technet.microsoft.com/en-us/library/bb727063.aspx

11.Your network consists of one Active Directory domain. All domain controllers run Windows Server 2008. You need to prepare the environment to provide a high-availability solution for a back-end Microsoft SQL Server 2005 data store.
What should you do?
A. Install a Windows Server 2003 Network Load Balancing cluster.
B. Install a Windows Server 2008 Network Load Balancing cluster.
C. Install a Windows Server 2008 failover cluster that has shared storage.
D. Install a Windows Server 2008 failover cluster that has direct attached storage.
Answer: C
Explanation:
To ensure the high availability of the data store, you need to use Windows Server 2008 failover cluster having a shared storage.
Failover clustering can help you build redundancy into your network and eliminate single points of failure. Administrators have better control and can achieve better performance with storage than was possible in previous releases. Failover clusters now support GUID partition table (GPT) disks that can have capacities of larger than 2 terabytes, for increased disk size and robustness. Administrators can now modify resource dependencies while resources are online, which means they can make an additional disk available without interrupting access to the application that will use it. And administrators can run tools in Maintenance Mode to check, fix, back up, or restore disks more easily and with less disruption to the cluster
You should not use Network Load Balancing (NLB) because it only allows you to distribute TCP/IP requests to multiple systems in order to optimize resource utilization, decrease computing time, and ensure system availability.
Reference: High Availability
http://www.microsoft.com/windowsserver2008/en/us/high-availability.aspx

12.Your company has one main office and 10 branch offices. The network consists of one Active Directory domain. All domain controllers run Windows Server 2008 and are located in the main office. You plan to deploy one Windows Server 2008 domain controller in each branch office. You need to recommend a security solution for the branch office domain controllers. The solution must prevent unauthorized users from copying the Active Directory database from a branch office domain controller by starting the server from an alternate startup disk.
What should you recommend on each branch office domain controller?

A. Enable the secure server IPsec policy.
B. Enable the read-only domain controller (RODC) option.
C. Enable Windows BitLocker Drive Encryption (BitLocker).
D. Enable an Encrypting File System (EFS) encryption on the %Systemroot%\NTDS folder.
Answer: C
Explanation:
To configure domain controller of each branch office to ensure to no unauthorized user should be allowed to copy the Active Directory database from a branch office domain controller by starting the server from an alternate startup disk, you need to use Windows BitLocker Drive Encryption (BitLocker)
BitLocker allows you to encrypt all data stored on the Windows operating system volume and use the security of using a Trusted Platform Module (TPM) that helps protect user data and to ensure that a computer running Windows Vista or Server 2008 have not been tampered with while the system was offline.
In addition, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable USB device, such as a flash drive, that contains a startup key. This process will ensure that all the users can access all files on the servers if they have the PIN. You cannot use an alternate startup disk to boot the disk.
Reference: BitLocker Drive Encryption Technical Overview
http://technet2.microsoft.com/windowsserver2008/en/library/a2ba17e6-153b-4269-bc46-6866df4b253c1033.mspx?mfr=true

13.Your network contains servers that run Windows Server 2008. Microsoft Windows SharePoint Services (WSS) are available on the network. WSS is only accessible from the internal network.
Several users use devices that run Windows Mobile 6.0. The users can establish only HTTP and HTTPS sessions from the Internet. You need to enable users to access WSS from the Internet by using their Windows Mobile devices. The solution must ensure that all connections from the Internet to WSS are encrypted.
What should you do?
A. Install Microsoft Internet Security and Acceleration (ISA) Server 2006 and create a HTTPS publishing rule.
B. Install Microsoft Internet Security and Acceleration (ISA) Server 2006 and create a Secure RPC publishing rule.
C. Install the Network Policy and Access Services (NPAS) role and enable Secure Socket Tunneling (SSTP) connections. Configure WSS to require Kerberos authentication.
D. Install the Network Policy and Access Services (NPAS) role and enable Secure Socket Tunneling (SSTP) connections. Configure WSS to require IPsec encryption.
Answer: A
Explanation:
To ensure that mobile users are allowed to access WSS from the Internet by using their Windows Mobile devices securely and to ensure that all the connections from the Internet to WSS are encrypted, you need to use external Firewall solution by using Microsoft Internet Security and Acceleration ISA Server 2006 and create a HTTPS publishing rule on ISA Server.
The Firewall will ensure a secure connection to the internal network of the company. When you publish an application through ISA Server 2006, you are protecting the server from direct external access because

the name and IP address of the server are not accessible to the user. The user accesses the ISA Server computer, which then forwards the request to the server according to the conditions of the server publishing rule.
When you create a secure Web publishing rule, you can configure how SSL requests will be redirected as Hypertext Transfer Protocol (HTTP) requests or as SSL requests.
Reference: Deploying Office SharePoint Server 2007 with ISA Server 2006 / No direct access to the server from the Internet
http://technet.microsoft.com/en-us/library/cc268368.aspx

14.Your company has one main office and 20 branch offices. Each office is configured as an Active Directory site. The network consists of one Active Directory domain. All servers run Windows Server 2008 R2 and all client computers run Windows 7. The main office contains three domain controllers.
You need to deploy one domain controller in each branch office to meet the following requirements:
- Authentication to a main office domain controller must only occur if a local domain controller fails.
- Client computers in the main office must not authenticate to a domain controller in a branch office.
- Client computers in a branch office must not authenticate to a domain controller in another branch office.
- Client computers in each branch office must attempt to authenticate to the domain controller at their local site first.
What should you do first?
A. Associate the IP subnet of each branch office to the Active Directory site of the main office.
B. Select the read-only domain controller (RODC) option and the Global Catalog option when deploying the branch office domain controllers.
C. Create a Group Policy object (GPO) that applies to all branch office domain controllers and controls the registration of DNS service location (SRV) records.
D. Configure only the main office domain controllers as global catalog servers. Enable Universal Group Membership Caching in the Active Directory site for each branch office.
Answer: C
Explanation:
To deploy domain controllers in the branch offices and make sure that the client computers in each branch office must attempt to authenticate to the domain controller at their local site first and the authentication to a main office domain controller must only occur if a local domain controller fails and to meet other specified requirements, you need to create a Group Policy object (GPO) for all branch office domain controllers to control the registration of DNS service location (SRV) records.
SRV records are used by Windows Server to locate domain controllers in specific domains, domain controllers in the same site, global catalogue servers, and key distribution centers.
Reference: DNS Service Records and Locating Domain Controllers
http://www.2000trainers.com/windows-2000/dns-service-records/

15.Your network consists of one Active Directory domain that contains only domain controllers that run Windows Server 2003. Your company acquires another company. You need to provide user accounts for the employees of the newly acquired company. The solution must support multiple account lockout policies.
What should you do?
A. Implement Authorization Manager.

B. Implement Active Directory Federation Services (AD FS).
C. Upgrade one domain controller to Windows Server 2008. Raise the functional level of the domain to Windows Server 2003.
D. Upgrade all domain controllers to Windows Server 2008. Raise the functional level of the domain to Windows Server 2008.
Answer: D
Explanation:
To support multiple account lockout policies, you need to upgrade all domain controllers to Windows Server 2008. In Microsoft® Windows 2000 and Windows Server 2003 Active Directory domains, you could apply only one password and account lockout policy. In Windows Server 2008, you can use fine-grained password policies to specify multiple password policies and apply different password restrictions and account lockout policies to different sets of users within a single domain.
Next you need to raise the functional level of the domain to Windows Server 2008 because Windows Server 2003 functional level does not support Windows Server 2008 domain controllers.
Reference: Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration
http://technet2.microsoft.com/windowsserver2008/en/library/2199dcf7-68fd-4315-87cc-ade35f8978ea1033.mspx?mfr=true
Reference: Appendix of Functional Level Features
http://technet2.microsoft.com/windowsserver2008/en/library/34678199-98f1-465f-9156-c600f723b31f1033.mspx?mfr=true

16.Your network consists of one Active Directory forest that contains four Active Directory domains named Sales, Marketing, Finance, and IT. The Finance domain contains a domain controller that runs Windows Server 2008. The Sales, Marketing, and IT domains contain only domain controllers that run Windows Server 2003. You need to prepare the environment for the deployment of a read-only domain controller (RODC) in the Finance domain and in the IT domain. You must ensure that the RODC can advertise itself as a global catalog server.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)
A. Upgrade all DNS servers to Windows Server 2008.
B. Run adprep /domainprep on the Sales, Marketing, and IT domains.
C. Install a Windows Server 2008 writable domain controller in the IT domain.
D. Configure the Windows Server 2008 domain controller in the finance domain as a global catalog server.
Answer: B, C
Explanation:
To deploy the read-only domain controller (RODC) in the Development domain and in the HR domain, you need to run adprep /domainprep on the Sales, Marketing, and HR domains to prepare your infrastructure to upgrade. Because this domain controller is the first Windows Server 2008 domain controller in Windows Server 2003 domains, you must prepare the domains by running adprep /domainprep on the infrastructure master.
Before you deploy the read-only domain controller (RODC) in the HR domain, you need to first install a Windows Server 2008 writable domain controller in the HR domain because the first Windows Server 2008 domain controller in an existing Windows Server 2003 domain cannot be created as an RODC. After a Windows Server 2008 domain controller exists in the domain, additional Windows Server 2008 domain

controllers can be created as RODCs.
Reference: Scenarios for Installing AD DS
http://207.46.196.114/windowsserver2008/en/library/708da9f7-aaad-4fa1-bccb-76ea8569da501033.mspx?mfr=true

17.Your network consists of one Active Directory domain. The domain contains servers that run Windows Server 2008.
The relevant servers are configured as shown in the following table. (Click the Exhibit)

Server name	Installed services
Server1	Active Directory Domain Services (AD DS)
Server2	-Microsoft System Center Configuration Manager (SCCM)
Server3	Microsoft System Center Virtual Application Server (SCVAS)
Server4	Terminal Services

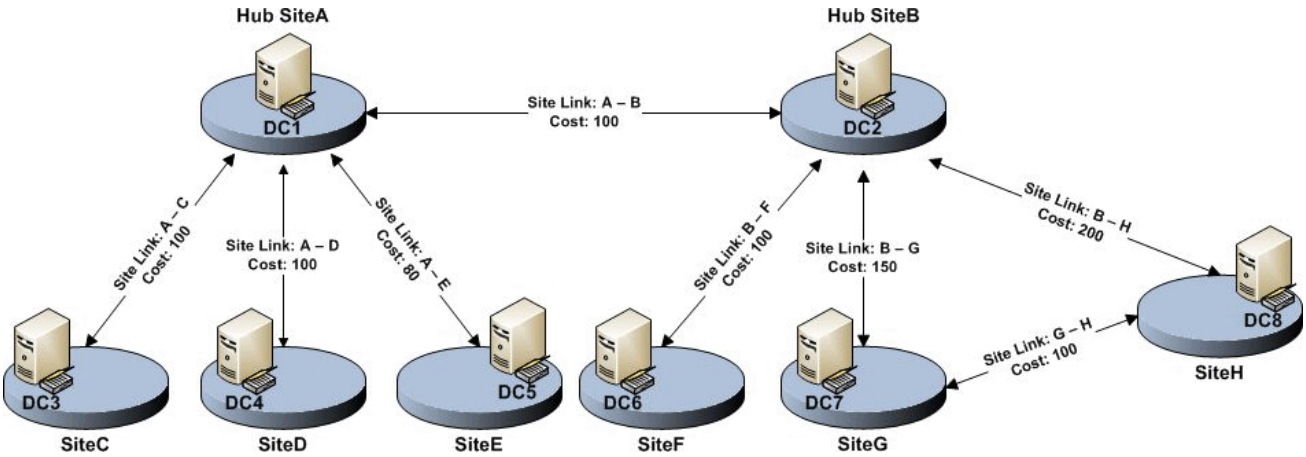
All client computers run Windows Vista. You plan to deploy two Java-based applications on all client computers. The two applications each require a different version of the Java Runtime Environment (JRE). After testing, you notice that the two JREs prevent the applications from running on the same computer. You need to recommend a solution that enables the two Java-based applications to run on all client computers.
What should you recommend?
A. Create two Windows Installer (MSI) packages that each contains one version of the JRE and one compatible application. On Server2, advertise both packages to all client computers.
B. Create two Windows Installer (MSI) packages that each contains one version of the JRE and one compatible application. On Server1, create a Group Policy object (GPO) that assigns both packages to all client computers.
C. Use the SoftGrid Sequencer to create two application packages that each contains one version of JRE and one compatible application. On Server3, stream both application packages to all client computers.
D. Install the two JRE versions and the two Java-based applications on Server4. Configure all client computers to connect to the Java-based applications by using Terminal Services RemoteApp (TS RemoteApp).
Answer: C
Explanation:
To run two Java-based applications that require different versions of Java Runtime Environment (JRE) on all the client computers of the department you need to create two application packages using the SoftGrid Sequencer. Each package should contain one version of JRE and its compatible application.
SoftGrid packages and virtualizes Windows applications for delivery as network services.
SoftGrid basically insulates an application from other applications such that they don't conflict with one another. In this scenario, where different versions of the Java Runtime are required to run two applications you can use SoftGrid to"sequence" the required version of the JRE with the application. When the application is executed it sees only the JRE that it needs and not the other JRE that is "sequenced" with the other application.
You need to stream both application packages to all client computers on the Server3 because you need

the execution of the application to happen on the Terminal Server so that applications can run on all client computers through Terminal Server. SoftGrid can be used on and Terminal Servers.
Reference: Re: SoftGrid General Queries
http://forums.microsoft.com/TechNet/ShowPost.aspx?PostID=3266992&SiteID=17
Reference: Application Packaging: The SoftGrid Sequencer
http://www.microsoft.com/systemcenter/softgrid/evaluation/sequencer.mspx

18.Your network consists of one Active Directory forest that contains two domains. All domain controllers run Windows Server 2003. The network contains file servers that run Windows Server 2003 R2. The files servers run DFS Replication. The forest root domain is named contoso.com and the child domain is named corp.contoso.com. You prepare the forest schema for the installation of domain controllers that run Windows Server 2008. You prepare the corp.contoso.com domain. You install a new domain controller that runs Windows Server 2008 on corp.contoso.com.
You need to plan an Active Directory implementation to meet the following requirements:
Enable DFS Replication support for SYSVOL on corp.contoso.com.
Allow the installation of new domain controllers that run Windows Server 2003 in the forest root domain.
What should you include in your plan?
A. Upgrade all file servers to Windows Server 2008.
B. Run adprep /domainprep /gpprep on the corp.contoso.com domain and run adprep /domainprep on the contoso.com domain.
C. Upgrade all Windows Server 2003 domain controllers to Windows Server 2008. Raise the functional level of the forest to Windows Server 2008.
D. Upgrade the Windows Server 2003 domain controllers in corp.contoso.com to Windows Server 2008. Raise the corp.contoso.com domain functional level to Windows Server 2008.
Answer: D
Explanation:
To enable DFS Replication support for SYSVOL on corp.contoso.com and to allow the installation of new domain controllers that run Windows Server 2003 in the forest root domain, you need to Upgrade the Windows Server 2003 domain controllers in corp.contoso.com to Windows Server 2008 and raise the functional level of corp.contoso.com domain to Windows Server 2008.
Upgrade the Windows Server 2003 domain controllers in corp.contoso.com to Windows Server 2008 enables you to use domain-based namespaces.
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 DSSYSVOL folder in domains that use the Windows Server 2008 domain functional level.
To facilitate migrating existing SYSVOL folders to DFS Replication, Windows Server 2008 includes a Dcpromo tool that helps to migrate the replication of existing SYSVOL folders from FRS to DFS Replication. The Windows Server 2008 will use DFS Replication for SYSVOL if the domain functional level is Windows Server 2008
Reference: Distributed File System
http://technet2.microsoft.com/windowsserver2008/en/library/1f0d326d-35af-4193-bda3-0d1688f90ea71033.mspx?mfr=true

19.Your Company has one main office and 50 branch offices. You have a wide area network (WAN) link that connects all branch offices to the main office. The network consists of 10 Active Directory domains. Users from all domains are located in the branch offices. You plan to configure each branch office as an Active Directory site.

The domain is configured as shown in the exhibit. (Click the Exhibit button.)



You need to plan the deployment of domain controllers in the branch offices to meet the following requirements:

- Users must be able to log on if a WAN link fails.
- Minimize replication traffic between offices.

What should you include in your plan?

A. Implement a domain controller in each branch office. Enable Universal Group Membership Caching.

B. Implement a domain controller in each branch office. Configure DNS to use a single Active Directory-integrated zone.

C. Implement a domain controller in each branch office. Configure the domain controller as a global catalog server.

D. Implement a read-only domain controller (RODC) in each branch office. Configure the domain controller as a global catalog server.

Answer: A

Explanation:

The replication traffic between the offices can be minimized with the use of Universal Group Membership Caching, which is used to locally cache a user's membership in universal groups on the domain controller authenticating the user.

This can help you to avoid global catalog (GC), which causes the extra WAN traffic that the GC needs to replicate with other domain controllers in the domain. The cached membership for UGMC can be refreshed every 8 hours to keep it up to date.

RODC cannot be configured in this scenario because it needs to use GC that increases the replication traffic.

Reference: When to use and not use universal group membership caching

http://www.windowsnetworking.com/kbase/WindowsTips/Windows2003/AdminTips/ActiveDirectory/Whentouseandnotuseuniversalgroupmembershipcaching.html

20.Your Company has one main office and four branch offices. Each branch office has a read-only domain controller (RODC). The network consists of one Active Directory domain. All domain controllers

run Windows Server 2008 R2. Some branch office users work in a department named Sales. Sales department users must be able to log on to all computers in their respective branch offices, even if a wide area network (WAN) link fails.
The company security policy has the following requirements:
- User account passwords must be replicated to the minimum number of locations.
- A minimum number of passwords must be replicated to the branch office domain controllers.
You need to configure a password replication policy that supports the company security policy.
What should you do?
A. Install a writable domain controller in all branch offices. Create one global group that contains all Sales department users. Create a fine-grained password policy and apply the policy to the group.
B. Install a writable domain controller in all branch offices. Create one global group that contains the computers of all Sales department users. Add the group to the Allowed RODC Password Replication Group in the domain.
C. Create one global group for each branch office that contains the Sales department users and computers in the corresponding branch office. Add all groups to Windows Authorization Access Group in the domain.
D. Create one global group for each branch office that contains the Sales department users and computers in the corresponding office. Add each group to the Password Replication Policy in the corresponding branch office.
Answer: D
Explanation:
To configure a password replication policy for the company keeping in mind the security policy of the company, you need to create one global group for each branch office that contains the Sales department users and computers in the corresponding office. This is because the password replication policy must include the appropriate user, computer, and service accounts in order to allow the RODC to satisfy authentication and service ticket requests locally. You need to then add each group to the Password Replication Policy in the corresponding branch office.
The Password Replication Policy acts as an access control list (ACL). It determines if an RODC should be permitted to cache a password. After the RODC receives an authenticated user or computer logon request, it refers to the Password Replication Policy to determine if the password for the account should be cached. The same account can then perform subsequent logons more efficiently
Reference: Password Replication Policy
http://technet2.microsoft.com/windowsserver2008/en/library/977fff54-0c7e-46cd-838b-1161aa09a46c1033.mspx?mfr=true