Microsoft

Exam Questions 70-646
Pro: Windows Server 2008 - Server Administrator
1. 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:

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.


6. Click O System.

7. Click O Password Settings Container.

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

8. Right-click O Password Settings Container, click New, and then click Object.

9. In the Create Object dialog box, under Select a class, click ADSI-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 must-have attributes.

2. 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 won’t change regardless of the location of that VM it will meet the third requirement. Ans D does not meet the 3rd requirement. Ans C won’t 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.

3. 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.

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

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

A. Install Windows PowerShell.
B. Install Windows Server Backup.
C. Modify the Windows Firewall settings.
D. Enable the IIS Management Service feature.

Answer: B,C

5. Your network is configured as shown in the following diagram.

Each office contains a server that has the File Services server role installed. The servers have a shared folder named Resources.

You need to plan the data availability of the Resources folder. Your plan must meet the following requirements:

- If a WAN link fails, the files in the Resources folder must be available in all of the offices.
- If a single server fails, the files in the Resources folder must be available in each of the branch offices, and the users must be able to use existing drive mappings.
- Your plan must minimize network traffic over the WAN links.
What should you include in your plan?  

A. a standalone DFS namespace that uses DFS Replication in a full mesh topology  
B. a domain-based DFS namespace that uses DFS Replication in a full mesh topology  
C. a standalone DFS namespace that uses DFS Replication in a hub and spoke topology  
D. a domain-based DFS namespace that uses DFS Replication in a hub and spoke topology  

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.  

6. 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:
7. 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?


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.

![Shadow Copies](image)

Figure 12-1 Enabling 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 12-2: Shadow 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 oldest shadow 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 previous shadow 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.


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 Directory-integrated zone for branch.contoso.com.
C. On one domain controller create an Active Directory-integrated zone for branch.contoso.com and create an Active Directory-integrated 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:


Understanding DNS Zone Replication in Active Directory Domain Services


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.

<table>
<thead>
<tr>
<th>Zone replication scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All DNS servers in the domain that are domain controllers running Windows Server 2003 or Windows Server 2008</td>
<td>Replaces zone data to all Windows Server 2003 and Windows Server 2008 domain controllers (DCs) in the AD DS forest. This option replicates zone data to the ForestDNSZones partition. Therefore, it provides the broadest replication scope.</td>
</tr>
<tr>
<td>All DNS servers in the domain that use domain controllers running Windows Server 2003 or Windows Server 2008</td>
<td>Replaces 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 domain DNSZones partition. It is the default setting for DNS zone replication in Windows Server 2003 and Windows Server 2008.</td>
</tr>
<tr>
<td>All domain controllers in the Active Directory Domain</td>
<td>Replaces zone data to all domain controllers in the Active Directory domain. If you use Windows 2003 DNS servers to load an Active Directory-integrated zone, you must specify this scope for that domain.</td>
</tr>
<tr>
<td>All domain controllers in a specified application directory partition</td>
<td>Replaces 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 the intended 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 across the entire forest. For more information, see Create an Application Directory Partition and Specify a DNS Server in a DNS Application Directory Partition.</td>
</tr>
</tbody>
</table>

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.

9. 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.

10. 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:

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.

11. 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, select the appropriate technologies. Select all that apply.

A. Group Policy deployment
B. Microsoft Application Virtualization (App-V)
C. Microsoft Enterprise Desktop Virtualization (MED-V)
D. Microsoft System Center Configuration Manager 2007 R2
E. Microsoft System Center Operations Manager 2007 R2
F. Windows Server Update Services (WSUS)

Answer: B,D

Explanation: B: Microsoft Application Virtualization (App-V) also helps enterprises handle application compatibility issues, but it addresses challenges differently than MED-V does. Specifically, App-V lets you resolve conflicts that arise between different applications or different versions of the same application.

D:

* App-V integrates with System Center Configuration Manager, so you can manage virtual and physical applications, along with hardware and software inventory, operating system and patch deployment, and more.

* Configuration Manager 2007 Software Update Management simplifies the complex task of delivering and managing updates to IT systems across the enterprise. IT administrators can quickly deliver updates of Microsoft products, third-party applications, custom in-house line-of-business applications, hardware drivers, and system BIOS to a variety of devices—including desktops, laptops, servers, and mobile devices.

* Configuration Manager 2007 allows you to perform tasks such as: Deploying operating systems Deploying software applications Deploying software updates Metering software usage Assessing variation from desired configurations Taking hardware and software inventory Remotely administering computers

Incorrect: Not C: The key benefit of MED-V is that it helps enterprises deal with incompatibility between applications and the operating system. Not E: Operations Manager 2007 R2 helps reduce the cost of datacenter management with end-to-end monitoring and management of Microsoft, UNIX, and Linux servers and workloads, while assuring delivery of IT services to expected and agreed levels. Not F: Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system.


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.

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.


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?
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 clusters. 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.


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 do not 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.
15. 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 applied 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.

16. 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.

17. 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.

18. 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 split-tunnel 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.
19. 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 user-defined 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.

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.


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
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

70-646 Practice Exam Features:

* 70-646 Questions and Answers Updated Frequently
* 70-646 Practice Questions Verified by Expert Senior Certified Staff
* 70-646 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 70-646 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 70-646 Practice Test Here